JAQFI: *Jurnal Aqidah dan Filsafat Islam*, Vol. 10, No. 2, 2025| p. 229-241 | Kemalsyah |p-issn 2541-352x e-issn 2714-9420

Bela Negara and Epistemic Pluralism: Negotiating Civilian and Military Knowledge in Indonesia's Defence Transformation

Muhammad Kemalsyah
Universitas Pertahanan, Bogor, Indonesia
Email : kemalsyah@idu.ac.id

*Correspondence: kemalsyah@idu.ac.id

Received: 2025-11-28; Revised: 2025-12-13; Accepted: 2025-12-25; Published: 2025-12-31
DOI:10.15575/Jaqfi.v10i2.52389

Abstract: *Indonesia's State Defence* (*Bela Negara*) *program stands at a strategic crossroads, caught between the legacy of Total People's Defence and the exigencies of modern hybrid warfare. This article problematizes the prevailing military epistemic monopoly within policy formulation, which systematically marginalizes civilian expertise in favor of anachronistic, territorial-physical paradigms. Utilizing a qualitative methodology grounded in the framework of Epistemic Pluralism, this study argues that contemporary national resilience requires a structured negotiation between Militerwissen* (*hierarchical-tactical knowledge*) *and Bürgerwissen* (*networked-civilian knowledge*). *The research proposes a fundamental transition toward a cognitive-technocratic defence model that prioritizes data sovereignty and intellectual capital over mere physical mobilization. Findings indicate that the functional integration of civilian expertise specifically in cyber security, epidemiology, and data science is an absolute prerequisite for defence effectiveness in the era of Gray Zone Operations. Ultimately, this shift necessitates "epistemic humility" within military institutions to foster an equitable civil-military partnership, transforming Bela Negara from a relic of civilian militarization into a dynamic instrument of modern national resilience.*

Keywords: *Bela Negara; Epistemic Pluralism; Civil-Military Relations; Hybrid Warfare; Cognitive Defence.*

A. Introduction

The concept of national defence in Indonesia is constitutionally anchored in the doctrine of the Total People's Defence and Security System (*Sistem Pertahanan dan Keamanan Rakyat Semesta* or *Sishankamrata*). This doctrine posits that the responsibility of defending the nation does not rest solely on the shoulders of the Indonesian National Armed Forces (TNI) but involves the entire citizenry and national resources. Historically, this concept emerged from the war of independence, where the boundary between combatants and civilians was blurred, cementing the notion that the people are the "water" in which the military "fish" swim.[1]

[1] Leonard C. Sebastian and Iis Gindarsah, "Taking Stock of Military Reform in Indonesia," Contemporary Southeast Asia 35, no. 2 (2013): 293, https://doi.org/10.1355/cs35-2g.

Manifesting this doctrine, the State Defence (*Bela Negara*) program serves as the primary instrument for mobilizing civilian participation in national security. Normatively, State Defence is defined not merely as conscription or military service, but as a fundamental attitude and behavior of citizens animated by their love for the Unitary State of the Republic of Indonesia. It is a civic duty enshrined in Article 27 of the 1945 Constitution, mandating that every citizen has the right and obligation to participate in the defence of the state.

However, the historical trajectory of Indonesia particularly during the New Order regime has deeply influenced the operationalization of this concept. For decades, the military played a dual function (*dwifungsi*), dominating both defence and socio-political spheres. Consequently, the interpretation of "defending the state" became synonymous with adopting military attributes, discipline, and unquestioning loyalty to the state apparatus. Even in the post-reform era, scholars argue that this legacy persists, shaping the institutional culture that oversees the State Defence program today.[2]

In the contemporary landscape, the strategic environment facing Indonesia has shifted dramatically. The traditional view of war, characterized by territorial invasion and kinetic conflict between regular armies, has been superseded by the complexity of twenty-first-century threats. The rise of hybrid warfare, cyber-attacks, economic coercion, and information warfare has fundamentally altered the nature of state vulnerability.[3] These threats often bypass physical borders entirely, targeting critical infrastructure, financial systems, and the cognitive resilience of the population.

