Image: Jurnal Riset Manajemen

E-ISSN: 2657-0688, P-ISSN: 2339-2878
Journal homepage: https://ejournal.upi.edu/index.php/image

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

Widiyanto Saputro[1*], Asep Adang Supriyadi[2], Guntur Eko[3]

[1] *Defence Management, Faculty of Defence Science, Indonesia Defense University, Jakarta, Indonesia*
[2] *Defence Science, Faculty of Defence Science, Indonesia Defense University, Jakarta, Indonesia*
[3] *Defence Economic, Faculty of Defence Science, Indonesia Defense University, Jakarta, Indonesia*

Abstract

The rapid advancement of Artificial Intelligence (AI) has significantly influenced global military strategies, leading to a paradigm shift in national defense policies. Countries such as the United States, China, and Russia have integrated AI into their defense frameworks, utilizing autonomous systems, cyber defense, and AI-driven decision-making processes. However, Indonesia's current defense policy remains heavily reliant on conventional approaches, necessitating an adaptive reformulation to incorporate AI technologies. This study employs a qualitative analytical approach, utilizing a thematic content analysis of 41 peer-reviewed journals sourced from Scopus and Elsevier. The research focuses on AI integration in national defense, strategic decision-making frameworks, cybersecurity policies, and ethical considerations. By examining AI-driven military applications and governance structures, this study aims to present actionable insights for policy reform. AI enhances military efficiency by enabling rapid decision-making, real-time intelligence analysis, and predictive modeling for conflict scenarios. However, challenges such as ethical dilemmas, cybersecurity vulnerabilities, and adversarial learning risks remain pressing concerns. Indonesia faces constraints in infrastructure, regulatory frameworks, and technological expertise, requiring immediate policy intervention to align national defense strategies with AI advancements. Reformulating Indonesia's defense policy to integrate AI is crucial for ensuring national security resilience in the digital era. The study recommends establishing a National AI Defense Agency, developing robust cybersecurity mechanisms, and enforcing ethical guidelines for autonomous military applications.

Article Info

Correspondence:
Widiyanto Saputro
(wsaputro@gmail.com)

Article History:
Submitted: 05-02-2025
Revised: 17-03-2025
Accepted: 21-04-2025
Published: 30-04-2025

JEL Classification:
M12, O15, J24

Keyword:
AI Ethics;
Artificial Intelligence;
Autonomous Systems;
Defense Decision-Making;
National Defense

1. INTRODUCTION

The paradigm shift of global conflict in the 21st century demands a profound transformation in national defense policy. The character of warfare has evolved from conventional combat to unconventional forms such as cyber warfare, asymmetric warfare, and proxy war that often do not have a clear front line. One of the main characteristics of this evolution is the involvement of disruptive technology, especially artificial intelligence (AI), in the planning and implementation of military operations (Johnson, 2022). Major

countries such as the United States, China, and Russia have integrated AI systems into various layers of defense strategy, from autonomous weapons systems to machine learning-based command control centers.

In the Indonesian context, contemporary threats such as digital disinformation, cyber network infiltration, and conflicts based on global economic-political interests demand rapid adaptation of national defense policy. Unfortunately, Indonesia's current defense policy framework still relies heavily on traditional approaches and has not been fully able to accommodate the need for fast, precise, and real-time data-based decision-making. This is a strategic gap that has the potential to be exploited by state and non-state actors.

According to Mahoney (2020), the development of AI will be a major determinant in the form and outcome of future warfare. Even in the realm of decision-making, AI can help produce strategic analysis in a very short time, reducing human error due to the pressure and complexity of information on the battlefield (Sun et al., 2021). However, the use of AI in the defense sector also invites new concerns such as loss of human control, algorithmic bias, and the potential for conflict escalation without rational intervention (Firlej & Taeihagh, 2021).

1.1. Problem Formulation

Based on this background, the main problems raised in this study are: 1. What is the existing condition of Indonesia's national defense policy in responding to the development of AI technology? 2. What are the opportunities and challenges of implementing AI in the country's defense decision-making system? 3. How can a defense policy reformulation framework that is adaptive to AI developments be designed strategically?

