Journal of Social Work and Science Education
Volume 7 (3) 2026, 1965-1973
E-ISSN 2723-6919, P-ISSN 2746-0827

Cyber Threats in Hybrid Warfare: A Strategic Mapping and Response Framework for National Defense

Shoraya Lolyta Octaviana[1], Totok Imam Santoso[1], Zainal Abidin Sahabuddin[1], Guntur Eko Saputro[1]
[1]Universitas Pertahanan, West Java, Indonesia

Corresponding author e-mail: guntur.saputro@idu.ac.id

Article History: Received on 2 March 2026, Revised on 15 May 2026, Published on 16 May 2026

Abstract: Hybrid warfare integrates military and non-military instruments, with cyberspace emerging as a critical domain. Cyber threats in this context are systemic, multidimensional, and difficult to attribute, yet existing studies often treat cybersecurity and hybrid warfare separately. This study maps cyber threats within hybrid warfare frameworks and formulates strategic responses to support national defense. A qualitative descriptive approach was used, combining systematic literature review (45 peer-reviewed articles and policy documents, 2018–2025), Soft System Methodology (SSM) for complexity analysis, and SWOT analysis for strategic formulation. Four principal cyber threat types were identified: attacks on critical infrastructure, cyber espionage, disinformation campaigns, and influence operations. Key characteristics include multidimensionality, attribution difficulty, asymmetry, and involvement of both state and non-state actors. SSM revealed interconnected systems across technology, governance, and society. SWOT analysis identified strengths (growing digital human resources) and weaknesses (limited inter-agency coordination). A strategic response model comprising system integration, capacity enhancement, and national coordination is proposed. National defense systems must adopt holistic, adaptive frameworks that integrate cyber capabilities, cross-sectoral collaboration, and societal resilience. Future research should empirically test the proposed model in national defense contexts.

Keywords: Cyber Threats and Cybersecurity, Hybrid Warfare, National Defense, Strategic Response

A. Introduction

The rapid advancement of information and communication technology has significantly transformed the nature of global conflict (Zhevelieva, 2025). Whereas traditional conflicts were predominantly characterized by conventional military engagements, contemporary warfare has evolved into more complex and multidimensional forms, commonly referred to as hybrid warfare (Krainiuk et al., 2025). This form of conflict integrates a wide range of instruments, both military and non-military, including economic pressure, political influence, information

manipulation, and, most notably, cyber operations (Bila, 2024). In this evolving landscape, cyberspace has emerged as a critical strategic domain, where cyber-attacks not only disrupt technological systems but also generate broader implications for social stability, economic resilience, and political legitimacy (Balan et al., 2025). Consequently, cyber threats are no longer isolated incidents but have become integral components of hybrid warfare strategies aimed at systematically weakening state capacity without direct military confrontation (Balan et al., 2025).

In the context of Indonesia, the rapid expansion of digitalization presents both opportunities and vulnerabilities (Zeeshan, 2025). The increasing reliance on digital infrastructure, coupled with the widespread adoption of information technology and the openness of public information ecosystems, has heightened exposure to cyber threats (Maltsev et al., 2025). These threats manifest in various forms, including attacks on critical infrastructure, the proliferation of disinformation, and the manipulation of public opinion, all of which pose significant risks to national stability and security (Wither et al., 2020). As a result, cybersecurity has become an essential component of national defense in the digital era.

Despite the growing recognition of cyber threats in global security discourse, existing studies tend to examine cybersecurity and hybrid warfare as separate domains (Kozachenko, 2025). Limited research has explicitly integrated cyber threats within the broader framework of hybrid warfare, particularly in relation to national defense strategies (Kovalchuk, 2025). This gap highlights the need for a more comprehensive analytical approach that bridges these domains and provides a systematic understanding of how cyber threats operate within hybrid warfare contexts (Zamykalová, 2025).

Therefore, this study aims to (1) map the forms of cyber threats within the framework of hybrid warfare, (2) analyze their characteristics and patterns, and (3) formulate strategic responses to support national defense. By integrating cyber threat analysis with hybrid warfare theory, this study seeks to contribute to the development of a more comprehensive and adaptive cyber defense framework capable of addressing the complexities of modern security challenges. This study addresses the following research questions: 1. How are cyber threats manifested within the framework of hybrid warfare in the context of national defense? 2. What are the characteristics, patterns, and strategic impacts of cyber threats as instruments of hybrid warfare against Indonesia's national security? 3. What strategic responses and cyber defense frameworks can be developed to enhance Indonesia's national defense capabilities in addressing cyber threats within hybrid warfare?