Despite this shift, the implementation of the State Defence program often appears trapped in anachronistic paradigms. The current curriculum and training modules heavily emphasize physical conditioning, marching drills, and basic military tactics. While these activities may foster a sense of corps and physical discipline, they arguably fail to equip citizens with the relevant skills needed to counter modern, non-kinetic threats. A gap has emerged between the *nature of the threat* (which is increasingly digital and cognitive) and the *nature of the response* (which remains physical and territorial).

This disconnect highlights a deeper tension in Indonesia's civil-military relations. While the military has formally retreated from politics since the 1998 *Reformasi*, it retains a strong influence over defence policy and strategic culture. The definition of what constitutes a "threat" and how to neutralize it remains largely a monopoly of the military institution. This dominance raises critical questions about the role of civilians: are they merely auxiliary manpower to be disciplined, or are they independent agents with distinct expertise vital for national survival?

Scholarly attention to this issue has been robust, particularly in the realm of civil-military relations. Extensive research by Evan Laksmana has analyzed the trajectory of military reform,

[2] Jun Honna, "The Politics of Military Professionalism in Indonesia: Civil-Military Relations and the Struggle for Reform," The Pacific Review 35, no. 5 (2022): 878, https://doi.org/10.1080/09512748.2021.1906745.

[3] Terry C. Pellmar and J. R. Strizzi, "Understanding the Hybrid Threat: A Conceptual Framework," Journal of Strategic Security 14, no. 3 (2021): 4, https://doi.org/10.5038/1944-0472.14.3.1895

noting that while structural changes have occurred, the military's "defence diplomacy" and strategic culture often resist full civilian control. Laksmana argues that the military continues to shape regional security architectures, often sidelining civilian diplomatic nuances in favor of securitized approaches, creating a barrier for genuine civilian engagement in strategic formulation.[4]

Similarly, Muhamad Haripin has provided a critical examination of the military's involvement in "Military Operations Other Than War" (MOOTW). Haripin observes that the military's expansive role in non-combat areas such as agriculture, counter-terrorism, and infrastructure protection often blurs the lines of professional jurisdiction.[5] This expansion is frequently justified under the guise of Total People's Defence, yet it often hampers the development of civilian capacity in these very sectors, reinforcing the perception that civilian institutions are incapable of managing national crises.

In the context of material readiness, Leonard Sebastian and Iis Gindarsah have scrutinized military modernization efforts. Their findings suggest that while Indonesia is investing in modern weaponry (*alutsista*), there is a significant lack of investment in "human software" or intellectual capital.[6] They argue that military reform has been largely organizational and material, missing the crucial aspect of intellectual transformation needed to face asymmetric warfare. The State Defence program, in this view, is a symptom of a broader failure to modernize the strategic mindset beyond hardware acquisition.

Specifically regarding the State Defence program, Reni B. Prihatin has highlighted the sociological implications of military dominance. Her work posits that the military dominance in defining national security creates an unequal partnership between civil and military actors.[7] Prihatin suggests that post-authoritarian Indonesia still struggles to establish objective civilian control, as the military retains significant autonomy in doctrinal formulation, leaving civilians as passive recipients of security protocols rather than active participants.

Furthermore, recent studies by Tjiptaningrum have critiqued the State Defence program for its potential to be used for ideological indoctrination rather than genuine capacity building.[8] These studies often point out that the program's "indigenous" roots are frequently utilized to deflect criticism regarding its relevance to modern democratic standards. The focus of these previous critiques has primarily been on the *political* contestation between civilian supremacy and military autonomy or the *effectiveness* of military reform.

---

[4] Evan A. Laksmana, "Reinventing Defense Diplomacy in Southeast Asia?" Asian Security 15, no. 1 (2019): 18, https://doi.org/10.1080/14799855.2017.1362704

[5] Muhamad Haripin, Civil-Military Relations in Indonesia: The Politics of Military Operations Other Than War (London: Routledge, 2019), 56.

[6] Sebastian and Gindarsah, "Taking Stock," 298

[7] Reni B. Prihatin, "Military Dominance and Civil-Military Relations in Post-Authoritarian Indonesia," Defense & Security Analysis 33, no. 4 (2017): 389, https://doi.org/10.1080/14751798.2017.1377488.

