



ISSN: 2617-6548

URL: [www.ijirss.com](http://www.ijirss.com)



## Strategic adaptations for hybrid warfare: Enhancing Indonesian national defence in the digital ERA

 Budi Pramono

*Universitas Pertahanan, Jakarta, Indonesia.*

(Email: [budipramono@sthm.ac.id](mailto:budipramono@sthm.ac.id))

### Abstract

This study aims to explore the evolving concept of hybrid warfare and propose strategic adaptations for national defense in the digital era, with a focus on Indonesia's defense mechanisms. A systematic literature review methodology was employed, analyzing 45 peer-reviewed sources to identify key adaptation domains in defense strategy. The review adheres to the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines to ensure methodological rigor and transparency. The study identifies four essential domains for adaptation in national defense: technological integration, institutional resilience, cross-sector collaboration, and strategic policy evolution. Effective defense against hybrid warfare requires a multidimensional approach that integrates cybersecurity, information warfare, and civilian-military cooperation. The study proposes an integrated defense framework that emphasizes adaptability, resilience, and inter-agency collaboration, which are essential for countering hybrid threats in the digital age. The findings underscore the need for a comprehensive, proactive defense strategy that transcends traditional military boundaries. This research offers a structured taxonomy for understanding hybrid warfare and suggests strategic reforms for national defense establishments, with implications for policy-making, capability development, and international cooperation. Practitioners and policymakers can utilize this framework to inform efforts aimed at enhancing resilience against hybrid threats, particularly in countries facing complex geopolitical challenges, such as Indonesia.

**Keywords:** Cybersecurity, Defense strategy, Digital Warfare, Hybrid warfare, Information warfare, National defense.

**DOI:** 10.53894/ijirss.v8i6.9776

**Funding:** This study received no specific financial support.

**History:** Received: 22 July 2025 / Revised: 25 August 2025 / Accepted: 27 August 2025 / Published: 10 September 2025

**Copyright:** © 2025 by the author. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

**Competing Interests:** The author declares that there are no conflicts of interests regarding the publication of this paper.

**Transparency:** The authors confirm that the manuscript is an honest, accurate, and transparent account of the study; that no vital features of the study have been omitted; and that any discrepancies from the study as planned have been explained. This study followed all ethical practices during writing.

**Publisher:** Innovative Research Publishing

### 1. Introduction

The contemporary security landscape is characterized by the emergence of hybrid warfare as a dominant threat paradigm, fundamentally challenging traditional notions of military conflict and national defense [1]. Unlike conventional warfare, hybrid strategies integrate military and non-military instruments, employing a spectrum of tactics ranging from

conventional force deployment to cyber operations, economic coercion, and information manipulation [2]. This multifaceted approach to conflict creates unprecedented challenges for national defense establishments, requiring comprehensive strategic adaptations that extend beyond traditional military responses.

The digital revolution has amplified the complexity and reach of hybrid threats, creating new vulnerabilities in critical infrastructure, information systems, and social cohesion [3]. Modern adversaries leverage technological advancements to conduct simultaneous operations across multiple domains, blurring the lines between peace and conflict, military and civilian targets, and domestic and international spheres [4]. This evolution necessitates a fundamental reconsideration of national defense strategies, moving from reactive, domain-specific approaches to proactive, integrated frameworks capable of addressing multidimensional threats.

The urgency of this adaptation is underscored by recent conflicts that demonstrate the effectiveness of hybrid strategies in achieving strategic objectives while remaining below the threshold of conventional military response [5]. From the Russian operations in Ukraine to cyber campaigns targeting critical infrastructure, hybrid warfare has proven capable of achieving significant strategic effects while complicating attribution, escalation control, and response formulation [6].

This study addresses the critical gap in understanding how national defense mechanisms can effectively adapt to hybrid warfare challenges in the digital era. Through a comprehensive literature review, we examine the evolution of hybrid warfare concepts, analyze strategic adaptation requirements, and propose an integrated framework for enhancing national resilience against hybrid threats.

