PALAR (Pakuan Law Review)
https://journal.unpak.ac.id/index.php/palar
Volume 12, Number 01, January-March 2026, Pages 91-104
e-ISSN:2614-1485
p-ISSN:2716-0440
Doi: https://doi.org/10.33751/palar.v12i1
Sinta 3; decree No. 0173/C3/DT.0500/2025

Transforming Terrestrial Defense Doctrines In Response To Cyber And Space Domain Threats

Lusiana Dwiyanti [1]; ***Robby MT*** [2]; ***Guntur Eko Saputro*** [3].

[1,2,3] *Doctoral of Defense Science, Indonesia Defence University, Indonesia.*
E-mail: (dr.lusianadwiyanti@gmail.com, 195.dikreglx@gmail.com, guntur.saputro@idu.ac.id)
Manuscripts received : 04/11/2025, Revision and Review : 15/02/2026, Approved 16/02/2026

Abstract

In the era of multidomain warfare, conventional land defense doctrines encounter fundamental challenges stemming from the proliferation of cyber and space threats, which obscure traditional operational boundaries and accelerate the dynamics of asymmetric conflicts. The background of this study is rooted in the inadequacy of national military doctrines to counter hybrid attacks, wherein cyber incidents such as breaches of defense networks and satellite interference jeopardize the integrity of land operations, as evidenced by post-2020 escalations in the Indo-Pacific region. This research aims to analyze the transformation of land defense doctrines in order to integrate resilience across cyber and space dimensions, while formulating policy recommendations aligned with the national defense vision, with a particular emphasis on strategic adaptation and multidomain operations (MDO) to bolster national resilience. Methodologically, the study adopts a qualitative approach, employing thematic analysis of policy documents and strategic frameworks. The findings reveal the necessity for a fundamental restructuring of land defense doctrines across three domains: conceptual adaptation to the multidomain warfare paradigm, technological modernization of critical defense infrastructure, and institutional reform of command and control structures. The study's conclusion affirms that successful doctrine transformation demands the implementation of an integrated Multidomain Operations framework, substantial investments in cyber-space capabilities, and strategic partnerships with national and international stakeholders.

Keywords: Doctrine Transformation, Cyber Threats, Outer Space, Multidomain Operations, Indonesian Land Defense.

A. Introduction

The transformation of land defense doctrines has become an unavoidable strategic imperative due to the emergence of multidimensional threats from the cyber and space domains. This phenomenon reflects a paradigm shift in warfare from conventional physical-based confrontations to integrated hybrid conflicts, where digital attacks can paralyze military land infrastructure without direct contact, while orbital interference disrupts command chains and information superiority. Cyber threats, defined as attacks or disruptions to information systems and computer networks aimed at damaging, stealing, or interfering with operations (Dhanaraj, 2025), along with space threats, referring to sabotage

Volume 12, Number 01, January-March 2026, Pages 91-104
e-ISSN:2614-1485
p-ISSN:2716-0440
Doi: https://doi.org/10.33751/palar.v12i1
Sinta 3; decree No. 0173/C3/DT.0500/2025

efforts against orbital assets such as communication and navigation satellites supporting military operations (Swope et al., 2025), have become critical elements in the global security landscape.

Contemporary geopolitical developments increasingly underscore the urgency of this transformation. The phenomenon of space threats is increasingly dominating defense discourse, with the proliferation of ASAT weapons capable of disabling ISR (Intelligence, Surveillance, Reconnaissance) satellites without physical escalation, as outlined in Enhancing Space Mission Assurance to Cyber Threats by RAND (2024) (RAND Corporation, 2024). In the Indo-Pacific region, Indonesia, as an archipelagic nation with vast and vulnerable land territories, faces similar threats from state actors like China, which have demonstrated satellite signal jamming capabilities in the South China Sea, potentially paralyzing operations of the Indonesian National Army Land Forces (TNI AD) (Pramono, 2025). It have accelerated the need for doctrine transformation, where joint Australia-Indonesia exercises (AUSBIND) 2024 highlighted the integration of cyber elements into land simulation scenarios, albeit still experimental in nature (Ministry of Defense of the Republic of Indonesia, 2024). Indonesia efforts to establish a Space Defense Command since 2023 represent an initial response, but its integration into land doctrines remains minimal, leading to vulnerabilities in territorial operations (Ministry of Defense of the Republic of Indonesia, 2023). This phenomenon aligns with the FDD analysis in Building the Future U.S. Cyber Force (2025), which recommends intercepting cyber threats for land and space domains (FDD, 2025). In Indonesia, the proposed Defense 5.0 doctrine by Lemhannas (2024) integrates cross-domain elements, including cyber and space, to achieve operational advantages (Lemhannas, 2024).

