

## **Hybrid Warfare And Total Defense Strategy: Indonesia's Comprehensive Security Framework In The Indo-Pacific Era**

**Heru Prasetyo<sup>1)</sup>\*, Priyanto Suharto<sup>2)</sup>, Totok Imam Santoso<sup>3)</sup>, Sulistyanto<sup>4)</sup>**

<sup>1,2,3,4)</sup>Program Studi Strategi Perang Semesta, Fakultas Strategi Pertahanan, Universitas Pertahanan RI

\*Corresponding Author

Email: [heruprasetyo100@gmail.com](mailto:heruprasetyo100@gmail.com)

---

### **Abstract**

*The Indo-Pacific region is witnessing a transformation in its security architecture, with hybrid warfare emerging as a dominant threat. This includes a blend of conventional military force, cyber operations, disinformation, economic coercion, and proxy conflicts. As the world's largest archipelagic state and a key middle power in Southeast Asia, Indonesia faces increasing pressure to adapt its national defense strategy. This study explores how Indonesia's Total Defense Strategy (Sishankamrata) addresses multidimensional hybrid threats and evaluates its effectiveness. Using a qualitative approach through a Systematic Literature Review (SLR) of sources from 2010 to 2024, the research highlights Indonesia's efforts to integrate cyber defense, civil-military cooperation, and public mobilization initiatives such as Bela Negara and the Reserve Component. While these reflect progress, challenges persist in the form of fragmented institutional coordination, limited technological capacity, and inconsistent implementation across the archipelago. The Total Defense Strategy provides a strong framework, yet structural and operational gaps hinder its full potential. To improve effectiveness, Indonesia must strengthen inter-agency synergy, upgrade early warning systems, and align defense strategy with national development. Regional collaboration through ASEAN and multilateral platforms is also critical. This research offers insights for other archipelagic and middle-power states facing similar hybrid threats.*

**Keywords:** *Hybrid Warfare, Total Defense, Indonesia, Indo-Pacific, Security Strategy*

---

## **INTRODUCTION**

The Indo-Pacific region has undergone a fundamental transformation in its security paradigm over the past two decades, marking a decisive shift from traditional state-centric military confrontations to complex, multidimensional hybrid warfare operations that blur the boundaries between war and peace. This transformation reflects broader changes in the global security environment, where "hybrid threats are a mix of military and non-military, covert and overt activities by state and non-state actors that occur below the line of conventional warfare" (Seebeck et al., 2022). The contemporary security landscape is characterized by the simultaneous employment of conventional military capabilities alongside cyber operations, information warfare, economic coercion, and proxy activities, creating a complex threat matrix that challenges traditional deterrence mechanisms and defense strategies. The rise of great power competition, particularly between the United States and China, has accelerated this transformation, with both nations employing sophisticated hybrid strategies to advance their strategic objectives without crossing the threshold of direct military confrontation (Beckley & Brands, 2022).

The strategic significance of this transformation cannot be overstated, as it fundamentally alters the nature of security competition in the world's most economically vital region. "This region has become the central theater in the competition between the United States and China to shape the course of the 21st century" (Center for a New American Security, 2024). Unlike conventional military conflicts that rely primarily on kinetic capabilities and territorial objectives, hybrid warfare in the Indo-Pacific operates across multiple domains simultaneously, including cyberspace, information environments, economic networks, and diplomatic channels. This multidomain approach enables state and non-state actors to achieve strategic objectives through sustained, coordinated campaigns that remain below the threshold of conventional

warfare while still imposing significant costs on adversaries. The integration of technological capabilities, particularly in cyber and information domains, has enabled hybrid actors to project power and influence across vast distances, making traditional geographical barriers increasingly irrelevant in contemporary security calculations (Hoffman, 2014).

The implications of this paradigmatic shift extend far beyond traditional military planning, requiring comprehensive adaptations in national security strategies, alliance structures, and defense capabilities across the Indo-Pacific region. Middle powers like Indonesia, Australia, and Japan find themselves navigating an increasingly complex security environment where traditional alliance relationships and bilateral security arrangements prove insufficient to address multifaceted hybrid threats. The challenge is compounded by the fact that "neither the United States nor China is clearly 'winning' the competition for influence in the Indo-Pacific region as whole, and they have varying levels of influence across countries" (RAND Corporation, 2024), creating a fluid strategic environment where smaller states must carefully balance competing pressures while developing autonomous capabilities to address hybrid threats. This new security paradigm demands innovative approaches to defense planning that integrate traditional military capabilities with comprehensive societal resilience, cyber defense, information security, and economic protection measures, fundamentally reshaping how nations conceptualize and implement their national security strategies.

