International Journal of Education, Vocational and Social Science
https://e-journal.citakonsulindo.or.id/index.php/IJEVSS
E-ISSN : 2963 4954
IJEVSS

Building Combat Cyber Intelligence Capabilities Within Indonesia's National Defense Framework

Teguh Prasetyo
Sekolah Tinggi Intelijen Negara

Corresponding Author: Teguh191prasetyo@gmail.com

Abstract

The rapid advancement of digital technology and the escalating spectrum of threats in cyberspace have positioned cyber intelligence as a strategic component of modern defense systems. Indonesia, as an archipelagic state with extensive geopolitical interests, faces an increasingly diverse range of cyber threats, including digital espionage, critical infrastructure sabotage, psychological operations, and hybrid warfare. These conditions necessitate the development of cyber combat intelligence capabilities that are not merely defensive in nature, but also adaptive, integrated, and oriented toward operational readiness. This article aims to analyze the concepts, challenges, and strategic approaches to developing cyber combat intelligence within the framework of Indonesia's national defense. The study employs a qualitative approach through literature review, policy analysis, and examination of national defense and cybersecurity doctrines. Data are analyzed thematically to identify structural, institutional, human resource, technological, and inter-agency coordination requirements. The findings indicate that the development of cyber combat intelligence in Indonesia encounters several major constraints, including fragmented institutional authority, limited system interoperability, gaps in human resource capacity, and the insufficient integration of cyber intelligence into military operational doctrines. Conversely, opportunities for strengthening these capabilities include establishing an integrated cyber intelligence architecture, developing specialized operational doctrines, investing in artificial intelligence–based analytical technologies, and enhancing cross-sectoral and international cooperation. This article concludes that the development of cyber combat intelligence must be positioned as a strategic priority within Indonesia's national defense transformation in order to enhance deterrence, conflict preparedness, and the protection of national interests in the digital domain. The proposed policy recommendations include regulatory harmonization, strengthening cyber intelligence governance, and sustained human resource development to address future

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License

threat dynamics.

Keywords: national defense, border bases, forward defense, geopolitics, Indonesia.

INTRODUCTION

The global strategic environment of the twenty-first century is characterized by the increasing dependence of states on digital technology and the recognition of cyberspace as a new domain of modern conflict. Cyber operations now encompass espionage, sabotage of critical infrastructure, information manipulation, and strategic influence operations that may affect political stability and national security. In this context, cyber intelligence has become a vital component of the national defense system, serving as an early warning mechanism, a source of support for strategic decision-making, and an instrument for achieving information superiority during conflict.

As an archipelagic country with a strategic geopolitical position in the Indo-Pacific region, Indonesia faces a high level of vulnerability to cyber threats. The growing reliance on digital systems in the government, defense, energy, transportation, and financial sectors has made national infrastructure a potential target for both state and non-state actors. Furthermore, intensifying regional geopolitical rivalry has increased the likelihood that cyber operations will be employed as part of hybrid conflict strategies. Within the national defense system, cyber threats cannot be regarded merely as technical network security issues. They must be treated as a strategic dimension equal in importance to conventional military domains. The development of combat cyber intelligence capabilities is required to support modern military operations, strengthen deterrence, and improve national preparedness in responding to a broad spectrum of non-conventional threats.

Although various cybersecurity policies have been developed, structural and institutional challenges continue to hinder the establishment of an integrated combat cyber intelligence system. The fragmentation of authority among institutions, limited system interoperability, and gaps in human resource capabilities are the main factors affecting the effectiveness of the national response. This article seeks to address the research gap by analyzing the concepts, challenges, and strategies involved in developing combat cyber intelligence within the framework of Indonesia's national defense.

RESEARCH METHODOLOGY

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License

This study employed a descriptive qualitative approach using literature review and policy analysis methods. The data were obtained from official government documents, national defense strategies, cybersecurity regulations, reports issued by international institutions, and scientific publications related to cyber warfare and cyber intelligence.

The analysis was conducted thematically through several stages, including document collection, coding of key concepts, classification of strategic issues, and synthesis of findings to identify structural, institutional, and operational challenges in the development of combat cyber intelligence. This approach enabled the researcher to examine the phenomenon comprehensively and formulate policy recommendations based on conceptual evidence.

