**JOIN (Jurnal Online Informatika)**
p-ISSN: 2528-1682, e-ISSN: 2527-9165
Volume 11 Number 1 | January 2026: 231-242
DOI: 10.15575/join.v11i2.1747

# Defense Policy Strategy based on Network Centric Warfare (NCW) toward Asymmetric Threats: Case study from an Indonesian Perspective

**I Nengah Putra[1], April Kukuh Susilo[2]**
[1]Indonesia Defense University, IPSC Sentul, Sukahati, Citeureup, Bogor, Jawa Barat, Indonesia
[2]Sekolah Tinggi Teknologi Angkatan Laut, Morokrembangan, Surabaya, Jawa Timur, Indonesia

**Article Info**

***Article history:***

Received July 9, 2025
Revised December 6, 2025
Accepted December 8, 2025
Published May 15, 2026

***Keywords:***

Asymmetric threats
Command Control Communications
Defense Strategy Intelligence
Network Centric Warfare
Policy Strategy
Reconnaissance

**ABSTRACT**

Implementation of NCW as a core element of defense policy requires a comprehensive strategic framework. Without these basic elements, NCW may remain underutilized or fail to deliver the desired results in the face of asymmetric threats. Therefore, it is important to explore a Network Centric Warfare (NCW)-based defense strategy in addressing asymmetric threats. This paper seeks to analyze the formulation of a defense policy strategy based on the principles of Network Centric Warfare (NCW) to effectively address asymmetric threats by exploring the theoretical foundations of NCW in Indonesia Perspective. The analysis of NCW implementation strategies focuses on information superiority, communication speed, and cross-unit coordination as strategic solutions for detecting and responding to non-linear attack patterns. NCW-based defense strategies require inter-sectoral synergy as part of a holistic national security approach. Given the nature of asymmetric threats, which often involve non-state actors and span multiple domains (physical, digital, social), collaboration between the Indonesian National Armed Forces (TNI), the Indonesian National Police (Polri), the National Cyber and Cryptography Agency (BSSN), the State Intelligence Agency (BIN), and government and private institutions is crucial. NCW provides a technological framework and systems that can integrate these various actors into a national defense strategy that is responsive, adaptive, and collaborative in addressing the complexity of contemporary threats. The primary contribution of this paper is to formulate a defense policy strategy based on Network-Centric Warfare (NCW) principles, which is not only important for assessing NCW in the naval domain but also has potential application in a joint, interagency environment in Indonesia.

***Corresponding Author:***

I Nengah Putra,
Informatics Indonesia Defense University
IPSC Sentul, Sukahati, Citeureup, Bogor, Jawa Barat 16810
Email: nengahputra35@gmail.com

## 1. INTRODUCTION

Asymmetric warfare, characterized by disparities in resources and tactics between the warring parties, poses unique challenges to conventional defense strategies [1], [2]. Traditional military strategies, often focused on large-scale deployments of forces, are likely to prove inadequate to address the multifaceted nature of asymmetric threats. Traditional definitions of security in terms of the protection of territory and sovereignty are being replaced by new security concepts that include the protection of information, knowledge, and technological assets [3]. The expanding scope of security due

p-ISSN: 2528-1682
e-ISSN: 2527-9165

to globalization means that the definition of security and the struggle to protect it will occur not only on the battlefield, but also in unconventional places against non-traditional security threats [4].

In conventional warfare, military action, supported by diplomacy, information operations, and economic pressure, is the primary mechanism for achieving the ultimate goal. Politics as a mechanism for goal realization dominates during the planning and preparation for conflict, but becomes secondary during the conflict itself [5]. In other words, politics in conventional conflicts is not dominant during the conduct of war, which makes it possible to distinguish between different actors: the government that guides the operations, the population that provides the means, and the military that uses them [2]. The beginning of the third millennium was accompanied by an increase in local conflicts and violence, as well as in terrorist attacks. These conflicts are often asymmetric, where one state or group has much greater power than its opponent. Often, the response to asymmetric violence is increased support, within the stronger party, for retaliatory aggression against weaker, vulnerable, and often dependent outside groups [6].

One of the fundamental issues the post-9/11 world must grapple with is the new meaning of security, marked by asymmetric threats. Security implies freedom from threats to core values (e.g., the protection of national sovereignty and territory) for both individuals and groups, but there is considerable disagreement about whether the primary focus of security should be at the individual, state, or international level. In the traditional sense of the term, security means national security and is largely defined in military terms. As a result, the primary area of interest for academics and statesmen has tended to be the military capabilities that states must have to defeat the threats they face [4].

In the contemporary world, states have professional militaries and capable intelligence services, and are less concerned with the prospect of conventional invasion by their neighbors. In contrast to historical experience, it appears that in the 21st century, the primary security threats are posed by hostile acts not attributable to aggressive nation states, as well as violence perpetrated by extremists, terrorists, and organized crime (non-state actors). These actors share the characteristic that they do not exist within defined territorial and legislative boundaries. Furthermore, this type of actor initiates conflicts and uses unconventional tactics to achieve political or other goals [2].

Asymmetric threats are dynamic, and attackers' techniques are constantly evolving. This model uses adaptive learning but still requires time to recognize and respond to new threat patterns [7]. The role of politics in asymmetric conflicts is very different. Given that both parties in the conflict are trying to influence public opinion, the political positions of both parties are paramount; the insurgents are trying to gain the trust and loyalty of the population while the counterinsurgents are trying to prevent the population from falling under the influence of the insurgents. In asymmetric conflicts, due to the specificity of the objectives and conduct of the conflict itself, politics is an active mechanism that ensures that every military action is viewed through the prism of potential costs and potential benefits. In conclusion, the key to the success of Asymmetric Threats is effective governance, as the entire conflict and its outcome are largely determined by the success of each party in gaining and maintaining credibility among the population [2].