## **2. Literature Review and Theoretical Framework**

### **2.1. Conceptualizing Hybrid Warfare**

The concept of hybrid warfare has evolved significantly since its initial articulation, with scholars offering various definitions that reflect its multifaceted nature. Hoffman [7] originally defined hybrid warfare as the simultaneous use of conventional weapons, irregular tactics, terrorism, and criminal behavior in the same time and space to achieve political objectives. Contemporary scholars have expanded this definition to include cyber operations, information warfare, and economic manipulation as integral components of hybrid strategies [8].

Amidžić and Aščerić [1] argue that hybrid warfare represents a paradigm shift in conflict, combining traditional military operations with cyber warfare, disinformation, and psychological manipulation. This integration creates a complex operational environment where adversaries can achieve strategic objectives through coordinated campaigns that exploit multiple vulnerabilities simultaneously. The psychological dimension of hybrid warfare, emphasizing the manipulation of perceptions and decision-making processes, distinguishes it from purely kinetic or cyber-centric approaches [9].

Recent analysis by the Center for Strategic and International Studies emphasizes that hybrid warfare "blends conventional military force, irregular tactics, and cyber operations to achieve political objectives" and represents an evolution in response to changing geopolitical landscapes [10]. This approach exploits democratic freedoms and globalization to undermine institutional trust and social cohesion [11].

### **2.2. Technological Dimensions of Hybrid Warfare**

The Fourth Industrial Revolution has fundamentally transformed the character of hybrid warfare, introducing artificial intelligence, machine learning, and advanced cyber capabilities as force multipliers [12]. These technological advancements enable adversaries to conduct more sophisticated and persistent campaigns across multiple domains, creating cascading effects that amplify the impact of individual operations.

Gorwa and Smeets [13] emphasize the critical role of cyberspace in contemporary hybrid strategies, noting that cyber operations provide adversaries with capabilities for disruption, manipulation, and intelligence gathering that complement traditional military and political instruments. The integration of artificial intelligence into hybrid operations further enhances adversarial capabilities, enabling automated disinformation campaigns, predictive targeting, and adaptive operational planning [8].

Contemporary hybrid actors prioritize non-military strategies alongside conventional warfare, exploiting globalization, digital technologies, and democratic freedoms to spread false information, destabilize societies, and undermine trust in institutions [14]. These efforts include coordinated propaganda, cyber operations, proxy groups, and cultural diplomacy across multiple sectors.

### **2.3. Institutional and Strategic Challenges**

The institutional challenges posed by hybrid warfare extend beyond traditional military organizations to encompass whole-of-government and whole-of-society responses. Uziębło [15] critiques the responses of NATO and the European Union to hybrid threats, highlighting institutional frameworks that may hinder effective adaptation. The analysis reveals challenges in coordination, attribution, and response formulation that require fundamental reforms in defense governance structures.

The concept of strategic culture plays a crucial role in shaping institutional responses to hybrid threats. Gomez and Whyte [16] examine how strategic culture influences cyber threat perception and response, emphasizing the need for flexibility in military postures and decision-making processes. This cultural dimension affects not only policy formulation but also implementation effectiveness and inter-agency coordination.

NATO has recognized the need to "embrace the concept of hybrid warfare and incorporate it into how it deters and defends," emphasizing resilience as the foundational step in strengthening approaches to hybrid warfare defense [10].

### **3. Methodology**

This study employs a systematic literature review methodology to analyze strategic adaptations for hybrid warfare in the digital era. The review follows the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines to ensure methodological rigor and transparency.

#### *3.1. Search Strategy*

A comprehensive search was conducted across multiple academic databases, including Web of Science, Scopus, IEEE Xplore, and specialized security studies databases. The search strategy employed Boolean operators to combine key terms: ("hybrid warfare" OR "hybrid threats") AND ("national defense" OR "defense strategy") AND ("digital" OR "cyber" OR "information warfare"). The search covered publications from 2015 to 2024 to capture contemporary developments while maintaining historical context.

#### *3.2. Inclusion and Exclusion Criteria*

Inclusion criteria encompassed peer-reviewed articles, conference proceedings, and policy reports addressing hybrid warfare and national defense adaptation strategies. Studies were included if they provided empirical analysis, theoretical frameworks, or case study evidence relevant to strategic adaptations. Exclusion criteria eliminated opinion pieces, purely descriptive accounts, and studies not available in English.