1.2. Lessons for Indonesia

The main objectives of this study are: 1. To examine the position and readiness of Indonesia's defense policy in facing the AI technology revolution. 2. Identifying the potential for utilizing AI to support military and defense decision-making. 3. Formulating a conceptual framework for the reformulation of AI-based national defense policies that are adaptive, ethical, and responsive.

1.3. Benefits of Research

This study is expected to provide theoretical and practical contributions as follows: (1) Theoretically, enriching the literature on defense science and public policy in the context of digital transformation. (2) Practically, providing evidence-based recommendations for policy makers in the reformulation of national defense strategies.

1.4. Brief Literature Review

The integration of AI in defense systems has become a dominant theme in various global studies. Johnson (2022) emphasized that AI utilized in the context of military strategy not only increases efficiency, but also risks reducing the role of humans in crucial decisions, which can have an impact on strategic stability. Crumpacker et al. (2022) and Yaozhong et al. (2023) show that reinforcement learning algorithms are capable of developing autonomous air tactics that even surpass human intuition. In addition, Firlej and Taeihagh (2021) emphasize the importance of human-in-the-loop policies in the use of autonomous weapons systems. Without it, the system can have serious ethical and legal implications. On the other hand, Khaleel et al. (2024) and Muhati & Rawat (2021) outline the need for AI-based adaptive cyber defense to counter complex and dynamic adversarial attacks. Gottemoeller et al. (2022) remind us of the importance of cross-domain integration land, sea, air, space, and cyber in NATO's strategic policy based on emergent technology. In this context, Indonesia needs to immediately respond to the challenges of digital defense policy so as not to be left behind by regional and global dynamics.

1.5. Evolution of Defense Strategy in the Era of Smart Technology

In the last decade, global defense strategy has undergone a fundamental shift influenced by the emergence of artificial intelligence (AI), big data, and autonomous system networks. Modern warfare is no longer solely determined by conventional military power, but by a country's ability to integrate high technology into its defense system (Mahoney, 2020). AI enables conflict scenario simulations, predictive analysis, and faster and more accurate decision execution, beyond the limits of human capabilities. This transformation also drives the emergence of what is known as machine-speed warfare, where strategic decisions can be made in milliseconds based on real-time information analyzed by algorithms (Johnson, 2022). In this context, humans are no longer the only actors in the military decision-making circle, but are beginning to share roles with machine learning-based AI systems.

1.6. Experience of Developed Countries: AI in Military Operations

The United States, through the Joint Artificial Intelligence Center (JAIC) program and the Defense Advanced Research Projects Agency (DARPA), has long developed an AI-based command and control system. This system not only functions to support decisions, but can also autonomously detect threats, provide response recommendations, and even execute commands in emergency contexts (Guice, 1998). On the other hand, China is targeting AI supremacy as part of its national military strategy through the Civil-Military Fusion initiative. This strategy utilizes the synergy between civil and military research in the development of cutting-edge technologies, including facial-based surveillance, UAVs (unmanned aerial vehicles), and cyber warfare systems (Gottemoeller et al., 2022). The use of AI has also been tested in air combat simulations. Sun et al. (2021) show how the Multi-Agent Hierarchical Policy Gradient algorithm is able to produce adaptive, effective, and unpredictable air tactics, even for experienced human pilots.

1.7. Domain Change and Multi-Domain Operations

The current military strategy is moving towards a cross-domain approach or known as Multi-Domain Operations (MDO). This approach involves the integration of operations on land, sea, air, space, and cyber, where AI acts as a connector and manager of information across all domains simultaneously (Gottemoeller et al., 2022). With AI, every sensor, weapon, and communication system can be interconnected, creating a responsive and adaptive defense ecosystem. For example, modern air defense systems can detect, classify, and engage targets in seconds after AI recognizes enemy attack patterns (Ayub Khan et al., 2023).