In the context of globally connected knowledge through complex adaptive connections of every description, terrorists exploit the very strategic power of the networked society, its openness and connectivity, to send shock waves that channel its flows of images, information, technology, people, and capital. We are only beginning to appreciate how shock waves will amplify the power of attacks as they move through the connectivity of the global society. Some clues to the likely nature of the wars already being waged are available from the new strategic discourse on Network Centric Warfare (NCW) developed by the US strategic community during the 1990s [8]. Integrating NCW principles into defense policy is critical for modern militaries seeking to maintain strategic superiority over adversaries using asymmetric tactics [9].

Network-centric warfare (NCW) is an emerging theory of warfare based on the concepts of nonlinearity and complexity. According to NCW doctrine, all combat entities, such as warfighters, manned and unmanned platforms, and command and control (C2) centers, are connected through a network architecture to share the battle situation. For example, network nodes are dynamically placed as entities are moved; traffic between nodes also changes whenever they interact in joint operations.

Thus, NCW should be analyzed based on communication interactions, which primarily include inter-entity traffic and intra-entity mobility [10]. The NCW concept emphasizes the transformation of military operations through increased connectivity between forces, enabling real-time information sharing and collaborative decision-making. By using networks to synchronize actions across multiple domains (land, air, sea, and cyber), militaries can achieve greater operational coherence and responsiveness [11].

NCW is characterized by the integration of robust computer networks with detectors, adapters, command and control centers, and weapons systems on the battlefield into a unified system that enables data fusion, dynamic coordination, information sharing, and the effective use of weapons systems. NCW supports superior decision-making and rapid response within the tactical time cycle, thereby providing advantages in speed, capacity, operational range, and command and control accuracy (Liang & Zhang, 2004). As illustrated in Figure 1, the NCW network architecture connects multiple operational entities, including detectors, adapters, command and control centers, weapon control stations, and node switches or routers through an IP backbone network. This architecture shows how battlefield information can be distributed across interconnected nodes to support coordination, situational awareness, and timely decision-making.

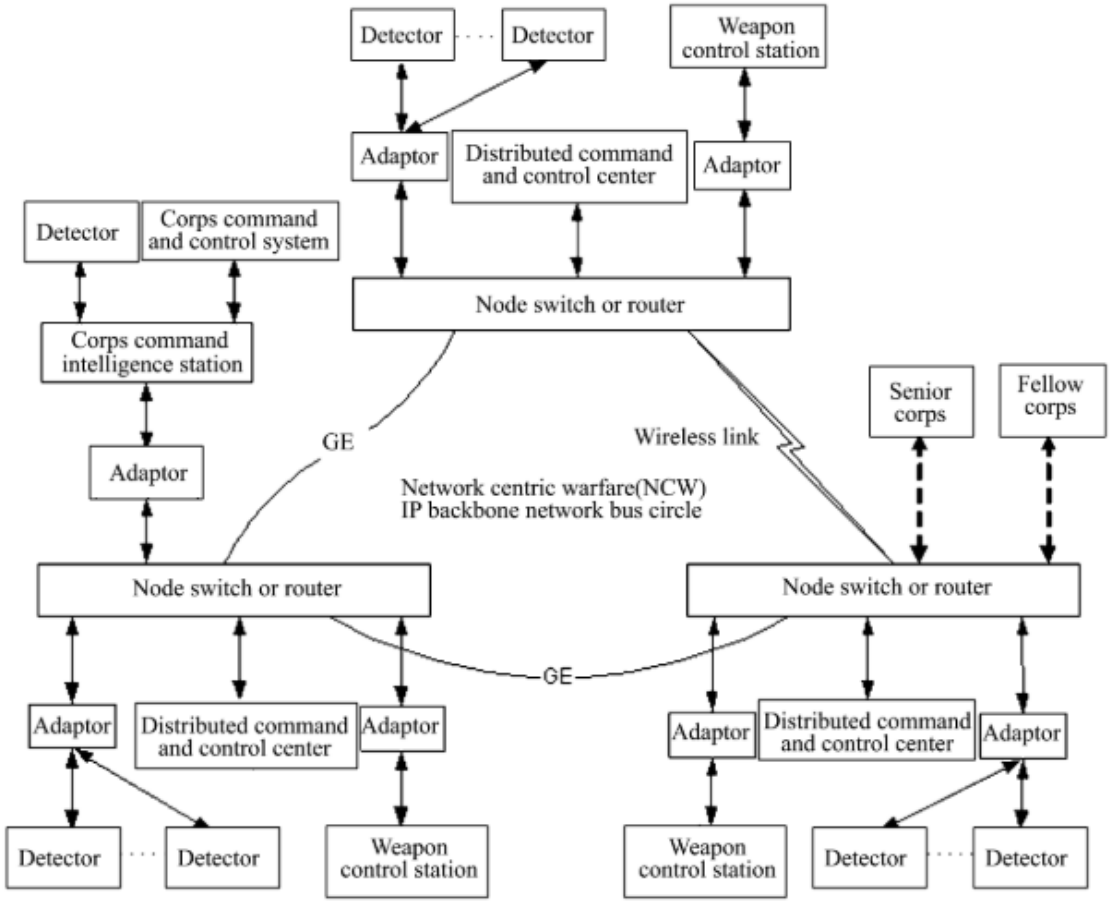


Figure 1. Schematic diagram of NCW network architecture.
Source: Liang & Zhang [13]

Network Centric Warfare (NCW) recognizes the centrality of information and its potential as a source of power. The RAND Corporation defines NCW as, "...the linking of multiple platforms into a shared awareness network to gain information superiority, penetrate the adversary's decision cycle, and rapidly end conflict." NCW is not just about technology, but about the emerging military response to the information age. NCW involves networks across all three domains and exhibits the following characteristics [22], [23]:

p-ISSN: 2528-1682
e-ISSN: 2527-9165

a. Physical Domain: All elements of the force are robustly connected to achieve secure and seamless connectivity and interoperability.
b. Information Domain: The force can share, access, and protect information to a level that enables it to establish and maintain information superiority over the adversary. In addition, the force can collaborate in the information domain, allowing the force to improve its information position through the processes of correlation, fusion, and analysis.
c. Cognitive Domain: The force has the ability to develop high-quality awareness and share this awareness. The force can also develop a shared understanding, including the commander's intent. In addition, the force can self-synchronize its operations.