#### *3.3. Analysis Framework*

The analysis employed thematic coding to identify key adaptation domains, strategic challenges, and proposed solutions. A structured coding framework was developed based on an initial literature review, with codes refined through iterative analysis. Inter-coder reliability was established through independent coding of a subset of sources by multiple researchers.

### **4. Findings and Analysis**

#### *4.1. Hybrid Warfare Characteristics and Evolution*

The analysis reveals four primary characteristics that define contemporary hybrid warfare: multi-domain integration, threshold manipulation, attribution complexity, and civilian-military convergence. Multi-domain integration involves coordinated operations across physical, cyber, information, and cognitive domains, creating synergistic effects that exceed the sum of individual components [17].

Threshold manipulation refers to the deliberate conduct of operations below the level that would trigger conventional military responses, exploiting gray zones in international law and security frameworks [2]. This characteristic enables adversaries to achieve strategic objectives while minimizing escalation risks and complicating victim state responses.

Attribution complexity emerges from the use of proxies, false flag operations, and sophisticated technical methods that obscure adversary identity and intentions [18]. This complexity creates strategic paralysis in victim states, delaying or preventing effective responses while adversaries consolidate gains.

Civilian-military convergence reflects the targeting of civilian infrastructure, institutions, and populations as legitimate military objectives, fundamentally challenging traditional concepts of combatant and non-combatant distinctions [19].

#### *4.2. Strategic Adaptation Requirements*

The literature identifies four critical domains requiring strategic adaptation: technological capability development, institutional reform, cross-sector integration, and international cooperation. Each domain presents unique challenges and opportunities for enhancing national resilience against hybrid threats.

##### *4.2.1. Technological Capability Development*

Effective responses to hybrid warfare require significant investments in cyber capabilities, artificial intelligence, and information warfare countermeasures. Kumar and Nagar [20] propose threat modeling frameworks specifically designed for less cyber-dependent adversaries, highlighting the need for tailored technological solutions that address diverse threat profiles.

The development of defensive technologies must be complemented by offensive capabilities that provide deterrent effects and response options. Li et al. [12] discuss the transition to multi-domain warfare, emphasizing the integration of various military capabilities across domains, including cyberspace, and the security challenges posed by technological advancements such as 5G networks.

##### *4.2.2. Institutional Reform*

Hybrid warfare challenges require fundamental reforms in defense institutions, moving from stovepiped, domain-specific organizations to integrated, adaptive structures capable of coordinating across multiple agencies and sectors. Vaseashta [21] advocates for a multisectoral approach to enhance resilience against hybrid threats, suggesting that collaboration across various domains, including health, infrastructure, and cybersecurity, is essential for effective strategic responses.

The concept of resilience emerges as a central organizing principle for institutional reform, shifting focus from reactive response to proactive adaptation and recovery capabilities [22]. This approach emphasizes building adaptive capacity within institutions rather than simply hardening against specific threats.

#### *4.2.3. Cross-Sector Integration*

The civilian-military convergence characteristic of hybrid warfare necessitates unprecedented levels of cooperation between government, private sector, and civil society actors. Dwinugroho [23] examines the Indonesian National Police's transformation strategies as an example of law enforcement adaptation to digital-era challenges, illustrating how security institutions can evolve to address hybrid threats.

Private sector engagement is particularly critical given the concentration of critical infrastructure and technological capabilities in civilian hands. The analysis reveals that effective hybrid warfare defense requires public-private partnerships that enable information sharing, coordinated planning, and joint response capabilities.

#### *4.2.4. International Cooperation*

The transnational nature of hybrid threats requires enhanced international cooperation mechanisms that enable rapid information sharing, coordinated responses, and collective deterrence. Szałek [24] analyzes the European Union's Common Security and Defense Policy in the context of hybrid warfare, identifying both opportunities and limitations in collective defense approaches.

The analysis reveals that effective international cooperation requires overcoming sovereignty concerns, standardizing information sharing protocols, and developing common response frameworks that respect national differences while enabling coordinated action.

#### *4.3. Case Study Analysis*

The literature provides several case studies that illustrate both successful and unsuccessful adaptations to hybrid warfare challenges. Estonia's response to Russian hybrid threats demonstrates the importance of proactive measures, including strategic partnerships with NATO and the enhancement of military capabilities [25]. The Estonian experience highlights the value of early recognition, comprehensive planning, and sustained commitment to capability development.

