JURNAL FUSION

Vol 6 No 7, Juli 2026
E-ISSN: 2775-6440 | P-ISSN: 2808-7208
Jurnal Homepage https://fusion.rifainstitute.com

STRATEGY FOR OPTIMISING THE ROLE OF INTELLIGENCE IN THE EARLY DETECTION AND PREVENTION OF SECURITY THREATS IN DOMESTIC HIGH-RISK AREAS TO SUPPORT THE NATIONAL DEFENCE STRATEGY

Baginta Bangun, Sigit Purwanto, Bangun Pandapotan Hutajulu
The Republic of Defense University
Email: dama.dika2018@gmail.com , sigit.purwanto@idu.ac.id , zulu97ph@gmail.com

Abstract

This study analyzes the implementation of intelligence roles in the early detection of security disturbances in vulnerable domestic areas, identifies factors influencing their effectiveness, and formulates optimization strategies to strengthen the national defense strategy. A qualitative descriptive-analytical approach was employed. Data were collected through in-depth interviews, observations, document analysis, and Focus Group Discussions (FGDs), and analyzed using the Miles, Huberman, and Saldaña interactive model integrated with SWOT analysis and the Ends–Ways–Means framework. The findings reveal that the intelligence organization possesses significant strengths, including extensive intelligence networks, regulatory support, experienced personnel, and improving interagency coordination. Nevertheless, challenges remain in information system interoperability, unequal digital technology implementation, and limited human resource competencies in digital intelligence analysis. SWOT analysis positions the organization in Quadrant I (Strength–Opportunity), indicating that a growth strategy is the most appropriate approach through the development of an Integrated Digital Intelligence System, an Artificial Intelligence and Big Data-based Early Warning System, enhancement of human resource competencies, strengthened interoperability, and the expansion of community intelligence. The study concludes that optimizing intelligence functions requires integrated digital transformation, stronger cross-sector collaboration, and continuous organizational capacity development to establish an adaptive and accurate early detection system capable of effectively supporting Indonesia's national defense strategy.

Keywords: *intelligence, early detection, national defense strategy, SWOT, digital transformation.*

Diterima: 10 Juni 2026 | Direvisi: 05 Juni 2026 | Diterbitkan: 20 Juli 2026

INTRODUCTION

DOI : https://doi.org/10.54543/fusion.v6i7.538
Published by : Rifa Institute

The evolution of the global strategic environment has fundamentally transformed the nature of threats to national security and defense from predominantly conventional military threats into multidimensional threats that are increasingly complex, dynamic, and difficult to predict. These threats no longer originate solely from military aggression but also encompass terrorism, radicalism, separatism, transnational organized crime, cross-border smuggling, cyberattacks, disinformation, and influence operations conducted through digital platforms. Such developments require every nation, including Indonesia, to establish an adaptive defense system that prioritizes early detection and early warning capabilities as primary instruments for preventing potential threats from escalating into security disturbances capable of undermining national stability (Ministry of Defense of the Republic of Indonesia [MoD RI], 2024; Republic of Indonesia, 2002).

Within this context, intelligence occupies a pivotal position as one of the foremost components of the national defense system. The function of intelligence is no longer confined to the collection of information but has evolved into a comprehensive process encompassing threat identification, situational analysis, risk assessment, and the provision of strategic recommendations to decision-makers. According to Lowenthal (2022), the quality of intelligence products is largely determined by an organization's ability to integrate all stages of the intelligence cycle, including planning, collection, processing, analysis, and dissemination. Accurate, timely, and reliable intelligence products enhance a state's capacity to prevent strategic surprise and strengthen the effectiveness of national defense strategies (Lowenthal, 2022).

As the world's largest archipelagic state, Indonesia faces highly diverse security challenges arising from its unique geographical, demographic, and geopolitical characteristics. Border regions, nationally strategic areas, critical national infrastructure, conflict-prone regions, and territories adjacent to neighboring countries exhibit relatively higher levels of security vulnerability than other areas. In addition to conventional physical threats, advances in information technology have generated non-physical threats, including digital propaganda, the dissemination of misinformation, cyberattacks, and foreign influence operations that have the potential to undermine national stability (National Cyber and Crypto Agency [BSSN], 2024; Geospatial Information Agency [BIG], 2023). These developments indicate that conventional security approaches are no longer sufficient, thereby necessitating an intelligence system capable of conducting continuous surveillance, monitoring, and analysis through the utilization of advanced technologies.

