International Journal Of Humanities Education And Social Sciences ***(IJHESS)*** *E-ISSN:* **2808-1765**
Volume 5, Number 2, October 2025, *Page. 1130 – 1142*
Email : editorijhess@gmail.com

Reformulation of State Defense Policy Based on IA Technology for Decision Making in State Defense

Adam Mardamsyah
The Republic of Indonesian Defense University

*Corresponding Author
Email: Adaminfantri94@gmail.com

Abstract

In today's landscape, as we know, traditional warfare has evolved into what we know as modern warfare. Modern warfare encompasses sophisticated weapons systems, particularly those involving precision-guided devices such as drones, long-range missiles, and advanced air defense mechanisms. The integration of artificial intelligence (AI) into today's warfare involves applications in combat contexts, analytical techniques, and logistical tasks. The writing method uses qualitative research with a review of several references. The results of the review study indicate that the use of artificial intelligence (AI) in protecting cybersecurity and defense infrastructure is a critical component for ensuring the resilience and sustainability of military operations. Technology can assist in rapid and accurate threat awareness, analysis and response, and protect critical infrastructure. The integration of the Secret Service and AI systems, increasingly integrated into the use of AI as a strategic step in the fight, can help countries achieve significant advantages in addressing the complex and diverse threats in today's military world. Therefore, it is highly relevant to formulate national defense policies using a technology-based approach to improve the effectiveness and efficiency of decision-making.

Keywords: Modern Warfare, Technology, Artificial Intelligence (AI), Military, National Defense Policy

INTRODUCTION

In today's landscape, traditional warfare as we know it has evolve become What Which We know as war contemporary. Form conflict modern This characterized by involvement military Which happen in today, by utilizing cutting-edge technology, innovative tactics, and a series of dynamics Which more complicated than war classic. Evolution war modern reflects progress technology And shift approach military. Countries And factions armed must quick adapt self with threats and opportunities that arise along with the development of the times. Unlike previous forms of military engagement, modern warfare operates in a which is not solely based on physical confrontation and presents a danger unique, so it requires strategy extensive to predict scenarios potential. Contemporary warfare involves advanced weapons systems, particularly precision equipment such as drones, long-range missiles, and advanced air defense mechanisms. The integration of artificial intelligence (AI) into combat time now covers its implementation in framework combat, analytical intelligence, and logistical tasks. So in modern warfare, cyber conflict is realized through attack cyber Which target infrastructure important, military communications and information networks (Breiman, 2001).

Besides That war proxy Also enter into the war modern Which characterized with various element interaction level national And country parts, which include: politics, economics, socio-cultural aspects, and legal frameworks. As technology advances, the nature and dynamics of conflict have shifted, making conventional warfare between nations increasingly seldom happened. Currently, the concern Which more A pressing issue is the emergence of proxy wars. Captain Inf Shokib Setyadi, Pasiter of the 0712 Military District Command (Kodim), described proxy wars as confrontations between major powers that utilize third-party agents to avoid direct involvement, thereby reducing the risks associated with a full-blown conflict. In proxy wars, it becomes difficult to distinguish allies from enemies. Signs of proxy wars in Indonesia have begun to emerge, including separatist actions, radical left- or right-wing movements, repressive tendencies toward anarchist groups, exploitative regulatory and trade

frameworks, the drug trade, sensationalist media narratives, student clashes, intergroup confrontations, and the rise of pornography, promiscuous behavior, and the LGBT agenda. These conflicts have also began to expand across various domains, including land, sea, air, spatial and cyberspace environments (Adam, 2016)

Thus, preventive action is needed from the government to overcome the above problems by reformulating the national defense policy based on IA technology in decision-making to maintain national defense and security. Considering that currently the phenomenon of civilian militarization reflects the integration of civilian technological innovation into in function military, such as utilizing satellites commercial For intelligence purposes (Adib, 2023)

By looking at the characteristics of modern warfare, the need for intelligence The Indonesian National Armed Forces (TNI) is clear in facing challenges and finding effective solutions. Simultaneously, the Chief of General Staff (Kasum) of the TNI delivered his remarks before the participants of the Communications and Electronics Coordination Meeting (Rakorkomlek), emphasizing that Network-Centric Warfare (NCW) is currently being developed by the TNI. Therefore, the TNI must incorporate network-centric warfare principles into its operational tasks to effectively address the demands of modern conflict. This approach is based on real-time communication and data connectivity between headquarters and operational units, which facilitates an effective response in contemporary warfare (Akbayrak, 2017).