1.8. Ethical and Strategic Tensions

However, the increasing use of AI in the defense context also raises strategic and ethical dilemmas. One of them is the risk of delegating military decisions to machines without human involvement, potentially creating an escalation of conflict without rational control (Johnson, 2022; Firlej & Taeihagh, 2021). In addition, there is the threat of information manipulation by non-state actors using deepfakes, bots, and AI-enhanced automated disinformation techniques (Whyte, 2020). In a study of military ethics, Brown-Gaston & Arora (2021) stated that military robots and autonomous weapons systems must be subject to universal moral principles, and equipped with design-based ethical tools to ensure compliance with international humanitarian law.

1.9. Lessons for Indonesia

Seeing these developments, Indonesia as a developing country with an important geostrategic position must immediately evaluate and adjust its defense strategy to be relevant to global dynamics. There needs to be an awareness that the integration of technology such as AI is not just an option, but a necessity in ensuring information superiority and speed of decision-making. The initial steps that can be taken are to build a

national defense data infrastructure, develop Indonesian contextual AI algorithms, and collaborate with research institutions and universities in developing AI-based decision support systems. In addition, it is necessary to formulate ethical policies and a legal framework to ensure accountability in the use of AI for military purposes. By understanding the global context and the dynamics of changes in the defense paradigm due to AI technological disruption, Indonesia can prepare strategic steps in formulating adaptive and intelligent technology-based defense policies.

1.10. Potential of Artificial Intelligence in Defense Systems

Artificial intelligence (AI) offers significant opportunities in supporting modern defense systems. One of the main advantages of AI is its ability to process large amounts of data in real-time and produce decision recommendations with high accuracy (Crumpacker et al., 2022). In military operations, the speed and accuracy of decision making are crucial factors that can determine the success or failure of a mission. Therefore, AI can be a force multiplier for the military through integration into control, navigation, and combat systems (Yaozhong et al., 2023). Sun et al. (2021) show how the application of AI in air tactics simulations produces adaptive strategies through self-play learning. This strengthens the argument that AI can contribute to more efficient tactical development compared to a purely human approach. Furthermore, Ayub Khan et al. (2023) stated that the application of AI and blockchain in military energy distribution and logistics can create a safe, transparent, and efficient system.

1.11. Application of AI in Decision Making

Decision making in the context of defense requires rapid response to complex and dynamic situations. AI supports decision making through prediction systems, risk classification, and enemy pattern recognition (Huang et al., 2021). In the case of combat operations, AI can integrate sensor data, satellite imagery, terrain reports, and enemy intelligence to provide tactical advice in a short time (Pan & Bao, 2021). Johnson (2022) warns that AI not only speeds up the analysis process but also opens up opportunities for autonomous decision-making models that reduce the role of humans. This can increase efficiency but also invites criticism from the side of accountability and civilian control over military decisions.

1.12. Strategic Risk and Technology Dependence

Although AI has many benefits, its implementation is not without challenges and risks. One of the main risks is dependence on algorithmic systems that can be the target of cyber attacks or data manipulation (Khaleel et al., 2024). Adversarial attacks can influence the decisions of AI systems by providing deliberate input to mislead predictions (Muhati & Rawat, 2021). Furthermore, Johnson (2022) highlights the potential for moral failure if AI is used to make life-and-death decisions without human participation. Autonomous weapons systems, while technically effective, can create ethical and legal dilemmas, especially when attacking civilian targets or misclassifying targets.

1.13. Ethical and Legal Risks

Firlej and Taeihagh (2021) emphasize the importance of implementing the principle of human-in-the-loop or meaningful human control in the use of AI-based weapons systems. Without human involvement, decisions made by the system may violate international humanitarian law or universal ethical values. Brown-Gaston and Arora (2021) suggest the importance of ethical software in the design of military AI systems that can identify violations of moral principles and prevent inhumane actions. This underscores that the integration of AI into defense systems requires not only technical excellence but also strong normative regulation.