From a normative perspective, Indonesia's intelligence system is supported by a robust legal framework through **Law Number 17 of 2011 concerning State Intelligence**, which stipulates that state intelligence is responsible for conducting intelligence operations, security measures, and influence activities to generate early detection and early warning of threats that may endanger national interests (Republic of Indonesia, 2011). Nevertheless, empirical evidence demonstrates that security disturbances continue to occur in several vulnerable regions, including armed group activities in Papua, narcotics smuggling and human trafficking along border areas,

territorial violations by foreign vessels in the Natuna waters, communal conflicts, and the increasing number of cyberattacks targeting national critical infrastructure. These conditions indicate that the existing early detection system has not yet fully anticipated the evolution of threats before they develop into actual security incidents (MoD RI, 2024; BSSN, 2024).

These challenges demonstrate that optimizing the role of intelligence requires not only enhancing the capacity of intelligence personnel but also strengthening inter-agency coordination, improving information system interoperability, expanding the utilization of emerging technologies such as artificial intelligence, big data analytics, and geospatial intelligence, and developing integrated intelligence-sharing mechanisms. Warner (2023) argues that an integrated intelligence system enhances comprehensive situational awareness, thus improving the quality of strategic decision-making. Therefore, developing an effective strategy for optimizing the role of intelligence in the early detection and prevention of security threats in domestic high-risk areas has become an urgent necessity for strengthening the effectiveness of Indonesia's national defense strategy while enhancing the country's capacity to address the increasingly complex spectrum of multidomain threats.

LITERATURE REVIEW

1. Strategy Theory

The strategic theory developed by Arthur F. Lykke Jr. is one of the most widely used concepts in defense and security strategy studies. Lykke (1989) explains that an effective strategy must be built through a balance between three main components: Ends (the desired goal), Ways (the means or approach to achieving the goal), and Means (the resources available to support the strategy's implementation). These three components must be in balance so that the strategy can be implemented effectively. If one component is inadequate, a strategic risk will emerge that has the potential to reduce the effectiveness of achieving organizational goals (Lykke, 1989).

In the context of national defense, the Ends–Ways–Means theory provides a systematic conceptual framework for designing national security policies. The primary objective (ends) is the realization of national security stability through the state's ability to prevent various threats from an early stage. Ways are realized through optimizing intelligence functions, improving early detection capabilities, strengthening inter-agency coordination, and utilizing information technology. Meanwhile, means (means) include intelligence human resources, budgets, regulations, information systems, artificial intelligence technology, big data analytics, and institutional support. Thus, the success of a defense strategy is determined not only by the size of the available resources, but also by the ability to integrate these three components proportionally (Gray, 2010).

Lykke's theory is highly relevant to this research because it provides a conceptual basis for formulating strategies to optimize the role of intelligence in vulnerable domestic areas. The strategies developed are not only oriented toward achieving national security

objectives but also consider the alignment between implementation methods and available resource capacity. Therefore, the strategic model developed in this research is expected to produce realistic, implementable, and sustainable recommendations to support the national defense strategy by increasing the effectiveness of early detection of various security threats (Lykke, 1989; Gray, 2010).

2. Intelligence Theory

Intelligence theory positions intelligence as a strategic instrument that functions to produce accurate, timely, and relevant information to support the decision-making process. According to Lowenthal (2022), intelligence is not simply an information-gathering activity, but rather a systematic process consisting of planning, collecting, processing, analyzing, and disseminating information, resulting in an intelligence product with strategic value. A quality intelligence product is capable of providing threat assessments, situational development projections, and policy alternatives that decision-makers can use to formulate responses to evolving threats.

From a national security perspective, the intelligence function has undergone significant developments as the complexity of multi-domain threats increases. Contemporary threats stem not only from military aggression but also include terrorism, radicalism, cybercrime, espionage, disinformation, and influence operations. This situation demands that intelligence organizations enhance their predictive analysis capabilities, utilize artificial intelligence, big data analytics, geospatial intelligence, and develop inter-agency intelligence sharing mechanisms to generate comprehensive situational awareness (Warner, 2023). Therefore, the success of an intelligence system is largely determined by the quality of coordination, information system interoperability, and human resource competency.

