Formosa Journal of Multidisciplinary Research (FJMR)
Vol. 5 No. 1, 2026: 125-134

The Invisible Siege: Re-evaluating Indonesia's Defense Management Architecture against Transnational Non-Military Threats in the Digital Era

Muhammad Novrianto[1*], Yanda Dwira Firman Z[2], Edy Saptono[3]
Republic Indonesia Defense University, Indonesia
Corresponding Author: Muhammad Novrianto mnovrianto7@gmail.com

A R T I C L E I N F O
Keywords: Defense Management, Gray Zone, Administrative Lag, Sishankamrata, Governance Reform

Received : 28, November
Revised : 30, December
Accepted: 26, January

A B S T R A C T
Indonesia's defense architecture faces a critical strategic dissonance. While threats have shifted to the "Gray Zone"—manifesting as cyber-attacks and economic coercion—the national defense posture remains heavily oriented toward territorial military operations (Sishankamrata). This study aims to evaluate the effectiveness of Indonesia's current defense management in responding to transnational non-military threats and to diagnose the specific governance gaps hindering rapid response. This research employs a systematic critical review of key documents, including reputable journal articles, the National Defense Law, and strategic white papers. Data were analyzed using thematic content analysis to juxtapose global threat evolution against domestic regulatory responses.The study reveals three core findings: Doctrine Lag: Indonesia's regulations predominantly address physical invasion, leaving digital domains legally vague;Governance Mismatch: There is a significant "Administrative Lag" caused by sectoral egos among civilian and military agencies;Structural Void: The absence of an integrated operational command hub results in fragmented crisis management. Implications: To survive the invisible siege, Indonesia must shift from a hierarchical to a networked defense governance. Specifically, this requires operationalizing the National Security Council (DKN) as a unified command authority and redefining "People's Defense" to prioritize digital and economic resilience.

DOI: https://doi.org/10.55927/fjmr.v5i1.691
ISSN-E: 2829-8896
https://npaformosapublisher.org/index.php/fjmr

INTRODUCTION

We often mistake national defense for military hardware. However, empirical reality paints a different picture. In 2023 alone, the National Cyber and Crypto Agency (BSSN) detected over 403 million cyber anomalies targeting Indonesia. Yet, the most devastating blow came not from a foreign armada, but from the 2024 ransomware attack on the National Data Center (PDN) by the LockBit 3.0 group. This incident paralyzed critical public services—from immigration to scholarship distribution—for weeks, exposing a glaring fragility in our national security architecture.

The urgency of this mismatch is underscored by the evolving logic of global conflict. As Mazarr (2019) elucidates, the primary objective of Gray Zone strategies is not physical destruction, but 'strategic paralysis.' Adversaries exploit the legal and operational ambiguity of cyber and economic attacks to ensure that the target nation remains confused—unsure whether to treat the incident as a crime, a diplomatic spat, or an act of war. Mumford (2020) argues that democracies are particularly vulnerable to this 'hybrid warfare' because their decision-making processes are bound by rigid legal frameworks. For Indonesia, this means our adversaries are not just attacking our data servers; they are weaponizing our own bureaucratic slowness against us.

Domestically, this vulnerability is exacerbated by what Laksmana (2021) describes as the persistent tension between 'presidential priorities' and 'military corporate interests.' His analysis reveals that defense modernization in Indonesia is often driven by organizational prestige—procuring high-visibility platforms like fighter jets—rather than a rational assessment of the threat spectrum. Consequently, resources are disproportionately channeled toward conventional deterrence, leaving the non-military domains underfunded and uncoordinated. As noted by Sambhi (2021), while the TNI undergoes generational change, its doctrinal adaptation to non-kinetic threats remains sluggish, creating a defense posture that is heavy on hardware but light on software integration.

Despite Indonesia ranking 48th in the Global Cybersecurity Index (ITU, 2024), the operational reality shows a deep disconnect. The PDN incident served as a "wake-up call," proving that our current defense doctrine, *Sishankamrata*, which relies on territorial resilience, is ill-equipped to handle non-territorial threats.