Indonesia, as the world's largest archipelagic state and a pivotal middle power in Southeast Asia, faces unprecedented security challenges that transcend conventional military threats. The rise of great power competition, technological warfare capabilities, and non-traditional security threats necessitates a comprehensive reevaluation of national defense strategies.

The contemporary threat landscape in the Indo-Pacific region is characterized by an unprecedented level of complexity, where traditional military threats have evolved into sophisticated multidimensional operations that simultaneously target military, economic, technological, and information domains. This multifaceted approach represents a fundamental departure from conventional warfare paradigms, as "states increasingly weaponize interdependence by leveraging global networks of informational and financial exchange for strategic advantage" (Farrell & Newman, 2019). The integration of these domains creates synergistic effects that amplify the impact of individual threat vectors while complicating attribution and response mechanisms. Cyber capabilities have emerged as a critical enabler of this multidimensional approach, with "governments across the Indo-Pacific region racing to develop their cyber capabilities in order to ensure their future security and prosperity", fundamentally altering the nature of state-to-state competition and creating new vulnerabilities in critical infrastructure and economic systems.

The economic dimension of these multidimensional threats has become particularly sophisticated, with state actors employing "weaponized interdependence" strategies that exploit asymmetric network structures in global economic systems to achieve coercive effects. "Dealing with China's weaponization of trade is a critical pre-requisite for the success of the Biden administration's strategic competition with China", highlighting how economic coercion has become a central feature of contemporary geopolitical competition. These economic warfare tactics include supply chain manipulation, technology transfer restrictions, investment screening mechanisms, and the strategic use of economic dependencies to influence political behavior. The technological domain has become equally contested, with advanced artificial intelligence technologies potentially enhancing capabilities to "conduct information operations at an unprecedented scale and sophistication (RAND Corporation, 2024), creating new vectors for influence operations and cognitive warfare that can shape public opinion and political decision-making processes across national boundaries.

The information domain represents perhaps the most insidious aspect of contemporary multidimensional threats, as it directly targets societal cohesion and democratic governance structures through sophisticated disinformation campaigns and cognitive warfare operations. The challenge is particularly acute in the Indo-Pacific region, where "Vietnam is the most targeted country to cyber-attacks in the region, followed by Indonesia; Taiwan remains a privileged focus for the Chinese hackers", demonstrating how cyber operations serve as enablers for broader information warfare campaigns. These operations are designed to create strategic ambiguity, undermine trust in institutions, and create social divisions that can be exploited during periods of crisis or conflict. The convergence of these four domains creates what military strategists term "multi-domain operations," where "Multi-Domain Task Forces integrate non-kinetic effects and kinetic capabilities under one commander while the unit's components conduct distributed operations to enhance survivability", requiring new organizational structures and strategic approaches to effectively counter these complex threat matrices.

**Table 1. Multidimensional Threat Matrix in the Indo-Pacific Region**

| Threat Domain        | Primary Characteristics   | Key Actors  | Target Vulnerabilities   | Impact Mechanisms   |
|----------------------|---|---|--|---|
| <b>Military</b>      | Conventional force projection<br>Gray zone operation<br>Proxy warfare<br>Maritime militarization        | State militaries,<br>Proxy forces and<br>Paramilitary units                                       | Critical infrastructure<br>Maritime chokepoints<br>Border regions<br>Allied relationships  | Deterrence erosion<br>Territorial coercion<br>Alliance strain<br>Escalation control         |
| <b>Economic</b>      | Trade weaponization<br>Investment coercion<br>Supply chain manipulation<br>Financial system leverage    | State economic agencies,<br>State-owned enterprises and<br>Strategic investors                    | Trade dependencies<br>Critical supply chains<br>Financial systems<br>Technology ecosystems | Economic dependency<br>Political influence<br>Strategic vulnerability<br>Technology denial  |
| <b>Technological</b> | Cyber espionage<br>Critical infrastructure attacks<br>Technology transfer coercion<br>Standards warfare | State cyber units,<br>Intelligence services,<br>Technology companies and<br>Research institutions | Digital infrastructure<br>Industrial systems<br>Research networks<br>Communication systems | Data theft<br>System disruption<br>Innovation suppression<br>Strategic dependence           |
| <b>Information</b>   | Disinformation campaigns<br>Cognitive warfare<br>Media manipulation<br>Social media exploitation        | Intelligence agencies,<br>Propaganda units,<br>Influence networks and<br>Bot farms                | Democratic processes<br>Social cohesion<br>Public opinion<br>Elite perceptions             | Political polarization<br>Decision paralysis<br>Social fragmentation<br>Strategic confusion |