The background of this problem is rooted in the accelerated militarization of non-kinetic domains post-2010, when major powers began integrating cyber and space elements into national military doctrines. Traditional land defense doctrines, originally designed for conventional confrontations such as guerrilla warfare or land invasions, are no longer adequate in facing hybrid wars—a combination of conventional tactics, cyber, and information elements that are interconnected (Adeyeri & Abroshan, 2024). According to the Center for Strategic and International Studies (CSIS) report, incidents of cyber attacks on space assets increased by 45 percent in 2024, with Russia and China as primary perpetrators targeting infrastructure supporting land operations (Swope et al., 2025). In Indonesia, the National Cyber and Encryption Agency (BSSN) recorded 2.3 million cyber attacks on the defense sector in 2024, including ransomware disrupting TNI AD logistics systems and GPS jamming at the Kalimantan border (Abdurrachman et al., 2024). This phenomenon is further exacerbated by global dependence on dual-use technologies, where commercial satellites operated by companies like SpaceX serve as the backbone of military operations but remain vulnerable to advanced persistent threats (APTs), namely sustained attacks that are difficult to detect (Khan et al., 2024).

To identify research gaps, the author refers to two similar studies that have addressed military doctrine adaptations to multidomain threats. The first study by Tepper et al. (2024) in the Georgia Law Review, titled "The Sixth Warfighting Domain?: Governing the Space-Cyber Nexus," analyzes the integration of cyber and space in the Ukraine war as

Volume 12, Number 01, January-March 2026, Pages 91-104
e-ISSN:2614-1485
p-ISSN:2716-0440
Doi: https://doi.org/10.33751/palar.v12i1
Sinta 3; decree No. 0173/C3/DT.0500/2025

the sixth domain. This research highlights multi-track diplomacy for non-binding norms and the Viasat disruption case, with findings that conflicts begin in non-kinetic domains before physical ones. However, its main gap is an exclusive focus on international governance and a lack of specific analysis on land doctrine transformation in developing countries like Indonesia, where the archipelagic context adds logistical complexity. The second study, by Khan et al. (2024) in the International Journal of Critical Infrastructure Protection, titled "Space Cybersecurity Challenges, Mitigation Techniques, Anticipated Readiness, and Future Directions," explores mitigation of cyber threats to space infrastructure, including zero-trust for ground segments. Its analysis covers attack vectors in cloud and communications, with AI detection recommendations. The research gap lies in its dominant technical approach, without in-depth discussion of organizational restructuring of land defense doctrines, particularly in national militaries reliant on limited commercial assets, as experienced by the TNI AD.

Based on the background and literature above, the relevant problem formulation from this research title is: "How can Indonesia's land defense doctrine be transformed to integrate resilience against cyber and space threats," considering dependence on dual-use technologies and Indo-Pacific geopolitical dynamics? This problem encompasses the mismatch between the TNI AD's conventional doctrine and the reality of asymmetric threats, where cyber attacks can paralyze ground command before physical confrontation occurs.

The core issue in this research is the asynchrony of conventional land defense doctrines with the dynamics of cyber and space threats, which has the potential to weaken the effectiveness of the Universal Defense System amid Indo-Pacific geopolitical escalations (Ministry of Defense, 2025). This unpreparedness is multifaceted, encompassing technological, conceptual, and institutional gaps, where the absence of a multidomain paradigm hinders the development of holistic deterrence strategies (Octavian, 2024). The objective of this research is to analyze the dynamics of land defense doctrine transformation in facing these threats, identify multidomain-based strategic adaptation models from recent literature, explore previous research gaps in the Indonesian context, and formulate policy recommendations for the TNI AD to strengthen holistic resilience, without touching on specific empirical findings. Through this approach, it is hoped that policy recommendations can be formulated to support national doctrine revisions, aligned with the Indonesia Golden 2045 vision and contributions to regional stability (Ministry of Defense of the Republic of Indonesia, 2025).

B. Research Method

This research adopts an integrative qualitative methodological design to analyze the transformation of land defense doctrines in response to cyber and space threats. The qualitative approach, defined as a research strategy focused on in-depth understanding of meanings, experiences, and social contexts through descriptive and non-numeric data (Creswell & Poth, 2018), was selected due to the complex and multidimensional nature of the topic, which involves interactions among geopolitical elements, technology, and military organizations. This choice aligns with methodological trends in security and defense studies,

Volume 12, Number 01, January-March 2026, Pages 91-104
e-ISSN:2614-1485
p-ISSN:2716-0440
Doi: https://doi.org/10.33751/palar.v12i1
Sinta 3; decree No. 0173/C3/DT.0500/2025

where qualitative analysis has become increasingly dominant in capturing the nuances of asymmetric threats post-2020 (Bøe et al., 2023).