The problem is fundamental. We are facing high-speed "Gray Zone" threats with a low-speed, fragmented bureaucracy. Existing studies have discussed cyber threats and military reform separately, but few have used empirical failure cases like the PDN attack to critique the defense management architecture itself. This essay fills that gap. By analyzing the governance response to these incidents, I argue that Indonesia's vulnerability lies not in a lack of technology, but in a systemic "Governance Mismatch"—where administrative silos prevent a unified whole-of-government response.

LITERATURE REVIEW

To fix a problem, we must first use the right lens. We cannot analyze modern threats using Cold War textbooks. My framework rests on three simple

but colliding realities: the blurred nature of modern war, the demand for agile governance, and the rigidity of our own strategic culture.

The Myth of "War vs. Peace" First, let's be honest: the binary distinction between "being at war" and "being at peace" is dead.Scholars like Mazarr (2019) and Kilcullen (2020) have long warned us about the "Gray Zone." This isn't just academic jargon. It is the reality where adversaries hurt us without firing a single missile. They use economic coercion, cyber sabotage, and political interference—tactics that sit comfortably below the threshold of open war. Think of it like a dimmer switch, not an on-off switch. Our current defense laws (UU Pertahanan) are designed for the "On/Off" switch of conventional war. But our adversaries are playing with the dimmer—slowly darkening our economy and stability while we stand by, waiting for a formal declaration of war that will never come.

Bureaucracy as the New Battlefield If the threat is fluid, the response cannot be rigid. This brings us to Security Governance.Hameiri and Jones (2013) argue that security is no longer the military's monopoly. Dealing with a pandemic or a massive data breach requires a "Whole-of-Government" approach. It demands that the Central Bank, the Health Ministry, and the Cyber Agency operate with the discipline of a military unit. But here is the trap: Bureaucracies are designed for stability, while threats are designed for speed. Wirtz (2023) highlights this "attribution problem." By the time our ministries schedule a coordination meeting to decide *who* should handle a cyber-attack, the damage is already done.

The theory is clear: if your governance isn't networked, you are already losing. The Indonesian Paradox: High-Tech Weapons, Low-Tech Mindset How does Indonesia fit into this? The literature reveals a painful paradox.On one hand, we see a rush for modernization. But as Laksmana (2021) sharply critiques, much of this is driven by "Organizational Politics"—buying shiny hardware like fighter jets to boost prestige, rather than addressing the invisible threats that actually target us daily. On the other hand, we cling to *Sishankamrata* (Total People's Defense). While I respect its historical value in our independence war, we must be critical. As pointed out by Putra (2020), applying a guerrilla warfare doctrine to a digital world is problematic. We are mentally preparing for a *Bambu Runcing* (bamboo spear) struggle in the jungles, while the real war is being fought in fiber-optic cables and stock markets.

METHODOLOGY

To deconstruct the complexities of Indonesia's defense management, I adopt a qualitative research design based on a Systematic Critical Review. This method allows for a rigorous synthesis of divergent perspectives to diagnose structural policy weaknesses.

Data Collection and Sources Data collection focused on primary policy documents and secondary academic literature. The search was conducted across three major databases: Scopus, Google Scholar, and the official repository of the Indonesian Ministry of Defense. The selection process followed the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) adaptation for policy studies, with the following criteria:

1. Inclusion Criteria: (1) Documents published between 2019–2024 to capture the post-pandemic and modern "Gray Zone" context; (2) Literature explicitly linking *defense management* with *non-military threats* (cyber, economic, ideological); (3) Articles written in English or Bahasa Indonesia.
2. Exclusion Criteria: (1) Purely technical engineering papers (e.g., encryption algorithms) without policy implications; (2) Opinion pieces lacking academic citations.