1.14. AI-Based Disinformation and Information Warfare

AI is also used by non-state actors to spread disinformation in information warfare. Deepfake technology, automated bots, and information distribution algorithms have been used to influence public opinion, undermine government credibility, and trigger domestic instability (Whyte, 2020). In the context of defense, AI's ability to filter and classify information is important to distinguish between valid news and propaganda. Without a reliable detection system, the military could make decisions based on false information, leading to misdirected targets or unnecessary escalation of conflict.

1.15. Implementation Challenges in Indonesia

Indonesia faces major challenges in adopting AI for defense purposes. Immature data infrastructure, lack of human resources with AI expertise, and dependence on foreign vendors are major obstacles. In addition, the absence of clear regulations regarding the limitations of the use of AI in the military realm also increases the potential for misuse or leakage of technology (Beusmans & Wieckert, 1989). To address this, a national roadmap is needed that includes research development, collaboration between the military and universities, and investment in cybersecurity and national data centers (Gottemoeller et al., 2022). By identifying the opportunities and risks of implementing AI in defense decision-making, Indonesia can develop a strategy that is not only technologically efficient but also upholds ethical values and national sovereignty.

2. METHODS

This study uses a qualitative-descriptive approach with a content analysis method on 41 relevant international scientific journals, obtained from the Scopus and Elsevier databases. This method aims to understand the strategic implications, opportunities, and risks of the integration of artificial intelligence (AI) in national defense policy in depth and systematically (Johnson, 2022; Firlej & Taeihagh, 2021). This research was conducted with a systematic literature review, which includes a study of previous research related to AI in military strategy, technology-based decision-making systems, cybersecurity, and ethical aspects in the use of AI for defense. The data collected were categorized based on four main themes: defense strategy, AI technology, military decision-making, and policy implications (Guice, 1998; Gottemoeller et al., 2022). In addition to document analysis, this study applies a comparative approach, by comparing the implementation of AI-based defense policies in various developed countries such as the United States and China (Mahoney, 2020). This study also examines algorithmic risks and conflict escalation, which are analyzed through case studies of the use of AI in autonomous weapon systems and combat strategy simulations (Crumpacker et al., 2022; Sun et al., 2021).

To ensure the validity and reliability of the research results, a data verification process was carried out with a triangulation approach, which involved comparisons between various academic sources and insights from defense policy experts (Brown-Gaston & Arora, 2021; Khaleel et al., 2024). With this methodology, this study is expected to provide adaptive, ethical, and technology-based policy recommendations to support the reformulation of Indonesia's defense policy in the era of artificial intelligence.

3. RESULT AND DISCUSSION

3.1. Urgency of Policy Reformulation

The rapid development of artificial intelligence (AI) technology has shifted the paradigm in the defense sector. Major countries such as the United States, China, and Russia have developed AI-based defense systems in various aspects, from reconnaissance, decision-making to autonomous weapons systems (Guice, 1998; Gottemoeller et al., 2022). Indonesia, as an archipelagic country with a strategic location in the Indo-Pacific region,

needs to immediately adjust its defense policy to be adaptive to this development. The urgency of policy reformulation arises because Indonesia's current national defense policy does not explicitly regulate the integration of AI into the defense system. In addition, there is no adequate regulatory and normative framework to manage the risks of using AI, both in terms of ethics, law, and national security. Therefore, a comprehensive approach is needed to develop a responsive and futuristic policy framework (Johnson, 2022).

3.2. Principles and Principles of Reformulation

In designing AI-based defense policies, there are a number of principles and principles that must be used as the main foundation: (1.) National Sovereignty: The use of AI in defense systems must continue to uphold the principle of national sovereignty and not reduce the role of humans in final decision-making (Firlej & Taeihagh, 2021). (2.) Human-in-the-loop and Accountability: All AI-based systems used in military operations must still involve meaningful human control, to ensure accountability and prevent violations of humanitarian law (Brown-Gaston & Arora, 2021). (3.) Ethics and Law: The use of AI must be subject to the principles of universal morality and international legal regulations, and must not be used for aggressive actions or human rights violations (Navas-Camargo & Ardila, 2022). (4.) Transparency and Auditability: Every AI system in defense must be auditable and its decision logic traceable, in order to avoid bias and systemic errors (Johnson, 2022).