Non-traditional or emerging threats demand new ways to drive rapid, well-coordinated crisis options. By their nature, transnational and asymmetric threats require multi-partner solutions. New data mining techniques and assessment methodologies offer tools to help predict early signs of crisis. New information technologies can be leveraged to rapidly establish crisis response teams within alliances, providing seamless access to relevant data and joint consultation for team members in widely disparate locations. New information assurance techniques can also help create the necessary barriers to protect certain categories of sensitive information [12].

The increasing relevance of NCW is particularly significant in addressing asymmetric threats, which often operate outside the bounds of conventional warfare norms (Liang & Zhang, 2005). Asymmetric actors tend to exploit weaknesses in traditional defense systems, employ irregular tactics, and use technological tools in unexpected ways. Consequently, a defense policy that incorporates NCW principles can provide a dynamic and adaptive response mechanism that is well suited to countering the fluid and elusive nature of asymmetric challenges [14]. By enhancing interoperability, speed, and precision, an NCW-based strategy enables a proactive rather than a reactive stance in national defense.

Despite its potential, the implementation of NCW as a core element of defense policy requires a comprehensive strategic framework. This includes the development of secure and robust communication networks, the integration of advanced surveillance and reconnaissance systems, and the development of a digitally literate military workforce [15]. Furthermore, such a strategy must be supported by strong political will, interagency coordination, and sustained investment in research and innovation. Without these basic elements, NCW may remain underutilized or fail to deliver the desired results in the face of asymmetric threats [8]. Therefore, it is important to explore a Network Centric Warfare (NCW)-based defense strategy in addressing asymmetric threats.

This paper aims to analyze the formulation of a defense policy strategy based on Network Centric Warfare principles to effectively counter asymmetric threats by exploring the theoretical underpinnings of NCW, examining its practical applications in various defense contexts, and assessing its relevance to contemporary security challenges. Theoretically, this study contributes to the academic discourse on national defense by enhancing the conceptual integration of NCW in security doctrine. In practical terms, this study provides actionable recommendations for defense policymakers, including strategies for infrastructure development, organizational reform, and human resource training. This contribution is intended to support the development of a resilient and responsive national defense system in an increasingly complex global security environment. The primary contribution of this paper is to formulate a defense policy strategy based on Network-Centric Warfare (NCW) principles, which is not only important for assessing NCW in the naval domain but also has potential application in a joint, interagency environment in Indonesia.

## 2. METHOD

This study uses a literature review method, described qualitatively within a descriptive approach. The qualitative descriptive approach uses scientific thinking grounded in a theory to obtain research data in the form of words and images that can be described. A qualitative descriptive design is appropriate for this research because the objective is to understand defense strategies grounded in Network Centric Warfare (NCW) principles to effectively address asymmetric threats, by exploring the theoretical foundations of NCW from an Indonesian perspective.

Data collected through a qualitative descriptive approach is analyzed in the form of words, images, or behavior, and cannot be expressed in numbers [35]. The data collection framework involved a literature review supported by semi-structured interviews, as this allows for information gathering using questions related to the research objectives to describe their experiences with Network Centric Warfare (NCW) principles in addressing asymmetric threats.

This method was chosen because the research focuses on theoretical exploration of the validity and reliability of instruments in the realm of educational research. Through extensive literature from credible scientific sources such as methodology books, national and international journal articles, and official documents, an in-depth understanding can be achieved without collecting data directly in the field [36]. In addition, this study is supported by expert opinions to strengthen the qualitative analysis of background experience in network and information systems. Twelve experts supported the research with a minimum education level of a bachelor's degree. Detailed information about the experts is presented in Table 1.

Table 1. Demographic information of experts

| Expert | Field | Position | Experience |
|---|---|---|---|
| **E1-E4** | Doctoral in Defense Policy Strategy | Academic | >25 years |
| **E4-E6** | Expert in Network Systems | Professional | >15 years |
| **E7-E9** | Expert in Cyber Systems | Professional | >15 years |
| **E10-E12** | Expert in Information Systems and Networks Industry | Academic & Professional | >25 years |

The research stages include problem identification as the initial step in defining the study's focus, collecting secondary data through relevant literature, and analyzing the content. The preparation phase in content analysis and the data recognition phase in thematic analysis are equivalent. Researchers are expected to transcribe interviews and gain an overall picture by reading the transcripts. Although thematic analysis researchers are primarily advised to consider both latent and manifest content in data analysis, content analysts can choose between manifest (developing categories) and latent (developing themes) content before proceeding to the next stage of data analysis.

Gathering codes based on subcategories/subthemes or potential categories/themes, and comparing emerging code clusters together and in relation to the overall data set constitutes the next stage of data analysis, called the organizing phase in content analysis. The same set of analytical interventions used in content analysis are applied in thematic analysis, with classification generating initial codes, defining and naming themes, reviewing themes, and searching for themes.

The final stage of data analysis in both approaches concerns reporting the results of the previous stages. This stage is specifically highlighted as the final opportunity for data analysis in thematic analysis. Furthermore, both approaches encourage researchers' creativity in presenting their findings in the form of storylines, maps, or models. This approach is considered effective for presenting an objective and comprehensive picture and for enabling critical evaluation of emerging theoretical perspectives. Therefore, the study results make a significant contribution to the development of research methodology related to defense policy strategy.

## 3. RESULT AND DISCUSSION

### *3.1 Defense Policy Strategy Based on Network Centric Warfare (NCW) in Facing Asymmetric Threats*

In the modern era marked by advances in information and communication technology, the Network Centric Warfare (NCW)-based defense policy strategy is becoming increasingly relevant to deal with asymmetric threats. NCW offers an approach that integrates various military and civilian elements through interconnected networks, enabling faster, more responsive decision-making in response to ever-changing threat dynamics. By utilizing sensor capabilities, advanced communication systems, and big data analysis, NCW not only increases operational effectiveness but also strengthens collaboration between defense and security institutions. In this context, a deep understanding of the characteristics of asymmetric threats—which are often unconventional and difficult to predict—is key to formulating an

p-ISSN: 2528-1682
e-ISSN: 2527-9165

effective strategy in maintaining national stability and security. Therefore, there is an analysis of the strategy for implementing NCW in sustainable defense policies to ensure readiness to face future challenges.