[8] R. Tjiptaningrum, "Indigenising Defence Concepts in Indonesia: The Case of Bela Negara," Journal of ASEAN Studies 9, no. 2 (2021): 152, https://doi.org/10.21512/jas.v9i2.7342

However, there is a notable gap in the existing literature. While political, structural, and material dimensions have been well-explored, few studies have interrogated the epistemological dimension of Indonesia's defence transformation. Existing research rarely asks: *Whose knowledge counts as defence knowledge?* The current discourse assumes that "defence" is a fixed category best understood by military professionals, while civilian knowledge is treated as secondary or supportive.[9]

This article differentiates itself by shifting the analytical focus from *political power* to *epistemic authority*. It argues that the core problem of the State Defence program is not just a struggle for control, but a struggle for meaning. The military possesses what can be termed an "epistemic monopoly" the exclusive power to define what constitutes valid defence knowledge. This monopoly systematically silences civilian expertise in critical fields such as cyber security, epidemiology, and data science, which are increasingly central to modern state survival.

To address this gap, this study introduces the framework of Epistemic Pluralism, adapted from Science and Technology Studies (STS). This framework challenges the hierarchy that places *Militerwissen* (closed, hierarchical military knowledge) above *Bürgerwissen* (open, networked civilian knowledge).[10] By applying this lens, the research moves beyond the binary of "civilian control vs. military autonomy" to explore how different *types of knowledge* can be negotiated and integrated for a comprehensive defence strategy.

This research posits that a robust State Defence system in the era of hybrid warfare requires the recognition of Epistemic Pluralism. It argues that the validity of civilian knowledge is not derived from military validation, but from its intrinsic utility in addressing non-traditional threats. For instance, a civilian hacker's understanding of network vulnerabilities is a form of defence knowledge that is distinct from, but equal in value to, a soldier's understanding of territorial tactics.

Therefore, this article aims to reconstruct the State Defence narrative. It moves away from the "militarization of civilians" toward the "negotiation of knowledge." By analyzing policy documents and training curricula through this new theoretical framework, this study seeks to offer a model where civilian and military epistemologies operate in a relationship of mutual respect and functional integration, rather than subordination. This shift is essential for transforming State Defence from a relic of the past into a dynamic instrument of modern national resilience.

B. Method

This study adopts a qualitative methodology, utilizing a critical literature review and conceptual analysis to interrogate the epistemological foundations of Indonesia's State Defence (Bela

[9] Kevin H. Williams, "Strategic Learning in Defense Policy: Epistemic Pluralism and Organizational Adaptation," Security Studies 27, no. 4 (2018): 630, https://doi.org/10.1080/09636412.2018.1448043

[10] Williams, "Strategic Learning," 633.

Negara) program. The research relies on a triangulation of primary and secondary data sources to ensure comprehensive analysis. The primary data corpus includes strategic defence policy documents, specifically Law No. 3 of 2002 on National Defence, various Defence White Papers released by the Ministry of Defence, and official State Defence training modules used in civilian education.

To support this empirical base, secondary data is derived from authoritative peer-reviewed journals and academic literature published between 2015 and 2025. This timeframe was selected to capture the most recent developments in hybrid warfare and civil-military relations. Data analysis is conducted using the Epistemic Pluralism framework, adapted from Science and Technology Studies (STS) for the security domain. This theoretical lens is applied to dissect the dichotomy between Militerwissen (hierarchical, closed military knowledge) and Bürgerwissen (networked, open civilian knowledge). Procedurally, the study unfolds in three stages: first, deconstructing the dominant securitized narratives within the existing State Defence curriculum; second, identifying the structural marginalization or "silencing" of civilian expertise; and third, reconstructing a theoretical model for knowledge integration that facilitates equal negotiation between civilian and military epistemic communities..

C. **Result and Discussion**

Military Epistemic Hegemony in *Bela Negara*

An analysis of policy documents and State Defence training curricula reveals that the program is historically and discursively constructed as an "extension" of the military institution.[11] This construction does not exist in a vacuum; rather, it is the residue of the long history of the military's sociopolitical role in Indonesia, placing soldiers as the primary guardians not only of territorial sovereignty but also of the nation's ideological stability.[12] Consequently, the definition of what it means to "defend the state" has undergone extreme narrowing, reduced to a series of physical rituals and symbolism of uniformity that mimic military barrack life.

