

Network Centric Warfare (NCW) as Defense Resilience: Strengthening National Defenses Through Integrated Air Defense Systems

Wisnu Candra Wijaya

Universitas Pertahanan, Indonesia

Email: Wisnunexus38@gmail.com

Abstract

This study discusses the importance of applying *Network-Centric Warfare* (NCW) to strengthen Indonesia's national air defense resilience. The primary issue identified is the low integration level of the TNI air defense system, resulting in weak air deterrence and frequent violations of Indonesian airspace by foreign aircraft. The research focuses on the national air defense system and *NCW* as a strategy for enhancement. Using a descriptive-analytical method, the study analyzes secondary data from official documents, defense policies, and TNI military doctrine, providing a comprehensive overview of the current air defense status and how *NCW* can enhance military operations. Findings reveal that *NCW* significantly improves situational awareness by enabling real-time information exchange among military components such as radars, sensors, and air weapons systems. It facilitates better unit coordination and faster battlefield decision-making. However, challenges remain due to reliance on diverse foreign military equipment with different communication standards, cybersecurity vulnerabilities, and limited human resources proficient in military communication technology. In conclusion, while *NCW* holds great potential to improve Indonesia's air defense resilience, its optimal implementation requires modernizing communication infrastructure, enhancing interoperability among military systems, and developing skilled human resources. With strategic coordination, *NCW* can become a robust backbone of air defense, effectively countering modern threats like stealth fighters, hypersonic missiles, and armed drones.

Keywords: Network-Centric Warfare; Air Defense; Integrated Communication Systems; Air Threats; Interoperability.

INTRODUCTION

Based on what is stated in the *Law of the Republic of Indonesia Number 3 of 2002*, the defense system adopted is universal or comprehensive and covers all aspects owned by the Indonesian nation (UURI Number 3, 2002). This system involves the participation of all citizens, regions, and national resources, including national infrastructure. The coaching aims to strengthen and improve the defense capabilities of the state and nation. The government implements this system, which is prepared early on through systematic measures to safeguard sovereignty and national security. In addition, this system also highlights the importance of preparedness of all elements of the nation in facing threats.

National resilience is the ability of a nation to maintain unity and integrity, increase the capacity to support survival, and face various existing threats so that they can live their lives for the sake of achieving national prosperity (Srilaksmi et al., 2023). Air defense is one of the main aspects in maintaining a country's sovereignty against ever-evolving modern air threats. This threat no longer includes only conventional warplanes but also advanced technologies such as stealth fighters that are difficult to detect by radar, cruise missiles, ballistic missiles including hypersonic missiles, and armed drones. The war in Ukraine has shown that drones and related technologies are key to military dominance. Drones, both military and commercial like the DJI Mavic 3, have changed war tactics by providing significant precision intelligence and strike capabilities. Both Russia and Ukraine utilize these drones to detect enemies and direct attacks appropriately, with the help of drone technology from other countries also influencing combat dynamics on the ground (Warnes, 2023).

Currently, to support the National Air Defense System, the TNI has a number of weapons and defense equipment capable of operating in three dimensions, with the largest quantity owned by the Indonesian Air Force. Joint air operations in these three dimensions require the support of the National Air Defense System, which needs integrated command and control. To carry out this function, the TNI requires a communication system as a means for command, information exchange, and execution of *hanud* defense equipment. These defense systems originate from various countries and exhibit different types and functions. While some, such as the F-16 and the Hawk Mk.109/209 made in the United States and Britain, use standard NATO communication systems, other defense systems, such as the Russian-made Sukhoi Su-27/30, have different standards. Currently, the full integration of the TNI's *hanud* defense equipment is not optimal. The non-optimization of *Sishanud* integration impacts the low deterrence of national air defense, as evidenced by numerous airspace violations by foreign aircraft in Indonesia. These violations, as conveyed by Admiral Yudo Margono, occurred during January–June 2023 and included incursions by the United States, the Czech Republic, and India (Kompas.com, 2023).