Source: processed by researchers (2025)

This comprehensive threat matrix illustrates the interconnected nature of contemporary security challenges in the Indo-Pacific region, where each domain reinforces and amplifies threats in other areas. The military domain provides the foundational deterrent effect that creates space for operations in other domains, while economic coercion creates dependencies that can be exploited during periods of tension. Technological threats enable information operations while simultaneously creating vulnerabilities that can be exploited for economic or military purposes. Information warfare operations, in turn, create the strategic ambiguity and social divisions that complicate effective responses to military, economic, and technological threats. The synergistic effects of these multidimensional operations create what scholars term "compound threats" that exceed the sum of their individual components, requiring comprehensive defense strategies that can address multiple domains simultaneously while maintaining strategic coherence and operational effectiveness.

Indonesia, as the world's largest archipelagic state, occupies a pivotal position at the intersection of the Indian and Pacific Oceans, making it a strategic fulcrum in the Indo-Pacific geopolitical landscape. This geostrategic location places Indonesia at the heart of major maritime trade routes, including the Strait of Malacca, the Sunda Strait, and the Lombok Strait—passages through which over 60% of global maritime trade transits (Kaplan, 2018). As geopolitical rivalries intensify between the United States and China, Indonesia's maritime domain becomes increasingly significant—not only as a strategic chokepoint but also as a buffer zone in regional balance-of-power dynamics. Consequently, Indonesia is both a beneficiary of economic connectivity and a potential frontline state in future hybrid conflicts involving state and non-state actors.

Given this strategic exposure, the concept of national defense in Indonesia can no longer be restricted to conventional military preparedness. The emergent nature of **hybrid warfare**, characterized by the blending of conventional military tactics with cyber operations, disinformation campaigns, economic coercion, and proxy warfare, demands a paradigm shift in defense doctrine (Fridman, 2018). Traditional defense postures, while still essential, are insufficient to address these multidomain threats that bypass clear boundaries of war and peace. Recent incursions by foreign vessels in Indonesia's exclusive economic zone (EEZ), digital espionage incidents, and coordinated information manipulation—particularly related to Papua—underscore the urgency of adaptive, whole-of-nation responses (Sarjito, 2025).

Indonesia's Total Defense Strategy (Sishankamrata) offers a foundational concept to counter hybrid threats by emphasizing civilian-military integration, resilience of critical infrastructure, and mass mobilization rooted in national ideology. However, the existing formulation, largely reactive and domestically focused, must evolve to become proactive, technologically agile, and globally oriented. The adoption of Sweden's and Finland's total defense models, which incorporate cyber defense, psychological preparedness, and cross-sectoral coordination, provides valuable lessons (Sederholm et al., 2025). To remain resilient, Indonesia must institutionalize hybrid threat response mechanisms across sectors—defense, intelligence, communication, digital economy—and cultivate strategic awareness among its citizens.

As a maritime middle power, Indonesia's security architecture must align with the Indo-Pacific's shifting threat environment. This alignment requires enhancing cyber defense capabilities, streamlining inter-agency coordination, and embedding total defense principles into national development policy. Additionally, expanding regional security cooperation under the ASEAN Outlook on the Indo-Pacific (AOIP) and leveraging multilateral forums such as the ADMM-Plus can strengthen deterrence and collective resilience (Abbondanza, 2022). The integration of the Total Defense Strategy into Indonesia's foreign and security policy frameworks represents not just a national imperative, but a contribution to regional stability in an increasingly complex and contested Indo-Pacific order.

The central problem addressed in this study revolves around understanding how the evolution of hybrid warfare influences Indonesia's comprehensive security framework, particularly in the context of the increasingly contested Indo-Pacific region. This research seeks to examine the extent to which Indonesia's Total Defense Strategy (Sishankamrata) has been effective in mitigating complex and multidimensional hybrid threats, such as cyber attacks, disinformation, and proxy conflicts. Furthermore, it aims to identify the key challenges in implementing a truly integrated and adaptive defense strategy, including institutional coordination, technological readiness, civil-military collaboration, and alignment with regional security dynamics.

This research aims to analyze Indonesia's adaptation to the evolving nature of hybrid warfare through the lens of its Total Defense Strategy (Sistem Pertahanan dan Keamanan Rakyat Semesta—Sishankamrata), assessing how effectively this approach addresses multidimensional threats in the Indo-Pacific security environment. Previous studies indicate that although Sishankamrata has been updated to reflect 21st-century security challenges, its implementation still faces substantial constraints, particularly in terms of budget limitations and defense equipment distribution across major islands, underscoring the need for mobilizing all national resources—natural, human, and artificial—while enhancing the Indonesian National Armed Forces' (TNI) human resource capacity to respond to hybrid threats (Hendra et al., 2024).

