



Indonesia's National Resilience through Adaptive Defense Governance in the Era of Hybrid Warfare

Delfiazi Puji Lestari¹, Tsulis Amiruddin Zahri²

¹Sekolah Tinggi Ilmu Administrasi dan Ilmu Pemerintahan Annisa Dwi Salfarizi

²Universitas Bangka Belitung, Indonesia

ARTICLE INFO

Article history:

Received 01/07/2026

Revised 13/07/2026

Accepted 16/07/2026

Abstract

The evolution of hybrid warfare has fundamentally reshaped national security threats from conventional military confrontation into multidimensional challenges involving cyberattacks, disinformation, economic coercion, and ideological influence. While previous studies have primarily examined defense modernization, military strategy, or cybersecurity separately, limited attention has been paid to how defense institutional transformation can strengthen national resilience through a public administration and governance perspective. This study aims to analyze the transformation of Indonesia's defense institutions in responding to hybrid warfare and to develop an adaptive defense governance model that integrates defense, governance, and national resilience. Employing a qualitative descriptive-analytical design, the study analyzes government regulations, strategic policy documents, institutional reports, and peer-reviewed literature using thematic analysis to identify patterns of institutional adaptation and governance transformation. The findings reveal four strategic dimensions of adaptive defense governance: (1) institutional adaptation through the establishment of the National Defense Council, (2) strengthened inter-agency coordination based on a whole-of-government approach, (3) integration of cyber defense and digital resilience into the national defense system, and (4) collaborative civil-military governance to enhance multidomain resilience. Nevertheless, institutional fragmentation, overlapping authority, limited policy interoperability, and weak strategic coordination remain significant barriers to effective implementation. This study contributes by proposing an adaptive defense governance framework that extends existing defense governance literature through the integration of national resilience, collaborative governance, and hybrid warfare perspectives. Practically, the proposed framework provides policy guidance for strengthening institutional coordination and developing a more integrated, adaptive, and resilient national defense system in addressing future hybrid threats.

Keywords: Adaptive Defense Governance, National Resilience, Hybrid Warfare, Collaborative Governance, Defense Transformation

*Penulis Korespondensi

E-mail : drdelfiads@gmail.com

INTRODUCTION

Recent developments in the global strategic environment have fundamentally transformed the nature of national security from

conventional military confrontation into multidimensional, asymmetric, and cross-sectoral threats. Contemporary security challenges increasingly involve cyberattacks,



Lisensi:

Lisensi Creative Commons Attribution 4.0 Internasional (CC BY)

digital disinformation, economic coercion, ideological infiltration, information warfare, and sociopolitical polarization that undermine national stability without direct military engagement. This phenomenon, commonly referred to as hybrid warfare, combines conventional and non-conventional instruments across multiple domains, blurring the distinction between military and civilian spheres (Hoffman, 2007). Consequently, national security can no longer be understood solely in terms of territorial defense but must also encompass institutional resilience, cybersecurity, strategic governance, and societal preparedness (Buzan & Wæver, 2022; Nye, 2021).

The urgency of strengthening national resilience has become increasingly significant amid escalating geopolitical competition in the Indo-Pacific region. As a strategically located archipelagic state controlling major maritime trade routes, Indonesia faces growing exposure to multidomain threats, including cyberattacks, foreign influence operations, information manipulation, and economic coercion. These threats have become increasingly tangible, as demonstrated by the ransomware attack on Indonesia's National Data Center (PDNS) in 2024, which disrupted public services and revealed structural weaknesses in national cybersecurity governance. Similarly, the widespread dissemination of digital disinformation during electoral periods illustrates how hybrid threats exploit information ecosystems to weaken democratic legitimacy and social cohesion. These developments indicate that Indonesia's national security challenges increasingly extend beyond military defense to

include governance capacity and institutional resilience.

Responding to these challenges, the Indonesian government has initiated several institutional reforms, including the establishment of the National Defense Council (*Dewan Pertahanan Nasional*/DPN), the strengthening of cyber defense institutions, and the adoption of a whole-of-government approach to national defense governance. These initiatives reflect a gradual shift from a military-centered defense paradigm toward a governance-oriented approach that emphasizes institutional coordination, policy integration, and adaptive responses to multidomain threats. From the perspective of adaptive governance, institutional flexibility, collaborative coordination, and continuous policy learning have become essential elements for maintaining national resilience under conditions of strategic uncertainty (Folke et al., 2022; Christensen & Lægreid, 2020).