Intelligence theory serves as the primary foundation of this research because the variables studied focus on optimizing the role of intelligence in supporting early detection of security disturbances in vulnerable domestic areas. Based on this theory, intelligence effectiveness is measured not only by the ability to obtain information but also by the ability to transform that information into strategic recommendations that can be used to prevent threats before they develop into security crises. Therefore, this research seeks to develop strategies that can improve the effectiveness of the intelligence function by strengthening coordination, utilizing technology, and integrating information to support national defense strategies (Lowenthal, 2022; Warner, 2023).

3. Early Detection and Early Warning Theory

The theory of Early Detection and Early Warning explains that an organization's success in responding to threats depends heavily on its ability to recognize early indicators that point to the emergence of risks or disruptions before they develop into crises. This concept is widely applied in the fields of national security, disaster management, health, and defense because it enables decision-makers to take preventive action based on quickly and accurately obtained information. According to the United Nations Office for Disaster

Risk Reduction (UNDRR, 2022), an effective early warning system must have four main components: risk identification, a monitoring system, rapid information communication, and coordinated response capabilities.

In the context of national defense, early detection systems are a key function of intelligence, enabling the state to identify changes in the strategic environment before threats develop into real security disruptions. Advances in digital technology have expanded the scope of early detection through the use of cyber intelligence, open-source intelligence, geospatial intelligence, artificial intelligence, and big data analytics to monitor threat dynamics in real time. The integration of these various information sources enhances the state's ability to build situational awareness, enabling faster, more accurate, and evidence-based decision-making (Lowenthal, 2022).

The Early Detection and Early Warning theories are highly relevant to this research, as they serve as a conceptual basis for explaining how optimizing the role of intelligence can increase the effectiveness of preventing security disturbances in vulnerable domestic areas. An integrated early detection system enables early threat identification, enabling the government to implement preventive measures before threats escalate into conflict or crises that impact national stability. Therefore, this research views strengthening early detection capabilities as a strategic element in supporting the success of the nation's defense strategy amidst increasingly complex multi-domain threats (UNDRR, 2022; Lowenthal, 2022).

METHODOLOGY

This study adopts a qualitative descriptive research design to examine strategies for optimizing the role of intelligence in the early detection and prevention of security threats in domestic high-risk areas in support of Indonesia's national defense strategy. A qualitative approach was selected because it enables an in-depth understanding of complex and context-dependent phenomena by exploring participants' experiences, perceptions, and organizational practices within their natural settings (Creswell & Poth, 2018). The study is grounded in the assumption that intelligence effectiveness is shaped by the interaction of organizational structures, human resources, inter-agency coordination, technological capabilities, and the evolving strategic environment.

The research was conducted in West Kalimantan Province, a strategically significant border region adjacent to Malaysia that faces multidimensional security challenges, including transnational crime, human trafficking, narcotics smuggling, illegal border crossings, and other hybrid threats. Primary data were collected through semi-structured in-depth interviews, non-participant observations, and document analysis involving representatives from the National Intelligence Agency (BIN), Indonesian Armed Forces Strategic Intelligence Agency (BAIS TNI), Indonesian National Police, the Ministry of Defense, and academic experts in intelligence and defense. Informants were selected using purposive sampling, followed by snowball sampling to identify

additional participants with specialized expertise relevant to the research objectives (Sekaran & Bougie, 2016).

To enhance the credibility of the findings, the study employed source, method, and time triangulation, enabling cross-verification of interview data, field observations, and official documents (Creswell & Poth, 2018). Data analysis followed the Interactive Model of Analysis proposed by Miles, Huberman, and Saldaña (2020), consisting of data condensation, data display, and conclusion drawing and verification. In addition, a SWOT analysis was applied to identify organizational strengths, weaknesses, opportunities, and threats, providing a systematic basis for formulating strategic recommendations. This integrated methodological framework ensures that the proposed intelligence optimization strategy is empirically grounded, analytically robust, and practically relevant for strengthening Indonesia's early detection capability and supporting an adaptive national defense strategy (Miles et al., 2020).