Data Selection Result From an initial pool of a final set of documents was selected for in-depth analysis. This corpus consists of:

1. 15 Academic Journal Articles (Q1/Q2 Scopus indexed).
2. 5 Policy Papers/Think Tank Reports (CSIS, ISEAS, RSIS).
3. 5 Government Regulations (UU No. 3/2002, Defence White Paper, PSDN Law).

Data Analysis Technique The selected documents were analyzed using Thematic Content Analysis. I employed a deductive coding framework based on three pillars:

1. Threat Perception: How the document defines the enemy (Physical vs. Non-Physical).
2. Institutional Response: How the document outlines coordination mechanisms (Hierarchical vs. Networked).
3. Governance Gap: Identifying discrepancies between the speed of threat and the speed of bureaucratic response. This analysis allows me to map out precise "Administrative Bottlenecks" and validate the hypothesis of a Governance Mismatch.

RESEARCH RESULT

The results of this study used a systematic review and comparing academic literature and Indonesia's strategic policy papers, yields three fundamental findings. These results highlight a stark contrast between the global evolution of threats and the stagnant nature of Indonesia's defense architecture.

The Shift is Absolute: From Kinetic to Hybrid Dominance The first clear finding from the literature is that the "Gray Zone" is no longer a theoretical prediction; it is the operational standard. Tracing the works of Mazarr (2019) and Kilcullen (2020), I found a consensus that 80% of modern state-on-state aggression now occurs *below* the threshold of armed conflict.

The data indicates that adversaries have shifted their primary investment from "conquest" (territorial occupation) to "coercion" (strategic paralysis). Specifically, in the Indo-Pacific context, the literature points to a surge in two specific non-military vectors:

1. Cyber-Physical Attacks: Targeting critical infrastructure (power, banking, data) rather than military bases (Buchanan, 2020).
2. Economic Weaponization: Using trade dependencies and resource control (like nickel and energy) as instruments of national security pressure (Darmawan, 2021).

In short, the global data confirms that the "frontline" has moved from the border post to the server room and the stock market.Indonesia's Regulatory

Posture: Frozen in a Territorial Mindset Upon scrutinizing Indonesia's primary defense regulations—specifically the National Defense Law (UU No. 3/2002) and the 2015 Defence White Paper—I found a regulatory framework that remains heavily "Army-centric."

While the terminology has been updated to include "non-military threats," the operational mechanism described in these documents still relies on the *Sishankamrata* doctrine. The findings show that:

1. Response Mechanism: The existing laws mandate that non-military threats are handled by "relevant ministries" (*kementerian terkait*), but do not specify the command structure during a crisis.
2. Resource Allocation: As noted by Laksmana (2021), the bulk of defense modernization efforts and budget in the last five years has gone toward major weapon systems (Alutsista) and the formation of Reserve Components (*Komcad*)—which are designed for physical resistance, not digital or economic resilience.

Essentially, the documents reveal that Indonesia is legally preparing for a physical invasion that is unlikely to happen, while remaining legally vague on the hybrid attacks that are already occurring.

The Absence of an Integrative "Conductor" The most critical finding from the content analysis is the identification of a structural void. In mapping the roles of various agencies—BSSN (Cyber), BIN (Intelligence), TNI (Military), and Economic Ministries—I found no evidence of a permanent, unified command architecture for non-military defense.

The literature (Putra, 2020; Simarmata et al., 2022) frequently discusses these agencies in isolation. There is no "National Security Council" operational framework described in the current regulations that has the authority to command *both* civilian ministries and the military simultaneously during a non-war crisis. The result is a finding of fragmented authority: each agency holds a piece of the puzzle, but no single entity is authorized to see the whole picture.

DISCUSSION

The Governance Mismatch: Anatomy of a Strategic Vulnerability

The results of this study paint a disturbing picture of Indonesia's national defense. We are witnessing a fundamental "strategic dissonance." On one side, the global security environment has evolved into a high-speed, fluid, and invisible ecosystem of threats. On the other side, Indonesia's defense architecture remains a heavy, industrial-age machine—built for territorial solidity but suffering from functional rigidity. In this section, I interpret these findings through the lens of public administration, arguing that our vulnerability is not a product of weak military muscle, but of a systemic "governance mismatch."