As for Network Centric Warfare (NCW) is approach contemporary to operation military Which emphasize communication time real And Data connectivity between command headquarters and combat units. This methodology accelerates decision-making by leveraging the most up-to-date data and information available. As draft operational Which Keep going develop, NCW signify a shift Soldier National Indonesia (TNI) from strategy war traditional, by integrating the roles of the TNI cyber unit, TNI Public Relations, intelligence, territorial troops, units task supporters, And initiative diplomatic. For implement capabilities NCW in a way effective, support technology advanced very important, exemplified by program Interoperability Kodal, Which has proposed to the Ministry Defense through procurement equipment defense foreign. In this modern context, the TNI must transition from being a mere public information entity to a proactive media warrior, engaging in media warfare to shape public opinion. Given the complex spectrum of threats currently faced, the organizational structure Which adaptive become must. Organization Which fail respond challenge new will surely down and lose the competition with other countries. To grow Power adaptation the, Indonesian National Armed Forces must own Spirit flexibility, recognizing trends, fertilize synergy, And avoid pattern think Which narrow. Matter this demands change fundamental in pattern think TNI, with realize the environment that dynamic And fast changed Which demand response Which fast. Besides that, development personnel Indonesian National Armed Forces must adhere to system based performance, by ensuring that the right individuals are placed in the right roles. Given that digital warfare is now a crucial aspect of contemporary conflict, encompassing various forms of hostilities that occur in cyberspace. This realm of warfare includes cyberattacks, cyberespionage, and disinformation efforts. carried out by individuals, groups, or countries (Anastassov, 2021)

Article 31 of Law Number 17 of 2011 concerning State Intelligence regulates the duties of the National Armed Forces Strategic Intelligence Agency. Indonesia (BAIS TNI). This agency is tasked with conducting strategic intelligence activities and operations, as well as enhancing strategic intelligence capabilities to support the TNI's primary duties. responsible answer in field intelligence military And domiciled in under command Headquarters Big (Headquarters) Indonesian National Armed Forces. Body This led by Head BAIS The TNI (Kabais TNI) is directly responsible to the TNI Commander. Please note, various state institutions in Indonesia have their own intelligence agencies, including the TNI. is at in lower BAIS. Besides That according to Chapter 5 And 6 Constitution Number 34 of 2004 concerning

the TNI, the TNI functions as a state apparatus in the defense sector which carries out its duties in accordance with state policies and political directions. As tool defense state, TNI on duty ward off military threats and armed aggression, whether originating from within or outside the country, so as to safeguard the country's sovereignty, territorial integrity, and security. Furthermore, the TNI has the authority to respond to all forms of threats and is obligated to restore security conditions disrupted by these disturbances. The role of TNI Intelligence includes various proactive efforts, activities and initiatives that aimed at carrying out early detection and early warning in order to prevent, prevent and address potential threats to interests and national security. The main objective of state intelligence is to detect, identify, review, analyze, interpret, and present intelligence information, so that it can provide early warnings to anticipate various potential and real threats to the safety and existence of the nation and state, as well as identify opportunities that can benefit the interests and National security. The functions of state intelligence include conducting investigations, ensuring security, and facilitating mobilization (Bourget, 2018)

So that with the existence of statement above then the capacity to process a number of big data, detect trends, And carry out decision in a way independent, intelligence artificial potential change method country designing, implementing, and evaluating defense strategies . Utilization of technology AI enables faster, more precise, and more effective decision making during condition emergency or in compile strategy initiative defense. However, to fully utilize the capabilities AI in the defense sector, necessary formulate return policy Which align technology This with the current national defense framework (Brisson, 2021).

article discusses how AI can be utilized in national defense to reformulate national defense policy based on AI technology for decision-making in national defense. Given the current trend of artificial intelligence (AI), it can facilitate this. utilized its uses for the sake of minimize risk Which happen And related with its development and application in the military world. So that things offered to the world by new technologies can be predicted and indicate that the possibility of military escalation, especially unintentional escalation and Undesirable, technological advances in general capabilities that AI might assist with will increase. Given the potential for military artificial intelligence to increase these threats, it is not highlighted (J. Cox and H. Williams, 2021). It is important to note that AI capabilities have significant implications, as they can affect international strategic stability. If a country implements strategic policies incorrectly, it will impact other strategic stability, including the stability of the world's major military powers. Considering that weaponry AI-based certain And technology Which new developed very effective and sophisticated so that can neutralize the effect (Johnson, 2020).

RESEARCH METHODS

This study uses a qualitative research methodology to analyze how AI is utilized in the field of national defense to reformulate state defense policies based on IA technology for decision-making in national defense. Reformulating state defense policies that integrate Information Technology and Artificial Intelligence is no longer merely an option, but a strategic necessity to ensure the security and sovereignty of the Unitary State of the Republic of Indonesia in the digital era and the ever-evolving threat landscape. This policy must include the development of technological infrastructure, human resource capacity building, adaptive regulations, and the ethics of using IA in the defense context.

A holistic and integrated approach encompassing strategic, technical, ethical, legal, and operational aspects is crucial for the successful reformulation of an IA-based national defense policy. This process must be adaptive and responsive to the rapid development of IA technology.

With the right holistic and integrated approach, the reformulation of an IA Technology-Based National Defense Policy will produce a robust, adaptive, and responsible framework.

RESULT AND DISCUSSION

Policies governing national defense are crucial for maintaining a nation's security and sovereignty. With rapid technological advances, particularly in artificial intelligence (AI), it is crucial to revise national defense policies to leverage these technological capabilities for more effective and efficient decision-making.