RESEARCH RESULT

4.2.1 Current Condition of Intelligence Implementation in Early Detection for Preventing Security Threats in Domestic High-Risk Areas

The findings indicate that intelligence organizations in Indonesia have progressively strengthened their role in the early detection and prevention of security threats through the integrated implementation of intelligence collection, security, and influence operations. Intelligence activities have evolved beyond the traditional function of information gathering to encompass strategic analysis, threat forecasting, and policy recommendations for national decision-makers. This transformation reflects a shift from a reactive intelligence model towards a proactive and predictive approach capable of addressing increasingly complex and multidimensional security challenges (Lowenthal, 2022).

The study further reveals that intelligence operations generally follow the modern Intelligence Cycle , consisting of planning and direction, collection, processing, analysis, and dissemination. Intelligence products are produced through systematic verification, validation, and interpretation processes before being delivered to policymakers, ensuring that strategic decisions are supported by reliable and evidence-based intelligence. Consequently, the effectiveness of intelligence is determined not only by the quantity of information collected but also by the quality of analytical products capable of reducing uncertainty in national decision-making (Lowenthal, 2022).

Qualitative coding identified several interconnected themes, including intelligence operations, threat identification, early detection mechanisms, Early Warning System (EWS) effectiveness, inter-agency coordination, regulatory frameworks, technological capabilities, and international cooperation. These findings demonstrate that intelligence functions as an adaptive organizational system in which human resources, institutional governance, information technology, and analytical capacity interact to

produce comprehensive situational awareness. Continuous organizational learning and innovation therefore remain essential for maintaining intelligence effectiveness within an evolving strategic environment (Miles et al., 2020).

The research also confirms that intelligence contributes significantly to Indonesia's national defense strategy by providing early warning that enables preventive rather than reactive responses to emerging threats. Nevertheless, the implementation of the Early Warning System (EWS) remains uneven across regions due to disparities in technological infrastructure, information interoperability, and institutional capacity. Such limitations reduce the speed and consistency of intelligence dissemination and highlight the need for greater integration of national intelligence systems (Herman, 2020).

Another important finding concerns inter-agency cooperation. Intelligence organizations, including BIN, BAIS TNI, the Indonesian National Police, the Ministry of Defense, and regional governments, have established coordination mechanisms through information sharing, joint analysis forums, and operational communication. Although this collaborative approach has improved the quality of intelligence assessments, institutional fragmentation, sectoral interests, and limited interoperability continue to constrain effective intelligence integration. According to Lykke's Ends–Ways–Means framework , these challenges demonstrate that strategic objectives (Ends) are clearly defined, whereas implementation mechanisms (Ways) and enabling resources (Means) require further alignment to maximize intelligence effectiveness (Lykke, 2001).

The findings further indicate that Indonesia's security environment is increasingly characterized by hybrid threats , including cyberattacks, disinformation, transnational crime, terrorism, radicalisation, and other non-military threats. These developments require intelligence organizations to strengthen digital intelligence capabilities, big data analytics, artificial intelligence applications, and real-time information sharing in order to enhance predictive intelligence and support comprehensive national security (Buzan & Hansen, 2020; Hoffman, 2021).

Overall, the study concludes that the current implementation of intelligence in domestic high-risk areas is moderately effective but requires further improvements in institutional integration, technological modernization, interoperability, human resource development, and governance. Strengthening these strategic dimensions will enable intelligence organizations to provide faster, more accurate, and integrated early warning, thereby enhancing Indonesia's national defense strategy and resilience against increasingly complex security threats (David et al., 2020; Lowenthal, 2022).

The results of the analysis show that the organization is at:

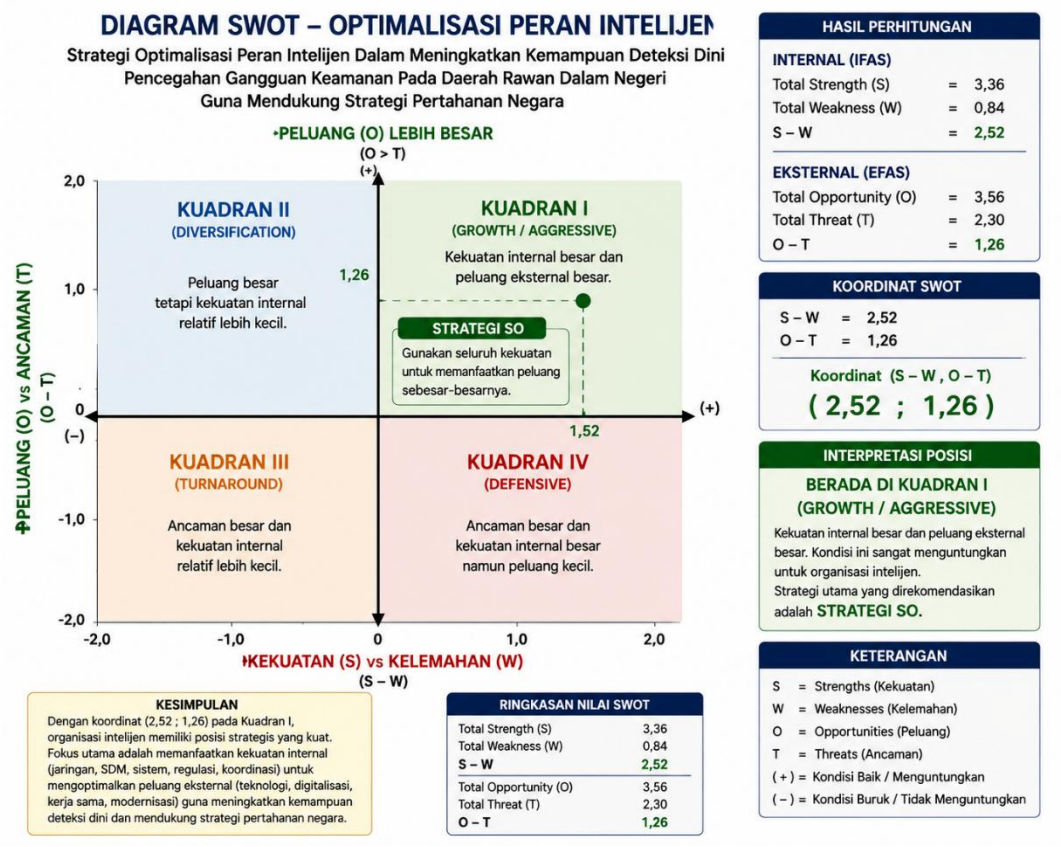

Figure 1 SWOT Quadrant

Source: Data Processed by Researchers, 2026

The SWOT analysis results indicate that the intelligence organization is in Quadrant I with coordinates (2.52; 1.26), indicating that internal strengths and external opportunities are more dominant than weaknesses and threats. This position indicates that the most appropriate strategy is a growth strategy, namely a strategy that utilizes all organizational strengths to capture strategic opportunities through innovation, digital transformation, and institutional capacity development. This condition indicates that the Indonesian intelligence organization has sufficient capital to modernize its intelligence system to improve early detection capabilities in preventing security disturbances in vulnerable areas within the country as part of strengthening the national defense strategy. In line with strategic management theory, organizations in a growth strategy position have the opportunity to build competitive advantage through the optimization of resources, organizational competencies, and strategic environmental support (David et al., 2020).

Research findings indicate that the most relevant priority strategy is the development of an Integrated Digital Intelligence System capable of connecting all stages of the intelligence cycle, from information collection and data processing to intelligence analysis, to delivering intelligence products to decision-makers in a fast, accurate, and integrated manner. This digital transformation is not only defined as the modernization of technological devices, but also as a comprehensive change to intelligence business

processes to produce strategic intelligence that supports national decision-making. This aligns with Lowenthal's (2022) view, which explains that modern intelligence organizations must be able to integrate various information sources into strategic intelligence that provides the government with a decision advantage in facing increasingly complex threat dynamics. Thus, digitalization becomes a force multiplier that increases the effectiveness of early detection while accelerating responses to potential security threats.

When analyzed using the Ends–Ways–Means theory, the resulting strategy demonstrates a balance between objectives (ends), implementation methods (ways), and resources (means) as proposed by Lykke (2001). The main objective to be achieved is to increase early detection capabilities in preventing the development of security disturbances, thereby supporting the national defense strategy. To achieve this goal, the study recommends various approaches, including the development of an Integrated Digital Intelligence System, strengthening inter-institutional interoperability, developing an Early Warning System (EWS), improving human resource competency, and strengthening cross-sector coordination. All of these strategies are supported by resources in the form of established intelligence networks, regulatory support, information technology developments, personnel operational experience, and the government's commitment to the digital transformation of the defense sector. The balance between these three elements indicates that the formulated strategy has a high level of implementability because each component supports each other in achieving strategic goals.