Despite these developments, the governance mechanisms through which defense institutions enhance national resilience remain insufficiently understood. Existing studies have primarily examined military modernization, cybersecurity, bureaucratic reform, or defense technology as separate research domains. Likewise, studies on hybrid warfare predominantly emphasize military or technological perspectives, while public administration research has rarely conceptualized defense governance as an adaptive institutional system capable of integrating defense, cybersecurity, collaborative governance, and national resilience. Consequently, there remains a significant knowledge gap regarding how adaptive governance can explain

the institutional transformation of defense organizations in responding to multidomain hybrid threats.

Accordingly, the central problem addressed in this study is the absence of an integrated governance framework capable of explaining how Indonesia's defense institutions can adapt to hybrid warfare while simultaneously strengthening national resilience through collaborative and adaptive governance mechanisms. Without such a framework, defense reforms risk remaining fragmented, limiting institutional interoperability, policy coordination, and the state's capacity to respond effectively to increasingly complex multidomain threats.

To address this gap, this study proposes the concept of Adaptive Defense Governance as an integrative analytical framework. Unlike previous studies that examine defense modernization, cybersecurity, or governance separately, this framework integrates four interrelated dimensions, namely institutional adaptation, collaborative governance, cyber defense integration, and multidomain national resilience. Through this integration, the study extends adaptive governance theory into the field of defense governance and offers a more comprehensive explanation of institutional transformation under hybrid warfare conditions.

Based on this perspective, the objectives of this study are twofold. First, it analyzes the transformation of Indonesia's defense institutions in responding to hybrid warfare from the perspective of national resilience. Second, it develops an Adaptive Defense Governance framework that explains the governance mechanisms linking institutional adaptation, collaborative governance, cyber

defense integration, and multidomain resilience.

This study contributes both theoretically and practically. Theoretically, it advances the international literature on defense governance and public administration by extending adaptive governance theory into the context of multidomain national defense, an area that has received limited scholarly attention, particularly in emerging Indo-Pacific democracies. Practically, the proposed framework provides policy guidance for strengthening institutional coordination, enhancing cyber defense integration, and developing a more adaptive, resilient, and collaborative national defense system capable of addressing future hybrid warfare challenges.

RESEARCH METHODS

This study employed a qualitative descriptive research design using a systematic literature review and qualitative document analysis to examine the transformation of Indonesia's defense institutions in strengthening national resilience amid hybrid warfare. A qualitative design was selected because the study seeks to understand institutional transformation, governance adaptation, and policy coordination rather than to test causal relationships statistically. The research emphasizes the interpretation of policy dynamics and governance mechanisms that shape Indonesia's defense transformation within an increasingly complex multidomain security environment. The study utilized both primary and secondary documentary sources. Primary sources consisted of Indonesian government regulations, national defense policies, presidential regulations, official speeches, Ministry of Defense strategic reports, National

Defense Council (DPN) documents, National Cyber and Crypto Agency (BSSN) publications, and other official documents concerning defense governance and national resilience during the administration of President Prabowo Subianto. Secondary sources comprised peer-reviewed journal articles, conference proceedings, academic books, policy papers, and reports published by international organizations discussing hybrid warfare, adaptive governance, cybersecurity, collaborative governance, defense transformation, and multidomain security.

The literature search followed a systematic procedure to ensure transparency and reproducibility. Scientific publications were retrieved from Scopus, ScienceDirect, SpringerLink, Google Scholar, and Garuda, while policy documents were obtained from official government repositories and international organizations.

The search employed combinations of the following keywords: "hybrid warfare"; "adaptive governance" ; "defense governance"; "defense transformation"; "national resilience"; "cyber defense"; "collaborative governance"; "multidomain security" using Boolean operators (AND, OR) to broaden or refine the search. Only publications published between 2020 and 2025 were considered to ensure the inclusion of contemporary developments in hybrid warfare and defense governance.