3.3. Strategic Pillars of Policy Reformulation

AI-based defense policy reformulation should include four main strategic pillars: (a) AI-Based Command and Control System. The application of AI in military command and control (C2) systems can improve communication efficiency, coordination, and reaction speed to threats. Crumpacker et al. (2022) showed that an AI-based dynamic programming approach can optimize combat maneuvers automatically. (b) Integration of AI in Simulation and War-Gaming. AI-based simulations enable the development of more realistic and data-driven tactics and strategies. Technologies such as deep reinforcement learning can be used for military training and conflict scenario prediction (Sun et al., 2021; Pan & Bao, 2021). (c) Strengthening Cyber Defense and Network Security. With the increasing cyber threats, AI is becoming an important tool in detecting and responding to attacks in real-time. AI-based cyber defense systems are able to classify anomalies, recognize zero-day attacks, and mitigate damage faster than conventional systems (Khaleel et al., 2024; Muhati & Rawat, 2021). (d) Development of Domestic Data and Technology Infrastructure. Dependence on foreign vendors in AI systems risks strategic leakage and dependency. Therefore, it is necessary to develop national technology through collaboration between the government, defense SOEs, universities, and the private sector (Beusmans & Wieckert, 1989; Gottemoeller et al., 2022).

3.4. Supporting Institutions and Governance

Policy reformulation must be accompanied by strengthening institutions and governance. Some recommended strategic steps are: (1.) Establishment of a National AI Agency for Defense: This institution is tasked with designing defense AI architecture, drafting ethical regulations, and ensuring interoperability between agencies. (2.) Military Doctrine and Curriculum Reform: Military education must include AI literacy, cyber defense, and technology ethics to equip soldiers and officers to face the digital era (Mahoney, 2020). (3.) Military AI Regulation and Operational Standards: A clear and binding legal framework is needed for the use of AI in all defense operations (Firlej & Taeihagh, 2021).

3.5. Implementation Strategy and Technology Roadmap

Policy implementation requires short-, medium-, and long-term roadmaps: (1.) Short Term (1–3 years): Preparation of regulations, audit of existing technology, and establishment of a defense AI coordination institution. (2.) Medium Term (4–6 years): Development of AI prototypes for combat simulations, smart logistics systems, and adaptive

cyber defense (Ayub Khan et al., 2023). (3.) Long Term (7–10 years): Full integration of AI systems into the national defense structure, increased autonomy of combat systems with human control, and Indonesia's active role in formulating global norms for the use of military AI.

3.6. Challenges and Solutions for Reformulation

Some of the major challenges in this reformulation include: (1.) Limited Human Resources and Research Capacity: The solution is to form strategic partnerships with universities, research and development institutions, and foreign institutions. (2.) Institutional Resistance: A transformative approach is needed that combines education, policy socialization, and technology adoption incentives. (3.) Risk of Technology Misuse and Leakage: A multi-layered control system and strengthening of cyber intelligence are needed (Whyte, 2020; Khaleel et al., 2024). By building a strong and adaptive policy foundation for the development of AI technology, Indonesia will not only have a responsive and modern defense system, but will also uphold the principles of sovereignty, ethics, and national security. This reformulation is a strategic investment towards smart and sovereign defense in the era of the industrial revolution 4.0 and beyond.