In evaluating the coherence of Indonesia's defense posture, scholars have identified that the internal orientation of Sishankamrata and multinational acquisition policies have at times produced fragmentation and interoperability issues. Addressing these requires a more integrated national defense strategy, with a stronger emphasis on Anti-Access/Area Denial (A2/AD) capabilities to safeguard strategic maritime and air domains (Daneswara & Nasution, 2025). Furthermore, while the 2018 Defense White Paper acknowledges the need to address hybrid threats—such as cyberattacks, terrorism, and other unconventional challenges—the current military doctrine remains largely conventional. This highlights the urgency of restructuring both defense organizations and doctrines to transition effectively toward hybrid warfare readiness (Asmoro et al., 2024).

Cybersecurity emerges as a critical pillar in this transformation. The establishment of the TNI Cyberforce represents a significant step in reinforcing Indonesia's digital defense, particularly following a series of cyberattacks on vital national infrastructure. Using an objectives–ways–means framework, this force plays a pivotal role in safeguarding the nation's digital sovereignty (Wulandari et al., 2025). Lessons from the Ukrainian conflict further emphasize the importance of countering hybrid threats such as disinformation and cyber aggression through the creation of a dedicated military cyber command and by deepening strategic cooperation with partners like the United States and Japan. Regional exercises under the ADMM-Plus framework are also essential to strengthen collective defense mechanisms in the Indo-Pacific.

Strategically, this study also draws upon the concept of the Nusantara Trident Shield (NTS), envisioned as an extension of the Minimum Essential Force (MEF), which integrates conventional capabilities with cyber warfare systems to enhance tri-service synergy and build national resilience (Hadianto & Kusuma, 2025). The significance of this research lies in its dual contribution: theoretically, it enriches the discourse on regional security studies by providing a nuanced understanding of how hybrid warfare is reshaping the strategic calculus of archipelagic states; practically, it offers actionable recommendations for institutional integration, policy innovation, and regional collaboration to strengthen Indonesia's hybrid defense posture.

## RESEARCH METHODS

This study employs a qualitative research design using the Systematic Literature Review (SLR) method to synthesize the evolving discourse on hybrid warfare and total defense within the Indo-Pacific context, with particular attention to Indonesia. The SLR approach provides a rigorous framework for identifying, selecting, evaluating, and integrating findings from existing scholarly literature and policy documents (Snyder, 2019). In addition to narrative synthesis, a meta-analytical lens is utilized to extract patterns, themes, and theoretical insights from diverse studies to generate an integrated understanding of the subject. To ensure the validity and reliability of conclusions, the study also applies data triangulation, encompassing academic literature, government reports, and strategic policy white papers (Denzin, 2012).

The literature search strategy involved accessing five major academic databases: Scopus, Web of Science, JSTOR, ProQuest, and Google Scholar, selected for their interdisciplinary coverage and high citation impact. The search was conducted using specific keywords, including “hybrid warfare,” “total defense,” “Indonesia,” “Indo-Pacific,” and “comprehensive security.” The publication window was limited to the period 2010–2024, capturing scholarly and policy responses during the rise of contemporary hybrid threats and geopolitical realignments in the Indo-Pacific. The inclusion criteria emphasized peer-reviewed journal articles, official government reports, and strategic policy documents with high relevance to the research objectives. This strategy enables the systematic capture of both theoretical developments and empirical insights critical to Indonesia’s security framework.

To enhance analytical rigor, inclusion and exclusion criteria were strictly applied. Included studies must (1) focus on hybrid warfare and total defense, (2) be geographically relevant to Indonesia or the broader Indo-Pacific, (3) be published in English or Indonesian, and (4) have been released within the last 15 years. Conversely, exclusion criteria filtered out non-peer-reviewed publications, studies irrelevant to the core geopolitical scope, and works with substantial data duplication or thematic overlap. By employing these methodological safeguards, the research ensures a balanced and academically grounded interpretation of Indonesia’s strategic posture amidst evolving hybrid threats.

## RESULT AND DISCUSSION

### **The Evolution of Hybrid Warfare in the Indo-Pacific**

The Indo-Pacific has emerged as a dynamic battleground for hybrid threats, where conventional military presence is increasingly complemented—and at times overshadowed—by non-kinetic forms of coercion. These include cyberattacks, disinformation campaigns, economic coercion, lawfare, and maritime gray-zone tactics (Erickson, 2022). Unlike traditional warfare, these threats operate below the threshold of open conflict, exploiting legal ambiguity and societal vulnerabilities to disrupt state stability. Regional flashpoints such as the South China Sea, Taiwan Strait, and critical infrastructure in Southeast Asia have become testing grounds for sophisticated hybrid operations that blend state and non-state actors across military, informational, and economic domains.