The literature selection adopted a PRISMA-inspired screening procedure consisting of four sequential stages: identification, screening, eligibility assessment, and inclusion. During the identification stage, 126 publications were collected from scientific databases and official policy repositories. Duplicate

publications were removed using reference management software, while titles and abstracts were screened according to predefined inclusion criteria. This process reduced the dataset to 74 publications. The eligibility stage involved a full-text assessment focusing on thematic relevance; methodological quality; publication credibility; direct discussion of hybrid warfare; adaptive governance; defense institutional transformation; national resilience. Following this assessment, 48 peer-reviewed journal articles and 17 official policy documents were retained as the principal analytical materials. The inclusion criteria prioritized: Scopus-indexed journals; peer-reviewed publications; official government documents; strategic reports issued by reputable international organizations. Publications lacking methodological clarity, theoretical relevance, or direct connection with Indonesia's defense governance were excluded.

The study employed thematic analysis to identify recurring governance patterns across the selected literature and policy documents. The analysis consisted of five iterative stages. First, all documents were read repeatedly to obtain a comprehensive understanding of defense governance transformation. Second, open coding was conducted by identifying meaningful concepts related to institutional adaptation, governance reform, cybersecurity, national resilience, and multidomain defense. Third, similar codes were grouped into broader analytical categories through axial coding. Fourth, these categories were synthesized into four principal analytical themes: (1) Institutional Adaptation; (2) Collaborative Governance; (3) Cyber

Defense Integration; (4) Multidomain National Resilience. Finally, selective coding was undertaken to examine the relationships among these themes and to explain how they collectively contribute to adaptive defense governance. The thematic analysis enabled the identification of governance patterns, institutional responses, and strategic interactions across various policy documents and academic studies (Gustafsson et al., 2025).

Beyond thematic analysis, this study employed conceptual synthesis to construct the proposed Adaptive Defense Governance Framework. The synthesis integrated empirical findings from policy documents with theoretical perspectives on adaptive governance, collaborative governance, cybersecurity governance, and national resilience. Rather than merely summarizing previous studies, the conceptual synthesis examined how these concepts interact within Indonesia's defense governance system under hybrid warfare conditions.

This process resulted in a conceptual framework that explains the governance mechanisms linking institutional adaptation, cyber defense integration, collaborative governance, and multidomain national resilience.

The overall analytical process followed the interactive model proposed by Miles, Huberman, and Saldaña (2020), consisting of data reduction; data display; conclusion drawing and verification. These activities were conducted iteratively throughout the research process.

The coded data were organized into thematic matrices to facilitate comparisons among institutional reforms, governance mechanisms, and national resilience strategies.

Patterns emerging from different data sources were continuously compared to refine interpretations and strengthen conceptual explanations.

To enhance the credibility and trustworthiness of the findings, several validation strategies were employed. Source triangulation was conducted by comparing government regulations, strategic policy documents, academic literature, and reports from international organizations.

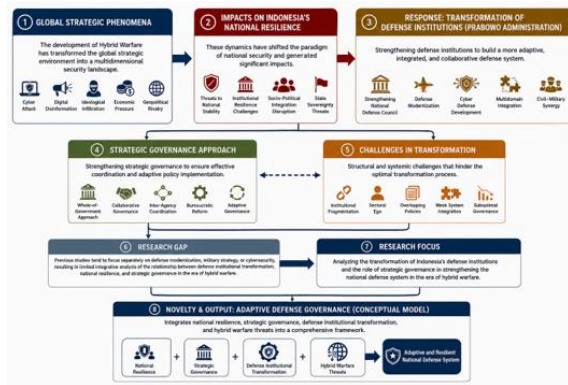
Methodological transparency was maintained by documenting every stage of literature identification, screening, coding, and conceptual synthesis. Peer debriefing was undertaken through continuous comparison between theoretical interpretations and documentary evidence to reduce interpretative bias.

Furthermore, an audit trail documenting coding decisions, thematic development, and analytical interpretations was maintained throughout the research process to improve dependability and confirmability.

The overall methodological framework consisted of six interconnected stages:

1. systematic literature identification;
2. document screening and eligibility assessment;
3. thematic coding;
4. thematic analysis;
5. conceptual synthesis;
6. development of the Adaptive Defense Governance Framework.

Figure 1 illustrates the methodological framework adopted in this study.