Figure 1. Applications of artificial intelligence in the defense sector
Source: (Adib Bin Rashid , 2023)

The strategic steps in reformulating national defense policy through the integration of AI technology in decision-making are:

A. Integration of AI Systems in Intelligence Analysis to Automate Decision Making in Crisis Scenarios

In times of emergency or crisis, rapid and accurate decision-making is crucial. AI technology can facilitate the development of automated systems that support decision-making during conflict situations by evaluating various factors such as troop movements, weather conditions, and other strategic elements through automated analysis. This allows decision-makers to concentrate on strategic and operational analysis while AI handles real-time data processing (Britannica, 2024) .

Current AI technology can significantly increase the speed and accuracy of intelligence data analysis. Using machine learning and advanced analytical algorithms, AI can assist in processing and identifying threat patterns, both domestically and internationally. This allows decision-makers to gain a clearer understanding of the situation and respond more quickly to potential threats (Button, 2018).

AI System Integration in Intelligence Analysis is the application of Artificial Intelligence (AI) technology to enhance the ability to collect, analyze, and interpret data relevant to security and intelligence. The use of AI in this field enables intelligence agencies to process large volumes of data, identify hidden patterns, and make more accurate and rapid threat predictions in responding to threats (Chen, 2021). The use of AI in technology-based national defense policy reformulation for national defense decision-making is due to:

- AI can process large amounts of data from various sources (such as social media, intelligence reports, satellite imagery, and digital communications) to identify relevant trends and patterns. This technology enables more efficient data processing than manual methods.

- AI uses machine learning algorithms to analyze data and improve predictions based on identified patterns. For example, in analyzing terrorism threats or cyberattacks, AI systems can identify emerging patterns from past data and predict potential future threats.
- NLP technology in AI enables text analysis of documents or conversations in multiple languages. In the intelligence context, NLP is used to process unstructured data, such as conversations in the form of text messages, emails, or even interview transcripts, to extract valuable information.
- With the help of AI-based image recognition and video analysis technology, intelligence agencies can analyze images or videos obtained from satellites or surveillance cameras to identify suspicious objects or events.
- AI can be used to detect anomalies or unusual activity in observed data. For example, if a seemingly unusual behavioral pattern emerges in communications data or network activity, AI can provide early warning of potential threats.
- AI is also used to strengthen cybersecurity by identifying potential attacks or data leaks and responding quickly. In surveillance, AI enables real-time analysis of large volumes of data, providing clues to potential threats or suspicious activity.

The main benefits of integrating AI systems into intelligence analysis include: AI enables fast and precise data analysis, providing a shorter time to respond to threats. AI machines and algorithms can also improve the accuracy of intelligence analysis by identifying patterns that human analysts might miss. With the ability to analyze large-scale data, AI can be more effective in detecting hidden threats and providing better predictions. This is because AI can automate the process of data collection and analysis, allowing human analysts to focus more on strategic decisions and more in-depth analysis. However, the application of AI in intelligence analysis also faces challenges, such as privacy concerns, the potential for misuse of the technology, and the need for strict regulations to ensure that AI is used ethically and legally. Overall, the integration of AI into intelligence analysis promises significant improvements in operational efficiency and effectiveness across various security and intelligence sectors (Egorov, 2024).

Considering that Big Data Processing in AI Integration into Intelligence Analysis is a crucial aspect, intelligence often involves the collection and analysis of vast and varied amounts of data. With advances in artificial intelligence technology, big data processing has become more efficient, faster, and can provide deeper insights for detecting threats, predicting critical events, and supporting better decision-making in the intelligence world (Fox, 2007)

Big Data, in the context of intelligence, refers to the volume, velocity, and variety of data collected from various sources relevant to intelligence analysis. This data can come from databases, analytical reports, and transaction records. It can also come from social media, email, instant messages, satellite imagery, audio recordings, and video, as well as data stored in XML or JSON formats that require further analysis and processing. With data arriving in such large quantities and at such high speeds, manual processing becomes nearly impossible, making AI technology essential for effectively analyzing and interpreting such data (GWS Hager 2021)

AI plays a crucial role in processing Big Data in intelligence analysis through several methods, such as automated data processing, specifically using machine learning and deep learning techniques, the output of which can automatically analyze large-scale data. This can certainly reduce the need for time-consuming manual analysis and minimize the possibility of human error. Furthermore, AI can also manage Big Data by filtering and organizing data. This is because the data collected in intelligence analysis is often very large and diverse. The purpose of AI can be used to filter and organize the data to make it easier to analyze. The next role of AI in managing Big Data is by conducting predictive analysis and identifying patterns and anomalies. This is because one of the strengths of AI in intelligence analysis is its ability to predict events or threats based on existing data. By using machine learning (Herrmann, 1955).