In this context, air defense integration is an inevitable strategy. An integrated air defense system is essential not only for effectiveness in facing air threats but also as a core part of the grand vision to reduce risks to national security. With good integration, air defense weapon systems can coordinate efficiently, providing a more adaptive response to existing threats. The concept of *Network-Centric Warfare (NCW)* is an important foundation in developing integrated air defense systems. *NCW* enables a wide range of air defense tools to work synergistically, enhancing the ability to detect, evaluate, and respond to air threats more effectively. An integrative approach like the one proposed by *NCW* includes not only improved communication, efficient data management, but also rapid and informed decision-making. An integrated communication system allows the various components in air defense to share information efficiently, speeding up decision-making, while good data management ensures information is accurate and available in a timely manner (Alberts and Stein, 2000).

The importance of *Network-Centric Warfare (NCW)* in modern defense systems has been widely discussed in previous studies. For instance, Singh (2019) examined the role of *NCW* in enhancing military interoperability but focused primarily on technical challenges, overlooking organizational and policy barriers that hinder integration. Similarly, Alberts and Hayes (2006) explored the theoretical framework of *NCW*, emphasizing its potential to improve situational awareness; however, their study lacked empirical analysis of its implementation in developing nations like Indonesia. These gaps highlight the need for a comprehensive study addressing both technical and non-technical challenges of *NCW* adoption, particularly in contexts with diverse defense equipment and limited infrastructure.

This research aims to fill these gaps by critically analyzing *NCW* implementation in Indonesia's air defense system, focusing on interoperability issues, cybersecurity threats, and human resource limitations. By leveraging secondary data from defense policies, military doctrines, and case studies, the study provides a holistic view of *NCW*'s potential and challenges in strengthening national air defense. The findings will offer actionable insights for policymakers and military strategists, contributing to modernization of Indonesia's defense infrastructure and enhancing resilience against evolving air threats.

RESEARCH METHODS

This research was designed to explore the problem of the need for Network-Centric Warfare (NCW) integration in strengthening the national air defense system. The research used the analytical descriptive method to gain an in-depth understanding of the concept of NCW and its implementation in the context of integrated air defense. In addition, the descriptive analysis method was used to describe and explain the ongoing situation based on the information and

data obtained from the research results. The data were then analyzed to produce conclusions that could answer the main problem at the research site.

To obtain data for this research, an approach was carried out by reviewing documents to gather relevant secondary data. These documents included state defense policies, TNI doctrines such as Tri Dharma Eka Karma (Tridek) and Swa Bhuna Paksa, as well as reports related to the development of communication and information technology within the TNI. In addition, data and information were also obtained from reliable news sites.

The data obtained from interviews and related documents were then analyzed descriptively. Descriptive analysis was chosen to detail the concept of NCW and its application in the context of national air defense.

RESULTS AND DISCUSSION

Common

In Law Number 2 of 2002 concerning State Defense, article 10 states that in the implementation of state defense, the TNI functions as the main component in the implementation of state defense. As part of the TNI, the Indonesian Air Force is responsible for air defense, including law enforcement and national airspace security as well as the application of ratified international law. In addition, the Indonesian Air Force plays a role in the development and development of air power, as well as the empowerment of air defense areas. Along with the development of the strategic environment, it is necessary to change the air defense system that is strong and reliable, which adopts the latest technology to deal with air threats, through capacity building, capability enhancement, and integration of defense systems in intelligence-based command (smart defense) (Law No. 3 of 2022).

Overview of NCW as the Essence of Integrated Air Defense

The main objectives of the Network-Centric Warfare (NCW) is to achieve victory in the battle by maximizing the use of integrated information networks. The NCW concept is based on the ability of military units connected through a solid and reliable communication network to share data in real-time. In this case, operational success is highly dependent on the quality of communication and mastery of information, which allows every element in military operations to act on accurate and timely information.

However, before achieving victory, there are some important achievements that must be obtained first. One such achievement is dominance on the battlefield, which includes the ability to detect, analyze, and respond to threats faster than enemies. To dominate the battle, each unit or supporting element involved must be connected to each other through a well-integrated communication network. This allows for efficient information exchange, accelerates decision-making, and provides a comprehensive understanding of the situation on the battlefield.

The NCW demands full control of communications and information infrastructure to ensure operational security and prevent adversaries from attempting to disable or intercept military communications networks. Reliable communication depends not only on the technology of the network itself, but also on protection against cyberattacks or attempts at sabotage of information by the adversary. In the context of air defense, the ability to secure communications networks is critical, given the operational nature of evolving threats, including attacks from armed drones, hypersonic missiles, or stealth fighters that are difficult to detect by conventional radar.