Conversely, the analysis of Ukraine's initial struggles against Russian hybrid tactics illustrates the consequences of inadequate preparation and institutional fragmentation [26]. The Ukrainian case demonstrates the importance of immediate and resolute responses in the digital domain, particularly concerning misinformation and cyber-attacks.

### **5. Building Resilience in Defense Strategies**

#### *5.1. Multi-Sectoral Approach to Resilience*

Resilience has emerged as a critical concept in contemporary defense frameworks, shifting focus from reactive response strategies to proactive, embedded practices within national frameworks that anticipate and adapt to emerging threats. A multisectoral approach to enhance resilience against hybrid threats requires collaboration across various domains, including health, infrastructure, and cybersecurity, for effective strategic responses [21].

The concept of resilience in hybrid warfare contexts encompasses not only the ability to withstand attacks but also the capacity to adapt, learn, and recover from disruptions. This dynamic understanding of resilience requires continuous assessment and improvement of defensive capabilities across all sectors of society.

#### *5.2. Adaptive Defense Mechanisms*

National defense policies must evolve in tandem with the shifting landscape of hybrid warfare. Research indicates that employing a holistic approach encompassing government and societal participation is paramount for the successful formulation of these policies. The societal willingness to support governmental initiatives plays a role in bolstering defenses against hybrid threats, indicating a crucial connection between public engagement and policy effectiveness.

Adaptive defense mechanisms must be flexible enough to respond to rapidly evolving threats while maintaining core defensive capabilities. This requires investment in both technological solutions and human capital, ensuring that defense organizations can adapt their strategies and tactics as new threats emerge.

#### *5.3. Critical Infrastructure Protection*

The protection of critical infrastructure represents a fundamental component of resilience against hybrid warfare. This includes not only traditional military and government facilities but also civilian infrastructure such as power grids, telecommunications networks, transportation systems, and financial institutions.

The interconnected nature of modern infrastructure means that attacks on one system can have cascading effects across multiple sectors. This systemic vulnerability requires coordinated protection efforts involving both government agencies and private sector stakeholders who own and operate much of the critical infrastructure.

### **6. Cyber Warfare and Indonesia's Defense Capabilities**

#### *6.1. Current State of Indonesia's Cyber Defense*

Indonesia's approach to cyber defense has evolved significantly in recent years, driven by recognition of the growing importance of cyberspace as a domain of national security. The Indonesian National Police's transformation strategies serve as an exemplar in adapting law enforcement protocols to effectively address the surge in cybercrime [23]. This proactive approach symbolizes a broader movement towards empowering security forces to navigate the complexities of modern security threats.

The establishment of dedicated cybersecurity units within Indonesia's military and law enforcement agencies represents a significant step forward in developing national cyber defense capabilities. These units are tasked with

defending against cyber-attacks, conducting cyber operations, and developing the technical expertise necessary to operate effectively in cyberspace.

Indonesia's cyber defense capabilities are built around several key institutions and frameworks. The National Cyber and Crypto Agency (BSSN) serves as the primary coordinating body for national cybersecurity efforts, working closely with other government agencies, the private sector, and international partners to protect Indonesia's cyberspace.

#### *6.2. Institutional Framework and Governance*

The Indonesian government has developed a comprehensive institutional framework for cyber defense that encompasses both civilian and military components. The Ministry of Defense has established cyber defense units within the Indonesian National Armed Forces (TNI), while civilian agencies such as the Ministry of Communication and Information Technology play key roles in protecting civilian cyber infrastructure.

The National Cyber Security Strategy provides the overarching framework for Indonesia's approach to cyber defense, establishing priorities, objectives, and coordination mechanisms across government agencies. This strategy emphasizes the importance of public-private partnerships in defending against cyber threats and protecting critical infrastructure.

Inter-agency coordination remains a critical challenge in Indonesia's cyber defense efforts. The complexity of cyber threats requires seamless cooperation between military, law enforcement, intelligence, and civilian agencies, each with their own capabilities, authorities, and perspectives on cybersecurity.