THEORETICAL FRAMEWORK

Harmonization of Legal Frameworks and the Indonesian National Armed Forces Cyber Defense Doctrine

Regulations and policies constitute the primary foundation for developing combat cyber intelligence because they define institutional mandates, limits of authority, and the legitimacy of operations in cyberspace. Libicki (2009) and Kello (2017) emphasize that ambiguity in legal norms and doctrines governing the use of cyber force may weaken deterrence effectiveness and military coordination. Accordingly, within the context of the Indonesian National Armed Forces (TNI), the integration of cyber intelligence must be aligned with the national defense strategy, joint operations doctrine, and national cybersecurity policies (Ministry of Defense of the Republic of Indonesia, 2021; BSSN, 2022).

Military cyber operations doctrines adopted by various countries also demonstrate that the successful integration of cyber intelligence largely depends on clearly defined relationships between civilian and military authorities, as well as strategic decision-making mechanisms (NATO CCDCOE, 2020). This framework serves as an analytical reference for assessing the extent to which Indonesia's national regulations support the role of combat cyber intelligence as an integral component of TNI defense operations.

Operational Command and Coordination Architecture

The institutional structure is understood as the organizational configuration, chain of command, and coordination mechanisms that enable cyber intelligence to be effectively integrated into military operations. Betts (2007) emphasizes that the effectiveness of intelligence within a defense system is largely determined by the institutional relationship between

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License

intelligence analysts and strategic decision-makers. In the cyber context, this challenge becomes increasingly complex because operations are cross-sectoral and involve various state and non-state actors (Healey, 2013).

Studies on network warfare also indicate that flexible and network-based command structures enhance response capabilities in digital conflicts (Arquilla & Ronfeldt, 1996). Accordingly, this study identifies the integration of cyber intelligence into the command structure of the Indonesian National Armed Forces, including its connectivity with strategic intelligence centers and joint operational mechanisms across military branches, as a key indicator of the effectiveness of national cyber defense.

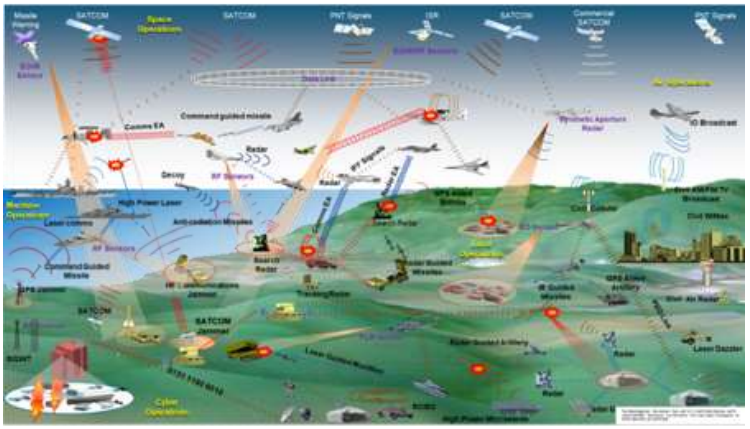


Figure 1. National Joint Operational Command

Professionalization of Cyber Soldiers and Digital Intelligence Personnel

Human resource development is a crucial element in building combat cyber intelligence capabilities. Singer and Friedman (2014) emphasize that advanced technology will not be effective without personnel who possess analytical competence, an understanding of military operations, and strategic awareness. From the perspective of modern conflict, the professionalization of cyber personnel must be placed on an equal footing with other combat specializations (Biddle, 2018).

Within the context of the Indonesian National Armed Forces, this dimension is analyzed through recruitment systems, tiered military education, the establishment of career paths for cyber soldiers, and the development of combat cyber training centers capable of simulating multidomain operations. This approach is consistent with the view that military organizations must adapt structurally and culturally to the characteristics of digital warfare (Rid, 2020).