RESULT AND DISCUSSION

Institutional Adaptation and Defense Governance Transformation

The findings indicate that Indonesia's defense transformation under the Prabowo Subianto administration represents more than a continuation of post-Reformasi military modernization. Rather than focusing solely on strengthening conventional defense capabilities, the current administration has initiated a broader institutional reconfiguration that emphasizes governance adaptability, multidomain coordination, and strategic integration. This shift reflects an emerging recognition that contemporary national security is increasingly shaped by hybrid threats that transcend traditional military domains.

Previous defense reforms primarily concentrated on the modernization of the Minimum Essential Force (MEF), the acquisition of advanced weapon systems, the revitalization of the domestic defense industry, and organizational reforms within the Indonesian National Armed Forces (TNI). Although these initiatives strengthened Indonesia's conventional defense posture, the findings suggest that they remained largely capability-oriented and insufficient to address increasingly complex multidomain threats, including cyberattacks, information

warfare, digital disruption, and strategic influence operations. Consequently, the current phase of defense transformation demonstrates a significant transition from military modernization toward governance adaptation.

One of the clearest manifestations of this institutional shift is the establishment of the National Defense Council (Dewan Pertahanan Nasional/DPN), whose formation fulfilled the mandate of Law No. 3 of 2002 after more than two decades of institutional delay. While previous studies have largely interpreted the DPN as an administrative mechanism for coordinating defense policy, the findings of this study reveal a broader institutional significance. The DPN functions as a governance platform that integrates defense, intelligence, cybersecurity, and national strategic policymaking within a unified decision-making structure directly under presidential leadership. Rather than merely creating an additional institution, its establishment reflects a fundamental transformation in the architecture of Indonesian defense governance from fragmented sectoral coordination toward integrated strategic governance.

The findings further demonstrate that institutional adaptation has expanded beyond conventional military organizations. Defense reform increasingly incorporates the revitalization of air defense systems, stronger intelligence coordination, digital defense governance, and the gradual development of space-based defense capabilities. These developments indicate that institutional flexibility has become an essential element of defense capacity. In this regard, national defense is no longer interpreted primarily as the

accumulation of military assets but increasingly as the state's ability to coordinate diverse institutional resources in responding to rapidly evolving security environments.

Taken together, these findings suggest that Indonesia's defense transformation reflects a broader shift in governance logic. Defense effectiveness is no longer determined exclusively by military capability but increasingly depends on institutional adaptability, strategic interoperability, and multidomain coordination. This transformation provides the empirical foundation for conceptualizing Adaptive Defense Governance, in which governance capacity itself becomes a strategic component of national defense.

Cyber Defense Integration and Multidomain Security

Another significant finding concerns the growing centrality of cyber defense within Indonesia's national defense architecture. The findings demonstrate that cyber resilience has evolved from a supporting technical function into a strategic pillar of national security governance. This transformation has been driven by the increasing frequency and sophistication of cyberattacks targeting government institutions, critical digital infrastructure, and public information systems.

The ransomware attack on Indonesia's National Data Center (PDNS) in 2024 represents a critical institutional turning point. Beyond exposing technical vulnerabilities, the incident revealed structural weaknesses in inter-agency coordination, crisis management, and digital governance. Consequently, the government accelerated institutional reforms that strengthened cooperation among the Ministry of

Defense, the National Cyber and Crypto Agency (BSSN), intelligence agencies, and other strategic institutions. The findings indicate that the significance of this response lies not only in improving cybersecurity capacity but also in redefining cyber defense as an integral component of national resilience.

More importantly, the findings reveal that cyber defense has become embedded within a broader multidomain governance framework. Digital threat monitoring, strategic intelligence sharing, cybersecurity policy, and institutional interoperability increasingly operate as interconnected governance mechanisms rather than isolated technical activities. This demonstrates that cyber resilience is fundamentally an institutional capability that enables governments to maintain policy continuity, protect critical infrastructures, and preserve public trust during multidomain crises.

These findings suggest that Indonesia is gradually moving toward a multidomain defense model in which military preparedness, cybersecurity, intelligence coordination, and digital governance are treated as mutually reinforcing components of national resilience. Such integration illustrates a broader transformation in defense governance, where the state's capacity to manage complexity becomes equally important as its conventional military strength.