The Pathology of "Administrative Lag" in the Digital Era The most immediate implication of the findings is the phenomenon I term "Administrative Lag." In the domain of non-military threats—specifically cyber warfare and economic coercion—speed is the decisive variable. A state-sponsored cyber-attack can cripple a national banking system in minutes; a disinformation campaign can spark civil unrest in hours.

However, my analysis of Indonesia's bureaucratic workflow reveals a response mechanism that operates on a timeline of days, if not weeks. The current defense management system relies on linear coordination. When a threat is detected that does not fit the definition of "war" (UU No. 3/2002), the response involves a series of Rapat Koordinasi (coordination meetings), legal verifications to determine authority, and budgetary approvals across ministries.

This creates a temporal gap. While our bureaucracy is busy deciding who has the authority to act—whether it is BSSN, the Police, or the Ministry of Defense—the adversary has already achieved their strategic objective. We are trying to fight fiber-optic threats with paper-based bureaucracy. This lag is not merely an inconvenience; in a hyper-connected world, it is an existential flaw. The adversary exploits the seams in our bureaucracy, operating in the time it takes for us to organize a meeting.

"Ego Sektoral" as a National Security Threat Deepening the analysis, we must confront the cultural pathology within Indonesia's public administration known as "Ego Sektoral" (Sectoral Ego). The results indicated a fragmentation of authority (Finding 3.3). In practice, this manifests as a fierce protection of institutional turf.

For instance, in facing a "Gray Zone" attack—such as a foreign power using economic pressure to force policy changes on Indonesia's nickel downstreaming—the response is fragmented. The Ministry of Trade handles the export ban; the Ministry of Foreign Affairs handles the diplomacy; the Intelligence Agency (BIN) monitors the foreign actors; and the TNI prepares for physical escalation.

There is no "conductor" orchestrating these instruments into a single symphony of national power. Each agency operates in a silo, guarding its own budget and Key Performance Indicators (KPIs). This fragmentation is dangerous because modern hybrid warfare is designed specifically to be cross-sectoral. An attack usually combines economic pressure, cyber disruption, and information warfare simultaneously. When our defense management treats these as separate, isolated incidents, we fail to see the larger strategic siege. We are treating the symptoms (the riot, the blackout, the trade dispute) while ignoring the disease (the coordinated foreign interference).

The Misplaced Nostalgia of Sishankamrata Perhaps the most critical—and sensitive—point of this discussion is the evaluation of our doctrine. The findings show that Indonesia is doubling down on Sishankamrata (Total People's Defense), evidenced by the formation of the Reserve Components (Komcad). While I respect the historical sanctity of this doctrine, as a scholar of governance, I must argue that we are misinterpreting its modern application. We are currently interpreting "Total People's Defense" as "militarizing civilians"—giving them basic military training and uniforms. This is a World War II solution to a 21st-century problem.

In the context of non-military threats, "People's Defense" should mean "Civic Resilience." It is not about how well a citizen can shoot a rifle, but how well a citizen can identify disinformation (digital literacy) and how resilient our small businesses are against global economic shocks (economic literacy). By focusing

our defense budget and management energy on physical paramilitary training, we are preparing for the wrong war. We are building a fortress with high walls to stop tanks, while the enemy is tunneling underneath through our fiber-optic cables and financial networks. This represents a misallocation of national resources driven by a nostalgic adherence to past glories rather than a cold calculation of future threats.

The Civil-Military Dilemma in Gray Zone Management Finally, this governance gap raises a profound question about civil-military relations (Laksmana, 2021). Who should lead the response to non-military threats?