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License

International Journal of Education, Vocational and Social Science
https://e-journal.citakonsulindo.or.id/index.php/IJEVSS
E-ISSN : 2963 4954
IJEVSS



Figure 2. Cyber Forces in Various Countries

Analytical Systems, Interoperability, and Joint Operations Support

The technological dimension focuses on the use of artificial intelligence, big data analytics, digital sensors, and command-and-control systems that enable cyber intelligence to support the entire military intelligence cycle. Clarke and Knake (2019), as well as Gartzke and Lindsay (2015), emphasize that strategic advantage in cyberspace is largely determined by analytical capabilities and interoperability among defence platforms.

Within the Indonesian National Armed Forces defence framework, cyber intelligence technology must be integrated with joint-service operational systems to establish integrated situational awareness. NATO CCDCOE (2020) indicates that technical interoperability is a key prerequisite for the effectiveness of joint operations in cyberspace. It therefore serves as an important variable in this research analysis.

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License

International Journal of Education, Vocational and Social Science
https://e-journal.citakonsulindo.or.id/index.php/IJEVSS
E-ISSN : 2963 4954
IJEVSS

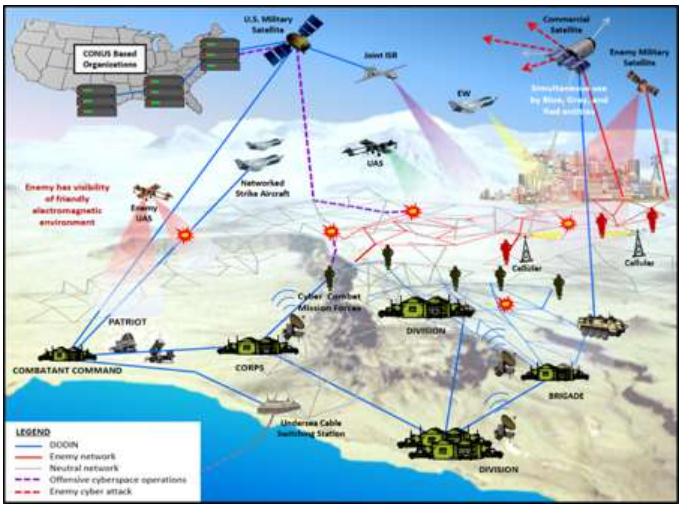


Figure 3. Conventional and Cyber Joint Operations

National Synergy and International Partnerships

Strategic cooperation is positioned as a key component in the development of combat cyber intelligence due to the transnational nature of cyber threats. Healey (2013) and UNODA (2021) emphasize the importance of confidence-building mechanisms, information exchange, and international norms in preventing the escalation of digital conflicts.

In the Indonesian context, cooperation between the Indonesian National Armed Forces (TNI) and national ministries and agencies, the defense industry, academic institutions, and regional partners such as ASEAN forms part of a layered defense strategy and defense diplomacy (ASEAN Secretariat, 2021). This study assesses such cooperation as a supporting variable in building a sustainable national cyber intelligence ecosystem while safeguarding the country's strategic interests.

CONCLUSIONS AND RECOMMENDATIONS

Conclusion

The increasingly digitalized global strategic environment has transformed cyberspace into a new domain of conflict with direct implications for national security. In the Indonesian context, the development of combat cyber intelligence capabilities is no longer merely a technical requirement for information security but an integral component of the transformation of the national defense system and the readiness of the Indonesian National Armed Forces (TNI) to confront a multidomain threat spectrum. This study demonstrates that the successful integration

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License

of cyber intelligence into the TNI's defense structure is largely determined by regulatory and doctrinal alignment, the effectiveness of institutional and command architecture, the professionalization of human resources, the readiness of interoperable technologies, and the strengthening of national and international cooperation.

The findings indicate that although Indonesia has established policy frameworks for cybersecurity and national defense, the primary challenges remain the fragmentation of authority among institutions, limited interoperability of systems across the military services, gaps in the capacity of military cyber personnel, and the suboptimal integration of cyber intelligence into the planning and implementation of TNI joint operations. These conditions may reduce the effectiveness of strategic early-warning functions and national deterrence capabilities amid the growing escalation of regional and global cyber threats.