Collaborative Governance and Whole-of-Government Approach

The findings also demonstrate that Indonesia's response to hybrid warfare increasingly relies on collaborative governance and whole-of-government approaches. Contemporary security threats simultaneously affect defense, digital

infrastructure, economic stability, public communication, and social cohesion, making unilateral institutional responses increasingly ineffective. Consequently, defense governance has expanded beyond the military sector toward broader intergovernmental collaboration.

The study finds increasing coordination among defense institutions, cybersecurity agencies, intelligence organizations, and strategic ministries in developing integrated responses to multidomain threats. This institutional convergence reflects a significant governance transition in which national defense is understood as a shared governmental responsibility rather than an exclusive military function. The findings therefore indicate that collaborative governance has become a strategic requirement for maintaining national resilience under conditions of increasing uncertainty.

Equally important is the growing recognition that information warfare and digital disinformation constitute strategic security challenges. Institutional reforms increasingly emphasize strategic communication, digital resilience, and coordinated responses to information manipulation capable of undermining social trust and political stability. These developments suggest that societal resilience has become an inseparable component of national defense governance. Consequently, the protection of national security increasingly depends on the ability of state institutions to coordinate responses across military, civilian, technological, and informational domains simultaneously.

Challenges of Adaptive Defense Governance

Despite these significant institutional developments, the findings reveal that Indonesia's transition toward adaptive defense governance remains incomplete. Persistent institutional fragmentation continues to constrain effective multidomain coordination. Sectoral interests, overlapping bureaucratic mandates, and limited interoperability among government agencies reduce the effectiveness of integrated responses to increasingly complex security challenges.

Cybersecurity governance illustrates this institutional challenge most clearly. Responsibilities remain distributed across multiple organizations with partially overlapping authorities, often resulting in fragmented decision-making and delayed policy responses during rapidly evolving cyber incidents. These findings suggest that institutional adaptation requires more than organizational expansion; it demands governance mechanisms capable of ensuring sustained coordination, information sharing, and strategic interoperability across institutional boundaries.

The study further indicates that the long-term sustainability of defense transformation depends heavily on policy continuity, regulatory harmonization, and organizational learning. Institutional reforms initiated under the current administration may strengthen national resilience only if they are accompanied by enduring mechanisms that facilitate adaptive learning, collaborative decision-making, and continuous policy adjustment in response to emerging multidomain threats.

Overall, the findings reveal that Indonesia's defense transformation represents a gradual shift from conventional defense modernization

toward Adaptive Defense Governance. Rather than emphasizing military capability as the sole determinant of national security, this emerging governance model positions institutional adaptability, multidomain coordination, cyber resilience, and collaborative governance as mutually reinforcing pillars of contemporary national defense. These empirical findings provide the basis for extending existing defense governance literature by demonstrating that governance capacity itself has become a strategic dimension of national resilience in the era of hybrid warfare.

DISCUSSION

The findings demonstrate that Indonesia's defense transformation under the Prabowo Subianto administration represents a fundamental shift in the logic of national defense governance rather than merely an acceleration of military modernization. While previous reforms primarily emphasized strengthening defense capabilities through the modernization of military assets and organizational restructuring, the present study reveals that contemporary defense effectiveness increasingly depends on the capacity of institutions to coordinate, learn, and adapt across multiple security domains. This transformation reflects a broader transition from a capability-oriented paradigm toward a governance-oriented paradigm in which institutional adaptability becomes a strategic determinant of national resilience.

This governance transition is largely driven by the changing character of hybrid warfare. Unlike conventional military conflict, hybrid threats simultaneously exploit cyber vulnerabilities, information

ecosystems, economic interdependence, political polarization, and institutional weaknesses. Consequently, national defense can no longer be conceptualized solely as the protection of territorial sovereignty through military force. Instead, defense increasingly depends upon governance systems capable of integrating military institutions, cybersecurity agencies, intelligence organizations, civilian authorities, and strategic policy actors into coherent multidomain responses. The empirical findings therefore suggest that institutional resilience has become as strategically important as conventional military capability.