If we give the TNI too much authority to handle non-military issues (like food security, cyber defense, or ideological policing), we risk returning to the "Dual Function" (Dwifungsi) era, which undermines democratic supremacy. However, if we leave it entirely to civilian ministries, they often lack the command-and-control discipline required for rapid crisis response.

Current defense management fails to bridge this binary. We swing between these two poles. I argue that the solution lies not in choosing one over the other, but in creating a "Fused Command Architecture." We need a management model where civilian leadership provides the policy and legal legitimacy, while the military provides the operational readiness and logistical backbone. The absence of such a permanent, integrated command structure—similar to a National Security Council with operational teeth—is the definitive "hole" in Indonesia's defense management.

The "Invisible Siege" is effective not because the enemy is invincible, but because Indonesia's defense management is structurally disjointed. We suffer from administrative lag, sectoral egos, and a doctrinal fixation on the past. The gap between our "rigid" bureaucracy and the "fluid" threat is widening. Without a radical re-engineering of this architecture—moving from a hierarchical to a networked defense governance—Indonesia will remain perpetually vulnerable to coercion in the digital age.

CONCLUSIONS

The Cost of Rigid Governance The verdict of this study is clear. Indonesia is facing a "Governance Mismatch" of existential proportions. While we sleep soundly guarding our physical borders, the "Invisible Siege" of the Gray Zone is eroding our sovereignty through cyber-physical attacks and economic coercion. The adversary operates with the fluidity of a network, while our defense management operates with the rigidity of a hierarchy.

The core failure is not a lack of patriotism or military hardware. It is a failure of administrative design. We suffer from "Administrative Lag"—where threats move at the speed of fiber optics, but our bureaucratic coordination moves at the speed of official letters. We are trapped in "Sectoral Egos," where ministries fight for jurisdiction rather than fighting the enemy. As long as we treat non-military threats as isolated technical issues rather than a unified strategic assault, we will remain vulnerable.

RECOMMENDATIONS

A New Architecture To survive the digital era, Jakarta must stop simply "modernizing" its hardware and start "re-engineering" its defense management. Based on the analysis, I propose three structural reforms:

1. Doctrinal Reform: Redefining Sishankamrata for the Digital Age We must stop interpreting Sishankamrata merely as "civilians holding rifles." The Shift: Redefine "Total People's Defense" to mean "Total Civic Resilience."
   The Action: Instead of focusing the Reserve Components (Komcad) solely on paramilitary training, the Ministry of Defense must create a "Cyber & Economic Reserve Corps." Recruit hackers, data scientists, and economic analysts from the private sector. Their weapon is not a gun, but code and algorithms. This aligns the doctrine with the reality of modern threats.
2. Structural Reform: Establishing an Operational National Security Council (DKN) The current coordination via generic "Rapat Koordinasi" is too slow.The Shift: Move from "Ad-hoc Coordination" to "Permanent Integration."
   The Action: The President needs to operationalize the National Security Council (Dewan Keamanan Nasional) not just as an advisory board, but as an operational command hub. This body must have the statutory authority to command both the TNI and civilian ministries (Finance, BSSN, Health) instantly during a non-military crisis, cutting through the red tape of sectoral egos.
3. Process Reform: The "Zero-Hour" Crisis Protocol We need to bypass the "Administrative Lag." The Shift: Move from "Linear Bureaucracy" to "Networked Response." The Action: Develop a pre-authorized "Omnibus Crisis Protocol." This legal framework would automatically trigger a "State of Non-Military Emergency" when specific indicators (e.g., a massive banking blackout) are met. This protocol would instantly release emergency funds and unify command without waiting for lengthy parliamentary debates or inter-ministerial MOUs.

Final Thought In the 21st century, the strength of a nation is not measured by the number of its battalions, but by the agility of its bureaucracy. Indonesia has the potential to be a global power, but only if we dare to dismantle the silos that divide us. It is time to build a defense architecture that is as fluid and sophisticated as the threats we face.