B. Methods

This study adopts a qualitative descriptive approach through a literature review method combined with a systems analysis perspective. Data were collected from a

range of credible sources, including national and international academic journals, scholarly books, government policy documents, and reports from international institutions related to cybersecurity, defense, and geopolitics (Hulak et al., 2025). The selection of these sources was based on several criteria, namely relevance to the research topic, credibility of the publication, and the recency and validity of the data to ensure the reliability of the analysis. In terms of data analysis, this study employs multiple analytical techniques. Content analysis is used to identify patterns of cyber threats and the defining characteristics of hybrid warfare. Furthermore, Soft System Methodology (SSM) is applied to understand the complexity of cyber threats within a systemic framework, involving stages such as problem identification, system mapping through rich pictures, and the development of conceptual models. In addition, SWOT analysis is utilized to formulate strategic responses by examining internal strengths and weaknesses as well as external opportunities and threats, thereby providing a comprehensive basis for strategic decision-making in the context of national defense.

C. Results and Discussion

Result

1. Mapping Cyber Threats in Hybrid Warfare

The results of this study indicate that cyber threats within the framework of hybrid warfare can be systematically categorized into four principal forms. First, attacks on critical infrastructure represent a highly disruptive threat targeting strategic sectors such as energy, transportation, communication, and finance, with the potential to paralyze state functions and generate large-scale instability. Second, cyber espionage constitutes covert and long-term intelligence operations aimed at acquiring sensitive and strategic information, thereby undermining national security at a structural level (Metreveli, 2025). Third, disinformation and digital propaganda involve the strategic manipulation of information through digital platforms to influence public perception, erode trust in governmental institutions, and exacerbate social polarization (Semenenko et al., 2025). Fourth, influence operations integrate technological capabilities with psychological strategies to shape public behavior and decision-making processes, ultimately affecting political and social stability.

2. Characteristics of Cyber Hybrid Threats

Furthermore, the analysis reveals that cyber threats in hybrid warfare exhibit several distinctive characteristics. These threats are inherently multidimensional, encompassing technological, informational, political, and social aspects simultaneously (Sembiring et al., 2025). They are also difficult to attribute due to the anonymity and complexity of cyberspace, which complicates response and accountability mechanisms. In addition, such threats are asymmetrical in nature,

enabling relatively weaker actors to exploit technological vulnerabilities against more advanced systems (Pramitasari, 2022). Moreover, they involve both state and non-state actors, thereby blurring the boundaries between traditional and non-traditional security threats.

3. System Analysis (SSM)

The application of Soft System Methodology (SSM) demonstrates that cyber threats in hybrid warfare constitute a complex and interconnected system involving multiple stakeholders across various sectors. These threats are not isolated phenomena but are embedded within a broader network of interdependent systems, including technological infrastructure, governance structures, and societal dynamics (Semenenko et al., 2024). Consequently, addressing these threats requires a holistic and cross-sectoral approach that integrates technological, institutional, and policy-based responses.

4. SWOT Analysis

The SWOT analysis provides a comprehensive framework for understanding the strategic landscape of cyber defense. From the internal perspective, strengths include the growing availability of digital human resources and the continuous expansion of technological infrastructure. However, these are counterbalanced by weaknesses such as limited inter-agency coordination and existing technological gaps (Lund, 2024). From the external perspective, opportunities arise from the potential for international cooperation and rapid advancements in artificial intelligence and cybersecurity technologies. At the same time, significant threats emerge from the increasing frequency and sophistication of cyber-attacks, as well as the escalating complexity of hybrid warfare dynamics (Zinchenko, 2025).

5. Strategic Response Model

Based on the findings, this study proposes a strategic response model comprising three interrelated components. First, system integration emphasizes the need to develop a unified and interoperable national cyber defense system capable of responding to multidimensional threats. Second, capacity building focuses on enhancing both human resources and technological capabilities to ensure adaptive and resilient defense mechanisms (Mitrović, 2019). Third, national coordination highlights the importance of strengthening synergy among institutions and sectors to enable a cohesive and effective response to hybrid threats. Collectively, these components form a comprehensive strategic framework for reinforcing national defense in the cyber domain (Sinani & Hoxha, 2025).