In addition to the role of AI in assisting the military in solving major problems, there are also challenges in processing Big Data in Intelligence. Although AI provides many benefits in processing Big Data, it is undeniable that there are several challenges that must be faced by user resources, including the increase in volume, which requires a very large storage capacity. This is because as the number of data sources increases, the volume of data that needs to be analyzed continues to increase. Handling this ever-growing data requires enormous storage capacity and computing power, as well as algorithms that can handle large-scale data effectively. Furthermore, most of the data used in intelligence analysis, such as social media conversations, reports, and audio recordings, is often unstructured. This unstructured data requires more advanced natural language processing (NLP) and pattern recognition techniques, which are a challenge for AI. Another challenge in processing Big Data for intelligence analysis is the major issue related to data privacy. The use of personal data or surveillance of individuals without permission can raise ethical and legal issues, which require strict regulations to ensure that AI is used legally and fairly. Equally important is the problem of analyzing data that cannot be interpreted by AI itself. While AI can analyze large-scale data, difficulties often arise in interpreting the results. Some results may not be immediately understandable without deeper contextual understanding, which often requires further analysis by humans. Considering a personalized approach to AI will require programming and design because, no matter how the above trends and innovations are combined, they all follow the same principles. Tenth, these seven patterns are used alone or in various combinations, depending on the specific issue to which AI is applied (Brisson, 2021). Considering Big Data Processing with AI in intelligence analysis is a crucial step in addressing modern challenges in the increasingly complex world of intelligence. AI's ability to handle large amounts of data with high speed and accuracy can help intelligence agencies identify threats, anticipate events, and make faster and more informed decisions. Despite the challenges, the benefits offered by AI in Big Data processing are far greater, making it an invaluable tool in maintaining global security and stability.

B. Utilizing AI as a Strategic Step in Military Combat

AI can be used to create more sophisticated and realistic simulations for military planning and training. AI-driven simulations can present a variety of potential scenarios that may arise in the field, leading to more comprehensive planning and better decision-making. Furthermore, incorporating AI into training can enhance personnel's defense capabilities by offering diverse and unpredictable scenarios (Ilcev, 2024).

With rapid technological advancements, AI is increasingly being used to improve the effectiveness, efficiency, and security of military operations. One such application is in Intelligence, Surveillance, and Reconnaissance (ISR). This is because AI can be used to collect, analyze, and interpret intelligence data more quickly and accurately than humans. With the ability to analyze satellite images, drone footage, or data from sensors, AI can assist in monitoring areas, detecting threats, and providing deeper insights into enemy movements. For example, AI is used in analyzing images from drones or satellites to detect the presence of enemies or strategic targets more quickly and precisely. Furthermore, AI can also be used in the autonomy of combat vehicles and weapons systems. Of course, AI can provide benefits for combat vehicles and weapons systems to operate autonomously (Ilcev, 2024). For example, automation in the movement of drones, armored vehicles, fighter aircraft, and warships that can operate without direct intervention from human operators, whether in surveillance, attacks, or other missions. In the current era, the application of automation in military combat vehicles has been implemented by developing countries such as the United States, which has developed autonomous ground vehicles, such as the Ground Combat Vehicle and Robotic Combat Vehicle (RCV), which are designed to support combat operations and reduce risks to human personnel. In addition, the United States is also a major user of combat drones such as the MQ-1 Predator and MQ-9 Reaper, which can identify, monitor, and attack enemy targets autonomously or with minimal human

intervention. So, in short, it is clear that the main purpose of these systems is to act spontaneously in a greater capacity in a dynamic environment and to manage any unexpected events that are very common on the battlefield. These systems based on the pattern of goal-driven systems will make things easier for the armed forces (Deadman and R.H. Gimblett, 1994).

The use of AI in military combat extends beyond the aforementioned areas. AI is also used to strengthen cyber warfare capabilities, both in attacking and protecting critical infrastructure. This aligns with the function of AI itself, which can be used to quickly detect and respond to cyber threats, as well as analyze potential vulnerabilities. With AI intelligence, military personnel in several countries have implemented or utilized more realistic combat simulations for military training. These simulations can simulate complex battlefield conditions with various variables, including dynamic enemy movements, weather, and tactics. The current use of AI, particularly in strategic military combat, is crucial because it significantly improves the precision of attacks by pinpointing precise targets and directing weapons to strike with high accuracy. This can be used to destroy enemy targets with a lower risk of collateral damage. AI can be used to detect hidden or otherwise invisible threats, such as landmines, explosives, or chemical weapons. With AI-powered sensors and algorithms, these threats can be identified and eliminated more quickly and efficiently (JR Thompson, & SB Reid. (2020)). This is in line with America, where since 2003, the 8-wheeled fighting vehicle known as the Stryker has been produced and used by the American military to bridge the capability gap between the Abrams and Bradley, which are heavy armored vehicles, and the High Mobility Multipurpose Wheeled Vehicle, which is a light armored vehicle (HMMWV), both equipped with AI. The Stryker's engine, transmission, hydraulics, wheels, and tires are shared by various types of vehicles, allowing for reconfiguration to perform various tasks (mobile weapon systems, infantry carriers, mortar carriers). In addition, Germany, Lithuania, Australia, and the Netherlands have also used the Boxer, a multipurpose armored fighting vehicle, since 2011. The Boxer consists of two important components: a platform and a detachable mission module (Li and B.I. Epureanu, 2020).