3.7. Multi-Level Policy

AI-based defense policy reformulation should be implemented at multiple policy levels to ensure its effectiveness. At the national level, defense policy should include the development of AI-based decision-making systems to improve the accuracy and speed of strategic analysis (Johnson, 2022). AI enables the integration of intelligence data from multiple sources, including satellite surveillance, cyber analysis, and predictive simulation (Guice, 1998). At the operational level, the integration of AI in UAV technology, military sensors, and combat automation is crucial to enhance the military's ability to respond to threats more quickly and accurately (Yaozhong et al., 2023). Machine learning technology can also be used in a more adaptive and efficient military logistics management system (Ayub Khan et al., 2023). At the normative level, the development of a military code of conduct is essential to ensure that the use of AI remains in accordance with international humanitarian law (Firlej & Taeihagh, 2021). The existence of AI-based surveillance devices must have clear regulations to avoid misuse and violations of human rights (Brown-Gaston & Arora, 2021).

3.8. Alliances and Collaborations

The application of AI in defense requires extensive collaboration between various sectors. Civil-military collaboration must be strengthened by the involvement of research institutions and universities in the development of AI systems based on national needs (Gottemoeller et al., 2022). Developed countries have demonstrated the success of this cooperation model through programs such as Civil-Military Fusion in China and DARPA in the United States (Mahoney, 2020). In addition, the involvement of the private sector and AI startups must be optimized to accelerate innovation in defense technology. Beusmans & Wieckert (1989) emphasized that the relationship between industry and the military can accelerate the development of strategic technology.

3.9. Implementation Recommendations

Several strategic steps are recommended to ensure the success of this policy reformulation: (1.) Establishment of the National AI Agency for Defense as an entity responsible for formulating AI policies and standards in the military sector (Johnson, 2022). (2.) Revise the national defense doctrine to include aspects of the use of AI and mitigating risks associated with this technology (Firlej & Taeihagh, 2021). (3.) Development of AI-based data and simulation centers that support tactical planning and conflict scenario prediction (Crumpacker et al., 2022). (4.) Strengthening the cybersecurity system to anticipate threats to digital defense infrastructure (Khaleel et al., 2024). By implementing

multi-level policies and strengthening cross-sector alliances and collaborations, Indonesia can build a defense system that is not only modern but also adaptive to the challenges of AI technology in the future.

4. CONCLUSION

The integration of AI into the national defense system is no longer an option, but a strategic necessity to ensure the effectiveness of decision-making and military superiority. Major countries have adopted AI in various aspects of defense, from command system management to the development of autonomous weapons (Gottemoeller et al., 2022; Sun et al., 2021). Indonesia needs to immediately respond to this development with a more progressive policy based on intelligent technology.

One of the biggest challenges in reformulating this policy is how to bridge technological advances with ethical and legal principles. AI in military systems has the potential to reduce human involvement in critical decisions, which can lead to moral and legal dilemmas (Johnson, 2022; Firlej & Taeihagh, 2021). Therefore, AI-based defense policies must continue to uphold the principle of human-in-the-loop to ensure human control in autonomous systems.

By building adequate technological infrastructure and reformulating national defense policies, Indonesia can increase the speed, accuracy, and adaptability of military decision-making. The development of data centers, AI-based simulation systems, and improving cybersecurity are key steps in creating a modern and sovereign defense system (Ayub Khan et al., 2023; Khaleel et al., 2024).

In conclusion, the urgency of reformulating AI-based defense policies is not only aimed at improving military capabilities but also maintaining national integrity, sovereignty, and security in the era of technological revolution. With a strategic, ethical, and innovative approach, Indonesia can build a defense system that is ready to face future challenges and ensure sustainability in adaptive and responsible military decision-making.