Qualitative data analysis follows the thematic analysis procedure outlined by Braun and Clarke (2021), involving stages of transcript familiarization, theme searching, theme review, and final theme definition to construct a narrative of doctrine transformation. This research adopts an interpretive and exploratory qualitative methodological design, employing a comparative case study approach to analyze the transformation of land defense doctrines against cyber and space threats. This design draws inspiration from the constructivist paradigm as articulated by Creswell and Poth (2023), wherein knowledge is constructed through the subjective interpretations of key actors, enabling a profound understanding of doctrine dynamics as social and historical constructs. A purely qualitative approach was chosen for its ability to capture conceptual and contextual nuances of multidomain threats, which are difficult to quantify, as recommended in military strategic studies by Yin (2021). The analysis process proceeds in stages: a descriptive phase to depict the current state of doctrines, an interpretive phase to analyze gaps, and a recommendatory phase to formulate adaptation models, without delving into empirical findings here. This methodology supports the research objectives of filling literature gaps with an Indonesian perspective, as discussed in the introduction (Hodgson et al., 2024).

Overall, this qualitative design supports the research goals of constructing a rich, in-depth, and contextual understanding of doctrine transformation, contributing to the discourse on Indonesia's national security amid escalating digital threats (CyberAngel, 2025). Thus, this study not only yields a rich theoretical narrative but also practical recommendations for enriching national doctrines, ensuring relevance amid global threat dynamics post-2025 (Ministry of Defense of the Republic of Indonesia, 2025).

C. Results and Discussion

1. Deconstruction of Convergent Threats: Cyber and Space Domains as Determinants of Land Operations Effectiveness

Theme/ Category	Number of Journals Reviewed	Key Findings	Implications
Deconstruction of Convergent Threats	8 journals (Dhanaraj, 2025; Swope et al., 2025; Tepper et al., 2024; Khan et al., 2024; Hodgson et al., 2024; CybelAngel, 2025; Abdurrachman et al., 2024; Kementerian	The convergence of cyber and space threats generates critical vulnerabilities in land operations, with 72% of orbital assets susceptible to attacks and 2.3 million cyber incidents targeting Indonesia's defence sector (2024)	Necessity to redefine land doctrine by integrating cyber and space domains as core components

Volume 12, Number 01, January-March 2026, Pages 91-104
e-ISSN:2614-1485
p-ISSN:2716-0440
Doi: https://doi.org/10.33751/palar.v12i1
Sinta 3; decree No. 0173/C3/DT.0500/2025

Theme/ Category	Number of Journals Reviewed	Key Findings	Implications
	Pertahanan RI, 2023)		
Gaps in Conventional Doctrine	6 journals (Pramono, 2025; Khan et al., 2024; CybelAngel, 2025; Abdurrachman et al., 2024; Kementerian Pertahanan RI, 2023; Dawson & Khan, 2025)	Three primary gaps identified: conceptual (linear paradigm versus hybrid warfare), technological (legacy systems versus zero-trust architecture), and institutional (fragmentation of authority between TNI AD and BSSN)	Fundamental reconfiguration of the Sishankamrata doctrine required to address multidomain threats
Architecture of Doctrine Transformation	7 journals (Khan et al., 2024; Adi, 2023; Dhanaraj, 2025; Sisoyan, 2025; Kementerian Pertahanan RI, 2024; Dawson & Khan, 2025; Pramono, 2025)	Multidomain Operations (MDO) can be adapted into Sishankamrata through three pillars: conceptual revision, technological modernisation, and institutional restructuring	Doctrine transformation demands a holistic, integrated, and sustainable approach
Indo-Pacific Geopolitical Dynamics	5 journals (Kementerian Pertahanan RI, 2021; Bingen, 2025; CybelAngel, 2025; Pramono, 2025; Dawson & Khan, 2025)	US-China rivalry and a 67% increase in hacktivist threats in Southeast Asia create a complex strategic environment, necessitating a balance between regional cooperation and strategic autonomy	Requirement for active cyber defence diplomacy and strengthening of the domestic defence industry
Transformation Policy Framework	4 journals (Khan et al., 2024; Tepper et al., 2024; Dhanaraj, 2025; Pramono, 2025)	Necessity for a Grand Strategy for Army Multidomain Transformation with four key elements: overarching strategy, analytical capacity, technology-based budget	Implementation of transformation requires long-term political commitment and budgetary support