Discussion

The findings of this study demonstrate that cyber threats within the framework of hybrid warfare constitute a complex, systemic, and multidimensional challenge that significantly reshapes the nature of contemporary conflict. Unlike conventional warfare, hybrid warfare integrates military and non-military instruments across interconnected domains such as cyberspace, information, politics, economics, and society (Nikolov, 2018). The study reveals that cyber threats are no longer limited to technical disruptions, but function as strategic instruments capable of influencing national stability, public trust, and state sovereignty. Furthermore, the findings indicate that effective responses to cyber hybrid threats require integrated approaches involving governance, institutional coordination, technological capability, and societal resilience. The interconnected nature of technological infrastructure and social systems also highlights the importance of adaptive and system-based defense strategies in addressing evolving cyber threats.

This study contributes to the development of Hybrid Warfare Theory by positioning cyber threats as a central and operationalized component of hybrid warfare rather than merely a supporting element (Poptchev, 2020). Existing studies often discuss cybersecurity and hybrid warfare separately; however, this research bridges the conceptual gap by integrating cyber threats into the broader strategic framework of national defense. The findings reinforce the argument that cyberspace has evolved into a strategic operational domain where state and non-state actors can exploit systemic vulnerabilities through disinformation, cyber-attacks, and influence operations. In this regard, the study extends Hybrid Warfare Theory by emphasizing that cyber operations possess strategic equivalence to conventional military actions due to their ability to weaken national resilience without direct physical confrontation.

The findings provide important implications for Indonesia and other countries facing similar digital transformation challenges. National defense systems should adopt a multidimensional and adaptive framework that integrates cyber capabilities into broader defense architecture. This includes strengthening cross-sectoral coordination among military institutions, cybersecurity agencies, government bodies, private sectors, and civil society. In addition, investment in human capital, technological innovation, digital literacy, and public awareness is essential to enhance societal resilience against disinformation and cyber influence operations (Zulfian & Rahmadan, 2025). For Indonesia, strengthening institutional synergy between defense and cyber governance institutions becomes particularly important to ensure rapid response and policy coherence in addressing hybrid cyber threats.

The findings of this study are consistent with prior international cyber defense frameworks, particularly those developed by NATO and the European Union, which emphasize resilience, collective defense, and cross-sectoral cooperation in responding to cyber threats. Similar to NATO's cyber defense approach, this study highlights the

importance of integrating cyber capabilities into national security and defense strategies. In addition, the findings align with the principles of the United Nations Group of Governmental Experts (UN GGE), which emphasize responsible state behavior, international cooperation, and the protection of critical infrastructure in cyberspace. However, this study differs from existing frameworks by focusing specifically on cyber threats as an operational component of hybrid warfare within the context of national defense and societal resilience, particularly in developing countries such as Indonesia.

This study has several limitations that should be acknowledged. First, the research relies primarily on a literature review approach without incorporating primary empirical data such as interviews, surveys, or field observations. As a result, the findings are largely conceptual and theoretical in nature. Second, the dependence on secondary sources may introduce publication bias, particularly because most available literature tends to focus on high-profile cyber incidents and perspectives from developed countries. Third, the rapidly evolving nature of cyber threats and technological developments means that some findings may become less applicable over time as new forms of hybrid warfare emerge. Therefore, the conclusions of this study should be interpreted within the scope and limitations of the available literature.

Future research should focus on empirically testing the strategic response model proposed in this study through qualitative and quantitative approaches. Case studies of major cyber-attacks within hybrid warfare contexts could provide deeper insights into operational patterns, institutional responses, and societal impacts. Comparative studies across countries would also be valuable in identifying differences in cyber defense readiness, governance structures, and resilience strategies between developed and developing nations. In addition, future studies may explore the role of emerging technologies such as artificial intelligence, big data analytics, and autonomous systems in both strengthening and challenging national cyber defense capabilities. Such research would contribute to the development of more adaptive and evidence-based frameworks for addressing hybrid cyber threats in the future.