This dominance creates a single standard of knowledge validity within the defence realm. Knowledge considered "legitimate" or authoritative within the State Defence ecosystem is instructional, hierarchical, and oriented toward physical mobilization, such as marching drills, ceremonial protocols, and light weaponry familiarization.[13] Within this framework, citizens' bodies are disciplined to become compliant (*docile bodies*) rather than enlightened to become critical defence agents. This method, while perhaps effective for 20th-century trench warfare,

[11] Ristian Atriandi Supriyanto, "Indonesia's Naval Modernization: A Sea Change?" *Journal of Strategic Studies* 39, no. 5–6 (2016): 750–773; R. Tjiptaningrum, "Indigenising Defence Concepts in Indonesia: The Case of Bela Negara," *Journal of ASEAN Studies* 9, no. 2 (2021): 145–163.

[12] Sebastian and Gindarsah, "Taking Stock," 295.

[13] Reni B. Prihatin, "Military Dominance and Civil-Military Relations in Post-Authoritarian Indonesia," *Defense & Security Analysis* 33, no. 4 (2017): 385–403

continues to be dogmatically maintained even though the threat landscape has drastically shifted to the non-military.

The direct consequence of this approach is the creation of systematic epistemic injustice against civilian expertise. In the hierarchy of knowledge constructed by military hegemony, civilian technocratic expertise is often positioned as secondary or auxiliary knowledge. A cyber security expert, epidemiologist, or macro-economic analyst is often deemed not to possess "sufficient" defence capacity if they have not undergone the process of "militarizing" the body and mind through basic military training.[14]

Furthermore, this hegemony gives rise to the myth of civilian incompetence in national security affairs. There is a tacit assumption that civilians are disorderly and undisciplined entities, such that their knowledge is only considered useful to the state after being "ordered" by military command logic.[15] This view ignores the fact that in the context of modern network-centric warfare, creativity and flexibility of thought hallmarks of civilian epistemology—are actually more strategically valuable than blind obedience.

The most tangible manifestation of this inequality is seen in the marginalization of strategic professions within the narrative of patriotism. An ethical hacker working silently to secure the state banking infrastructure from ransomware attacks often receives no recognition as a "defender of the state" in formal terminology simply because they work behind the scenes without uniform attributes.[16] Conversely, participation in grand assemblies or ceremonial physical exercises is often glorified as the pinnacle of defence dedication, creating a concerning distortion of values regarding the substance of defence itself.

The greatest danger of this epistemic dominance is the creation of a fatal "strategic blind spot." When the state focuses too heavily on physical defence parameters such as the number of reserve personnel who can execute drill commands it becomes complacent regarding vulnerabilities in the non-military sector. The military may possess unrivaled expertise in securing geographical borders from physical invasion, yet the institution often falters and lacks the tactical vocabulary to face threats attacking information infrastructure, mass psychological stability, or biological resilience, which are the native domains of civilian expertise.[17]

This strategic blindness is exacerbated by institutional resistance to sharing authority. Military hegemony in State Defence tends to create a closed system, where input or criticism from civilian experts is often viewed with suspicion as a form of doctrinal weakening or a lack of nationalism.[18] In reality, academic criticism and data analysis offered by civilians are forms of

[14] Kevin H. Williams, "Strategic Learning in Defense Policy: Epistemic Pluralism and Organizational Adaptation," *Security Studies* 27, no. 4 (2018): 629–654

[15] Honna, "The Politics of Military Professionalism," 880.

[16] Muhammad A. Rochman and M. Yola, "Collaborative Governance in The Cyber Defense Sector: Indonesia's Perspective," *Journal of Human Security* 19, no. 1 (2023): 22–35

[17] Fitriani, "Re-evaluating Indonesia's Defence Strategy: The Case of the Essential Force," *Journal of Defence Studies* 20, no. 1 (2018): 1–18

[18] Haripin, Civil-Military Relations, 78.

open-source intelligence crucial for detecting hybrid threats early on. The rejection of knowledge pluralism renders the defence system rigid and brittle.

Moreover, the military-dominated State Defence curriculum often fails to transfer relevant skills (*skill transferability*) for facing real crises.[19] Training focused on physical motion uniformity provides no competence whatsoever when the state faces disinformation attacks that fracture social cohesion on social media. Citizens trained in State Defence may have high spirits, but without relevant cognitive knowledge, they lack the tools to defend the state from non-kinetic attacks.