One of the most significant contributions of this study is the conceptualization of Adaptive Defense Governance (ADG) as an analytical framework for understanding defense transformation under conditions of multidomain hybrid threats. Existing literature generally examines military modernization, cybersecurity governance, collaborative governance, and adaptive governance as separate analytical perspectives.

However, the findings indicate that these perspectives become increasingly inseparable within contemporary defense environments. Adaptive Defense Governance therefore refers to a governance model characterized by institutional adaptability, multidomain coordination, cyber resilience, collaborative policymaking, and strategic interoperability, enabling governments to respond dynamically to rapidly evolving security challenges. Rather than positioning governance as an administrative support function, the proposed framework conceptualizes governance capacity itself as a

strategic component of national defense.

The proposed framework also extends adaptive governance theory. Adaptive governance has traditionally been applied within environmental governance, disaster management, and public policy, emphasizing institutional learning, flexibility, and collaborative problem solving under conditions of uncertainty (Folke et al., 2022). The findings of this study demonstrate that defense governance operates under substantially different conditions. Institutional adaptation in the defense sector must occur simultaneously across military, intelligence, cyber, diplomatic, and civilian governance systems, all of which interact under high levels of strategic uncertainty and geopolitical competition. Consequently, Adaptive Defense Governance expands existing adaptive governance theory by incorporating multidomain security coordination and strategic interoperability as essential dimensions of institutional adaptation.

Similarly, the findings extend collaborative governance theory developed by Ansell and Gash (2021). Collaborative governance emphasizes consensus building and cross-sectoral coordination among multiple stakeholders in addressing complex public problems. However, the empirical evidence presented in this study suggests that collaboration alone is insufficient within hybrid warfare environments. Effective defense governance additionally requires rapid strategic decision-making, institutional interoperability, intelligence integration, and coordinated cyber resilience that operate under conditions of time-sensitive security threats. Therefore, this study argues that collaborative governance within national defense

requires a stronger emphasis on strategic integration and operational adaptability than has been recognized in existing governance literature.

The establishment of the National Defense Council (DPN) provides empirical evidence supporting this theoretical argument. Rather than functioning merely as a coordinating institution, the DPN represents an institutional mechanism through which fragmented defense authorities are progressively reorganized into an integrated strategic governance architecture. The significance of this institutional innovation lies not simply in organizational restructuring but in its capacity to facilitate cross-sectoral coordination among defense, intelligence, cybersecurity, and strategic policymaking institutions.

This finding illustrates how institutional architecture itself becomes a strategic resource for strengthening national resilience against multidomain threats.

The findings further demonstrate that cyber defense has evolved beyond its traditional role as a technological security function. The ransomware attack on Indonesia's National Data Center (PDNS) exposed structural weaknesses in institutional coordination rather than merely technical vulnerabilities. Consequently, cyber resilience should be understood as an institutional capability that enables governments to sustain governance continuity, maintain public trust, and coordinate strategic responses during digital crises. This interpretation extends contemporary cyber governance literature by emphasizing that cybersecurity constitutes a governance capability embedded within broader national resilience systems rather than an isolated technological domain.

Another important implication concerns the implementation of the Whole-of-Government approach. While previous studies frequently describe Whole-of-Government as an administrative coordination mechanism, the findings indicate that its strategic value lies in enhancing institutional adaptability across multiple governance domains. The integration of defense institutions, cybersecurity agencies, intelligence organizations, economic policymakers, and civilian actors demonstrates that effective national defense increasingly depends upon governance networks rather than hierarchical organizational structures alone. This multidomain institutional integration represents one of the defining characteristics of Adaptive Defense Governance.

Nevertheless, the findings also reveal important limitations that prevent Indonesia's defense transformation from fully realizing adaptive governance principles. Institutional fragmentation, overlapping authorities, sectoral competition, and limited interoperability continue to constrain effective multidomain coordination. These structural constraints suggest that institutional expansion alone cannot guarantee governance effectiveness. Instead, successful defense transformation requires sustained organizational learning, regulatory harmonization, interoperable digital infrastructure, and continuous policy adaptation across institutional boundaries. In this regard, Adaptive Defense Governance should be understood as a continuous governance process rather than a fixed institutional arrangement.