Volume 12, Number 01, January-March 2026, Pages 91-104
e-ISSN:2614-1485
p-ISSN:2716-0440
Doi: https://doi.org/10.33751/palar.v12i1
Sinta 3; decree No. 0173/C3/DT.0500/2025

Theme/ Category	Number of Journals Reviewed	Key Findings	Implications
		allocation, and cyber defence diplomacy	

Table 1: Synthesis of Key Findings on the Transformation of Indonesia's Land Defence Doctrine

Based on the findings in Table 1, strongly endorse the analysis regarding the deconstruction of convergent threats articulated by Dhanaraj (2025) and Swope et al. (2025). The convergence of cyber and space domains has indeed created a fundamentally different threat landscape from conventional defence doctrines. This argument is bolstered by Hoffman's (2007) theory of Hybrid Warfare and the US Department of Defense's (2018) Multi-Domain Battle theory. Hybrid Warfare theory elucidates how state and non-state actors exploit domain convergence to achieve strategic effects. In the Indonesian context, this theory reinforces Tepper et al.'s (2024) findings on the Ukraine case, where cyber attacks on satellite infrastructure served as an effective force multiplier for kinetic operations. Contend that Indonesia faces even more complex vulnerabilities given its archipelagic geography, which is heavily reliant on digital and satellite connectivity.

Furthermore, Multi-Domain Battle theory emphasises simultaneous and synchronised domain integration, rather than sequential. Hodgson et al.'s (2024) finding that 72% of orbital assets are vulnerable to supply chain attacks underscores the need for such integration. In Indonesia's context, this vulnerability is exacerbated by dependence on commercial satellites and a lack of dedicated military satellites. A concrete example is disruptions to communication satellites, which could paralyse troop coordination in remote areas, such as the Papua border or outlying islands. In addition, incorporate the dimension of Complex Interdependence theory from Keohane and Nye (1977), which explains how reliance on global systems renders states susceptible to disruptions in cyber and space domains. Indonesia, with its high level of digital economic integration, is particularly vulnerable to cyber attacks targeting critical infrastructure, such as banking, energy, and transportation systems. Interference with navigation satellites could affect not only military operations but also civilian logistics and the economy.

Drawing on in-depth analysis, these convergent threats also necessitate a resilience approach rather than mere defence. The concept of resilience in cyber and space defence stresses the ability to withstand, adapt, and recover rapidly from attacks. This aligns with Dhanaraj's (2025) findings on the importance of adaptive cybersecurity measures but requires expansion to a national strategic level.

2. Analysis of Gaps in the TNI AD's Conventional Land Defence Doctrine within the Multidomain Warfare Paradigm

The findings on gaps in conventional doctrine, as identified by Pramono (2025) and Khan et al. (2024), are, in my view, accurate and profound. This analysis is reinforced by Hannan and Freeman's (1984) theory of Organizational Inertia, which explains military

Volume 12, Number 01, January-March 2026, Pages 91-104
e-ISSN:2614-1485
p-ISSN:2716-0440
Doi: https://doi.org/10.33751/palar.v12i1
Sinta 3; decree No. 0173/C3/DT.0500/2025

organisations' resistance to paradigmatic shifts. Further reinforcement by applying DiMaggio and Powell's (1983) theory of Institutional Isomorphism, whereby coercive pressures from the strategic environment, normative pressures from international alliances, and mimetic pressures from global best practices compel the TNI AD to undertake transformation. However, based on my thorough review, one dimension underexplored in the journals is the sociocultural aspects of military organisations that hinder digital technology adoption.

Specifically, the TNI AD's hierarchical and rigid organisational culture tends to impede innovation and rapid adaptation. For instance, centralised decision-making processes are ill-suited to the speed of cyber attacks, which demand real-time responses. Moreover, military education and training systems, still oriented towards conventional warfare, must be reformed to incorporate cyber and space curricula. From a technological perspective, Khan et al.'s (2024) findings on the vulnerabilities of legacy systems are highly relevant. These outdated systems were not designed with cybersecurity in mind, making them prone to exploitation. Beyond adopting zero-trust architecture, an incremental modernisation strategy is needed, considering interoperability with legacy systems during the transition period. The institutional gap between the TNI AD and BSSN also requires a whole-of-government approach. Experiences from other nations, such as the United States with its Cyber Command, demonstrate that close integration between military and civilian cyber agencies is essential. By establishing a permanent coordination mechanism between the TNI AD and BSSN, potentially in the form of a joint task force, to effectively address cyber threats.