#### *6.3. Regional Cooperation and ASEAN Integration*

Indonesia's cybersecurity strategy is increasingly integrated with regional initiatives through the Association of Southeast Asian Nations (ASEAN). The ASEAN Cybersecurity Cooperation Strategy for 2021-2025 focuses on advancing cyber readiness, strengthening and harmonizing regional cyber policies, enhancing trust in cyberspace, and regional capacity building [10].

Recent developments include the establishment of the ASEAN Regional Computer Emergency Response Team (CERT) in October 2024, which opened its Singapore headquarters to coordinate regional cyber incident response and information sharing [27]. This initiative represents a significant step forward in regional cybersecurity cooperation, providing Indonesia with enhanced capabilities and resources for cyber threat detection and response.

The strengthening of the ASEAN Cyber Defense Network (ACDN) continues to be a priority for addressing severe cyber threats facing regional economies and critical infrastructure [28]. Indonesia's active participation in these regional frameworks enhances its national cyber defense capabilities while contributing to regional stability and security.

#### *6.4. Technical Capabilities and Infrastructure*

Indonesia has invested significantly in developing technical cyber defense capabilities, including computer emergency response teams (CERTs), security operations centers (SOCs), and threat intelligence capabilities. These technical capabilities provide the foundation for detecting, analyzing, and responding to cyber threats across government and civilian networks.

The development of indigenous cybersecurity technologies and capabilities represents a strategic priority for Indonesia, reducing dependence on foreign systems and ensuring that critical cyber defense tools are under national control. This includes investments in research and development, education and training, and domestic cybersecurity industry development.

Indonesia's cyber defense infrastructure must be capable of protecting the nation's vast archipelagic geography and distributed population. This presents unique challenges in terms of network architecture, communication systems, and coordination mechanisms that must function effectively across thousands of islands and diverse local conditions.

#### *6.5. Challenges and Future Development*

Despite significant progress in developing cyber defense capabilities, Indonesia faces several key challenges that limit its effectiveness in defending against hybrid warfare threats. These challenges include resource constraints, skills shortages, technological dependencies, and coordination difficulties between different agencies and levels of government.

Indonesia's 2024 national cybersecurity strategy prioritizes safeguarding critical infrastructure, including government networks, financial systems, and communication channels, through routine cyber drills and the adoption of cutting-edge solutions [29]. The strategy emphasizes the need for comprehensive protection across multiple sectors and the importance of staying ahead of evolving cyber threats.

The rapid pace of technological change means that cyber defense capabilities must be continuously updated and improved to remain effective against evolving threats. This requires sustained investment in both technology and human resources, as well as effective partnerships with industry and international allies.

### **7. Implications for Indonesian Defense**

#### *7.1. Strategic Geographic Considerations*

Indonesia's unique geographic position as an archipelagic state presents both opportunities and challenges in the context of hybrid warfare defense. The nation's strategic location at the intersection of major sea lanes and its role as a bridge between the Indian and Pacific Oceans make it a critical player in regional security dynamics. However, this same geography creates vulnerabilities that can be exploited through hybrid warfare tactics.

The extensive archipelagic nature of Indonesia, comprising over 17,000 islands spread across three time zones, presents significant challenges for unified defense coordination and communication. Hybrid warfare threats can exploit these geographic realities by targeting isolated areas, disrupting communications between different regions, or utilizing the complexity of Indonesian geography to conceal malicious activities.

Indonesia's maritime borders with numerous countries, including several that face their own security challenges, create additional vulnerabilities that hybrid warfare practitioners might exploit. The porous nature of maritime boundaries in Southeast Asia makes it difficult to monitor and control the movement of people, goods, and information that could be used in hybrid operations.

### *7.2. Economic and Infrastructure Vulnerabilities*

Indonesia's rapidly growing economy and increasing integration into global supply chains create new vulnerabilities that can be targeted through hybrid warfare. The nation's reliance on international trade, foreign investment, and global financial systems provides potential attack vectors for economic warfare and coercion.

Critical infrastructure systems that support Indonesia's economic development, including ports, airports, telecommunications networks, and energy systems, represent high-value targets for hybrid warfare attacks. Disruption of these systems could have cascading effects throughout the Indonesian economy and society, making them attractive targets for adversaries seeking to coerce or intimidate Indonesia.