D. Conclusions

This study concludes that cyber threats have emerged as a central and defining component of hybrid warfare, fundamentally transforming the landscape of contemporary conflict. These threats are inherently complex and multidimensional, encompassing technological, informational, political, and social domains that interact in a dynamic and often unpredictable manner. As such, cyber threats cannot be effectively addressed through fragmented or sectoral approaches. Instead, they require a comprehensive and integrated strategic response that reflects the systemic nature of hybrid warfare. In this regard, the study proposes a strategic response model that emphasizes three key pillars: system integration, capacity enhancement, and

national coordination. System integration is essential to ensure the interoperability and effectiveness of national cyber defense mechanisms across sectors. Capacity enhancement focuses on strengthening both human resources and technological capabilities to improve resilience and adaptability in the face of evolving threats. Meanwhile, national coordination underscores the importance of synergy among institutions, stakeholders, and sectors in implementing a unified and coherent defense strategy. Collectively, these elements provide a robust framework for reinforcing national defense and enhancing resilience against the growing complexity of hybrid cyber threats.

E. Acknowledgement

We would like to express sincere gratitude to Universitas Pertahanan Indonesia for providing academic support and an enabling research environment that contributed to the completion of this study. Appreciation is also extended to all individuals, colleagues, and institutions whose insights, discussions, and resources have enriched the research process. Any remaining limitations or errors in this work remain the sole responsibility of the author.

References

Balan, S., Balan, L., Vorotynskyy, V., Rybak, I., & Tarasiuk, V. (2025). State Information Policy in The Context of Hybrid Threats: Legal and Political Aspects. *Social And Legal Studios*, *8*(1). https://doi.org/10.32518/Sals1.2025.165

Bila, A. V. (2024). Modern Problematic Aspects of Forensics in The Context of Martial Law in Ukraine and Global ThreATS. *Alfred Nobel University Journal of Law*, *2*(9). https://doi.org/10.32342/3041-2218-2024-2-9-10

Dr. Muhammad Hatim, Dr. Adeel Irfan, Elahi Umar Ranjha, Haroon Shah, & Muhammad Ahmad. (2025). Hybrid Conflict in the 21st Century: Pakistan's Security Dilemmas and Responses. *Social Science Review Archives*, *3*(2). https://doi.org/10.70670/Sra.V3i2.684

Farrand, B., Carrapico, H., & Turobov, A. (2024). The New Geopolitics of EU Cybersecurity: Security, Economy and Sovereignty. *International Affairs*, *100*(6). https://doi.org/10.1093/Ia/Iiae231

Hulak, N., Ilyenko, A., & Dubchak, O. (2025). Practical Aspects of Using Cryptographic Methods to Protect Databases from Unauthorized Access. *Cybersecurity Education Science Technique*. https://doi.org/10.28925/2663-4023.2025.28.786

Kovalchuk, M. (2025). Hybrid Threats and Economic Coercion: Contemporary Challenges to Economic Security in The Digital Environment. *Bulletin of the*

Academy of Labor, Social Relations and Tourism. Series: Economics, Psychology and Management. https://doi.org/10.54929/3041-2390-2025-05-01-04

Kozachenko, R. (2025). Comparison Of National Security Strategies: Approaches of Large and Small States in Ensuring Their Own Security and Their Impact on International Relations. *Epistemological Studies in Philosophy Social and Political Sciences*, *8*(1). https://doi.org/10.15421/342527

Krainiuk, O., Yevseiev, S., Didenko, N., & Piksasov, M. (2025). Transformation of the Regulatory and Legal Framework for Cybersecurity in Ukraine: Analysis of Compliance with The Requirements of The Nis2 Directive and The Cybersecurity Act. *Terra Security*, *1*(3). https://doi.org/10.20998/3083-6298.2025.03.05

Lund, M. S. (2024). Hybrid Threats in Cyberspace: What Do Russia's Cyberspace Operations in Ukraine Tell Us? In *Preparing for Hybrid Threats to Security: Collaborative Preparedness and Response*. https://doi.org/10.4324/9781032617916-7

Maltsev, V., Sharko, D., & Dashkovskyi, A. (2025). State Security of Ukraine in The Face of Modern Challenges and Threats. *The Scientific Journal of The National Academy of National Guard "Honor and Law,"* *3*(94). https://doi.org/10.33405/2078-7480/2025/3/94/349247

Metreveli, S. (2025). The Impact of Hybrid Threats on National Security: Mechanisms for Conflict Prevention and Transformation. (4). https://doi.org/10.61446/Ds.4.2025.10467

Mitrović, M. (2019). Hybrid Genesis of Information Operations in Cyberspace. *Teme*. https://doi.org/10.22190/Teme1804359m

Nawaz, Dr. F. (2025). Psychological Warfare in The Digital Age: Strategies, Impacts, And Countermeasures. *Journal of Future Building*, *2*(1).