With the connection of various military elements through a solid communication network, TNI units can share data with each other Real-time. For example, data from radars or sensors that detect enemy movements can be directly relayed to warplanes on the ground, allowing for rapid action. Ability to update data from various sensors and manage information in a timely manner Real-time creates a significant advantage in terms of situational awareness (situational

awareness). This information not only helps the troops know the position of their own forces and the enemy, but also understands the enemy's strength and terrain conditions, which are essential for drawing up an effective and efficient operational plan.

The mastery of information provides a very significant advantage over the enemy. Troops that have access to accurate, detailed, and timely information can respond more quickly and on target, while enemies who are disconnected from information sources tend to act sluggishly or incorrectly in decision-making. In the NCW system, all units involved in military operations can share information with each other, whether it is from sensors, radar, or available intelligence data. This collective knowledge allows for more comprehensive and dynamic planning and can change adaptively depending on the situation on the ground.

Excellence in information mastery not only includes the preparation of tactical plans but also includes the ability to execute well-coordinated operations. In air defense operations, for example, the NCW allows for full integration between air defense weapon systems, radars, fighter aircraft, and command units, so that they can act in harmony to repel incoming threats. The NCW also enhances the ability to coordinate joint operations between the three dimensions of the TNI – the Army, Navy, and Air Force – which is critical in the context of integrated defense. In the context of NCW operations, the division of roles between the TNI Headquarters (TNI Headquarters), the Headquarters of each force, and the Kotama (Main Command) is very important. The TNI Headquarters acts as the highest authority at the strategic level, with the responsibility to formulate doctrine, policies, and budget support. The TNI Headquarters also coordinates with the government and relevant ministries to ensure that military operations run smoothly and in accordance with national policies. On the other hand, the headquarters of each force, such as the Air Force Headquarters for air defense, is tasked with fostering the forces under the command of Kotama in accordance with the guidelines that have been set.

At the operational level, Kotama plays an important role in carrying out NCW's mission. They are responsible for ensuring that each military unit involved in the operation is able to work efficiently and in a coordinated manner. NCWs on the battlefield require personnel, military equipment, and command systems that are able to interact and maintain situational alertness. This involves the collection and exchange of information through various transmission media, such as HF/VHF/UHF radio, as well as the use of satellites and other Broadband lines. Interoperability between dimensions is also key to NCW's successful operations. Each dimension must be able to communicate and exchange data in real-time through an integrated communication network. This is very important to support the smooth running of integrated air defense operations, which include the TNI's Integrated Trimatra Operation. At the operational level, this interoperability allows the various weapon systems and sensors to work in harmony, accelerating responses to threats and maximizing the efficiency of the use of existing resources.

This system integrates all air defense components under the control of the central command at the TNI Headquarters. This communication at the national level is essential to ensure good coordination between all military units involved in defense operations. This national communication system also uses a variety of advanced tools and technologies, including satellites, strategic communication equipment, and other Broadband lines. In large-scale operations, the NCW allows every element of defense to stay connected, both at the operational and strategic levels, which is critical to maintaining information superiority and dominance on the battlefield.

Overall Network-Centric Warfare provides many benefits to the TNI's air defense capabilities. With an integrated communication network, the TNI can respond to threats faster, more accurately, and more effectively. NCW allows each unit to share data in real-time, improves situational awareness, and enables faster and more informed decision-making. However, the implementation of NCW also requires a large investment in communication

technology infrastructure, as well as serious efforts to integrate various defense equipment owned by the TNI. Nonetheless, with the right strategy, NCW can provide a significant advantage in maintaining the sovereignty of Indonesia's airspace and ensuring that the TNI is always ready to face threats in this era of modern warfare.