**a. Characteristics of Asymmetric Threats and Challenges**

Asymmetric threats are a form of threat that is not balanced in terms of military strength, strategy, and the actors involved. Unlike conventional warfare that openly involves a country's military strength, asymmetric threats are often carried out by non-state actors such as terrorist groups, separatists, armed criminals, or cyber actors. They do not operate in regular military formations, but use unconventional methods such as guerrilla attacks, sabotage, propaganda, and ideological infiltration. These characteristics make asymmetric threats more difficult to detect and counter using traditional military approaches.

The main challenge in dealing with asymmetric threats is their hidden, flexible, and adaptive nature. Perpetrators often exploit gaps in security systems, fragile socio-political conditions, and technological advances such as the internet to spread ideology or carry out cyber-attacks. In addition, asymmetric attacks are often not aimed at achieving military victory, but rather to create fear, chaos, and national instability. This requires the government and security forces to always be on alert, even in peaceful situations.

The response to asymmetric threats cannot only rely on military power, but also requires a multidimensional approach involving intelligence, diplomacy, law enforcement, and social and cultural approaches. A defense system is needed that is capable of carrying out early detection, rapid response, and effective cross-sector coordination. It is in this context that strategies such as Network Centric Warfare become relevant, because they provide advantages in information management and coordination between stakeholders to deal with complex and widespread threats.

**b. Network Centric Warfare (NCW) as a New Defense Paradigm**

Network Centric Warfare (NCW) is a new paradigm in modern defense strategy that focuses on the integration of information systems and communication networks to create information superiority and combat superiority. In this approach, military strength is no longer determined solely by the number of troops or weapons owned, but by the ability to connect various defense components - such as command, sensors, shooters, and support units - in a real-time integrated information network. With this connectivity, each element has access to data and operational situations simultaneously, allowing for much faster and more precise coordination and decision-making.

The NCW paradigm is based on the principle that "shared awareness" of the battle situation will produce greater synergy and increase mission effectiveness. Information obtained from various sensors (e.g. satellites, drones, radars) can be analyzed and disseminated directly to all relevant combat elements. This allows each unit, from the command base to the frontline troops, to act based on the same understanding of the battle conditions. As a result, NCW accelerates the OODA loop (Observe, Orient, Decide, Act) cycle, which is the core of excellence in military operations.

The implementation of NCW also demands structural and cultural transformation in military organizations. The traditional hierarchical command system must be replaced by a more flexible and decentralized structure, where small units can operate independently but remain integrated into a large network. In addition, mastery of information technology and cybersecurity is a key component in ensuring the effectiveness of NCW. Without strong protection of networks and data, information superiority can become a weak point exploited by the enemy, especially in the context of cyber warfare.

As a new paradigm, NCW has high relevance in facing contemporary threats, especially asymmetric threats that are stealthy, fast, and unpredictable. With the ability to detect threats early and deploy coordinated responses, NCW is able to provide flexibility and precision in defense operations. Moreover, NCW also opens up opportunities for collaboration between sectors, such as the military, intelligence, homeland security, and the private sector in building an adaptive and technology-based national defense system.

### c. NCW-based Defense Strategy in Dealing with Asymmetric Threats

Network Centric Warfare (NCW) based defense strategy offers an adaptive and responsive approach in dealing with asymmetric threats, such as terrorism, cyber warfare, separatist movements, and non-military infiltration. Unlike conventional conflicts that usually involve open military forces, asymmetric threats are hidden, unpredictable, and exploit gaps in the defense system. Therefore, NCW which focuses on information superiority, speed of communication, and cross-unit coordination, is the right strategic solution in detecting and responding to these non-linear attack patterns.

In this context, the advantage of NCW lies in the ability of the network system to connect various intelligence, military, and non-military elements in one integrated information ecosystem. Surveillance sensors, satellite systems, big data analytics, and patrol units in the field can share information in real time. This allows early identification of enemy movements, cyber-attack patterns, infiltration of terrorist elements, or other hidden threats. That way, the response given can be carried out faster, more targeted, and with minimal risk to casualties or damage to infrastructure.

This strategy also facilitates the improvement of operational capabilities of troops by strengthening situational awareness at all levels of command and combat units [28], [37]. When the threat does not come in the form of a conventional military formation, NCW allows small units on the front line to make tactical decisions autonomously but still in integrated strategic coordination. This is very important in dealing with sporadic attacks such as sabotage, hijacking, or local terror that require a quick response without having to wait for hierarchical orders from the command center.

NCW-based defense strategy demands synergy between sectors as part of a holistic national security approach. Given the asymmetric nature of threats that often involve non-state actors and are cross-domain (physical, digital, social), collaboration between the TNI, Polri, the National Cyber and Crypto Agency (BSSN), the State Intelligence Agency (BIN), and government and private agencies is crucial. NCW provides a technological and system framework that can integrate these various actors in a national defense strategy that is responsive, adaptive, and collaborative to the complexity of today's threats.

### d. Implementation of Network Centric Warfare (NCW) from an Indonesian Perspective

Implementation of a Network Centric Warfare (NCW)-based defense strategy in the context of Indonesia faces its challenges, given the geographical characteristics of the archipelagic country, the diversity of threats, and the limitations of defense infrastructure and technology. However, this strategy remains relevant and crucial in increasing deterrence against increasingly complex asymmetric threats, such as terrorism, digital radicalism, cyber-attacks on vital national infrastructure, and infiltration of foreign powers through non-military channels [38]. By utilizing the NCW approach, the TNI can build command, control, communication, computer, intelligence, surveillance, and reconnaissance (C4ISR) capabilities more effectively and in an integrated manner.