Research also shows that the success of intelligence transformation depends heavily on the quality of human resources. Technological modernization will not produce optimal results unless accompanied by increased personnel competency in utilizing Artificial Intelligence (AI), Big Data, Data Analytics, Open Source Intelligence (OSINT), machine learning, and multi-domain analysis techniques. Future intelligence analysts are no longer required to possess only conventional analytical skills, but must also be able to process large amounts of data, identify threat patterns, develop predictive analyses, and generate actionable intelligence as a basis for strategic decision-making. Lowenthal (2022) emphasized that the strength of a modern intelligence organization lies in the analyst's ability to transform raw data into accurate, relevant, and timely strategic information. Therefore, investment in education, training, professional certification, and mastery of digital technology are key factors in strengthening national intelligence capacity.

In addition to improving personnel competency, research reveals that the use of Artificial Intelligence and Big Data has significant potential in strengthening predictive intelligence capabilities. This technology enables intelligence organizations to analyze millions of data points from various sources simultaneously, thereby detecting patterns, anomalies, and threat trends that are difficult to identify through manual methods. This predictive analysis capability provides a longer lead time for the government to implement preventive measures before threats develop into real security disruptions.

Herman (2020) explains that an effective Early Warning System must be able to produce information that is timely, accurate, relevant, and actionable. Therefore, the development of an EWS based on Big Data and AI is one of the main strategies in building an early detection system that is more adaptive to multidimensional threats.

Further research findings indicate that strengthening coordination, synergy, and inter-institutional interoperability is a crucial prerequisite for enhancing the effectiveness of the national intelligence system. Successful early detection no longer relies on the capabilities of a single institution, but rather on effective collaboration between the State Intelligence Agency (BIN), the Indonesian National Armed Forces (TNI), the Indonesian National Police (Polri), the Ministry of Defense, local governments, and other ministries and institutions. Information integration through real-time information sharing mechanisms enables each institution to obtain a more comprehensive picture of threats, thereby enhancing the quality of strategic analysis. From a national security perspective, a whole-of-government approach is highly relevant because contemporary security threats are cross-sectoral and cannot be addressed in isolation (Buzan & Hansen, 2020). Therefore, developing information system interoperability is a key foundation for creating an integrated and responsive national intelligence system.

The research also emphasizes the importance of developing community intelligence as a strategy for strengthening early detection. The public is positioned as a strategic partner, acting as an early sensor, providing initial information on potential security threats. Advances in communication technology enable the public to quickly disseminate information through various digital platforms, thereby expanding the reach of intelligence gathering. This approach aligns with the concept of a universal defense system, which positions all components of the nation as part of the national defense system, according to their respective functions and capacities. With increased public participation, intelligence organizations' ability to detect threats at an early stage is strengthened, enabling national resilience to be built in a more participatory and sustainable manner.

The strategies generated by this research also have high relevance in addressing the increasingly complex development of hybrid threats. Current security threats are no longer limited to armed conflict, but have evolved through cyberattacks, disinformation, digital propaganda, transnational crime, economic pressure, and information manipulation exploiting technological advances. Hoffman (2021) explains that hybrid threats combine various military and non-military instruments simultaneously, thus requiring an intelligence system capable of rapid and adaptive multi-domain analysis. Therefore, the development of an Integrated Digital Intelligence System, Big Data-based EWS, AI, and enhanced intelligence analysis capabilities are appropriate strategies for enhancing national preparedness in facing hybrid threats.

Overall, the research findings indicate that the strategy for optimizing the role of intelligence must be directed at comprehensive organizational transformation through the digitization of intelligence systems, strengthening the Early Warning System, enhancing human resource competency, building inter-agency interoperability, developing

community intelligence, and utilizing Artificial Intelligence and Big Data technology. This strategy not only increases the effectiveness of early detection but also strengthens the quality of strategic intelligence, which serves as the basis for national defense decision-making. The synthesis of these findings suggests that the success of national defense strategies in the future is largely determined by the ability of intelligence organizations to build adaptive, collaborative, technology-based systems capable of integrating all information in real time. Thus, optimizing the role of intelligence not only results in increased early detection capabilities for various potential security threats but also strengthens national resilience through a modern, responsive, and prevention-oriented intelligence system in accordance with the demands of the contemporary strategic environment (David et al., 2020; Herman, 2020; Hoffman, 2021; Lowenthal, 2022; Buzan & Hansen, 2020).