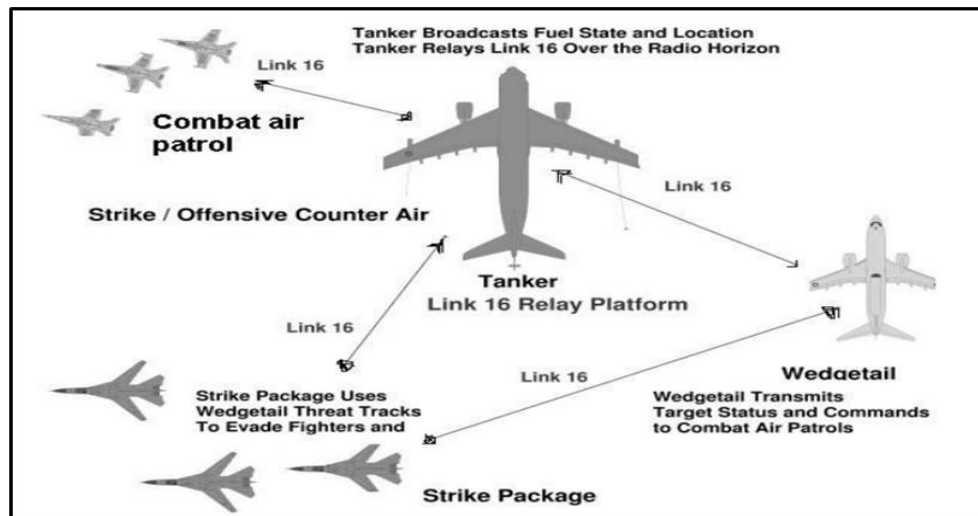


Figure 1. Data Link that connects each unit

Source : Kopp, 2005

The urgency of the TNI in adopting NCW

In the context of state defense regulated by the Law of the Republic of Indonesia Number 3 of 2002, the defense system adopted is universal or comprehensive. This system includes all elements of the nation, territory, and national resources, and involves national infrastructure to defend state sovereignty and maintain national security. This emphasizes the need for preparedness from all elements of the nation in facing various threats, both from within and outside the country. One of the threats that is the main focus is the air threat that is growing with rapid technological advances, so it requires a new approach in defending national air sovereignty.

Air defense is one of the main elements in maintaining a country's sovereignty. As technology develops, air threats are no longer limited to conventional fighters as they were in the past but instead include advanced technologies such as stealth fighters (Stealth), ballistic missiles, cruise missiles, hypersonic missiles, as well as armed drones. These threats require a more sophisticated and integrated response to be effectively addressed. In this context, the adoption of the concept Network-Centric Warfare (NCW) is important to increase the deterrence of national air defense.

Currently, one of the main challenges in national air defense is the not optimal integration between various defense equipment owned by the TNI. Various defense equipment owned by the TNI comes from different countries, with different communication standards. For example, the F-16 and Hawk Mk.109/209 fighters made in the United States and the United Kingdom use NATO's standard communication systems, while the Russian-made Sukhoi Su-27/30 fighter aircraft have different standards. This non-optimization in integration results in the national air defense deterrence still being weak, as evidenced by the frequent violations of airspace by foreign aircraft, as reported to have occurred throughout January to June 2023.

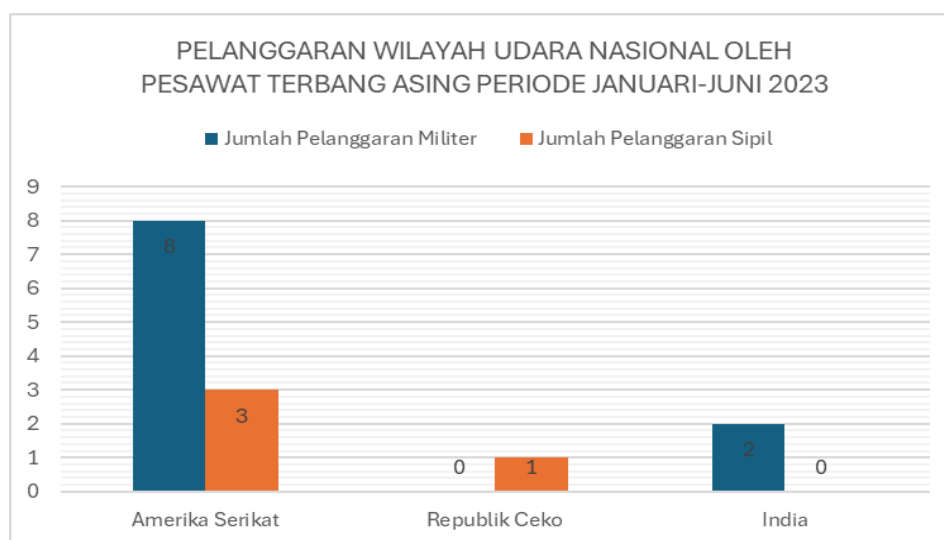


Figure 2. List of airspace violations for the January-June 2023 period
Source: Kompas.Com, 2023