In practice, Indonesia has begun to build several supporting elements of NCW, such as the development of an integrated radar system, communication satellites, and the integration of cross-dimensional command systems under the Joint Regional Defense Command (Kogabwilhan) organization. This system aims to create an interconnected information network between the Army, Navy, and Air Force, and support military operations other than war (OMSP) such as countering terrorism and natural disasters. However, the development of this network is still partial and requires acceleration of integration and modernization of communication and sensor systems in all strategic areas, especially on the border and conflict-prone areas.

The implementation of NCW also requires increasing human resource capacity, both in terms of technical, tactical, and strategic aspects. The TNI needs to equip soldiers with operational capabilities based on information technology and data analytics, as well as develop cyber defense units and operational drones that are able to operate independently but are integrated into the central system. In addition, increasing interoperability between the TNI and other security agencies, such as the National Police, BSSN, and BIN is very important so that information can be absorbed and disseminated quickly to anticipate potential asymmetric threats that cross domains.

The success of implementing the NCW-based defense strategy in Indonesia is highly dependent on the sustainability of the national defense modernization policy, adequate budget allocation, and commitment to developing an inclusive and responsive digital defense ecosystem. Strategic policies are

p-ISSN: 2528-1682
e-ISSN: 2527-9165

also needed that regulate the synergy between the domestic defense industry, research institutions, and the national digital private sector to create an NCW system that is not only resilient but also in accordance with the unique needs of Indonesia as an archipelagic country with ever-growing asymmetric threats.

### *3.2 Discussion*

In this modern era, asymmetric threats are increasingly complex and require a new approach in defense strategy [18], [39]. Network Centric Warfare (NCW) as a new paradigm in defense offers an effective solution by integrating various defense elements through interconnected information networks [40]. This approach allows for faster and more responsive decision-making to unconventional threats, such as terrorism, separatist movements, and cyber-attacks.

The advantage of Network-Centric Warfare (NCW) lies in its ability to create real-time situational awareness across command levels, which is critical in dealing with unpredictable and hidden threats. By utilizing information and communication technologies, NCW enables the integration of data from multiple sources, including sensors, combat platforms, and intelligence [41]. This provides a clearer picture of the situation on the ground, so that decision-makers can respond quickly and effectively to emerging threats. In this context, NCW is not just a military strategy, but also a holistic approach that prioritizes collaboration between units and stakeholders to achieve common goals in maintaining national security [42].

The relevance of NCW increases with the increasing complexity of asymmetric threats in the modern world. Threats such as terrorism, cyber warfare, and unconventional conflicts demand a more flexible and responsive adaptation of military strategies [39]. In this regard, NCW provides a framework that allows the armed forces to operate synergistically and efficiently. Thus, the implementation of NCW becomes essential in maintaining national security because it not only increases operational effectiveness but also strengthens the ability to detect potential threats early.

Asymmetric threats, often carried out by non-state actors, exploit the imbalance of power between the parties involved [43]. Unlike conventional warfare, these threats are more covert and operate under unpredictable conditions [4]. For example, terrorists or separatist groups use unconventional methods, such as guerrilla attacks, sabotage, or propaganda, to create fear and chaos in society. This makes asymmetric threats very difficult to detect with traditional military approaches that rely on physical force or hierarchical structures [19]. Therefore, an NCW-based defense strategy that emphasizes the integration of information and communication systems is very important in creating synergy between various parties, both military and non-military, in responding to these threats effectively.

As a new paradigm in defense strategy, NCW offers a very different approach from traditional methods. NCW focuses on the integration of various defense elements in an information network that enables shared awareness of the operational situation [11], [24]. This enables fast, precise, and coordinated decision-making between the various units involved. For example, with the use of technologies such as satellites, drones, radars, and other sensor systems, information obtained from various sources can be analyzed and disseminated to all relevant units. Thus, every unit, from the central command to the troops in the field, can act based on the same understanding of the situation, which increases efficiency and effectiveness in responding to asymmetric threats [9], [44].

However, the implementation of NCW also requires a transformation in the structure and culture of military organizations. The hierarchical command system must be replaced by a more decentralized structure, where small units can operate independently while remaining connected to a larger information network [8]. This approach provides flexibility in decision-making, which is particularly important when dealing with asymmetric threats that do not always manifest as open combat. In addition, NCW requires greater technical capacity and cybersecurity, as the information advantage gained can become a weakness if not properly protected [10]. Therefore, technical readiness and data protection are key to maintaining NCW's effectiveness.

Indonesia, as the world's largest archipelagic country, faces unique geographic challenges in implementing a Network-Centric Warfare (NCW) strategy. With more than 17,000 islands spread along the equator, maritime territory management and surveillance are extremely complex. The existence of an integrated radar system and communication satellites is an important step to improve the ability to detect and respond to threats that may emerge from the sea. In addition, the integration of the cross-dimensional command system under the Joint Defense Area Command (Kogabwilhan) aims to create synergy among different armed forces, enabling them to respond to threats more quickly and effectively.

However, challenges remain in terms of ensuring that all these elements function harmoniously and in an integrated manner. On the other hand, although these steps show progress, there are still significant shortcomings in terms of modernizing defense infrastructure, especially in border areas and conflict-prone areas. Limited resources and technology are obstacles in accelerating the development of an information technology-based defense system needed to create an adaptive and resilient defense. Therefore, Indonesia needs to strengthen international cooperation and investment in research and development to overcome these shortcomings. Thus, the country can build a defense capacity that is not only capable of facing asymmetric threats but also adapting to the ever-changing dynamics of global security.

In addition, the implementation of the NCW strategy in Indonesia also requires an increase in human resources that can operate and utilize high technology. The development of cyber defense units and the operation of drones as part of the defense fleet must be encouraged. In the context of asymmetric threats, Indonesia must also strengthen collaboration between the TNI, Polri, the National Cyber and Crypto Agency (BSSN), the State Intelligence Agency (BIN), and the private sector involved in digital security. This collaboration is very important to ensure that the information collected can be immediately analyzed and disseminated quickly, so that the response to threats can be carried out more effectively and efficiently. Strengthening synergies between these sectors will ensure Indonesia's readiness to face increasingly dynamic and complex asymmetric threats.