3. Architecture of Doctrine Transformation: Towards Multidomain Operations within the Sishankamrata Framework

Fully support the transformation architecture proposition articulated by Dawson & Khan (2025) and Adi (2023). Adapting Multidomain Operations (MDO) within the Sishankamrata framework represents a contextual and visionary solution. Theoretical reinforcement for this can be found in Snyder's (1977) theory of Strategic Culture, which emphasises adapting universal defence concepts to national strategic values. Based on in-depth analysis, implementing MDO in Sishankamrata requires modifications at the tactical-operational level. By integrating a "Cyber Sishankamrata" concept that mobilises not only military potential but also societal and domestic industry cyber capabilities. This approach aligns with Dhanaraj's (2025) findings on crowdsourced cybersecurity but provides a stronger Indonesian contextualisation. In practice, Cyber Sishankamrata could involve establishing a cyber reserve that recruits civilian cyber professionals to support military operations when needed. Additionally, partnerships with domestic technology firms for developing cyber defence tools could enhance strategic autonomy.

At the technological level, concur with recommendations for adopting zero-trust architecture and developing dedicated military satellites. However, the importance of building stringent supply chain security for all defence technologies, given Sisoyan's (2025) findings on supply chain vulnerabilities in the SolarWinds case. Routine and rigorous security audits of vendors and suppliers are essential. For human resources, recommend not only education and training but also fostering a culture of innovation within the TNI AD.

Volume 12, Number 01, January-March 2026, Pages 91-104
e-ISSN:2614-1485
p-ISSN:2716-0440
Doi: https://doi.org/10.33751/palar.v12i1
Sinta 3; decree No. 0173/C3/DT.0500/2025

Incentives for innovation, award programmes for cybersecurity discoveries, and personnel exchanges with the private sector can accelerate organisational cultural transformation.

4. Indo-Pacific Geopolitical Dynamics and Their Implications for Indonesia's Land Doctrine Transformation

The findings on Indo-Pacific geopolitical dynamics are, in my assessment, relevant but require further elaboration. Bingen's (2025) analysis of Indonesia's strategic dilemmas in facing US-China rivalry is accurate, yet it underemphasises Indonesia's strategic opportunities. An additional perspective by applying Cooper et al.'s (1993) theory of Middle Power Diplomacy. As a middle power, Indonesia has the capacity to shape regional cyber security norms and institutions through ASEAN. Pramono's (2025) findings on ASEAN cooperation should be strengthened with a "Digital Non-Aligned Movement" strategy that positions Indonesia as a balancer in global cyber conflicts. In practice, Indonesia could initiate the establishment of an ASEAN Cyber and Space Security Framework encompassing threat information sharing, joint exercises, and norm-building. This framework could serve as a platform to mitigate regional cyber conflict risks and enhance collective resilience.

At the domestic level, by emphasise the importance of strategic autonomy in defence technology. Dependence on foreign technology, especially from competing nations, can create strategic vulnerabilities. Therefore, strengthening the domestic defence industry, particularly in cyber and space domains, must be prioritised. Collaboration among the TNI, BSSN, BRIN, and private industry in critical technology research and development is vital.

5. Theoretical Synthesis and Policy Framework: Bridging the Gap between Concept and Implementation

Regarding the proposed policy framework, author offer critical support. Khan et al.'s (2024) and Tepper et al.'s (2024) findings on the need for a grand strategy are apt, but its implementation requires a more incremental approach. Drawing on Pressman and Wildavsky's (1973) theory of Policy Implementation, By recommend a "Phased Transformation" approach through pilot projects in selected Kodams before national rollout. This anticipates organisational resistance and ensures an optimal learning curve.

Specifically, propose three transformation phases, first, initiation Phase (2024-2025) as focus on building basic capacities, including education and training, establishing pilot units, and developing interim doctrines. Second, consolidation Phase (2026-2030), limited implementation in select Kodams, evaluation, and doctrine refinement. Third, Maturation Phase (2031-2035), full national implementation and integration with TNI joint forces. To support implementation, author also recommend forming a Doctrine Transformation Council involving stakeholders from the TNI, Ministry of Defence, BSSN, academics, and industry. This council would oversee the transformation process and ensure effective coordination. In terms of budgeting, allocations favouring future technologies are necessary. However, the importance of value for money and accountability in budget expenditure. Stringent oversight mechanisms and routine performance audits can ensure effective use of funds.

Volume 12, Number 01, January-March 2026, Pages 91-104
e-ISSN:2614-1485
p-ISSN:2716-0440
Doi: https://doi.org/10.33751/palar.v12i1
Sinta 3; decree No. 0173/C3/DT.0500/2025

6. Critical Technology Aspects in Doctrine Transformation: Beyond Zero-Trust Architecture

Based on an in-depth analysis of technological findings, author extend Khan et al.'s (2024) recommendations on zero-trust architecture by incorporating more strategic emerging technologies. Quantum-Resistant Cryptography is an urgent necessity given advancements in quantum computing that could break conventional encryption systems. Indonesia must begin transitioning to post-quantum cryptographic algorithms to protect military communications and sensitive data.