The manifestation of hybrid warfare in the Indo-Pacific is multifaceted and asymmetrical. Cyber operations targeting state institutions, electoral systems, and critical infrastructure are increasingly used to undermine sovereignty and sow mistrust among populations. Disinformation and influence operations, often conducted through proxy media and social media bots, are designed to manipulate public narratives and erode democratic legitimacy. Economic coercion, through weaponized trade dependencies or debt leverage (e.g., strategic ports or telecom

infrastructure), has become another tool in the hybrid arsenal, particularly in smaller Indo-Pacific states with limited strategic depth (Htwe, 2025). These activities often remain unattributable or deniable, complicating response mechanisms and diplomatic retaliation.

Hybrid warfare in the Indo-Pacific involves both state and non-state actors operating in coordination or independently. China, through the People's Liberation Army Strategic Support Force (PLASSF) and affiliated actors such as maritime militias and media networks, represents the most sophisticated state actor in the region's hybrid landscape. Meanwhile, non-state actors—including cybercriminal syndicates, information trolls-for-hire, and extremist groups—often serve as plausible deniability tools for state sponsors or exploit the chaos created by hybrid tactics. The blurred lines between espionage, information operations, and cyber sabotage necessitate a whole-of-government and whole-of-society response (Rid & Buchanan, 2015).

### **Adaptation of Indonesia's Total Defense Strategy**

Indonesia's defense posture has undergone a significant transformation in response to the increasingly complex security environment in the Indo-Pacific. Traditionally anchored in a territorial defense paradigm, Indonesia's doctrine has evolved toward a comprehensive security approach that blends conventional deterrence with multidimensional resilience. This shift is reflected in the Indonesian National Defense Doctrine (Doktrin Pertahanan Negara) and strategic documents such as the Defense White Paper (2015), which emphasize the need to anticipate hybrid threats and non-traditional security challenges through integrated civil-military preparedness. This doctrinal evolution underscores a recalibration of Indonesia's strategic thinking from static, land-centric defense toward a dynamic, adaptive, and layered security architecture.

One of the hallmarks of this transformation is the integration of Indonesia's tri-matra armed forces—the Army (TNI-AD), Navy (TNI-AL), and Air Force (TNI-AU)—with emerging security domains such as cyberspace and outer space. The establishment of Satuan Siber TNI (TNI Cyber Unit) and the gradual recognition of space-based surveillance capabilities illustrate this institutional adaptation. These expansions allow the Indonesian Armed Forces (TNI) to detect, respond to, and recover from hybrid incursions that originate in non-physical realms but have strategic consequences. This comprehensive posture also facilitates cross-domain interoperability, enabling joint operations that span kinetic and non-kinetic arenas, from maritime gray-zone operations to digital defense and satellite monitoring (Sianturi & Saputro, 2025).

Another critical component of Indonesia's Total Defense Strategy is the mobilization of civilian capacity, particularly through the Bela Negara (State Defense) program and the development of a Komponen Cadangan (Reserve Component). These initiatives are embedded in Law No. 23/2019 on National Resource Management for State Defense and reflect a whole-of-society approach to national security. The Bela Negara program focuses on cultivating civic awareness, ideological resilience, and digital literacy as defenses against psychological and informational dimensions of hybrid warfare. Meanwhile, the Reserve Component—comprising trained civilians ready to be mobilized during national emergencies—offers a strategic layer of depth and redundancy in human resources, enhancing national readiness in the face of persistent and adaptive threats.

### **Effectiveness of the Comprehensive Security Framework**

The effectiveness of Indonesia's comprehensive security framework, particularly through the lens of its Total Defense Strategy, lies in its ability to blend hard and soft power instruments into a unified and adaptive defense architecture. The core strength of this framework is its multi-layered approach, which ensures that military, civilian, and socio-political components collaborate to secure the nation across traditional and non-traditional domains. This design aligns with the broader concept of human security, which expands defense beyond territorial integrity to include resilience against hybrid threats such as cyberattacks, disinformation, and economic subversion (Caballero-Anthony & Cook, 2013). Indonesia's emphasis on civic engagement

through Bela Negara and reserve forces contributes to a bottom-up dimension of defense, empowering the population to recognize and resist sub-threshold aggressions.