Based on the theoretical framework applied in this study, this article emphasizes that the development of combat cyber intelligence must be positioned as a national strategic priority integrated into the TNI's defense doctrine, long-term force planning, and modern command-and-control systems. Such integration is intended not only to strengthen the protection of defense infrastructure but also to enhance information superiority, conflict preparedness, and the state's strategic decision-making capabilities in the digital domain.

Recommendations

Based on the research findings and conclusions, several strategic recommendations are proposed to strengthen the integration of combat cyber intelligence into Indonesia's Indonesian National Armed Forces (TNI) defense system, as follows:

1. Strengthening Regulations and Operational Doctrine
   The government and the TNI need to harmonize cybersecurity regulations with the national defense doctrine and the concept of joint operations. The formulation of a specific combat cyber intelligence doctrine governing mandates, authorization, operational procedures, and integration with the land, maritime, and air domains is urgently required to ensure clarity of roles and effective implementation in the field.
2. Reforming Institutional and Command Structures
   The institutional architecture must be strengthened to integrate cyber intelligence functions into the TNI's strategic chain of command. Interagency coordination mechanisms should be designed to be more adaptive without undermining the principle of military control in national defense operations, particularly during crises and armed conflicts.

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License

3. Developing Human Resources on a Sustainable Basis
   The TNI is advised to establish a specialized recruitment system for cyber personnel, expand cyber intelligence education and training programs, and create competitive professional career pathways. The establishment of a national combat cyber training center featuring multidomain conflict scenarios is also essential to improve personnel operational readiness.
4. Modernizing Technology and Enhancing System Interoperability
   Investment in artificial intelligence-based analytical technologies, intelligence big data systems, and integrated command-and-control platforms should be prioritized. Standardizing systems across military services and strengthening interoperability with other national institutions are crucial for developing integrated situational awareness at both strategic and operational levels.
5. Strengthening National and International Cooperation
   The TNI and the government need to expand cooperation with ministries and government agencies, the domestic defense industry, higher education institutions, and regional and international partners through joint exercises, technological research, and strategic information exchange. Such cooperation should be directed toward strengthening national capacity while safeguarding Indonesia's sovereignty and strategic interests.

REFERENCES

Arquilla, J., & Ronfeldt, D. (1996). The advent of netwar. RAND Corporation.

ASEAN Secretariat. (2021). ASEAN cyber security cooperation strategy. ASEAN.

Badan Siber dan Sandi Negara. (2022). Strategi keamanan siber nasional. BSSN.

Betts, R. K. (2007). Enemies of intelligence: Knowledge and power in American national security. Columbia University Press.

Biddle, S. (2018). Military power: Explaining victory and defeat in modern battle (2nd ed.). Princeton University Press.

Clarke, R. A., & Knake, R. K. (2019). The fifth domain: Defending our country, our companies, and ourselves in the age of cyber threats. Penguin Press.

Gartzke, E., & Lindsay, J. R. (2015). Weaving tangled webs: Offense, defense, and deception in cyberspace. Security Studies, 24(2), 316–348. https://doi.org/10.1080/09636412.2015.1038188

Healey, J. (Ed.). (2013). A fierce domain: Conflict in cyberspace, 1986–2012. Cyber Conflict Studies

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License

Association.

Kello, L. (2017). The virtual weapon and international order. Yale University Press.

Kementerian Pertahanan Republik Indonesia. (2021). Buku putih pertahanan Indonesia. Kementerian Pertahanan RI.

Kementerian Pertahanan Republik Indonesia. (2023). Strategi pertahanan negara. Kementerian Pertahanan RI.

Libicki, M. C. (2009). Cyberdeterrence and cyberwar. RAND Corporation.

NATO Cooperative Cyber Defence Centre of Excellence. (2020). Cyberspace operations doctrine primer. NATO CCDCOE.

Rid, T. (2020). Active measures: The secret history of disinformation and political warfare. Farrar, Straus and Giroux.

Singer, P. W., & Friedman, A. (2014). Cybersecurity and cyberwar: What everyone needs to know. Oxford University Press.

UN Office for Disarmament Affairs. (2021). Developments in the field of information and telecommunications in the context of international security. United Nations.

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License