This phenomenon also reflects a mismatch between resource allocation and threat reality. Large budgets allocated for militaristic-style training become inefficient when the greatest threats come from cyberspace or global pandemics.[20] Military epistemic hegemony prevents the reallocation of intellectual and financial resources toward the development of "smart defence" based on technological superiority and research, which should be the realm of equal civil-military collaboration.

Finally, it must be acknowledged that maintaining military epistemic hegemony in State Defence is not merely a matter of tactical ineffectiveness, but an existential risk to national resilience. In an era where the boundary between war and peace is blurred (*gray zone*), the monopoly of defence interpretation by a single institution is a recipe for failure. The sustainability of the state no longer depends on how many citizens can bear arms, but on how effectively the state can integrate civilian intelligence and military strength in a harmonious defence orchestration, without one dominating the other.[21]

The New Paradigm: From Territorial to Cognitive Defence

This research formulates an urgent paradigm shift in the concept of State Defence, moving from a conventional approach centered on territorial occupation toward a contemporary approach focused on cognitive dominance. In the old, territorial paradigm, Indonesia's defence architecture was designed with the assumption that the greatest existential threat was a foreign military invasion aiming to occupy land, water, and air. However, this assumption has been fundamentally disrupted by the reality of fifth-generation warfare, where the battlefield has shifted from geographical frontlines to abstract spaces such as cyber, economic, and mass psychology.[22]

The shift in threat focus is the primary driver of this transformation. Full-scale kinetic invasion has become increasingly unlikely due to high political and economic costs. Instead, the state now faces silent yet lethal hybrid threats, such as information warfare, digital infrastructure

[19] Laksmana, "Reinventing Defense Diplomacy," 20.

[20] Marcus Mietzner, "Populist Anti-Scientism, Religious Polarisation, and Institutionalised Corruption: How Indonesia's Democratic Decline Shaped its COVID-19 Response," *Journal of Current Southeast Asian Affairs* 39, no. 2 (2020): 227–249

[21] Williams, "Strategic Learning," 635.

[22] Fitriani, "Re-evaluating Indonesia's Defence Strategy," 5.

sabotage, engineered pandemics, and economic coercion.[23] In this context, the doctrine that only trains citizens to march or shoot static targets becomes irrelevant, as the enemy no longer arrives in military uniforms, but through fiber optic cables and algorithms that destabilize social cohesion.

The shift in defence domains also demands a redefinition of sovereignty. If sovereignty was previously measured by physical border markers, data sovereignty and cyber integrity are now the primary parameters of state survival. The new paradigm acknowledges that the "homeland" (*tanah air*) now includes the "digital realm," where strategic data theft or the paralysis of the national banking system has destructive impacts equivalent to the bombing of physical infrastructure.[24] Therefore, cognitive defence demands the capability to secure narratives and data, not merely territory.

The implications of this domain shift drastically alter the profile of primary actors in total defence. In the territorial paradigm, the military hierarchy and physical reserve components were the main protagonists. However, in the cognitive/hybrid paradigm, the status of "state defender" undergoes radical democratization. A technology expert patching security holes in election commission servers, a scientist developing indigenous vaccines, or "organized netizens" countering separatist disinformation are the true vanguard.[25] In this paradigm, military rank no longer guarantees knowledge authority; technical and intellectual competence becomes the new currency in defence.

Consequently, the form of State Defence must transform from "bearing arms" to "bearing competence." Basic military training (bootcamps) is no longer adequate as the sole method of development. The new paradigm demands a curriculum emphasizing advanced digital literacy, community-based food security, and strategic research.[26] The ability to verify information amidst a flood of hoaxes (*counter-disinformation*) becomes a tactical skill as important as the ability to disassemble and reassemble weapons in the past.

Furthermore, this new paradigm places civilian expertise as primary defence, not merely logistical support. Historically, civilians were positioned as objects to be protected or administrative auxiliary forces for the military. However, studies show that in modern crises like the COVID-19 pandemic, civilian leadership supported by data science proved more effective in mitigating threats than rigid militaristic command approaches.[27] This recognition demands a restructuring of the state's view of its civilian assets.