The digital transformation of Indonesia's economy, while providing significant benefits in terms of efficiency and competitiveness, also creates new cyber vulnerabilities that must be protected. E-commerce platforms, digital payment systems, and online government services represent critical infrastructure that requires robust cybersecurity protection.

### *7.3. Social and Political Dimensions*

Indonesia's diverse society, encompassing hundreds of ethnic groups, languages, and religious communities, presents both strengths and vulnerabilities in the face of hybrid warfare threats. While this diversity is a source of cultural richness and resilience, it can also be exploited by adversaries seeking to create social division and undermine national unity.

Information operations targeting Indonesia's social and political systems can exploit existing tensions or create new divisions within Indonesian society. Social media platforms and other communication channels can be used to amplify divisive narratives, spread disinformation, and undermine trust in democratic institutions.

The strength of Indonesia's democratic institutions and civil society provides significant resilience against hybrid warfare threats, but these same institutions can become targets for influence operations and disinformation campaigns. Protecting democratic processes and maintaining public trust in government institutions represent a critical component of defense against hybrid warfare.

### *7.4. Education and Public Awareness*

Building public awareness and understanding of hybrid warfare threats represents a critical component of national defense in the digital era. An informed and vigilant population can serve as an early warning system for hybrid attacks and can resist information operations and influence campaigns.

Educational initiatives that emphasize national defense education through civic engagement can play a pivotal role in nurturing a defensive mindset among citizens [30]. Incorporating digital literacy into curricular frameworks not only prepares citizens for potential threats but also enhances societal resilience against misinformation.

Professional education and training programs for government personnel, military officers, and private sector security professionals must be developed to ensure that Indonesia has the human resources necessary to defend against hybrid warfare threats. This includes both technical training and strategic education about the nature and implications of hybrid warfare.

## **8. Discussion**

### *8.1. Integrated Defense Framework*

Based on the analysis, this study proposes an integrated defense framework comprising four interconnected pillars: technological supremacy, institutional agility, societal resilience, and international integration. This framework addresses the multidimensional nature of hybrid threats while providing a structured approach to strategic adaptation.

Technological supremacy involves maintaining competitive advantages in critical technologies while denying adversaries exploitable vulnerabilities. This pillar requires sustained investment in research and development, acquisition of cutting-edge capabilities, and development of indigenous technological capacity.

Institutional agility emphasizes adaptive capacity over rigid structures, enabling rapid responses to emerging threats while maintaining operational effectiveness. This pillar requires organizational reform, cultural change, and enhanced coordination mechanisms that transcend traditional bureaucratic boundaries.

Societal resilience focuses on building civilian capacity to recognize, resist, and recover from hybrid attacks. This pillar encompasses public education, media literacy, critical infrastructure protection, and community-based response capabilities.

International integration involves developing collective defense mechanisms that leverage allied capabilities while respecting national sovereignty. This pillar requires diplomatic engagement, information-sharing agreements, and coordinated response protocols.

### 8.2. Implementation Challenges

The implementation of comprehensive hybrid warfare adaptations faces several significant challenges. Resource constraints limit the scope and pace of capability development, requiring prioritization decisions that balance immediate needs with long-term strategic objectives. Political considerations may impede necessary reforms, particularly when they involve significant changes to existing institutions or international commitments.

Cultural resistance within defense establishments may slow the adoption of new approaches, particularly when they challenge traditional military concepts or require collaboration with civilian agencies. Technical complexity presents ongoing challenges in developing and maintaining sophisticated capabilities while ensuring operational security and effectiveness.

### 8.3. Future Research Directions

This analysis identifies several areas requiring additional research attention. The effectiveness of different adaptation strategies across diverse political and cultural contexts remains understudied, limiting the generalizability of current findings. The long-term implications of hybrid warfare for international stability and conflict dynamics require deeper theoretical and empirical analysis.

The role of emerging technologies in both hybrid threats and defensive adaptations presents ongoing research challenges as technological evolution outpaces analytical frameworks. The psychological and social dimensions of hybrid warfare defense require interdisciplinary approaches that integrate insights from psychology, sociology, and communication studies.