One of the biggest advantages of the application of NCW in air defense systems is the ability to collect and manage information in real-time, which is critical in the face of modern threats such as armed drones and hypersonic missiles. Integrated sensor and radar systems can provide a clearer and more complete picture of the air situation around Indonesian territory, making it easier for the TNI to take preventive and counter-threat measures.

NCW also enables faster and more precise decision-making. In the context of airspace violations, speed in detecting and responding to threats is critical. With an integrated communication system, the command center can immediately issue orders to fighter aircraft or other air defense units to pursue, identify, or act against foreign aircraft that violate airspace. This will certainly reduce the risk of violations that are not detected or handled late.

In addition, NCW also improves efficiency in the use of resources. With an integrated system, the Indonesian Air Force can coordinate its various defense equipment more efficiently. For example, fighter aircraft and ground air defense systems can work synergistically to repel threats, thereby reducing the risk of overlap or redundancy in resource usage.

Airspace violations are a serious threat to state sovereignty, and the TNI, especially the Indonesian Air Force, must be able to respond to these threats more quickly and efficiently. In the face of increasingly complex air threats, the adoption of Network-Centric Warfare (NCW) has become very important. NCW enables better integration between various defense systems and air defense systems, as well as accelerating the decision-making process through information management Real-time.

Development Challenges Network Centric Warfare

Network Centric Warfare (NCW) aims to integrate information from various elements within the military operations environment to improve combat effectiveness. By connecting sensors, decision-makers, and action enforcers into a single, unified network, NCW enables troops to share information in real-time, speed up decision-making processes, and improve maneuverability. However, while the NCW concept offers many potential benefits, its implementation faces significant challenges in terms of technology, organization, and policy.

Technological challenges are one of the main obstacles in the development of NCW. An efficient military network system requires a highly reliable and secure telecommunications infrastructure to handle large and sensitive data. In combat situations, these network systems must be resistant to cyberattacks and electronic signal interference. One oft-cited challenge is NCW's reliance on the reliability of satellite communications and other network systems, which

are often the primary targets in electronic warfare (Singh, 2019). Attacks on this network infrastructure can lead to the paralysis of communications between military units, thus hampering operations that rely on real-time data. In addition, the integration of various systems used by land, sea, and air forces presents compatibility issues. Various military platforms are often developed by different contractors and use different communication protocols. For example, it is difficult to integrate sensors from aerial surveillance systems with naval combat management systems, which have different communication architectures and standards (Wang et al., 2021). These interoperability issues require significant time, cost, and effort to resolve.

Cybersecurity is another crucial aspect in NCW. In the modern scenario, the threat of cyberattacks by state and non-state actors increases significantly. Cyberattacks on NCW systems can result in the leakage of very important information, or even worse, data manipulation on the network that can mislead decision-makers (Pernik, 2020). Information security is a tough challenge because every node in the NCW network is a potential point for hackers to attack. This is further complicated by the fact that the more nodes or devices connected to the network, the wider the attack surface available to the enemy. In addition, network reliability is also an important issue. In combat situations, the environment is often highly dynamic with distractions from bad weather, complex topography, and enemy attacks targeting communications infrastructure. For example, technologies such as satellite communications can be easily disrupted by weather or jamming from the enemy, thus depriving troops in the field of access to the information needed (Gallagher, 2022).

The NCW also faced significant challenges in terms of organizational adaptation and changes in military doctrine. The implementation of NCW demands a profound cultural change among the military, which is often dominated by hierarchical structures and centralized command systems. A more decentralized and horizontally distributed network approach can be at odds with traditional command structures (Alberts & Hayes, 2006). Military forces have long been accustomed to rigid chains of command.