Despite its conceptual robustness, the implementation of Total Defense in Indonesia faces structural and institutional weaknesses. Fragmented defense policy execution, overlapping jurisdictions, and lack of interoperable protocols between military and non-military institutions continue to impede coordinated responses to hybrid threats. Research by Heiduk (2022) suggests that countries in the Indo-Pacific often struggle with vertical and horizontal coordination, where strategic alignment between central and local governments remains inconsistent. In Indonesia's context, this is reflected in the uneven preparedness of regional governments to execute defense-related mandates, particularly in cyber surveillance and critical infrastructure protection.

A crucial component in the success of a comprehensive security framework is interagency coordination, particularly among the Indonesian National Armed Forces (TNI), the National Police (Polri), key ministries (Defense, Communication and Information, Foreign Affairs), and civil society organizations. While there have been promising developments—such as the joint TNI–Polri counterterrorism task forces and increased cyber drills involving BSSN (National Cyber and Crypto Agency)—these efforts often lack institutional permanence and standardized operating procedures (Jung & Tan, 2024). The absence of a unified national security doctrine that mandates interagency cooperation at strategic and tactical levels remains a persistent barrier to operational integration.

In terms of early warning capabilities and rapid response, Indonesia continues to develop its technological and human infrastructure. However, challenges persist in establishing real-time threat detection systems and digital forensics capacities that can match the speed and complexity of hybrid attacks. While the establishment of TNI's Cyber Unit (Satsiber) and increasing collaboration with international cybersecurity actors is commendable, investment in technical expertise, satellite-based surveillance, and artificial intelligence-driven analysis remains insufficient (Lee et al., 2025). Moreover, lagging coordination between defense and civilian technology sectors slows down the cycle from detection to action, especially in fast-moving domains like information warfare and critical network intrusions.

To advance the effectiveness of its comprehensive security architecture, Indonesia must prioritize policy coherence, institutional synergy, and adaptive doctrine development. The complexity of hybrid threats demands not only a whole-of-government but also a whole-of-nation response, where public awareness, digital hygiene, and societal resilience are continuously cultivated. Incorporating lessons from Nordic and Baltic total defense models—where interagency drills and scenario-based planning are routine—can serve as strategic references. Ultimately, enhancing Indonesia's strategic readiness requires sustained political commitment, budgetary prioritization, and a cultural shift toward proactive security thinking across the nation's governing institutions and civilian populace

### **Challenges and Opportunities**

Indonesia's pursuit of a robust Total Defense Strategy in the Indo-Pacific context is constrained by limited resources and technological capacities, particularly in critical areas such as cybersecurity, early warning systems, and satellite-based intelligence. Despite the growing acknowledgment of hybrid threats, Indonesia's defense budget remains relatively modest compared to regional powers such as China, Japan, and Australia (SIPRI, 2023). This financial limitation impacts the acquisition of modern defense technologies, the development of cyber infrastructure, and the recruitment of high-skilled personnel necessary for operating in new domains of warfare. Furthermore, the defense-industrial base is still developing and lacks integration with civilian technological innovation sectors, making it difficult to build a self-reliant and adaptive total defense ecosystem (Kurç & Bitzinger, 2018).

The geographical complexity of Indonesia as an archipelagic state, with over 17,000 islands and expansive maritime boundaries, adds another strategic challenge. Ensuring

synchronized implementation of the Total Defense Strategy across such a vast and diverse landscape demands decentralized coordination mechanisms, interoperable communication systems, and local civilian engagement. However, disparities in infrastructure, digital connectivity, and logistical capabilities between Java-centric administrative hubs and outer islands hinder this process. As noted by Sumadinata et al. (2022), the decentralization of security governance in Indonesia often leads to fragmented local responses, inconsistent threat assessments, and uneven participation in national resilience programs. These structural limitations require tailored, region-specific policy instruments that account for socio-cultural and geographic variations.

Despite these hurdles, Indonesia possesses significant opportunities for regional and international cooperation to enhance its hybrid threat preparedness. Initiatives such as the ASEAN Defence Ministers' Meeting (ADMM-Plus), the ASEAN Regional Forum (ARF), and bilateral partnerships with countries like Australia, the United States, and Japan provide frameworks for capacity building, intelligence sharing, and joint training exercises. Programs such as the Malacca Strait Patrol and regional cyber capacity-building projects have demonstrated the potential of multilateral security cooperation in enhancing maritime and cyber domain security (Zimmerman, 2018). Furthermore, Indonesia's active role in multilateral forums positions it as a normative leader in advocating for comprehensive, rules-based regional security mechanisms.