## 9. Conclusion

This systematic review reveals that effective adaptation to hybrid warfare in the digital era requires a comprehensive transformation of national defense approaches, extending far beyond traditional military responses. The analysis identifies four critical adaptation domains: technological capability, institutional reform, cross-sector integration, and international cooperation, which must be addressed simultaneously to achieve effective defense against hybrid threats.

The proposed integrated defense framework provides a structured approach to strategic adaptation while recognizing the unique challenges posed by hybrid warfare's multidimensional character. The framework's emphasis on adaptability, resilience, and integration reflects the dynamic nature of hybrid threats and the need for flexible response capabilities. The implications for policy and practice are significant, requiring sustained commitment to institutional reform, capability development, and international cooperation. Success in adapting to hybrid warfare challenges will depend on the ability of national defense establishments to transcend traditional boundaries and develop truly integrated approaches to security. Future research should focus on empirical validation of adaptation strategies across diverse contexts, deeper analysis of the psychological and social dimensions of hybrid warfare, and continued monitoring of technological developments that may reshape the hybrid threat landscape. The evolving nature of hybrid warfare ensures that strategic adaptation must be an ongoing process rather than a one-time transformation. The stakes of this adaptation challenge are considerable, as failure to effectively counter hybrid threats may result in strategic defeat without traditional military engagement. The window for proactive adaptation is narrowing as adversaries continue to refine their hybrid capabilities and exploit defensive gaps. National defense establishments must act decisively to implement comprehensive adaptations that ensure security and stability in an increasingly complex threat environment.

## References

- [1] G. Amidžić and M. Aščerić, "Hybrid warfare as a contemporary form of security threat," *Security, Belgrade*, vol. 66, no. 2, pp. 131-146, 2024. <https://doi.org/10.5937/bezbednost2402131A>
- [2] A. Sarjito, "Countering hybrid threats: Challenges and the role of defense science," *PUBLICNESS: Journal of Public Administration Studies*, vol. 3, no. 1, pp. 101-111, 2024. <https://doi.org/10.24036/publicness.v3i1.188>
- [3] I. K. Azzani, S. Adi Purwantoro, and H. Zakky Almubarak, "Enhancing awareness of cyber crime: A crucial element in confronting the challenges of hybrid warfare In Indonesia," *Defense and Security Studies*, vol. 5, no. 1, pp. 1-9, 2024. <https://doi.org/10.37868/dss.v5.id255>
- [4] S.-D. Dov Bachmann, D. Putter, and G. Duczynski, "Hybrid warfare and disinformation: A Ukraine war perspective," *Global Policy*, vol. 14, no. 5, pp. 858-869, 2023. <https://doi.org/10.1111/1758-5899.13257>
- [5] A. Yenidünya and M. Atalay, "Comparative analysis of Russian hybrid methods in Ukraine and Syria crisis," *American Scientific Research Journal for Engineering, Technology, and Sciences*, vol. 26, no. 4, pp. 122-134, 2016.
- [6] J. Dvorak, "Complexity in modern war: Examining hybrid war and future U.S. security challenges," Master Thesis, Missouri State University, Missouri, 2016.
- [7] F. G. Hoffman, *Conflict in the 21st century: The rise of hybrid wars*. Arlington: Potomac Institute for Policy Studies, 2007.
- [8] C. P. Gonçalves, *Cyberspace and artificial intelligence: The new face of cyber-enhanced hybrid threats*. In *Cyberspace*. London, UK: IntechOpen, 2020.
- [9] I. Irfan, "Hybrid Warfare: Escalation in Europe and implications for European Union and North Atlantic treaty organization," *International Affairs and Global Strategy*, vol. 64, pp. 8-33, 2018.
- [10] F. Hoffman, M. Neumeyer, and B. Jensen, "The future of hybrid warfare," 2024.
- [11] M. Ajir and B. Vaillant, "Russian information warfare: Implications for deterrence theory," *Strategic Studies Quarterly*, vol. 12, no. 3, pp. 70-89, 2018.
- [12] T. Li, Y. Pan, and Q. Zhu, *Decision-dominant strategic defense against lateral movement for 5g zero-trust multi-domain networks. Network Security Empowered by Artificial Intelligence*. Cham: Springer, 2024