Mass psychology also becomes a crucial battleground in the cognitive paradigm. Enemies in hybrid warfare aim to break the nation's political will without firing a single bullet. Therefore,

---

[23] Terry C. Pellmar and J. R. Strizzi, "Understanding the Hybrid Threat: A Conceptual Framework," Journal of Strategic Security 14, no. 3 (2021): 1–17, https://doi.org/10.5038/1944-0472.14.3.1895

[24] Rochman and Yola, "Collaborative Governance," 25.

[25] Siwage D. Negara, "Indonesia's Digital Economy: Trends, Opportunities, and Challenges," Journal of Southeast Asian Economies 40, no. 1 (2023): 45–68, https://doi.org/10.1355/ae40-1c.

[26] Tjiptaningrum, "Indigenising Defence Concepts," 150.

[27] Mietzner, "Populist Anti-Scientism," 230.

the new style of State Defence must focus on building the "cognitive immunity" of society. This is not about blind indoctrination, but about building citizens' critical reasoning so they are not easily politicized or pitted against one another by foreign influence operations.[28]

On the economic front, the new paradigm integrates economic resilience as an integral part of defence. Dependence on vulnerable global supply chains can be weaponized by adversaries. Therefore, entrepreneurs strengthening national industrial independence and innovators reducing dependence on strategic technology imports are tangible manifestations of modern patriotism. Their contribution is not ceremonial, but substantial in maintaining the state's economic sovereignty from external pressure.[29]

However, the transition to this cognitive paradigm faces significant strategic cultural challenges. There is still a strong tendency among policymakers to measure defence strength based on the number of personnel and physical hardware, while neglecting investment in intellectual capacity (software). The hegemony of the old paradigm often hinders budget allocation for defence research or cyber infrastructure development, which are, in fact, the backbone of future defence.[30]

In conclusion, maintaining the old paradigm amidst a changing threat landscape is a recipe for strategic collapse. Indonesia must dare to leave behind the romanticization of past guerilla warfare and begin building sophisticated cognitive defence capacities. In this era, civilian expertise in analyzing big data, securing networks, and mitigating social crises is the purest and most needed form of *Bela Negara*.[31]

Knowledge Negotiation: The *Boundary Spanning* Mechanism

To realize the cognitive defence paradigm discussed previously, the state can no longer rely on a single command. A formal mechanism called knowledge negotiation is required—a dialectical process where decision-making authority is distributed based on the relevance of expertise, not rank hierarchy. In this context, negotiation is not a sign of state weakness, but a rational adaptation strategy. The main challenge is to dismantle the institutional walls that have long separated the closed "military world" from the open "civilian world," enabling a smooth flow of information and innovation between the two.

Case studies on the initial response to the COVID-19 pandemic in Indonesia provide valuable lessons regarding the dangers of epistemic monopoly. In the early phase of the crisis, the dominant approach was securitization, where health data was treated like military secrets and the command structure was dominated by retired generals. The result was a stuttering response: non-transparent data hindered mitigation, and disciplinary approaches failed to stop the spread

[28] Williams, "Strategic Learning," 640

[29] Laksmana, "Reinventing Defense Diplomacy," 22.

[30] Haripin, Civil-Military Relations, 82.

[31] Fitriani, "Re-evaluating Indonesia's Defence Strategy," 10

of a biological virus.[32] This failure demonstrated that military logic accustomed to fighting visible enemies lacked the adequate epistemological tools to fight microscopic enemies.

The effectiveness of crisis handling only began to appear when there was a strategic shift toward collaboration. The turning point occurred when the government began to open space for knowledge negotiation, giving the stage to epidemiologists, biostatisticians, and civilian medical associations to lead the narrative and technical strategy. In this phase, the military was not sidelined, but its role was reduced and respecified to logistical support and field protocol enforcement. This synergy proved that protecting the state in facing non-traditional threats requires deference to civilian scientific authority.

This phenomenon of successful collaboration is known in academic literature as boundary spanning. This concept refers to an organization's capacity to bridge its internal boundaries to absorb external resources. In the context of hybrid defence, boundary spanning allows for an ideal division of labor: the military provides solid command infrastructure and logistical discipline, while civilian actors inject analytical content, precision data, and technological innovation.[33] Without this boundary spanning, the state will be trapped in rigid and lagging responses.