The success of the implementation of the NCW-based defense strategy in Indonesia is highly dependent on sustainable policies in terms of defense modernization, adequate budget allocation, and cooperation between the government and private sectors. Increasing the capacity of defense infrastructure and strengthening the information technology-based defense system must continue to be a priority. In addition, the domestic defense industry sector also needs to play an active role in providing technological solutions that support NCW-based defense. With planned and integrated steps, Indonesia can optimize the potential of NCW to face asymmetric threats and maintain national stability and security amid increasingly complex global challenges.

### *3.3 Implications*

**Theoretical implications**. Information dominance is the main foundation in modern defense strategy, especially in facing asymmetric threats that are hidden and unconventional. Strategy theory that was previously only seen as a complement to conventional power is now emphasized as the main instrument in winning battles, both in the physical and non-physical realms. With the NCW approach that integrates information systems, sensors, and communication networks in real time, national defense no longer depends only on the quantity of military power, but on the quality of information control. This implication strengthens the theoretical construction that information superiority can be a determinant of strategic dominance in the modern warfare landscape.

In addition, this study has implications for expanding defense theory, which previously focused more on conventional threats (state vs. state), to be more inclusive of non-traditional threats such as terrorism, cyber warfare, separatism, and ideological infiltration. The intangible asymmetric threat within formal military formations requires defense theory to adopt a multidimensional approach that integrates military, civilian, intelligence, and private-sector elements. Thus, the NCW-based strategy not only addresses operational needs but also enriches theoretical perspectives by introducing a collaborative, integrated, and adaptive defense model relevant to the complexity of contemporary threats.

**Practical implications.** A need to accelerate the development and modernization of national defense information technology infrastructure. The results of the discussion show that the effectiveness of NCW is highly dependent on integrated communication networks, sensor systems, radars, satellites, and data centers. In the context of Indonesia as a vast archipelagic country, the need for this infrastructure is very important, especially in border areas, conflict-prone areas, and strategic sea and

p-ISSN: 2528-1682
e-ISSN: 2527-9165

air routes. Without adequate infrastructure support, the NCW system cannot run optimally, so that early detection, surveillance, and rapid response efforts to asymmetric threats will be hampered.

In addition, NCW not only demands technological superiority, but also changes in the organizational structure and work culture of the military. Practically, this requires a transformation from a hierarchical command model to a more flexible and decentralized one, where small units in the field have the tactical authority to act autonomously but remain within the framework of strategic coordination. This requires personnel retraining, adjustments to operational doctrine, and the formation of special units that can utilize the NCW system effectively. A military culture that is adaptive to new technologies, collaborative across units, and responsive to threat dynamics must be developed.

## 4. CONCLUSION

The results of this study confirm that asymmetric threats have become the dominant form of contemporary security challenges, characterized by their hidden, adaptive, and unpredictable nature. These threats, which are often carried out by non-state actors through terrorism, cyber-attacks, sabotage, and ideological infiltration, cannot be effectively addressed using conventional military approaches alone. Therefore, a multi-dimensional defense strategy that integrates military power with intelligence, technology, law enforcement, and social resilience is essential to ensure national stability and security.

Network Centric Warfare (NCW) emerges as a highly relevant and transformative defense paradigm in responding to these asymmetric threats. By emphasizing information superiority, real-time data sharing, and integrated command and control, NCW enables faster, more precise, and more coordinated decision-making across all levels of operation. Through the integration of sensors, communication systems, intelligence platforms, and operational units, NCW strengthens situational awareness and accelerates the OODA loop. However, its successful implementation also requires organizational transformation, decentralization of command, strong cybersecurity, and continuous improvement of human resource capabilities.

From the Indonesian perspective, the implementation of NCW is both a strategic necessity and a long-term challenge. Indonesia's vast archipelagic geography and diverse threat landscape demand an integrated C4ISR system supported by modern infrastructure, skilled human resources, and strong inter-agency cooperation. Although significant progress has been made through the development of joint command structures, radar systems, and communications satellites, gaps in technology, infrastructure modernization, and resource availability remain. Therefore, sustainable defense modernization policies, adequate budgeting, domestic defense industry development, and cross-sector collaboration are crucial to optimizing NCW implementation and ensuring Indonesia's readiness to face increasingly complex asymmetric threats in the future. The primary contribution of this paper is to formulate a defense policy strategy based on Network-Centric Warfare (NCW) principles, which is not only important for assessing NCW in the naval domain but also has potential application in a joint, interagency environment in Indonesia

This study has several limitations and provides room for future research. First, although the NCW concept relies heavily on the integration of information and communication systems, the reality in Indonesia still shows limitations in ICT infrastructure, especially in remote, border, and conflict-prone areas. This infrastructure gap can hinder the effectiveness of NCW implementation on a national scale. Future research needs to focus on strategies to accelerate the development of defense ICT infrastructure, including optimizing communications satellites, integrated radar systems, and secure, reliable military internet networks, especially in border and remote island areas, using a qualitative method to explore them.

Second, implementing NCW requires synergy among the TNI, Polri, BSSN, BIN, and the private sector. However, the rigid sectoral bureaucratic culture, sectoral egos, and differences in operational standards are obstacles to realizing solid and integrated collaboration. Further studies are needed to formulate an effective institutional integration model, including the development of integrated standard operating procedures (SOPs), information sharing mechanisms between institutions, and strategies to

strengthen coordination in crises involving asymmetric threats. Third, the ability of personnel to operate high technology, such as the C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance) system, big data analytics, and cyber defense is still not evenly distributed across units. In addition, an organizational culture that is not fully adaptive to digital transformation is also an obstacle. Future research should examine integrated technology-based training models for both military and non-military human resources. In addition, studies related to strategies for changing the culture of military organizations towards a more adaptive, innovative, and collaborative mindset in the NCW ecosystem are also very necessary. A mixed-methods approach can be used.