CONCLUSIONS

Based on the research results, it can be concluded that the Indonesian intelligence organization is in a strategic position to undertake institutional transformation to improve its early detection capabilities against domestic security threats. The SWOT analysis, which places the organization in Quadrant I, indicates that internal strengths and external opportunities can be optimally utilized through growth strategies based on innovation, digitalization, and strengthening organizational capacity. The main recommended strategy is the development of an Integrated Digital Intelligence System capable of optimizing the entire intelligence cycle through the use of Artificial Intelligence, Big Data, Early Warning Systems, and predictive analysis. The success of this strategy is largely determined by improving human resource competency, strengthening inter-agency interoperability, and establishing *a whole-of-government coordination mechanism* . Furthermore, community involvement through *community intelligence* is a crucial element in expanding early detection capabilities against threats. Thus, optimizing the role of intelligence not only strengthens the prevention function but also supports the national defense strategy through an intelligence system that is adaptive, integrated, and responsive to the development of multidimensional threats.

BIBLIOGRAFI

Aspinall, E., & Mietzner, M. (2019). Problems of democratization in Indonesia: Elections, institutions and society. Institute of Southeast Asian Studies.

Buzan, B. (1991). People, states and fear: An agenda for international security studies in the post-Cold War era (2nd ed.). Lynne Rienner Publishers.

Buzan, B., & Hansen, L. (2020). The evolution of international security studies. Cambridge University Press.

Clausewitz, C. von. (1976). On war (M. Howard & P. Paret, Eds. & Trans.). Princeton University Press. (Original work published 1832).

Creswell, J. W., & Poth, C. N. (2018). Qualitative inquiry and research design: Choosing among five approaches (4th ed.). SAGE Publications.

Dahl, E. J. (2013). Intelligence and surprise attack: Failure and success from Pearl Harbor to 9/11 and beyond. Georgetown University Press.

David, FR, David, FR, & David, ME (2020). Strategic management: A competitive advantage approach, concepts and cases (17th ed.). Pearson.

Gray, C.S. (2020). Modern strategy (Updated ed.). Oxford University Press.

Hill, C.W.L., Schilling, M.A., & Jones, G.R. (2021). Strategic management: Theory and cases (14th ed.). Cengage Learning.

Jensen, B. M. (2019). The cyber character of political warfare. Oxford University Press.

Johnson, L. K. (2017). Handbook of intelligence studies. Routledge.

Johnson, L. K. (2020). National security intelligence (3rd ed.). Polity Press.

Lincoln, Y.S., & Guba, E.G. (1985). Naturalistic inquiry. SAGE Publications.

Lowenthal, M. M. (2022). Intelligence: From secrets to policy (9th ed.). CQ Press.

Lykke, A. F. (2001). Toward an understanding of military strategy. US Army War College.

Merriam, S. B., & Tisdell, E. J. (2016). Qualitative research: A guide to design and implementation (4th ed.). Jossey-Bass.

Miles, M.B., Huberman, A.M., & Saldaña, J. (2020). Qualitative data analysis: A methods sourcebook (4th ed.). SAGE Publications.

Moleong, LJ (2021). Qualitative research methodology (Revised edition). PT Remaja Rosdakarya.

Nye, J. S. (2020). Do morals matter? Presidents and foreign policy from FDR to Trump. Oxford University Press.

Patton, M. Q. (2015). Qualitative research & evaluation methods (4th ed.). SAGE Publications.

Rangkuti, F. (2023). SWOT Analysis: Techniques for Dissecting Business Cases (Revised Edition). PT Gramedia Pustaka Utama.

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

Sekaran, U., & Bougie, R. (2016). Research methods for business: A skill-building approach (7th ed.). Wiley.

Sugiyono. (2023). Qualitative research methods (4th Edition). Alfabeta.