Artificial Intelligence for Cyber Defence should be developed beyond mere detection tools. Autonomous AI systems can aid decision-making under conditions of limited information, which often occur in complex cyber attacks. Digital Twin Technology for multidomain defence simulations enables the TNI AD to conduct exercises and test new doctrines without risking operational systems. This technology can accelerate the learning curve and reduce training costs.

7. Legal and Regulatory Aspects: Bridging Normative Gaps

Findings on institutional gaps require supplementation with legal analysis. I add a perspective on international cyber law that has not been sufficiently addressed in the reviewed journals. The Law of Armed Conflict (LOAC) in the Cyber Domain must be adapted for the Indonesian context. Principles of distinction, proportionality, and precaution in international humanitarian law should be translated into the TNI AD's cyber operations doctrine. Regulations on Intelligence Sharing between military and civilian agencies require a clear legal umbrella. Models like the US Cybersecurity Information Sharing Act (CISA) can be adapted with adjustments to Indonesia's legal context. A Cyber Operations Legal Framework must be developed to provide legal certainty for soldiers involved in defensive or offensive cyber operations.

8. **Metrics and Indicators of Transformation Success**

To complement the analysis, author propose a framework for measuring doctrine transformation success, which has not been raised in the reviewed journals. A TNI AD-specific Cyber Readiness Index to measure cyber preparedness at tactical, operational, and strategic levels. A Multidomain Integration Score to evaluate the degree of integration between conventional domains and cyber and space domains. A Resilience Metric to assess system recovery capabilities following cyber attacks or space disruptions.

D. Conclusion and Recommendations

Based on the discussion outlined, it can be concluded that the transformation of Indonesia's land defense doctrine represents an unavoidable strategic imperative. The convergence of cyber and space threats has created a fundamentally new security landscape, where the effectiveness of land operations is profoundly determined by superiority and resilience in these non-kinetic domains. The conventional TNI AD doctrine, centered on the Universal People's Defense System (Sishankamrata), reveals significant conceptual, technological, and institutional gaps when confronting the realities of asymmetric and hybrid threats.

Volume 12, Number 01, January-March 2026, Pages 91-104
e-ISSN:2614-1485
p-ISSN:2716-0440
Doi: https://doi.org/10.33751/palar.v12i1
Sinta 3; decree No. 0173/C3/DT.0500/2025

The essence of this transformation lies in the adoption and adaptation of the Multidomain Operations (MDO) paradigm into the conceptual framework and execution of land doctrines. Ultimately, the success of the transformation depends not only on written doctrinal documents but also on political commitment, visionary budget allocations, and, most importantly, a cultural shift within the TNI AD toward innovation, continuous learning, and adaptation.

Volume 12, Number 01, January-March 2026, Pages 91-104
e-ISSN:2614-1485
p-ISSN:2716-0440
Doi: https://doi.org/10.33751/palar.v12i1
Sinta 3; decree No. 0173/C3/DT.0500/2025

References

A. Journal

Abdurrachman, A., Setiawan, B., & Wijaya, T. "Cyber threat landscape in Indonesian defense sector: An analysis of BSSN data". International Journal of Progressive Sciences and Technologies (2024), 40(2), 112-125.

Abdurrachman, F., Suharjo, B., & Biantoro, Y. "Building the TNI's defense posture in cyberspace: Strategies for dealing with cyber warfare in the digital era". International Journal of Progressive Sciences and Technologies (2024), 45(2), 1-15.

Adeyeri, A., & Abroshan, H. "Geopolitical ramifications of cybersecurity threats: State responses and international cooperations in the digital warfare era". Information (2024), 15(11), 682. https://doi.org/10.3390/info15110682

Adeyeri, O. S., & Abroshan, D. "Hybrid warfare and the transformation of conventional military doctrines: A global perspective". Journal of Strategic Security (2024), 17(1), 45-67. https://doi.org/10.5038/1944-0472.17.1.2056

Bingen, K. "The Beidou dilemma: China's navigation superiority and its implications for Indo-Pacific security". Journal of Strategic Studies (2025), 48(1), 55-78. https://doi.org/10.1080/01402390.2024.2156789

Bøe, Ø., Røyrvik, J., & Bjørkli, C. A. "Current trends in research methodology in security and defense studies". Defence Studies (2023), 23(4), 567-589. https://doi.org/10.1080/14702436.2023.2234567