Therefore, AI has significant potential to enhance military combat capabilities. From surveillance and intelligence analysis to increased precision strikes and logistical maintenance, AI helps create operational and strategic advantages that are crucial in the modern military. As AI technology continues to advance, the military's ability to respond to threats, adapt to situations, and make rapid and accurate decisions will be further enhanced (Jia, 2016).

C. AI as a Cybersecurity System and National Defense Infrastructure Protection

In recent decades, developments in information and communication technology (ICT) have transformed the way countries, organizations, and individuals interact, work, and manage data. In the military and defense sector, reliance on advanced technologies such as weapons control systems, communications networks, IoT devices, and autonomous platforms has increased. However, this reliance also carries significant risks of cyber threats that can disrupt or damage critical infrastructure, both in the cyber and physical worlds (Kiono, 2023).

Cybersecurity in the military is becoming increasingly important because cyberattacks are now carried out not only by individuals or small groups, but also by countries with high technological capabilities. These threats, including malware, distributed denial-of-service (DDoS) attacks, ransomware, and zero-day attacks, can compromise vital defense systems, disrupt communications, or even control autonomous devices, such as unmanned aerial vehicles (UAVs) or combat robots (L. Zeng, & KY Xu. 2019).

To address these threats, countries around the world are increasingly relying on artificial intelligence (AI) as a key system for cybersecurity and defense infrastructure protection. As technology advances, cyber threats are becoming increasingly sophisticated and difficult to detect. Attacks on national defense systems or critical infrastructure can now be carried out in stealthier and more dangerous ways. Therefore, traditional methods of addressing cyber threats are no longer effective. Smarter cyberattack technologies, such as those that use machine learning

algorithms to evade detection, are on the rise. This requires more sophisticated and responsive security systems. Systems that connect the virtual and physical worlds (cyber-physical systems), such as weapons control systems or autonomous vehicles, are now becoming targets of attack. These threats are increasingly impacting the continuity of military operations and can have fatal consequences (Leonard, 2015).

In the military, threats don't just come from foreign countries or terrorist groups, but can also stem from previously unseen cyberattacks. Traditional cybersecurity systems, which are more reactive in nature, often delay in detecting and responding to threats. Cybersecurity systems that utilize IA can detect threats more quickly and provide a more appropriate response, preventing further damage. This is crucial, as fast response times can mean the difference between failure and success in defending critical infrastructure. By using machine learning, IA can identify patterns or anomalies that traditional security systems might miss, such as attacks carried out in novel ways (You, 2023).

Furthermore, defense infrastructure, such as communications systems, command centers, and weapons control, is a prime target for cyberattacks. Destruction or disruption of these infrastructures can destabilize a nation and undermine defense capabilities. Systems that manage advanced weapons must have a very high level of protection to prevent hacking or misuse by unauthorized parties. AI is being used to provide deeper protection and faster threat detection. Data and communications security are crucial for the smooth running of military operations. Attacks on these communications could disrupt coordination between military units or misinform troops (Nunes, 2021).

The use of autonomous technologies, such as unmanned combat vehicles, drones, and IoT (Internet of Things) devices, is growing in the military. While these technologies increase military efficiency and capabilities, they also open new opportunities for cyberattacks. Autonomous vehicles and platforms used in military operations require enhanced protection, as they are highly vulnerable to disruptions caused by cyberattacks. For example, the seizure of control of a drone or combat vehicle could be devastating. IoT devices, such as surveillance sensors or tracking devices, are increasingly used in military contexts. Therefore, protecting these IoT devices from cyberthreats is crucial, especially when they are connected to larger systems (Nunes, 2022).

Rapid advances in artificial intelligence (AI) and machine learning are opening up opportunities to enhance threat detection and critical infrastructure protection. AI's ability to process and analyze massive amounts of data at high speed makes it highly effective for intrusion detection, post-attack recovery, and enhancing system resilience. AI can not only detect threats quickly but also respond automatically, isolate them, and restore affected systems. AI-based systems can also autonomously address potential damage and resume critical operations (Paramasivam, 2024).

Countries with critical defense infrastructure are becoming targets of increasingly sophisticated cyberattacks, which can threaten data security, engagement in conflicts, and national defense policies. Adversaries or terrorist groups can use hacking techniques to access sensitive data or compromise systems that manage military operations. Protecting defense infrastructure involves protecting not only weapons or devices but also the data used in strategic decision-making. Failure to protect this data can lead to significant losses (R. Legvold, 2020).

Therefore, the use of artificial intelligence (AI) as a cybersecurity system and defense infrastructure protection is rooted in the need to protect critical infrastructure that is increasingly vulnerable to sophisticated attacks. Facing increasingly complex and diverse threats, AI offers solutions to improve detection, analysis, response, and recovery from cyber threats with greater speed and accuracy. Given the importance of cybersecurity in the defense sector, AI is a crucial element in maintaining the sustainability and security of national defense operations (Sari, 2024).