Network Centric Warfare (NCW) is a modern concept in military strategy that utilizes the integration of information and communication technologies to enhance combat capabilities through real-time information sharing among military units. The application of NCW allows for the creation of shared situational awareness, so that all elements in military operations can access the same data simultaneously, accelerating decision-making and the effectiveness of actions in the field (Cebrowski & Garstka, 1998). Although this concept has been adopted by many developed countries such as the United States, the implementation of NCW in Indonesia still faces various significant challenges, both in terms of infrastructure, human resources, and coordination between defense agencies.

The main challenge in the development of NCW in Indonesia is the limited military communication and information technology infrastructure. NCW needs a reliable and fault-resistant communication network, but most of Indonesia's communication infrastructure does not meet this standard. Indonesia, which is the largest archipelagic country in the world, faces geographical problems in the equitable distribution of communication networks, especially in border and remote areas (Wibowo, 2015). This slowed down the development of network-based systems that relied on high-speed and stable connectivity. Another challenge is network security, where military networks must be protected from cyber threats, such as hacking and sabotage, which have the potential to damage the integrity of data as well as the military's operational capabilities (Tantowi, 2019).

The development of NCW requires military personnel who are skilled in information and communication technology, however, currently, Indonesia still lacks experts in this field. Limited human resource capacity in terms of technology understanding, system maintenance, and data analysis is a major obstacle. The lack of relevant intensive training for Indonesian

military personnel in this area creates a gap in the effective implementation of NCW (Purwanto, 2020).

The implementation of NCW in Indonesia is also hit by bureaucratic problems and inter-agency coordination. NCW not only involves the armed forces, but also other agencies such as the State Cyber and Cryptography Agency (BSSN), the State Intelligence Agency (BIN), as well as related ministries, such as the Ministry of Communication and Information. Without good coordination, NCW-based defense systems can experience information fragmentation, which actually hinders operational effectiveness (Laksamana, 2020). Bureaucratic barriers in cross-agency information exchange also add to the complexity of NCW implementation, where each institution has different rules, procedures, and policies regarding access and distribution of information.

One of the other factors that slowed down the development of NCW in Indonesia was the limited defense budget. The development of NCW requires enormous investments, not only to build a strong technological infrastructure, but also to train personnel, develop new operating doctrines, and update military equipment compatible with network-based systems (Wardhani, 2018). Although Indonesia's defense budget continues to increase every year, the proportion allocated for modernization of NCW-based systems is still relatively small compared to the ever-growing technological needs.

The development of NCW also requires the support of a strong domestic defense industry to produce hardware and software that suits the needs of the military. However, Indonesia's defense industry is still lagging behind in terms of technological innovation. Dependence on importing military equipment from abroad is a challenge in itself, as the integration of foreign technology with domestic systems often experiences compatibility constraints. In addition, access to high technology is often limited by global regulations and politics, which makes it difficult for Indonesia to obtain the advanced technology needed to build a reliable NCW system (Widjajanto, 2016).

As a system that relies heavily on information technology, NCW is particularly vulnerable to cyberattacks. With the increasing threat from countries with high cyber capabilities, Indonesia needs to improve its cyber defense capabilities to protect NCW infrastructure. Failure to maintain network security can result in strategic information leakage and disruption to military operations (Tantowi, 2019). Therefore, the development of NCW must be accompanied by an improvement of a cybersecurity system that can detect and respond effectively to cyber threats.

Indonesia also faces challenges in catching up with technology compared to neighboring countries that are more advanced in NCW development, such as Singapore and Australia. This technological gap can affect Indonesia's military competitiveness in the regional region, especially in the context of regional defense cooperation such as ASEAN (Laksamana, 2020). Without serious efforts to catch up, Indonesia risks losing its strategic capabilities in maintaining national security and regional stability.

Efforts to improve the implementation of NCW

Network Centric Warfare (NCW) has great potential in improving the effectiveness of military operations through the integration of information networks that connect sensors, decision-makers, and troops on the ground in real-time. However, significant challenges in terms of technology, organization, and policy hinder the implementation of this concept in many countries, including Indonesia. One of the biggest challenges is the limitation of telecommunications infrastructure. To address this, Indonesia must improve its military communications network, especially in border and remote areas. The approach that can be taken is to expand the fiber optic network or high-power satellite communication technology, as well as create network redundancy to ensure operational continuity despite disruptions from weather

factors or electronic warfare. This modernization of infrastructure not only improves the reliability of communications, but also strengthens defenses against enemy signal interference, such as jamming or cyberattacks.