Finally, the role of defense diplomacy emerges as a strategic asset for Indonesia in managing rising tensions and avoiding escalation in the Indo-Pacific. Through soft power engagements, military-to-military dialogues, and strategic partnerships, Indonesia has been able to project itself as a neutral and stabilizing actor amid great power rivalries. Defense diplomacy also enables Indonesia to balance deterrence with engagement—maintaining strategic autonomy while fostering collaborative threat mitigation. As Sumadinata et al. (2022) argue, defense diplomacy plays a crucial role in building transparency, trust, and confidence among states, especially in regions marked by overlapping security interests. For Indonesia, this diplomatic approach complements the Total Defense framework by ensuring that preventive measures are as robust as reactive ones.

## CONCLUSION

The evolving nature of hybrid warfare has significantly reshaped the security landscape in the Indo-Pacific, demanding a fundamental shift in national defense doctrines. For Indonesia, the rise of multidimensional threats—including cyberattacks, economic coercion, disinformation, and proxy conflicts—necessitates the transformation of its traditional security framework into a comprehensive and adaptive Total Defense Strategy. This study finds that while Indonesia has made notable progress through doctrinal reforms, the establishment of cyber units, and the mobilization of civil society via programs like *Bela Negara* and the Reserve Component, structural and institutional challenges persist. Fragmented coordination, limited technological capacity, and uneven regional implementation hinder the full realization of an integrated defense architecture. Nonetheless, Indonesia's strategic positioning and its commitment to a rules-based regional order offer significant potential for enhanced resilience through proactive adaptation and regional cooperation.

The findings underscore the urgency for Indonesia to institutionalize a proactive, hybrid-resilient defense posture. Policymakers must prioritize the development of an integrated national security doctrine that mandates interagency coordination, real-time cyber defense infrastructure, and public-private partnerships in technology development. Investing in digital literacy and societal resilience must be a national priority, enabling citizens to function as active participants

in resisting hybrid threats. Additionally, embedding Total Defense principles into national development planning and foreign policy—particularly through ASEAN mechanisms and minilateral cooperation frameworks—will enhance Indonesia’s strategic depth and regional influence. Lessons from Nordic and Baltic states suggest that regular scenario-based drills, centralized command protocols, and multi-sectoral governance structures are essential to building long-term hybrid threat preparedness.

Academically, this research contributes to the expanding discourse on hybrid warfare and comprehensive security by contextualizing the Indo-Pacific power competition through the lens of middle-power adaptation. It offers a nuanced understanding of how hybrid threats necessitate an evolution of traditional defense paradigms, especially in archipelagic and decentralized states like Indonesia. Theoretically, it extends the concept of Total Defense by incorporating cognitive warfare, cyber operations, and economic coercion as integral domains of modern security. Practically, the study provides a structured evaluation of Indonesia’s strategic transformation, identifying critical gaps in implementation while offering concrete policy pathways. These insights are valuable not only for Indonesian defense stakeholders but also for other maritime or developing states navigating similar hybrid threat environments.

## REFERENCES

- Abbondanza, G. (2022). Whither the Indo-Pacific? Middle power strategies from Australia, South Korea and Indonesia. *International Affairs*, 98(2), 403–421. <https://doi.org/10.1093/ia/iiab231>
- Beckley, M., & Brands, H. (2022). *Danger zone: The coming conflict with China*. WW Norton & Company.
- Caballero-Anthony, M., & Cook, A. D. (2013). *Non-traditional security in Asia: Issues, challenges and framework for action*. Institute of Southeast Asian Studies.
- CNAS. (2024). Indo-Pacific security challenges and opportunities. In *Center for a New American Security*. <https://www.cnas.org/research/indo-pacific-security>
- Daneswara, M. R., & Nasution, M. T. A. (2025). *Rethinking Indonesia’s Defense Strategy: Aligning the Total People’s Defense (Sishankamrata) with Contemporary Defense Challenges*. *Indonesian Quarterly*, 52(4).
- Denzin, N. K. (2012). Triangulation 2.0. *Journal of Mixed Methods Research*, 6(2), 80–88. <https://doi.org/10.1177/1558689812437186>
- Erickson, A. S. (2022). *Maritime gray zone operations: challenges and countermeasures in the Indo-Pacific*. Taylor & Francis.
- Farrell, H., & Newman, A. L. (2019). Weaponized Interdependence: How Global Economic Networks Shape State Coercion. *International Security*, 44(1), 42–79. [https://doi.org/10.1162/isec\\_a\\_00351](https://doi.org/10.1162/isec_a_00351)
- Fridman, O. (2018). *Russian" hybrid warfare": Resurgence and politicization*. Oxford University Press.
- Hadianto, M., & Kusuma, G. A. (2025, July 28). Indonesia’s grand strategy for integrated deterrence and defense modernization. The Jakarta Post.
- Heiduk, F. (2022). Security in the Indo-Pacific: The Asianisation of the regional security architecture. *SWP Research Paper*.
- Hendra, H., Sumertha, I. G., & Suharto, P. (2024). *The Role of the Indonesian National Army (TNI) in the Total People’s Defense and Security System (SISHANKAMRATA) in Facing Hybrid Threats*. *QISTINA: Jurnal Multidisiplin Indonesia*. <https://doi.org/10.57235/qistina.v4i1.6246>
- Hoffman, F. G. (2014). Hybrid warfare and challenges. In *Strategic Studies* (pp. 329–337). Routledge.