5. REFERENCES

Aldossary, R. S., Almutairi, M. N., & Dursun, S. (2023). Personal protective equipment detection using computer vision techniques. *Society of Petroleum Engineers – Gas and Oil Technology Showcase and Conference (GOTS 2023)*. https://doi.org/10.2118/214093-MS

Arreguín-Toft, I. (2001). How the weak win wars: A theory of asymmetric conflict. *International Security, 26*(1), 93–128. https://doi.org/10.2307/3092079

Ashfaq, S., Chandre, P., Pathan, S., Mande, U., Nimbalkar, M., & Mahalle, P. (2024). Defending against vishing attacks: A comprehensive review for prevention and mitigation techniques. In N. R. Roy, A. S. Bhuvana, & S. Salahdine (Eds.), *Cyber Security and Digital Forensics* (Vol. 896, pp. 411–422). Springer. https://doi.org/10.1007/978-981-99-9811-1_33

Ayub Khan, A., Ali Laghari, A., Rashid, M., Li, H., Rehman Javed, A., & Reddy Gadekallu, T. (2023). Artificial intelligence and blockchain technology for secure smart grid and power distribution automation: A state-of-the-art review. *Sustainable Energy Technologies and Assessments, 57*, 103282. https://doi.org/10.1016/j.seta.2023.103282

Beusmans, J., & Wieckert, K. (1989). Computing, research, and war: If knowledge is power, where is responsibility? *Communications of the ACM, 32*(8), 939–951. https://doi.org/10.1145/65971.65973

Biddle, S. (2004). *Military power: Explaining victory and defeat in modern battle*. Princeton University Press.

Boot, M. (2006). *War made new: Weapons, warriors, and the making of the modern world*. Gotham Books.

Broglio, S. P., McCrea, M., McAllister, T., Harezlak, J., Katz, B., Hack, D., ... & Dykhuizen, B. H. (2017). A national study on the effects of concussion in collegiate athletes and US military service academy members: The NCAA–DoD Concussion Assessment, Research and Education (CARE) Consortium structure and methods. *Sports Medicine, 47*(7), 1437–1451. https://doi.org/10.1007/s40279-017-0707-1

Brown-Gaston, R. D., & Arora, A. S. (2021). War and peace: Ethical challenges and risks in military robotics. *International Journal of Intelligent Information Technologies, 17*(3), 1–12. https://doi.org/10.4018/IJIIT.2021070101

Brubaker, R. (2004). In the name of the nation: Reflections on nationalism and patriotism. *Citizenship Studies, 8*(2), 115–127. https://doi.org/10.1080/1362102042000214705

Clausewitz, C. von. (1984). *On war* (M. Howard & P. Paret, Eds. & Trans.). Princeton University Press.

Crumpacker, J. B., Robbins, M. J., & Jenkins, P. R. (2022). An approximate dynamic programming approach for solving an air combat maneuvering problem. *Expert Systems with Applications, 203*, 117448. https://doi.org/10.1016/j.eswa.2022.117448

Dressler, J. C., Bronk, C., & Wallach, D. S. (2015). Exploiting military OpSec through open-source vulnerabilities. *IEEE Military Communications Conference (MILCOM)*, 450–458. https://doi.org/10.1109/MILCOM.2015.7357484

Echevarria II, A. J. (2007). *Clausewitz and contemporary war*. Oxford University Press.

Firlej, M., & Taeihagh, A. (2021). Regulating human control over autonomous systems. *Regulation and Governance, 15*(4), 1071–1091. https://doi.org/10.1111/rego.12344

Gottemoeller, R., Hedgecock, K., Magula, J., & Poast, P. (2022). Engaging with emerged and emerging domains: Cyber, space, and technology in the 2022 NATO strategic concept. *Defence Studies, 22*(3), 516–524. https://doi.org/10.1080/14702436.2022.2082955

Gray, C. S. (1999). *Modern strategy*. Oxford University Press.

Guice, J. (1998). Controversy and the state: Lord ARPA and intelligent computing. *Social Studies of Science, 28*(1), 103–138. https://doi.org/10.1177/030631298028001004

Handel, M. I. (2001). *Masters of war: Classical strategic thought*. Frank Cass.

Huang, L., Fu, M., Qu, H., Wang, S., & Hu, S. (2021). A deep reinforcement learning-based method applied for solving multi-agent defense and attack problems. *Expert Systems with Applications, 176*, 114896. https://doi.org/10.1016/j.eswa.2021.114896

Johnson, J. (2022). Delegating strategic decision-making to machines: Dr. Strangelove redux? *Journal of Strategic Studies, 45*(3), 439–477. https://doi.org/10.1080/01402390.2020.1759038

Kaldor, M. (2012). *New and old wars: Organized violence in a global era* (3rd ed.). Polity Press.