Another challenge is related to interoperability between different military systems. In this regard, it is important to develop a common communication standard that can bring together various military systems developed by different contractors. These solutions can include the implementation of an open architecture that allows for the integration of sensors and platform from various military forces, both land, sea, and air. In addition, the government and armed forces must work closely with the domestic defense industry to ensure that the technology developed is in accordance with national needs and standards, reducing reliance on imported devices that are often incompatible with domestic systems.

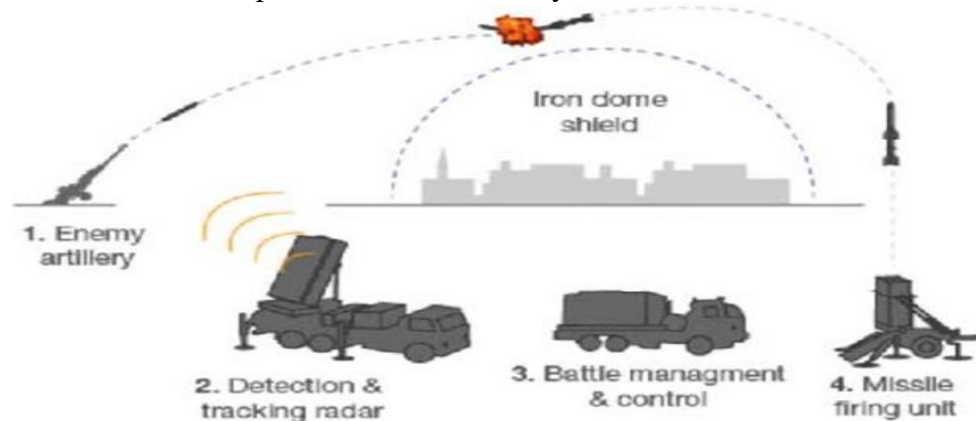


Figure 3. Interceptor Missile System

Source: Sweep, 2023

Cybersecurity is a major concern in the implementation of NCW, given the increasing number of cyberattacks targeted at military networks. To address this, Indonesia must invest in the development of advanced encryption technologies as well as increase cyber threat detection and mitigation capacity. This can be realized through more intensive personnel training in the field of cybersecurity, strengthening collaboration between defense agencies such as the State Cyber and Cryptography Agency (BSSN) and the State Intelligence Agency (BIN), and developing a layered security system that is able to withstand attacks from state and non-state actors. These improvements need to be supported by simulated cyber exercises to test the system's response and resilience to real attacks.

In terms of military organization and doctrine, changes in the culture and command structure are significant challenges. The tradition of centralized command in the Indonesian military needs to adapt to the concept of NCW which is decentralized and network based. To address this, it is important to integrate NCW training into the military curriculum and change military doctrine that allows for faster and more responsive decision-making. As such, military commanders need to be given greater autonomy in decision-making on the ground, while information continues to flow to higher command levels for strategic coordination.

In addition, increasing the capacity of human resources (HR) is a priority in the implementation of NCW. Indonesia still lacks experts in the field of information and communication technology, especially in the military context. Therefore, intensive training for military personnel involved in NCW should be expanded, both through formal education and exchange programs with countries that are already advanced in NCW development, such as the United States or Singapore. The development of these skills will not only accelerate the adoption of new technologies but also ensure that personnel can perform system maintenance and data analysis effectively.

Inter-agency coordination is also a key factor in the implementation of NCW. Without good cooperation between institutions such as BSSN, BIN, and the Ministry of Communication and Informatics, the NCW system can be disrupted by information fragmentation. To address these challenges, governments need to develop policies that encourage cross-agency information exchange with clear and standardized protocols. In addition, the establishment of an integrated command center that can supervise and coordinate information from various agencies is essential to maintain operational continuity.

Finally, budget limitations are an obstacle in the modernization of NCW-based defense systems. To overcome this, the Indonesian government needs to prioritize the defense budget with a focus on modernizing communication technology and cyber defense. In addition, cooperation with the private sector and other countries can be leveraged to reduce the cost of developing military technology. For example, offset programs with developed countries can help Indonesia access advanced technology while strengthening the local defense industry.