## ACKNOWLEDGEMENTS

This research was supported by the Indonesian Defense University. The author would like to express his deepest gratitude to all parties who have contributed to the success of this research. Special thanks are extended to the experts and practitioners who participated in the data collection process and provided invaluable insights into the implementation of NCW-based defense in Indonesia.

## REFERENCES

[1] M. Corominas-Bosch, "Bargaining with asymmetric threat points," *Econ. Lett.*, vol. 69, no. 3, pp. 333–339, 2000, doi: 10.1016/S0165-1765(00)00319-0.
[2] N. Brzica, "Understanding contemporary asymmetric threats," *Croat. Int. Relations Rev.*, vol. 24, no. 83, pp. 34–51, 2018, doi: 10.2478/cirr-2018-0013.
[3] T. Hovardas, "An 'asymmetric Threat' That Should Have Been Anticipated: Political Discourse on 2007 Wildfires in Greece," *Environ. Commun.*, vol. 9, no. 4, pp. 409–427, 2015, doi: 10.1080/17524032.2014.981282.
[4] S. Lee, "Terrorism and asymmetric war: Is North Korea a threat?," *East Asia An Int. Q.*, vol. 20, no. 2, pp. 21–47, 2003.
[5] D. Snowden, "Perspectives around emergent connectivity, sense-making and asymmetric threat management," *Public Money Manag.*, vol. 26, no. 5, pp. 275–277, 2006, doi: 10.1111/j.1467-9302.2006.00539.x.
[6] I. Maoz and C. McCauley, "Threat, dehumanization, and support for retaliatory aggressive policies in asymmetric conflict," *J. Conflict Resolut.*, vol. 52, no. 1, pp. 93–116, 2008, doi: 10.1177/0022002707308597.
[7] A. Almalawi, S. Hassan, A. Fahad, A. Iqbal, and A. I. Khan, "Hybrid Cybersecurity for Asymmetric Threats: Intrusion Detection and SCADA System Protection Innovations," *Symmetry (Basel).*, vol. 17, no. 4, 2025, doi: 10.3390/sym17040616.
[8] M. Dillon, "Network Society, Network-centric Warfare and the State of Emergency," *Theory, Cult. Soc.*, vol. 19, no. 4, pp. 71–79, 2002, doi: 10.1177/0263276402019004005.
[9] N. H. Nguyen, M. A. Vu, A. N. Ta, D. V. Bui, and M. D. Hy, "Optimizing fire allocation in a Network Centric Warfare-type model," *J. Def. Model. Simul.*, vol. 19, no. 4, pp. 691–701, 2022, doi: 10.1177/15485129211022861.
[10] B. G. Kang, K.-M. Seo, and T. G. Kim, "Communication analysis of network-centric warfare via transformation of system of systems model into integrated system model using neural network," *Complexity*, vol. 2018, 2018, doi: 10.1155/2018/6201356.
[11] C. K. Pang and J. Mathew, "Dynamically reconfigurable command and control structure for network-centric warfare," *Simulation*, vol. 91, no. 5, pp. 417–431, 2015, doi: 10.1177/0037549715581076.
[12] D. M. Gormley and D. M. Hart, "Extending network-centric warfare to coalition crisis management and assessment," *RUSI J.*, vol. 145, no. 2, pp. 67–72, 2000, doi: 10.1080/03071840008446512.
[13] Y. S. Liang and N. T. Zhang, "Study on QOS routing in network centric warfare," *Chinese J. Aeronaut.*, vol. 18, no. 3, pp. 250–255, 2005, doi: 10.1016/S1000-9361(11)60306-3.
[14] H. D. Tunnell, "The U.S. Army and network-centric warfare a thematic analysis of the literature," *Proc. - IEEE Mil. Commun. Conf. MILCOM*, vol. 2015-Decem, pp. 889–894, 2015, doi: 10.1109/MILCOM.2015.7357558.
[15] H. Li, G. Yan, X. Zhao, J. Zhang, and M. Lyu, "Tactical mission event logic graph construction for Network-Centric Warfare," *Alexandria Eng. J.*, vol. 61, no. 11, pp. 9161–9173, 2022, doi: 10.1016/j.aej.2022.02.055.
[16] K. S. Kolet, "Asymmetric Threats to the United States," *Comp. Strateg.*, vol. 20, no. 3, pp. 277–292, 2001, doi: 10.1080/014959301753228894.
[17] N. Carpintero-santamaría, "Terrorism : An Electronic Journal and Knowledge Base Volume I , Number 2 Asymmetric Threats," vol. I, no. 2, 2012.
[18] S. Lambakis, J. Kiras, and K. Kolet, "Understanding 'Asymmetric' Threats to the United States," *Comp. Strateg.*, vol. 21, no. 4, pp. 241–277, 2002, doi: 10.1080/01495930290043065a.
[19] S. Blank, "Rethinking the concept of asymmetric threats in u.s. strategy," *Comp. Strateg.*, vol. 23, no. 4–5, pp. 343–367, 2004, doi: 10.1080/01495930490898759.
[20] T. Yan and B. Wang, "Grid architecture model of network centric warfare," *J. Syst. Eng. Electron.*, vol. 17, no. 1, pp. 121–125, 2006, doi: 10.1016/S1004-4132(06)60022-4.
[21] Y. Liang and N. Zhang, "Research on performance of ethernet interface in network centric warfare," *J. Syst. Eng. Electron.*, vol. 15, no. 4, pp. 546–552, 2004, [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-13944279230&partnerID=40&md5=3453f837184f69b1cd94d104ae576019
[22] S. Mishra, "Network centric warfare in the context of 'operation Iraqi freedom,'" *Strateg. Anal.*, vol. 27, no. 4, pp. 546–562, 2003, doi: 10.1080/09700160308450107.
[23] A. J. Masys, "Syndromic surveillance and bioterrorism: Embracing the network-centric warfare paradigm," *Disaster Prev.*