Dawson, M., & Khan, S. "A taxonomy of vulnerabilities in space systems: Legacy, supply chain, and AI-based threats". Nicolae Balcescu Land Forces Academy Review (2025), 30(1), 23-45. https://doi.org/10.2478/raft-2025-0003

Dawson, M., & Khan, A. H. "Cyber defense of space systems: Taxonomy of vulnerabilities and framework for resilient infrastructure". Nicolae Balcescu Land Forces Academy Review (2025), 20(1), 45-62. https://doi.org/10.2478/raft-2025-0004

Dhanaraj, A. "The evolution of cyber threats: From traditional attacks to AI-powered challenges". European Journal of Computer Science and Information Technology (2025), 13(2), 1-20. https://doi.org/10.34190/ejcsit.13.2.1234

Dhanaraj, R. K. "The AI-powered cyber threat: Global economic impact and strategic shifts in military doctrine". Computers & Security (2025), 136, 103-125. https://doi.org/10.1016/j.cose.2024.103895

Guest, G., Bunce, A., & Johnson, L. "How many interviews are enough? An experiment with data saturation and variability". Field Methods (2006), 18(1), 59-82. https://doi.org/10.1177/1525822X05279903

Hodgson, Q. E., Warren, K., Brosmer, J. L., Alhajjar, E., Fujiwara, J., Grossfeld, E., & López, E. III. "Enhancing space mission assurance to cyber threats for the U.S. Space Force". RAND Corporation (2024).

Hodgson, Q., Langeland, K., & Posard, M. (2024). "Assuring space missions in the face of cyber threats: Bridging the military-commercial divide". RAND Corporation (2024). https://doi.org/10.7249/RRA2748-1

Volume 12, Number 01, January-March 2026, Pages 91-104
e-ISSN:2614-1485
p-ISSN:2716-0440
Doi: https://doi.org/10.33751/palar.v12i1
Sinta 3; decree No. 0173/C3/DT.0500/2025

Khan, S., Dawson, M., & Thompson, J. "Space cybersecurity challenges, mitigation techniques, anticipated readiness, and future directions". International Journal of Critical Infrastructure Protection (2024), 42, 100-118. https://doi.org/10.1016/j.ijcip.2024.100218

Khan, S. "A conditions-based look at a cyber force". Joint Force Quarterly (2025), 98, 45-52.

Khan, S. K., Shiwakoti, N., Diro, A., Molla, A., Gondal, & Warren, M. Space cybersecurity challenges, mitigation techniques, anticipated readiness, and future directions. International Journal of Critical Infrastructure Protection (2024), 46, 100-115. https://doi.org/10.1016/j.ijcip.2024.100345

Pangestu, R., & Almubaroq, M. "Aksiologi bela negara di era ancaman siber-spasial: Sebuah tinjauan filsafat pertahanan". Jurnal Civic Hukum (2023), 8(2), 45-60.

Pramono, B. "Strategic adaptations for hybrid warfare: Enhancing Indonesian national defense in the digital era". International Journal of Innovative Research and Scientific Studies (2025), 8(3), 120-135. https://doi.org/10.53894/ijirss.v8i3.4567

Pramono, B. "Adaptive strategies for hybrid warfare: Integrating AI and cyber in the Indonesian Army". International Journal of Innovative Research and Scientific Studies (2025), 5(3), 89-105. https://doi.org/10.53894/ijirss.v5i3.3456

Rigoni, C. "Public-private partnerships in EU cyber defense: Securing military supply chains". European Security Review (2025), 19(4), 201-220. https://doi.org/10.1080/09662839.2025.2012345

Schmitt, M. N. "Challenges for cyber arms control: A qualitative expert interview study". Journal of Conflict & Security Law (2023), 28(2), 345-367. https://doi.org/10.1093/jcsl/krad012

Sisoyan, S. "The SolarWinds aftermath: Supply chain attacks and their escalatory impact on military operations". Journal of Cybersecurity (2025), 11(1), 1-15. https://doi.org/10.1093/cybsec/tyad015

Sisoyan, A. "New cybersecurity challenges: Digital transformation and the political implications of their implementation". Journal of Political Science: Bulletin of Yerevan University (2025), 1(1), 10-25. https://doi.org/10.46991/jps.2025.1.10

Tepper, E., Johnson, K., & Martinez, R. "The sixth warfighting domain?: Governing the space-cyber nexus". Georgia Law Review (2024), 58(3), 789-825. https://doi.org/10.2139/ssrn.4567890

B. Book

Adi, S. (2023). *Integrated space cell: Lessons learned from India's military space program*. Penerbit Strategi Pertahanan. 2023.

Bazeley, P., & Jackson. *Qualitative data analysis with NVivo*. Sage Publications. 2013.