In today's digital landscape, cyber threats pose significant challenges to national security. Policies incorporating AI must be complemented by robust cybersecurity measures to protect critical infrastructure. While AI can improve detection and response to cyber threats, prioritizing the protection of sensitive data and defense systems remains crucial. Artificial Intelligence (AI) plays a crucial role in cybersecurity and the protection of defense infrastructure. As cyber threats , whether from attacks by states or terrorist groups, become increasingly complex, AI technology provides the ability to detect, analyze, and respond to threats more quickly and efficiently than traditional methods. Furthermore, AI can be used to secure military communications networks, which are the backbone of defense operations. AI-based systems can automatically assess risks, identify potential vulnerabilities, and optimize protection against cyber threats, both in network and communications infrastructure. Critical infrastructure that manages weapons control systems, energy, and other systems requires special protection. AI can identify and counter cyber threats that could damage or control these systems (Shahbakhsh, 2022).

AI also helps manage data encryption to ensure that sensitive data, both in transit and at rest, remains secure from attacks. AI-based algorithms can be used to detect potential data leaks or unauthorized access and immediately secure the data. AI-based systems can be used to improve access control and authentication in military infrastructure by using biometric recognition (e.g., fingerprints or facial scans) and layered verification to prevent unauthorized access (Sirry, 2024).

AI also serves as a defense system against AI-enabled attacks. The threat of cyberattacks is growing with the adoption of AI by attackers. AI can be used to launch more sophisticated cyberattacks, such as Distributed Denial of Service (DDoS) attacks or automated phishing, which are very difficult to detect by traditional defenses. Therefore, defense systems must be equipped with AI that can counter these types of attacks automatically and effectively. By using AI, the system can continuously adapt to new and more sophisticated threats, thus responding appropriately to AI-driven attacks (Stubbs, 1994).

In the event of a successful attack, AI can be used to accelerate recovery through automation. AI can detect vulnerabilities and quickly repair them or isolate the infected portion of the network, minimizing damage and ensuring that military systems remain functional. AI-based systems can help design defense infrastructure that is more resilient to attacks by modeling threats and developing mitigation measures to minimize the impact of potential attacks. AI is also being used to protect military IoT devices. With the increasing use of IoT devices in defense systems, such as sensors, surveillance devices, and autonomous weapons, AI is crucial for maintaining the security of these devices. Attacks on IoT devices could expose sensitive data or compromise the system. Therefore, AI is being used to monitor and assess the security of IoT devices in real-time to detect threats and intrusions against devices connected to military networks (Via, 2024).

By integrating artificial intelligence into national defense strategies, countries can enhance their analytical and decision-making capabilities to address increasingly complex challenges. However, it is crucial that this approach be accompanied by strict regulations and adequate training to ensure effective implementation. However, it is important to remember that the accuracy of AI processing and augmentation systems is highly vulnerable to fraud, despite this being a persistent intelligence and strategic issue predating the cyber era. Reliance on AI combined with the exploitation of the technology by malicious actors can significantly exacerbate disinformation operations. Therefore, the solution is for governments to establish a legislative framework that can regulate and determine how new technologies interact proportionally and effectively. These facts regarding AI must be considered because they threaten global peace and stability (Anastassov and R. Legvold and C.F. Chyba, 2021).

Given the benefits and uses described above, the importance of AI in national decision-making, particularly in supporting the nation's defense and security system, is supported by the increasing importance of artificial intelligence technology in the defense sector, which is felt

along with rapid technological advances. Therefore, the use of AI in decision-making in the defense sector can accelerate and simplify large-scale data analysis, increase accuracy, and provide better insights for leaders in formulating policies. Therefore, reformulating national defense policies with an AI-based approach is highly relevant to increasing the effectiveness and efficiency of decision-making. Considering that the goal and benefit of policy reformulation is to increase the speed of decision-making, it can also improve the accuracy of predictions supported by AI algorithms that can be used to analyze patterns and trends in intelligence data to provide more accurate projections of potential threats that may arise, this certainly can formulate more appropriate strategies. Furthermore, with the involvement of AI, the state can achieve efficiency in resource management, especially in the budget (Wang, 2016).

Steps in implementing the reformulation of AI involvement policies in decision-making can start from the integration of AI technology in the Command and Control System, the development of AI-based cybersecurity systems, training and development of human resources in AI technology, increasing international cooperation in the development of AI technology to establish intelligent diplomacy relations between two or more countries and most importantly the importance of creating ethical and regulatory policies for AI technology in defense. Reformulation of national defense policies based on AI technology for decision-making has great potential in increasing the effectiveness and accuracy in responding to threats and increasing the efficiency of defense resource management. However, the successful implementation of this policy is highly dependent on technological readiness, human resource training, and proper management of existing risks and challenges (Xu, 2024).