In order to answer the challenges faced in the implementation of NCW, a combination of technology investment, policy change, and human resource development is the key to success. While the road to effective implementation of NCW remains a long one, coordinated strategic measures can enhance the capabilities of the Indonesian military to deal with modern threats and maintain national and regional security stability.

CONCLUSION

The application of *Network-Centric Warfare (NCW)* in Indonesia remains in the developmental stage, facing significant challenges such as limited communication infrastructure—especially in border and remote areas—and the incompatibility of communication systems from diverse foreign defense equipment. These issues contribute to suboptimal air defense capabilities, as evidenced by frequent airspace violations. Additionally, shortages in skilled human resources for information and communication technology, rising cybersecurity threats, and bureaucratic coordination problems further hinder *NCW* implementation. To overcome these barriers, Indonesia must modernize its communication infrastructure by expanding fiber optic networks and satellite reliability, establish common communication standards across military platforms, and enhance cybersecurity training to strengthen human capital. Improved inter-agency coordination with integrated command centers and clear information-sharing policies are also essential. Future research should focus on developing tailored frameworks for cybersecurity resilience within *NCW* implementations in Indonesia, addressing both technical and organizational dimensions to safeguard military communication networks against evolving cyber threats.

REFERENCE

- Alberts, D. S., & Hayes, R. E. (2006). *Understanding command and control*. CCRP Publication Series.
- Alberts, D. S., & Stein, F. P. (2000). *Network centric warfare: Developing and leveraging information superiority*. CCRP Publication Series.
- Cebrowski, A. K., & Garstka, J. J. (1998). Network-centric warfare: Its origin and future. *US Naval Institute Proceedings*, 124(1), 28–35.
- Gallagher, S. (2022). *Electronic warfare: Strategies and vulnerabilities in modern military communication*. *Defense Tech Journal*, 12(4), 56–71.
- Kompas.com. (2023, July 11). The TNI commander revealed that US military aircraft often violate airspace. *Kompas.com*.
<https://nasional.kompas.com/read/2023/07/11/09284011/panglima-tni-ungkap-pesawat-militer-as-sering-langgar-wilayah-udara>

- Kopp, C. (2005). Understanding network centric warfare. *AusAirPower.net*. <https://www.ausairpower.net/TE-NCW-JanFeb-05.html>
- Laksamana, A. (2020). Interagency coordination in Indonesia's cyber defense: Challenges and policy options. *Indonesian Journal of Strategic Studies*, 6(1), 55–70.
- Pernik, P. (2020). Cyber security risks in network centric warfare. *NATO Cooperative Cyber Defence Centre of Excellence*.
- Purwanto, A. (2020). Information technology in Indonesia's defense system: Challenges and solutions. *Journal of Defense*, 10(4), 123–140.
- Singh, R. (2019). Network-centric warfare and its implications for the future of military operations. *Military Communication Journal*, 25(3), 45–60.
- Srilaksmi, N. K. T., Irnadianis, B., Estiningtyas, D., Delareiza, M., Sulistiowati, S., & Nilam, A. (2023). State defense: Challenges towards digitalization. *Journal of Digital Law and Policy*, 2(2). <https://doi.org/10.58982/jdlp.v2i2.313>
- Tantowi, R. (2019). Cyber threats in the development of NCW in Indonesia. *Indonesian Defence Review*, 7(1), 65–78.
- Wardhani, T. (2018). Modernization of the main tools of the weapon system and the implementation of network centric warfare in Indonesia. *Indonesian Military Strategy*, 12(3), 78–92.
- Widjajanto, A. (2016). The readiness of the defense industry to support the development of network-centric warfare. *Indonesian Journal of Defence Technology*, 8(1), 102–120.
- Wibowo, H. (2015). Geographical challenges in the development of defense technology in Indonesia. *Geopolitics Indonesia*, 5(3), 88–95.
- Wang, Y., Li, Z., & Zhang, M. (2021). Challenges of interoperability in joint operations: Integration of air, land, and naval systems. *Journal of Military Technology*, 34(2), 67–79.
- Warnes, R. (2023). The role of drones in modern warfare: Lessons from the Russia–Ukraine conflict. *Defense Intelligence Quarterly*, 29(1), 12–28.