*Manag. An Int. J.*, vol. 13, no. 5, pp. 351–355, 2004, doi: 10.1108/09653560410568462.
[24] E. J. Dahl, "Network centric warfare and the death of operational art," *Def. Stud.*, vol. 2, no. 1, pp. 1–24, 2002, doi: 10.1080/14702430208405009.
[25] V. Krishnamurthy, "Emission management for low probability intercept sensors in network centric warfare," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 41, no. 1, pp. 133–152, 2005, doi: 10.1109/TAES.2005.1413752.
[26] B. J. Archuleta, "Rediscovering Defense Policy: A Public Policy Call to Arms," *Policy Stud. J.*, vol. 44, pp. S50–S69, 2016, doi: 10.1111/psj.12157.
[27] J. Liedtka, "In defense of strategy as design," *Calif. Manage. Rev.*, vol. 42, no. 3, pp. 8–30, 2000.
[28] M. Cepik and F. Licks Bertol, "Defense policy in Brazil: bridging the gap between ends and means?," *Def. Stud.*, vol. 16, no. 3, pp. 229–247, 2016, doi: 10.1080/14702436.2016.1180959.
[29] M. S. Alexander, "Did the Deuxieme Bureau Work? The Role of Intelligence in French Defence Policy and Strategy, 1919–39," *Intell. Natl. Secur.*, vol. 6, no. 2, pp. 293–333, 1991, doi: 10.1080/02684529108432105.
[30] C. Leuprecht and J. J. Sokolsky, "Defense Policy 'Walmart Style': Canadian Lessons in 'not-so-grand' Grand Strategy," *Armed Forces Soc.*, vol. 41, no. 3, pp. 541–562, 2015, doi: 10.1177/0095327X14536562.
[31] D. L. Bland, "Controlling the Defense Policy Process in Canada: White Papers on Defense and Bureaucratic Politics in the Denartment of National Defence," *Def. Anal.*, vol. 5, no. 1, pp. 3–17, 1989, doi: 10.1080/07430178908405374.
[32] C. Hoeffler and J. Joana, "The impact of austerity: spending cuts, coping strategies and institutional change in the case of French defense policy," *Def. Stud.*, vol. 22, no. 3, pp. 448–463, 2022, doi: 10.1080/14702436.2022.2080660.
[33] M. Steinbrecher and H. Biehl, "Military Know-Nothings or (At Least) Military Know-Somethings?: Knowledge of Defense Policy in Germany and Its Determinants," *Armed Forces Soc.*, vol. 46, no. 2, pp. 302–322, 2020, doi: 10.1177/0095327X18811384.
[34] A. Dorman, "Reconciling Britain to Europein the Next Millennium: The Evolution of British Defense Policy in the Post-Cold War Era," *Def. Anal.*, vol. 17, no. 2, pp. 187–202, 2001, doi: 10.1080/07430170120064258.
[35] A. Barokah, N. Nurmalia, F. M. Putri, and M. Nurholizah, "STUDI LITERATUR : ANALISIS EFEKTIVITAS PENGGUNAAN MEDIA TSTS (TWO STAY TWO STRAY) TERHADAP KEMAMPUAN BERPIKIR KRITIS PESERTA DIDIK SEKOLAH DASAR PADA MATA PELAJARAN IPA," *Bunayya J. Pendidik. Anak*, vol. 10, no. 1, pp. 73–87, 2024.
[36] I. P. Syafa, M. Putri, N. Z. E. Setiawati, and A. Marin, "Pengaruh Media Pembelajaran Literasi Berbasis E-Modul terhadap Pembentukan Karakter Siswa Sekolah Dasar (Studi Literatur)," *J. Pendidik. Dasar Dan Sos. Hum.*, vol. 2, no. 2, pp. 315–330, 2022, [Online]. Available: https://www.bajangjournal.com/index.php/JPDSH/article/view/4228/3202
[37] I. Onodera, "Japan's New National Security Policy and Defense Strategy in a New Era," *Asia-Pacific Rev.*, vol. 26, no. 2, pp. 37–49, 2019, doi: 10.1080/13439006.2019.1688928.
[38] D. Güres, "Turkey's Defence policy: The role of the armed forces and strategy, concepts and capabilities," *RUSI J.*, vol. 138, no. 3, pp. 1–6, 1993, doi: 10.1080/03071849308445707.
[39] J. B. Lyons, S. D. Swindler, and J. A. White, "Network centric warfare: Organizational collaboration as a key enabler," *2008 Int. Symp. Collab. Technol. Syst. CTS'08*, pp. 367–374, 2008, doi: 10.1109/CTS.2008.4543952.
[40] M. Guha, "Technical ecstasy: Network-centric warfare redux," *Secur. Dialogue*, vol. 53, no. 3, pp. 185–201, 2022, doi: 10.1177/0967010621990309.
[41] M. Persson and G. Rigas, "Complexity: The dark side of network-centric warfare," *Cogn. Technol. Work*, vol. 16, no. 1, pp. 103–115, 2014, doi: 10.1007/s10111-012-0248-1.
[42] W. Cheng and W. Chu, "SOA-based network-centric software architecture for warfare simulation applications," *Xitong Fangzhen Xuebao / J. Syst. Simul.*, vol. 28, no. 1, pp. 77–82, 2016, [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-84960401434&partnerID=40&md5=5ad6316708c1dd498ed1f88c84ea0043
[43] D. M. Johnston, "An asymmetric counter to the asymmetric threat," *Rev. Educ. Pedagog. Cult. Stud.*, vol. 35, no. 1, pp. 9–14, 2013, doi: 10.1080/10803920.2013.757955.
[44] J. Tawa, "Asymmetric peer selections among Blacks, Asians, and Whites in a virtual environment: Preliminary evidence for triangulated threat theory," *J. Soc. Psychol.*, vol. 157, no. 6, pp. 736–753, 2017, doi: 10.1080/00224545.2017.1294140.