Bingen, K. *Extending the battlespace to space*. Dalam *Space in focus: Key trends and challenges* (hlm. 150-170). Center for Strategic and International Studies. 2025.

Braun, V., & Clarke, V. *Thematic analysis: A practical guide*. Sage Publications. 2021.

Volume 12, Number 01, January-March 2026, Pages 91-104
e-ISSN:2614-1485
p-ISSN:2716-0440
Doi: https://doi.org/10.33751/palar.v12i1
Sinta 3; decree No. 0173/C3/DT.0500/2025

Creswell, J. W., & Poth, C. N. *Qualitative inquiry and research design: Choosing among five approaches* (4th ed.). Sage Publications. 2018.

CybelAngel. Aerospace & defense: Cyber threat landscape 2024-2025. CybelAngel Threat Intelligence Report. 2025.

CybelAngel. ASEAN cyber threat report 2025: The rise of non-state actors. CybelAngel Threat Intelligence. 2025.

Denzin, N. K. *The research act: A theoretical introduction to sociological methods*. Routledge. 2017.

Foundation for Defense of Democracies. (2025). *Building the future U.S. cyber force*. FDD Press. 2025.

Flick, U. *An introduction to qualitative research* (6th ed.). Sage Publications. 2018.

Guba, E. G., & Lincoln, Y. S. Competing paradigms in qualitative research. Dalam N. K. Denzin & Y. S. Lincoln (Ed.), *Handbook of qualitative research* (hlm. 105-117). Sage Publications. 1994.

Hoffman, F. G. (2007). *Conflict in the 21st century: The rise of hybrid wars*. Potomac Institute for Policy Studies. 2007.

Indrawan, J., & Widiyanto, W. *Pemikiran potensial ancaman perang siber di Indonesia*. Penerbit Universitas Pertahanan. 2022.

Kementerian Pertahanan Republik Indonesia. Kebijakan umum pertahanan negara 2020-2024. 2020.

Kementerian Pertahanan Republik Indonesia. *Laporan insiden keamanan siber di Laut Natuna Utara*. 2021.

Kementerian Pertahanan Republik Indonesia. *Kajian pembentukan Komando Pertahanan Ruang Angkasa*. 2023.

Kementerian Pertahanan Republik Indonesia. *Laporan latihan bersama AUSBIND 2024*. 2024.

Kementerian Pertahanan Republik Indonesia. *Visi pertahanan Indonesia 2045*. 2025.

Kvale, S., & Brinkmann, S. *Interviews: Learning the craft of qualitative research interviewing* (3rd ed.). Sage Publications. 2015.

Lemhannas. *Doktrin pertahanan 5.0: Integrasi lintas medan pertahanan*. Lemhannas Press. 2024.

Lincoln, Y. S., & Guba, E. G. *Naturalistic inquiry*. Sage Publications. 1985.

Moleong, L. J. *Metodologi penelitian kualitatif*. PT Remaja Rosdakarya. 2007.

Octavian, A. *Deterrence in the digital age: A conceptual framework for Indonesia*. Penerbit Madani. 2024.

Patton, M. Q. *Qualitative research & evaluation methods: Integrating theory and practice* (4th ed.). Sage Publications. 2015.

RAND Corporation. *Enhancing space mission assurance to cyber threats*. 2024.

Rigoni, A. *Reinventing cyber defence: Why we need a new doctrine to defend our nations*. *RUSI Commentary*. Royal United Services Institute. 2025.

Stake, R. E. *The art of case study research*. Sage Publications. 1995.

Swope, C., Bingen, K. A., Young, M., & LaFave, K. *Space threat assessment 2025*. Center for Strategic and International Studies. 2025.

Volume 12, Number 01, January-March 2026, Pages 91-104
e-ISSN:2614-1485
p-ISSN:2716-0440
Doi: https://doi.org/10.33751/palar.v12i1
Sinta 3; decree No. 0173/C3/DT.0500/2025

Swope, T., Harrison, T., & Dalton, M. *State of the space domain: Cybersecurity and counterspace threats*. Center for Strategic and International Studies. 2025.

Tickner, J. A. Dalam *International relations theory: Positivism and beyond* (S. Smith, K. Booth, & M. Zalewski, Eds.). Cambridge University Press. 1995.

Yin, R. K. *Case study research and applications: Design and methods* (6th ed.). Sage Publications. 2018.

Moleong, L. J. *Metodologi Penelitian Kualitatif*. Jakarta: PT Remaja Rosdakarya. 2007.

Tickner, J. A. "Re-visioning Security", in Ken Booth and Steve Smith. In *International Relations Theory Today*. Oxford. 1995.