The findings additionally raise important normative considerations regarding democratic governance. The expansion of defense institutions

into cyber governance, strategic communication, and civilian policy coordination inevitably broadens the influence of security institutions within public governance. Although such expansion may strengthen national resilience against hybrid threats, it simultaneously increases the risk of excessive securitization, bureaucratic dominance, and weakened civilian oversight if appropriate accountability mechanisms are not maintained.

Therefore, strengthening Adaptive Defense Governance must be accompanied by transparent governance arrangements, democratic accountability, and clear institutional boundaries that preserve civilian supremacy while enabling effective multidomain coordination.

From a public administration perspective, this study contributes to the growing literature on governance under conditions of complexity and uncertainty. The findings demonstrate that state capacity in the contemporary era should no longer be assessed primarily through administrative efficiency or military capability alone. Instead, governance effectiveness increasingly depends upon the ability of public institutions to integrate policy sectors, coordinate multidomain actors, facilitate institutional learning, and maintain strategic adaptability amid rapidly changing security environments. This perspective broadens traditional understandings of public administration by positioning national defense as an evolving governance system rather than an exclusively military function.

Finally, the theoretical contribution of this study lies in demonstrating that contemporary defense transformation should be interpreted as a process of governance adaptation rather than military

modernization alone. The proposed Adaptive Defense Governance framework advances existing defense governance literature by integrating institutional resilience, collaborative governance, cyber defense, multidomain coordination, and strategic interoperability into a single analytical perspective. This framework offers a broader conceptual foundation for understanding how emerging democracies can strengthen national resilience amid increasingly complex hybrid warfare environments.

Consequently, the study contributes not only to explaining Indonesia's ongoing defense transformation but also to expanding comparative governance scholarship on multidomain security in the twenty-first century.

CONCLUSION

This study concludes that Indonesia's defense transformation under the Prabowo Subianto administration represents a fundamental shift from a military capability-centered paradigm toward a governance-centered approach to national resilience. Rather than relying solely on conventional force modernization, contemporary defense effectiveness increasingly depends on the state's ability to coordinate institutions, integrate cyber capabilities, and adapt governance mechanisms to multidomain hybrid threats. The findings demonstrate that governance capacity has become a strategic component of national defense, positioning institutional adaptability alongside military capability as a critical determinant of national resilience.

The principal theoretical contribution of this study is the development of the Adaptive Defense

Governance (ADG) framework. Unlike existing perspectives that examine military modernization, cybersecurity, or collaborative governance separately, ADG conceptualizes defense governance as an integrated system built upon five interrelated dimensions: institutional adaptability, multidomain coordination, cyber resilience, collaborative governance, and strategic interoperability.

This framework extends adaptive governance and collaborative governance theories by demonstrating that defense governance in hybrid warfare environments requires not only institutional flexibility and collaboration but also the capacity to integrate military, cyber, intelligence, and civilian institutions into a coherent governance architecture.

Consequently, Adaptive Defense Governance provides a broader analytical perspective for understanding defense transformation in emerging democracies confronting increasingly complex multidomain security challenges.

From a policy perspective, the findings suggest that Indonesia's future defense reforms should move beyond organizational expansion and prioritize governance integration. Three strategic priorities emerge from this study. First, the government should strengthen institutional interoperability by establishing integrated coordination mechanisms among the Ministry of Defense, the National Cyber and Crypto Agency (BSSN), intelligence institutions, and other strategic agencies through interoperable governance protocols and shared strategic planning.

Second, cybersecurity should be institutionalized as a core element of national defense policy by

developing an integrated national cyber defense architecture supported by joint operational standards, information-sharing mechanisms, and continuous institutional capacity building.

Third, strengthening adaptive defense governance must be accompanied by regulatory harmonization, transparent accountability mechanisms, and robust civilian oversight to ensure that expanded defense coordination remains consistent with democratic governance principles.

Beyond Indonesia, the proposed Adaptive Defense Governance framework also offers practical relevance for ASEAN member states that are increasingly exposed to hybrid warfare, cyber threats, and geopolitical competition in the Indo-Pacific. By emphasizing governance adaptability rather than military capability alone, the framework provides a potential reference for strengthening regional resilience and multidomain security cooperation within Southeast Asia.

This study has several limitations. First, the analysis is primarily based on qualitative policy analysis and documentary evidence, limiting direct observation of institutional practices and operational coordination among defense agencies.