The application of boundary spanning is most starkly visible in the cyber defence domain. The anarchic and machine-speed landscape of cyber threats stands in sharp contrast to bureaucratic and hierarchical military culture. Vertical command structures, designed to prevent insubordination in conventional war, become fatal obstacles in cyber war. Decisions that must pass through tiered chains of command often make military responses lag behind decentralized hacker attacks.[34]

This is where the urgency of the civilian network role lies. The community of ethical hackers and network security experts operates in fluid, meritocratic, and adaptive structures. They are accustomed to sharing vulnerability information in real-time within global networks without being bound by rigid protocols. In many cases of national data breach incidents, it is this civilian community that first detects, verifies, and provides early warning, long before formal defence institutions are aware. Therefore, cyber defence effectiveness depends on the military's ability to negotiate and partner with this “wild” yet competent civilian ecosystem.[35]

For this negotiation to be equitable, a psychological-institutional prerequisite called epistemic humility is required. This concept demands that the military institution possess the professional maturity to “know its place” and acknowledge the limits of its expertise. Epistemic humility is not an admission of defeat, but a strategic awareness that in non-military domains—

[32] Mietzner, "Populist Anti-Scientism," 235.
[33] Rochman and Yola, "Collaborative Governance," 28.
[34] Negara, "Indonesia's Digital Economy," 50.
[35] Rochman and Yola, "Collaborative Governance," 30

such as the digital economy, public health, or social psychology leadership must be yielded to civilian experts.[36]

This attitude requires the military to dare to step back from the position of primary decision-maker to become a facilitator or supporter in the context of non-military State Defence. For example, in facing currency speculation attacks threatening economic sovereignty, a four-star general must be willing to be led by the central bank governor or civilian economists. Command logic must submit to market logic. Without this humility, military intervention in the civilian realm will only muddy the waters and create policy distortions.

However, realizing epistemic humility and boundary spanning is not an easy task as it clashes with strategic culture established over decades. Sectoral ego and distrust toward civilian competence remain major obstacles. Often, civilian involvement in defence is merely cosmetic or ceremonial, without real delegation of authority. Therefore, this knowledge negotiation mechanism must be institutionalized in binding regulations, not merely as ad-hoc initiatives when crises occur.[37]

In conclusion, the future of Indonesia's national resilience depends on the state's ability to manage the negotiation between the sword and the pen, between the uniform and the lab coat, between command and algorithm. Through boundary spanning mechanisms based on epistemic humility, State Defence can transform into an orchestration of smart power. In this new ecosystem, the rigid military hierarchy is no longer the sole pillar, but stands equally alongside adaptive and innovative civilian intelligence networks.[38]

D. Conclusion

The current dominance of the military paradigm in the concept of State Defence is identified as a historical residue that hampers the modernization of Indonesia's defence, as this physical-territorial approach has become anachronistic amidst the complexity of 21st-century hybrid threats. Consequently, this study urges the adoption of "Epistemic Pluralism" as an urgent operational necessity, wherein civilian knowledge must be acknowledged as possessing strategic validity equivalent to military knowledge within a total defence system. Implementing this concept demands radical policy reforms, ranging from the diversification of the State Defence curriculum separating conventional physical tracks from professional technocratic tracks—to the institutionalization of a civil-military forum based on the meritocracy of expertise, where leadership authority is determined by technical competence rather than military rank. This transformation must culminate in a visionary budget reallocation, shifting the state's investment focus from mere hardware procurement to the strengthening of intellectual capacity (brainware)

[36] Williams, "Strategic Learning," 645

[37] Haripin, Civil-Military Relations, 90.

[38] Negara, "Indonesia's Digital Economy," 55.

and strategic research, marking a fundamental shift from the "militarization of civilians" toward an adaptive cognitive defence paradigm.

References

Fitriani, F. "Re-evaluating Indonesia's Defence Strategy: The Case of the Essential Force." *Journal of Defence Studies* 20, no. 1 (2018): 1–18. https://doi.org/10.1080/14799855.2018.1504823.

Haripin, Muhamad. *Civil-Military Relations in Indonesia: The Politics of Military Operations Other Than War*. London: Routledge, 2019.

Honna, Jun. "The Politics of Military Professionalism in Indonesia: Civil-Military Relations and the Struggle for Reform." *The Pacific Review* 35, no. 5 (2022): 876–902. https://doi.org/10.1080/09512748.2021.1906745.