Khaleel, Y. L., Habeeb, M. A., Albahri, A. S., Al-Quraishi, T., Albahri, O. S., & Alamoodi, A. H. (2024). Network and cybersecurity applications of defense in adversarial attacks: A state-of-the-art using machine learning and deep learning methods. *Journal of Intelligent Systems, 33*(1), Article 20240153. https://doi.org/10.1515/jisys-2024-0153

Luttwak, E. N. (2001). *Strategy: The logic of war and peace* (Rev. & enlarged ed.). Belknap Press.

Mahoney, C. W. (2020). United States defence contractors and the future of military operations. *Defense and Security Analysis, 36*(2), 180–200. https://doi.org/10.1080/14751798.2020.1750182

Mearsheimer, J. J. (2001). *The tragedy of great power politics*. W. W. Norton & Company.

Muhati, E., & Rawat, D. B. (2021). Asynchronous advantage actor-critic (A3C) learning for cognitive network security. In *Proceedings of the 2021 IEEE Conference on Trust, Privacy and Security in Intelligent Systems and Applications* (pp. 106–113). IEEE. https://doi.org/10.1109/TPSISA52974.2021.00012

Navas-Camargo, F., & Ardila Castro, C. A. (2022). Cyberspace, artificial intelligence, and the domain of war: Ethical challenges and the guidelines proposed by the Latin American Development Bank. In J. Cayón Peña (Ed.), *Security and Defence: Ethical and Legal Challenges in the Face of Current Conflicts* (*Advanced Sciences and Technologies for Security Applications*, pp. 37–55). Springer. https://doi.org/10.1007/978-3-030-95939-5_3

Nye, J. S. (2004). *Soft power: The means to success in world politics*. PublicAffairs.

O'Hanlon, M. E. (2009). *The science of war: Defense budgeting, military technology, logistics, and combat outcomes*. Princeton University Press.

Pan, F., & Bao, H. (2021). Research progress of automatic driving control technology based on reinforcement learning. *Journal of Image and Graphics, 26*(1), 28–35. https://doi.org/10.11834/jig.200428

Pape, R. A. (1996). *Bombing to win: Air power and coercion in war*. Cornell University Press.

Posen, B. R. (1984). *The sources of military doctrine: France, Britain, and Germany between the world wars*. Cornell University Press.

Smith, R. (2005). *The utility of force: The art of war in the modern world*. Knopf.

Sun, Z., Piao, H., Yang, Z., Zhao, Y., Zhan, G., Zhou, D., ... & Lu, Y. (2021). Multi-agent hierarchical policy gradient for air combat tactics emergence via self-play. *Engineering Applications of Artificial Intelligence, 98*, 104112. https://doi.org/10.1016/j.engappai.2020.104112

Van Creveld, M. (1991). *The transformation of war*. Free Press.

Warden III, J. A. (1989). *The air campaign: Planning for combat*. National Defense University Press.

Watts, B. D. (2004). *Clausewitzian friction and future war* (Rev. ed.). National Defense University Press.

Whyte, C. (2020). Problems of poison: New paradigms and "agreed" competition in the era of AI-enabled cyber operations. In *Proceedings of the 2020 International Conference on Cyber Conflict (CyCon)* (pp. 215–232). IEEE. https://doi.org/10.23919/CyCon49761.2020.9131717

Yaozhong, Z., Zhuoran, W., Zhenkai, X., & Long, C. (2023). A UAV collaborative defense scheme driven by DDPG algorithm. *Journal of Systems Engineering and Electronics, 34*(5), 1211–1224. https://doi.org/10.23919/JSEE.2023.000128

Yarger, H. R. (2006). *Strategic theory for the 21st century: The little book on big strategy*. Strategic Studies Institute.