Nikolov, O. (2018). Building Societal Resilience Against Hybrid Threats. *Information & Security: An International Journal*, *39*(1). https://doi.org/10.11610/Isij.3908

Poptchev, P. (2020). NATO-EU Cooperation in Cybersecurity and Cyber Defence Offers Unrivalled Advantages. *Information & Security: An International Journal*, *45*. https://doi.org/10.11610/Isij.4503

Pramitasari, A. W. (2022). The Role of Intelligence in Dealing with The Threat of Hybrid War. *The International Journal of Business Management and Technology*, *6*(1).

Sembiring, H., Supriyadi, A. A., & Ghazalie, G. (2025). Network Centric Warfare (NCW)-Based Defense Policy Strategy for Addressing Asymmetric Threats. *Jurnal Ilmiah Global Education*, *6*(4). https://doi.org/10.55681/Jige.V6i4.4847

Semenenko, O., Kirsanov, S., Movchan, A., Sliusarenko, M., & Horhulenko, V. (2025). Addressing The Legal Gaps in AI Regulation for National Security: The Case of Ukraine's Defense Sector. *Revista De Direito, Estado E Telecomunicacoes*, *17*(2). https://doi.org/10.26512/Lstr.V17i2.56351

Semenenko, O., Koval, V., Vodchyts, O., & Dobrovolskyi, Y. (2024). A Multi-Domain Operation – A Modern View at The Forms and Methods of Military Operations Adapting to The Environment of Challenges and Threats Transformation. *Міжнародний Науковий Журнал «Military Science»*, *2*(1). https://doi.org/10.62524/Msj.2024.2.1.02

Sinani, T., & Hoxha, B. (2025). The Security Strategy of Small States in the 21st Century and Beyond. *Academic Journal of Business, Administration, Law and Social Sciences*, *11*(1). https://doi.org/10.2478/Ajbals-2025-0004

Suhirwan Suhirwan, & Mia Kusmiati. (2025). Integrative Model Defense Indonesian Hybrid in Face Dynamics ASEAN Conflict. *Management Dynamics: International Journal of Management and Digital Sciences*, *2*(4). https://doi.org/10.70062/Managementdynamics.V2i4.422

Wither, J. K., Iasiello, E. J., John, C., Neal, J., Army, U. S., Ryan, C., Worthan, L., Cantwell, L. D., Pernik, P., & Jezewski, C. R. (2020). Perspectives On Hybrid Warfare. *Journal Of European Security and Defence Issues*, *10*(1).

Zamykalová, Š. (2025). Critical But Also Strategic Infrastructure Must Be More Resilient Than Ever. *Central European Journal of Security Studies*, *2025*(Issue 1). https://doi.org/10.15804/Cejss.2025106

Zeeshan, F. (2025). Russia-Ukraine Cyber Warfare and Its Impacts on Poland's National Security. *Wah Academia Journal of Social Sciences*, *4*(1).

Zhevelieva, I. S. (2025). Criminal Legal Qualification of Offenses in The Field of Use of Electronic Computing Machines (Computers), Systems and Computer Networks and Electric Communication Networks. *Uzhhorod National University Herald. Series: Law*, *4*(91). https://doi.org/10.24144/2307-3322.2025.91.4.8

Zinchenko, O. (2025). Cybersecurity As an Element of Democratic Consolidation: Lessons from Kharkiv Region. *The Journal of V. N. Karazin Kharkov National University. Issues Of Political Science*, (47). https://doi.org/10.26565/2220-8089-2025-47-06

Zulfian, M. H., & Rahmadan, Y. (2025). Analyzing Russia's Hybrid Warfare Strategy Through Hermeticwiper Against Ukraine: A Cybersecurity and Desecuritization Approach. *Politeia: Journal of Public Administration and Political Science and International Relations*, *3*(3). https://doi.org/10.61978/politeia.V3i3.673