CONCLUSION

The use of artificial intelligence (AI) in cybersecurity and defense infrastructure protection is increasingly becoming a crucial element in ensuring the resilience and sustainability of military operations. AI technology helps detect, analyze, and respond to threats quickly and accurately, enhancing the protection of critical infrastructure. AI provides the ability to process large amounts of intelligence data and generate insights automatically. In crisis situations, where decisions must be made quickly, AI-based systems can analyze information in real time, identify suspicious patterns, and provide optimal recommendations for action. By using machine learning algorithms and big data analytics, AI enables faster and more accurate decision-making, reducing the risk of human error, which can be fatal in critical situations. Automation in Decisions AI can support decision-making, especially in scenarios that require a rapid response to incoming threats. In the military, AI is increasingly being used as an integral part of combat strategy. AI can assist in designing tactics, optimizing weapons control, and enhancing the capabilities of autonomous vehicles and drones in military operations. The use of AI enables greater efficiency and effectiveness in combat, providing a significant competitive advantage. Tactical and Strategy Optimization: AI is used to design and test tactical scenarios that can be used by troops, both on the conventional battlefield and in cyber conflict. The use of AI in cybersecurity and defense infrastructure protection is a crucial strategic step in the digital era and modern warfare. AI not only strengthens cyber defenses by automatically detecting threats and responding quickly, but also supports better decision-making in crisis scenarios, increases efficiency in combat, and ensures that the country's critical infrastructure is optimally protected. With the increasingly deep integration of AI systems in intelligence analysis and decision-making automation, and By utilizing AI as a strategic step in combat, a country can gain a significant advantage in facing the complex and diverse threats in today's military world. Therefore, reformulating national defense policy with an AI technology-based approach is highly relevant for increasing the effectiveness and efficiency of decision-making.

REFERENCES

Adib Bin Rashid, A. K. K., Ahamed Al Hassan Sunny, & Mehedy Hassan Bappy. (2023). *Artificial intelligence in the military: An overview of the capabilities, applications, and challenges*. Industrial and Production Engineering Department, Military Institute of Science and Technology (MIST), Dhaka, Bangladesh.

Adam, E. F., Brown, S., Nicholls, R. J., et al. (2016). A systematic assessment of maritime disruptions affecting UK ports, coastal areas and surrounding seas from 1950 to 2014. *Natural Hazards, 83*(1), 691–713.

Akbayrak, E., & Tural, M. K. (2017). Maritime search and rescue (MSAR) operations: An analysis of optimization asset allocation. In *Proceedings of the Modeling, Dynamics, Optimization and Bioeconomics II*, Cham, France.

Anastassov. (2021). Artificial intelligence and its possible use in international nuclear security law. *BAS Humanities and Social Sciences, 1*.

Bourget, N., Deblock-Bellamy, A., Blanchette, A. K., et al. (2018). Use and psychometric properties of the Reintegration to Normal Living Index in rehabilitation: A systematic review. *Annals of Physical and Rehabilitation Medicine, 61*(4), 262–269.

Breiman, L. (2001). Random forests. *Machine Learning, 45*(1), 5–32. https://doi.org/10.1023/A:1010933404324

Brisson, G., Pereira, R., & Prada, R. et al. (2021). Artificial intelligence and personalization opportunities for serious games. *Proceedings of the AAAI Conference on Artificial Intelligence and Interactive Digital Entertainment, 8*(5), 51–57.

Britannica, The Editors of Encyclopaedia. (2024, May 7). United States Coast Guard. *Encyclopedia Britannica*. https://www.britannica.com/topic/United-States-Coast-Guard

Button, R. (2018). International law and search and rescue. In J. Schildknecht, R. Dickey, & M. Fink (Eds.), *Operational Law in International Straits and Current Maritime Security Challenges* (pp. 101–141). Springer.

Chen, M., Zeng, F., Xiong, X., et al. (2021). A maritime emergency search and rescue system based on unmanned aerial vehicle and its landing platform. In *2021 IEEE International Conference on Electrical Engineering and Mechatronics Technology (ICEEMT)* (pp. 758–761). IEEE.

Cox, J., & Williams, H. (2021). The unavoidable technology: How artificial intelligence can strengthen nuclear stability. *The Washington Quarterly, 44*(1), 69–85.

Deadman, P., & Gimblett, R. H. (1994). A role for goal-oriented autonomous agents in modeling people–environment interactions in forest recreation. *Mathematical and Computer Modeling, 20*(8), 121–133.

Egorov, V. V., & Maslakov, M. L. (2024). Increasing the probability of transfer GMDSS broadcast messages when transmitted over HF channel in case fading. *Proceedings of Telecommunication University, 10*(1), 58–64.

Fox, U. H. (2007). Maritime search and rescue: Benefits or burden for society? *WMU Journal of Maritime Affairs, 6*(1), 75–87.