Sun Tzu. (2005). The art of war (SB Griffith, Trans.). Oxford University Press.
Warner, M. (2023). The rise and fall of intelligence: An international security perspective. Georgetown University Press.
Yin, R. K. (2018). Case study research and applications: Design and methods (6th ed.). SAGE Publications.

Akter, S., Michael, K., Uddin, M.R., McCarthy, G., & Rahman, M. (2021). Transforming business using digital innovations: The application of AI and big data analytics. Journal of Big Data, 8(1), 1–27.
Gürel, E., & Tat, M. (2021). SWOT analysis: A theoretical review and its application in strategic management. Journal of Business Research, 134, 124–135.
Herman, M. (2020). Intelligence and warning in contemporary security environments. Intelligence and National Security, 35(6), 807–822.
Hoffman, F.G. (2021). Hybrid threats and contemporary conflict: Evolution of modern warfare. Joint Force Quarterly, 101(2), 14–23.
Mantovani, M., & Berni, M. (2020). Strategy and the ends–ways–means paradigm in contemporary security studies. Journal of Strategic Studies, 43(6–7), 945–968.
Raska, M. (2021). Military modernization and defense innovation in the Indo-Pacific: Strategic implications for regional security. Journal of Indo-Pacific Affairs, 4(2), 1–19.

ASEAN. (2020). ASEAN Political-Security Community Blueprint 2025. ASEAN Secretariat.
Geospatial Information Agency. (2023). Indonesian geospatial information 2023. BIG.
State Intelligence Agency. (2023). State Intelligence Agency Performance Report. BIN.
National Narcotics Agency. (2024). Indonesia Drugs Report 2024. BNN.
National Narcotics Agency of the Republic of Indonesia. (2024). BNN RI Annual Report 2024. BNN RI.
National Border Management Agency. (2024). BNPP Performance Report 2024. BNPP.
National Counterterrorism Agency. (2025). BNPT Performance Report 2024. BNPT.
Central Bureau of Statistics. (2024). Indonesian Statistics 2024. BPS.
Central Statistics Agency of West Kalimantan Province. (2025). West Kalimantan Province in Figures 2025. BPS West Kalimantan Province.
National Cyber and Crypto Agency. (2024). National Cyber Security Report 2024. BSSN.
National Cyber and Crypto Agency. (2024). Indonesian Cyber Security Annual Report 2024. BSSN.
European Center of Excellence for Countering Hybrid Threats. (2023). Hybrid Threats: Trends and Future Challenges. Hybrid CoE.
Ministry of Defense of the Republic of Indonesia. (2015). Indonesian Defense White Paper. Ministry of Defense of the Republic of Indonesia.
Ministry of Defense of the Republic of Indonesia. (2023). Indonesian Defense White Paper 2023. Ministry of Defense of the Republic of Indonesia.
Ministry of Defense of the Republic of Indonesia. (2023). Indonesian National Defense Doctrine. Ministry of Defense of the Republic of Indonesia.

Ministry of Defense of the Republic of Indonesia. (2024). National Defense Policy 2024. Ministry of Defense of the Republic of Indonesia.
National Resilience Institute of the Republic of Indonesia. (2023). Study of Indonesian National Resilience. Lemhannas RI.
LIPI. (2021). Dynamics of Social Conflict in Indonesia. LIPI.
North Atlantic Treaty Organization. (2022). NATO Strategic Concept 2022. NATO.
West Kalimantan Regional Police. (2024). Profile of the Security Intelligence Directorate of the West Kalimantan Regional Police. West Kalimantan Regional Police.
West Kalimantan Regional Police. (2024). West Kalimantan Regional Police Annual Report 2024. West Kalimantan Regional Police.
Indonesian National Army. (2024). Report of the RI–Malaysia Border Security Task Force. Indonesian Army.
United Nations Office for Disaster Risk Reduction. (2022). Early Warning Systems for Risk Reduction. UNDRR.
United Nations Office on Drugs and Crime. (2023). Global Report on Transnational Organized Crime. UNODC.
United Nations Office on Drugs and Crime. (2023). Transnational Organized Crime in Southeast Asia. UNODC.
United Nations Office on Drugs and Crime. (2024). Transnational Organized Crime in Southeast Asia: Regional Report. UNODC.
World Economic Forum. (2025). The Global Risks Report 2025. World Economic Forum.