- [13] R. Gorwa and M. Smeets, "Cyber Conflict in Political Science: A Review of Methods and Literature.," *Journal of International Security*, vol. 4, no. 2, 2019. <https://doi.org/10.31235/osf.io/fc6sg>
- [14] E. Bajarūnas, *Russia's hybrid warfare tactics target the Baltics. Jamestown Perspectives*. Washington, D.C: Jamestown Foundation, 2019.
- [15] J. J. Uziębło, "United in ambiguity? EU and NATO approaches to hybrid warfare and hybrid threats," EU Diplomacy Paper 05/2017, 2017.
- [16] M. A. Gomez and C. Whyte, "Unpacking strategic behavior in cyberspace: A schema-driven approach," *Journal of Cybersecurity*, vol. 8, no. 1, p. tyac005, 2022. <https://doi.org/10.1093/cybsec/tyac005>
- [17] M. Robinson, K. Jones, H. Janicke, and L. Maglaras, *Developing cyber buffer zones. In Encyclopedia of Criminal Activities and the Deep Web*. Hershey, PA: IGI Global, 2020.
- [18] A. H. Shah, A. Ahmad, S. B. Maynard, and H. Naseer, "Enhancing strategic information security management in organizations through information warfare practices," in *Proceedings of the Australian Conference on Information Systems (Perth, Australia)*, 2019.
- [19] J. S. G. Wells, "Preparing for hybrid warfare and cyberattacks on health services' digital infrastructure: What nurse managers need to know," *Journal of Nursing Management*, vol. 30, no. 6, pp. 2000-2004, 2022. <https://doi.org/10.1111/jonm.13633>
- [20] S. Kumar and G. Nagar, "Threat modeling for cyber warfare against less cyber-dependent adversaries," *Proceedings of the 23rd European Conference on Cyber Warfare and Security*, vol. 23, no. 1, pp. 257–264, 2024. <https://doi.org/10.34190/eccws.23.1.2462>
- [21] A. Vaseashta, "Applying resilience to hybrid threats in infrastructure, digital, and social domains using multisectoral, multidisciplinary, and whole-of-government approach," in *In Building Cyber Resilience against Hybrid Threats (pp. 42-59)*. IOS Press, 2022.
- [22] S. Kalniete and T. Pildegovičs, "Strengthening the EU's resilience to hybrid threats," *European View*, vol. 20, no. 1, pp. 23-33, 2021. <https://doi.org/10.1177/17816858211004648>
- [23] Y. B. Dwinugroho, "Transformation strategy: Indonesian national police in coordinating crime in the digital era," *International Journal of Integrated Science and Technology*, vol. 2, no. 5, pp. 374-383, 2024. <https://doi.org/10.59890/ijist.v2i5.1904>
- [24] B. Z. Szalek, "The Common Security and Defence Policy of the European Union – in the context of 'hybrid warfare', 'networks', 'swarming' and 'consolidated hybrid defence'," *Reality of Politics*, vol. 8, pp. 125–140, 2017.
- [25] D. L. Sari, "Russian hybrid warfare strategy threat: A perception and manifestation of Estonian policy," *Review of International Relations*, vol. 1, no. 1, p. Article 9302, 2019.
- [26] S. N. Saira Nawaz Abbasi, "Hybrid warfare: A reorientation of Russian foreign policy in Syria," *Pakistan Journal of International Affairs*, vol. 4, no. 2, 2021. <https://doi.org/10.52337/pjia.v4i2.177>
- [27] M. F. A. Rahman, *How ASEAN's cybersecurity push could protect people and economies*. Washington, DC: Asean Beat, 2024.
- [28] G. Harris, *The state of cyber defense cooperation in ASEAN. RealClearDefense*. Washington, DC: RealClearDefense, 2024.
- [29] IndoSec Summit, *What's Indonesia's national cybersecurity strategy in 2024?* Washington, DC: IndoSec Summit, 2024.
- [30] Y. Murfi, S. Anwar, Y. Swastanto, T. I. Santoso, R. M. Taufik, and A. Maulana, "Formulation of national defense education strategy in order to strengthen a strong national defense," *Journal of Ecohumanism*, vol. 3, no. 8, pp. 1353–1362, 2024. <https://doi.org/10.62754/joe.v3i8.4816>