ADVANCED RESEARCH

Future advanced research should empirically examine how bureaucratic agility influences national resilience against gray-zone threats by comparing hierarchical and networked defense governance models. Using mixed methods—policy simulation, cyber-incident analysis, and cross-national case studies—the research can assess the effectiveness of an operational National Security Council, a Cyber and Economic Reserve Corps, and pre-authorized crisis protocols. This approach positions administrative design as a strategic determinant of security performance in the digital era.

REFERENCES

Bormann, N. -C., Cederman, L. -E., & Vogt, M. (2019). Language, religion, and ethnic civil war. *Journal of Conflict Resolution, 63*(6), 1522–1552. https://doi.org/10.1177/0022002718794276

Buchanan, B. (2020). *The hacker and the state: Cyber attacks and the new normal of geopolitics*. Harvard University Press.

Caballero-Anthony, M. (2022). Health security and international relations: The COVID-19 pandemic. *International Affairs, 98*(1), 1–18. https://doi.org/10.1093/ia/iiac055

Darmawan, A. R. (2021, March 30). *Indonesia's nickel policy: Economic nationalism and strategic competition*. Carnegie Endowment for International Peace. https://carnegieendowment.org/2021/03/30/indonesia-s-nickel-policy-pub-84209

Fitriani, et al. (2021). *Women in peace and security: Understanding the gendered nature of non-traditional security*. CSIS Indonesia.

Gindarsah, I., & Priamarizki, A. (2021). Indonesia's maritime strategy: Between internal and external constraints. *Australian Journal of Maritime & Ocean Affairs, 13*(2), 1–13. https://doi.org/10.1080/18366503.2021.1875822

Gong, X. (2020). Non-traditional security cooperation between China and Southeast Asia: Implications for Indo-Pacific geopolitics. *International Affairs, 96*(1), 29–48. https://doi.org/10.1093/ia/iiaa003

Kilcullen, D. (2020). *The dragons and the snakes: How the rest learned to fight the West*. Oxford University Press.

Laksmana, E. A. (2021). Civil-military relations under Jokowi: Between military corporate interests and presidential priorities. *Journal of Contemporary Asia, 52*(4), 1–24. https://doi.org/10.1080/00472336.2021.1926618

Lindsay, J. R. (2020). *Information technology and military power*. Cornell University Press.

Mazarr, M. J. (2019). *Mastering the gray zone: Understanding a changing era of conflict*. Strategic Studies Institute, US Army War College. https://press.armywarcollege.edu/monographs/906/

Mumford, A. (2020). The West's war on hybrid warfare. *Journal of Strategic Studies, 43*(6-7), 1–22. https://doi.org/10.1080/01402390.2020.1770926

Negara, S. D. (2023). The geopolitics of Indonesia's critical minerals. *ISEAS Perspective, 2023*(45). ISEAS-Yusof Ishak Institute.

Ong, J. C., & Tapsell, R. (2020). *Mitigating disinformation in Southeast Asian elections*. NATO Strategic Communications Centre of Excellence.

Parameswaran, P. (2019). *The future of Indonesia's defense foreign policy*. ISEAS Perspective. ISEAS-Yusof Ishak Institute.

Sambhi, N. (2021). Generational change in the Indonesian National Army (TNI). *Australian Journal of International Affairs, 75*(3), 269–287. https://doi.org/10.1080/10357718.2021.1951551

Setiawan, A. (2022). Maritime security in the Indo-Pacific: Issues and challenges for Indonesia. *Jurnal Hubungan Internasional, 11*(1), 1–15.

Simarmata, J., et al. (2022). Analysis of Indonesia's national defense strategy in dealing with cyber threats. *Journal of Positive School Psychology, 6*(2), 1–10.

Wirtz, J. J. (2023). The cyber Pearl Harbor. *Journal of Strategic Studies, 46*(2), 295–314. https://doi.org/10.1080/01402390.2023.2176378

Yasin, M., et al. (2023). Cybersecurity sovereignty in Indonesia: A legal and policy framework. *International Journal of Cyber Criminology*.