Second, the study focuses exclusively on Indonesia under the current administration, thereby limiting comparative assessment across different governance contexts. Third, because the Adaptive Defense Governance framework is conceptually developed from a single-country case, its broader applicability requires empirical validation in other national settings.

Future research should therefore empirically test the Adaptive Defense Governance

framework using comparative and mixed-method approaches.

Comparative studies involving ASEAN countries, Indo-Pacific partners, and NATO member states would provide valuable evidence regarding the applicability of the framework across different institutional and geopolitical contexts.

Future studies should also examine measurable indicators of institutional adaptability, cyber resilience, and strategic interoperability to enable the operationalization and empirical evaluation of Adaptive Defense Governance as a governance model for multidomain security in the twenty-first century.

REFERENCES

- Ansell, C., & Gash, A. (2021). Collaborative governance in theory and practice. *Journal of Public Administration Research and Theory*, 18(4), 543–571.
- Buzan, B., & Wæver, O. (2022). *Regions and powers: The structure of international security*. Cambridge University Press.
- Christensen, T., & Lægreid, P. (2020). The whole-of-government approach to public sector reform. *Public Administration Review*, 67(6), 1059–1066.
- CoE, H. (2023). *Hybrid threats: A comprehensive resilience ecosystem*. European Centre of Excellence for Countering Hybrid Threats. https://www.hybridcoe.fi/wp-content/uploads/2023/04/COR_E_comprehensive_resilience_ecosystem.pdf
- Danylenko, S. (2025). Cross-sectoral resilience: Lessons from Ukrainian local governance under hybrid threats. *Discover*

- Social Science and Health*.
- Folke, C., Hahn, T., Olsson, P., & Norberg, J. (2022). Adaptive governance of social-ecological systems. *Annual Review of Environment and Resources*, 30(1), 441–473.
- Gustafsson, M., Wihlborg, E., Borodin, Y., & Kvitka, S. (2025). Adaptive governance amidst the war: Overcoming institutional challenges through collaborative digital service delivery in Ukraine. *Government Information Quarterly*, 42(3), 102056. <https://doi.org/10.1016/j.giq.2025.102056>
- Hoffman, F. G. (2007). *Conflict in the 21st century: The rise of hybrid wars*. Potomac Institute for Policy Studies.
- Indonesia, M. of D. of the R. of. (2025). *Indonesia defense policy and strategic transformation report 2025*. Ministry of Defense of the Republic of Indonesia.
- Kunce, B. (2025). *Strengthening societal resilience against hybrid warfare*. Daniel K. Inouye Asia-Pacific Center for Security Studies.
- Mietzner, M. (2025). Civil–military relations and democratic resilience in Indonesia’s contemporary governance. *Asian Survey*, 65(1), 33–57.
- Miles, M. B., Huberman, M. A., & Saldana, J. (2020). *Qualitative Data Analysis: A Methods Sourcebook (4th ed.)* (4th ed.). SAGE Publications.
- NATO. (2024). *NATO hybrid threats and resilience framework report 2024*. North Atlantic Treaty Organization.
- Nye, J. S. (2021). *The future of power*. Public Affairs.
- Pierre, J., & Peters, B. G. (2020). *Governance, Politics and the State* (2nd ed.). Palgrave Macmillan.
- Pramono, B. (2025). Strategic adaptations for hybrid warfare: Enhancing Indonesian national defence in the digital era. *International Journal of Innovative Research and Scientific Studies*, 8(6), 974–981. <https://doi.org/10.53894/ijirss.v8i6.9776>
- Pramudya, R., Hidayat, T., & Kurniawan, A. (2026). National resilience and multidomain defense challenges in Southeast Asia. *Journal of Defense and Security Studies*, 12(1), 22–39.
- RI, S. (2025). *Pembentukan Dewan Pertahanan Nasional sebagai strategi penguatan pertahanan negara*. Sekretariat Kabinet Republik Indonesia.
- Sukma, R. (2023). Indonesia and Indo-Pacific strategic competition: National resilience and regional security challenges. *Pacific Review*, 36(4), 611–629.
- Union, I. T. (2024). *Global cybersecurity report 2024*. ITU Publications.