Laksmana, Evan A. "Reinventing Defense Diplomacy in Southeast Asia?" *Asian Security* 15, no. 1 (2019): 13–31. https://doi.org/10.1080/14799855.2017.1362704.

Mietzner, Marcus. "Populist Anti-Scientism, Religious Polarisation, and Institutionalised Corruption: How Indonesia's Democratic Decline Shaped its COVID-19 Response." *Journal of Current Southeast Asian Affairs* 39, no. 2 (2020): 227–249. https://doi.org/10.1177/1868103420935561.

Negara, Siwage D. "Indonesia's Digital Economy: Trends, Opportunities, and Challenges." *Journal of Southeast Asian Economies* 40, no. 1 (2023): 45–68. https://doi.org/10.1355/ae40-1c.

Pellmar, Terry C., and J. R. Strizzi. "Understanding the Hybrid Threat: A Conceptual Framework." *Journal of Strategic Security* 14, no. 3 (2021): 1–17. https://doi.org/10.5038/1944-0472.14.3.1895.

Prihatin, Reni B. "Military Dominance and Civil-Military Relations in Post-Authoritarian Indonesia." *Defense & Security Analysis* 33, no. 4 (2017): 385–403. https://doi.org/10.1080/14751798.2017.1377488.

Rochman, Muhammad A., and M. Yola. "Collaborative Governance in The Cyber Defense Sector: Indonesia's Perspective." *Journal of Human Security* 19, no. 1 (2023): 22–35. https://doi.org/10.3316/JHS0123022.

Sebastian, Leonard C., and Iis Gindarsah. "Taking Stock of Military Reform in Indonesia." *Contemporary Southeast Asia* 35, no. 2 (2013): 291–313. https://doi.org/10.1355/cs35-2g.

Tjiptaningrum, R. "Indigenising Defence Concepts in Indonesia: The Case of Bela Negara." *Journal of ASEAN Studies* 9, no. 2 (2021): 145–163. https://doi.org/10.21512/jas.v9i2.7342.

Williams, Kevin H. "Strategic Learning in Defense Policy: Epistemic Pluralism and Organizational Adaptation." *Security Studies* 27, no. 4 (2018): 629–654. https://doi.org/10.1080/09636412.2018.1448043.

Haripin, Muhamad. *Civil-Military Relations in Indonesia: The Politics of Military Operations Other Than War*. London: Routledge, 2019.

Honna, Jun. "The Politics of Military Professionalism in Indonesia: Civil-Military Relations and the Struggle for Reform." *The Pacific Review* 35, no. 5 (2022): 876–902. https://doi.org/10.1080/09512748.2021.1906745.

Laksmana, Evan A. "Reinventing Defense Diplomacy in Southeast Asia?" *Asian Security* 15, no. 1 (2019): 13–31. https://doi.org/10.1080/14799855.2017.1362704.

Pellmar, Terry C., and J. R. Strizzi. "Understanding the Hybrid Threat: A Conceptual Framework." *Journal of Strategic Security* 14, no. 3 (2021): 1–17. https://doi.org/10.5038/1944-0472.14.3.1895.

Prihatin, Reni B. "Military Dominance and Civil-Military Relations in Post-Authoritarian Indonesia." *Defense & Security Analysis* 33, no. 4 (2017): 385–403. https://doi.org/10.1080/14751798.2017.1377488.

Sebastian, Leonard C., and Iis Gindarsah. "Taking Stock of Military Reform in Indonesia." *Contemporary Southeast Asia* 35, no. 2 (2013): 291–313. https://doi.org/10.1355/cs35-2g.

Tjiptaningrum, R. "Indigenising Defence Concepts in Indonesia: The Case of Bela Negara." *Journal of ASEAN Studies* 9, no. 2 (2021): 145–163. https://doi.org/10.21512/jas.v9i2.7342.

Williams, Kevin H. "Strategic Learning in Defense Policy: Epistemic Pluralism and Organizational Adaptation." *Security Studies* 27, no. 4 (2018): 629–654. https://doi.org/10.1080/09636412.2018.1448043.

© 2020 by the authors. Submitted for possible open access publication under the terms and conditions of the Licensed under Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) license(Deed - Attribution-NonCommercial 4.0 International - Creative Commons).