GWS Hager. (2021). *Machine learning for cybersecurity: A review. Synthesis Lectures on Artificial Intelligence and Machine Learning, 15*(2), 1–52. https://doi.org/10.2200/S00184ED1V01Y202103AIM060

Herrmann, F., & Mandol, L. (1955). Studies of pH of sweat produced by different forms of stimulation. *Investigative Dermatology, 24*, 225–246. https://doi.org/10.1038/jid.1955.36

Ilcev, D. S. (2024). Architecture and characteristics of antenna systems onboard Inmarsat spacecraft for mobile satellite communications. *Journal of Maritime Research, 21*(1), 1–9.

Jia, M., Chew, W. M., Feinstein, Y., Skeath, P., & Sternberg, E. M. (2016). Quantification of cortisol in human eccrine sweat by liquid chromatography–tandem mass spectrometry. *Analyst, 141*, 2053–2060. https://doi.org/10.1039/c5an02387d

Johnson, J. (2020). Artificial intelligence in nuclear warfare: A perfect storm of instability? *The Washington Quarterly, 43*(2), 197–211.

Kiono, F., & Indriyati, R. (2023). Optimization tool and system GMDSS as rescue efforts soul on KN. SAR Sadewa 231. In *Proceedings of the National Seminar on Maritime and Interdisciplinary Studies, 2*(1), 71–77.

Legvold, R., & Chyba, C. F. (2020). Introduction: The search for strategic stability in a new nuclear era. *Dædalus, 149*(2), 6–16.

Leonard, T. J., Gallo, P., & Véronneau, S. (2015). Security challenges in United States sea ports: An overview. *Journal of Transportation Security, 8*(1), 41–49.

Li, B. I., & Epureanu, B. I. (2020). AI-based competition of autonomous vehicle fleets with application to fleet modularity. *European Journal of Operational Research, 287*(3), 856–874.

L. Zeng, & Xu, K. Y. (2019). *Deep learning and its applications to natural language processing. Synthesis Lectures on Artificial Intelligence and Machine Learning, 10*(1), 20–40. https://doi.org/10.2200/S00288ED1V01Y201902AIM030

Ma, Y., Wang, Z., Yang, H., & Yang, L. (2020). Artificial intelligence applications in the development of autonomous vehicles: A survey. *IEEE/CAA Journal of Automatica Sinica, 7*(2), 315–329.

Nunes, M. J., Cordas, C. M., Moura, J. J. G., Noronha, J. P., & Branco, L. C. (2021). Screening of potential stress biomarkers in sweat associated with sports training. *Sports Medicine Open, 7*, 8. https://doi.org/10.1186/s40798-020-00294-3

Nunes, M. J., Valério, G. N., Samhan-Arias, A., Moura, J. J. G., Rouco, C., Sousa, J. P., & Cordas, C. M. (2022). Screen-printed electrodes testing for detection of potential stress biomarkers in sweat. *Electrocatalysis.* https://doi.org/10.1007/s12678-022-00709-7

Paramasivam, R., Kumar, P., Lai, W. C., et al. (2024). Deep ensemble model-based moving object detection and classification using SAR images. *Frontiers in Earth Science, 11*, 1288003.

Sari, R. D. A. K., Nalurita, W., & Dewa, R. D. (2024). The role of coastal radio stations in maritime safety in Muara waters. *Journal of Shipping Management National, 7*(1).

Shahbakhsh, M., Emad, G. R., & Cahoon, S. (2022). Industrial revolutions and transition of the maritime industry: The case of seafarer's role in autonomous shipping. *Asian Journal of Shipping and Logistics, 38*(1), 10–18.

Sirry, J., & Patra, A. N. (2024). Harnessing modern technological advances in search and rescue missions. In *SoutheastCon 2024* (pp. 240–249). IEEE.

Stubbs, C. B. B. (1994). The US Coast Guard: A unique instrument of US national security. *Marine Policy, 18*(6), 506–520.

Thompson, J. R., & Reid, S. B. (2020). Applications of reinforcement learning in autonomous systems. *Synthesis Lectures on Artificial Intelligence and Machine Learning, 12*(3), 67–98. https://doi.org/10.2200/S00334ED1V01Y202005AIM034

Via, J. P., Sigouin, D., & St. Laurent, M. H. (2024). Seasonal shifts in the habitat selection patterns of male American Marten (*Martes americana*) at a fine spatial scale. *Journal of Mammalogy.*

Wang, Y., & Zhu, X. X. (2016). Robust estimators for multipass SAR interferometry. *IEEE Transactions on Geoscience and Remote Sensing, 54*(2), 968–980.

Xu, J., Fan, X., Jian, H., et al. (2024). YoloOW: A spatial scale adaptive real-time object detection neural network for open water search and rescue from UAV aerial imagery. *IEEE Transactions on Geoscience and Remote Sensing.*

Yokota, Y., Ishikawa, T., & Watanabe, S.-I., et al. (2016). Seafloor geodetic constraints on interplate coupling of the Nankai Trough megathrust zone. *Nature, 534*(7607), 374–377.

Zhou, X., Cheng, L., Min, K., et al. (2020). A framework for assessing the capability of maritime search and rescue in the South China Sea. *International Journal of Disaster Risk Reduction, 47*, 101568.