- Htwe, T. M. (2025). China's Global South Strategy in the Mekong Region in Geopolitical Implications, Economic Prospects, and Challenge. In *Implications, Prospects, and Challenges in China's Global South Strategy* (pp. 149–182). IGI Global. <https://doi.org/10.4018/979-8-3373-0938-5.ch006>
- Jung, S. C., & Tan, E.-W. (2024). Middle powers and minilateralism against hybrid threats in the Indo-Pacific: South Korea, Singapore, and Taiwan. *Australian Journal of International Affairs*, 78(6), 889–910. <https://doi.org/10.1080/10357718.2024.2399339>
- Kaplan, R. D. (2018). *The Revenge of Geography: What the Map Tells Us About Coming Conflicts and the Battle Against Fate*. Random House.
- Kementerian Pertahanan RI. (2015). *Buku putih pertahanan Indonesia*. Kementerian Pertahanan RI.
- Kurç, Ç., & Bitzinger, R. A. (2018). Defense industries in the 21st century: A comparative analysis—The second e-workshop. *Comparative Strategy*, 37(4), 255–259. <https://doi.org/10.1080/01495933.2018.1497318>
- Lee, B. T. F., Kornphetcharat, K., Sims, J. P., Linh Dieu, D., & Salman Ali, B. (2025). ASEAN Cybersecurity Cooperation Strategy: Combating Cyber Terrorism and Hackers Through CERT Coordination. *International Journal of Law and Public Policy (IJLAPP)*, 7(1), 20–30. <https://doi.org/10.36079/lamintang.ijlapp-0701.788>
- RAND Corporation. (2024). *U.S.-China competition in the Indo-Pacific*. RAND Project Air Force. <https://www.rand.org/paf/projects/us-china-competition.html>
- Rid, T., & Buchanan, B. (2015). Attributing Cyber Attacks. *Journal of Strategic Studies*, 38(1–2), 4–37. <https://doi.org/10.1080/01402390.2014.977382>
- Sarjito, A. (2025). Evaluating Indonesia's National Defense Policy in Shaping an Effective Area Denial Strategy. *Journal of Political Issues*, 6(2), 124–134. <https://doi.org/10.33019/jpi.v6i2.216>
- Sederholm, T., Rannikko, R., & Salo, M. (2025). Total defence model at the heart of Finland's national defence and resilience. In *Total defence model at the heart of Finland's national defence and resilience* (pp. 115–134). Routledge.
- Seebeck, L., Williams, E., & Wallis, J. (2022). Countering the Hydra: A proposal for an Indo-Pacific hybrid threat centre. In *Australian Strategic Policy Institute*. <https://www.aspi.org.au/report/countering-hydra/>
- Sianturi, K., & Saputro, G. E. (2025). Transformation Of The Indonesian National Army's Doctrine And Strategy In Facing Multidimensional Threats: Towards The Vision Of Golden Indonesia 2045. *JHSS (JOURNAL OF HUMANITIES AND SOCIAL STUDIES)*, 9(1), 138–145.
- SIPRI. (2023). *SIPRI Military Expenditure Database*. SIPRI. <https://www.sipri.org/databases/milex>
- Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, 104, 333–339. <https://doi.org/10.1016/j.jbusres.2019.07.039>
- Sumadinata, R. W. S., Achmad, W., & Riyadi, S. F. (2022). Indonesian Border Defense Policy: A Case Study on the Interoperability of the joint regional defense command. *Central European Management Journal*. <https://doi.org/10.57030/23364890.cemj.30.4.87>
- Wulandari, R., Priyanto, P., & Hendra, A. (2025). *The Indonesia's Cyber Security Strategy in the Face of Evolving Modern Warfare Threats*. *Formosa Journal of Applied Sciences*, 4(2).
- Zimmerman, E. (2018). Security cooperation in the Indo-Pacific: non-traditional security as a catalyst. In *Geo-economics and Geo-securities in the Indian Ocean Region* (pp. 33–47). Routledge.