JIGE 7 (2) (2026) 1862-1874
JURNAL ILMIAH GLOBAL EDUCATION
ejournal.nusantaraglobal.ac.id/index.php/jige
DOI: https://doi.org/10.55681/jige.v7i2.5767

Restructuring National Defense Policy through the Integration of Artificial Intelligence for Strategic Decision-Making

M. Taher AM[1], Joni Widjayanto[1], Rodon Pedrason[1], Robby M. Taufiq[1], Asep Adang Supriyadi[1]
[1] Republic of Indonesia Defense University, Indonesia
*Correspondence: taher@doktoral.idu.ac.id

Article Info

Article history:

Received April 12, 2026
Approved May 19, 2026

Keywords:

Artificial Intelligence; National Defense Policy; Strategic Decision-Making; Responsible AI; Security Governance

ABSTRACT

The rapid development of artificial intelligence (AI) has changed the strategic environment of national defense by increasing the speed, volume, and complexity of information that must be processed before policy and operational decisions are made. This article analyzes how AI can be integrated into national defense policy as a strategic decision-support capability while maintaining legal, ethical, and institutional control. Using a qualitative literature study and policy analysis, the article synthesizes peer-reviewed studies, defense policy documents, and responsible-AI governance frameworks published between 2018 and 2024. The analysis shows that AI can strengthen defense decision-making through intelligence data fusion, predictive threat assessment, cyber defense, logistics optimization, command-and-control support, and military training simulation. However, AI integration also creates risks related to algorithmic bias, data security, accountability, human oversight, interoperability, technological dependence, and uneven institutional readiness. The article proposes a policy reformulation model based on six pillars: clear legal mandate, responsible AI governance, secure data and digital infrastructure, human-AI teaming, accountable acquisition and testing, and cross-sector collaboration. The study concludes that AI should not be positioned as a replacement for commanders or policymakers, but as a controlled decision-support instrument that improves the quality and timeliness of strategic choices. A defense policy that combines technological innovation with human judgment, ethical safeguards, and institutional resilience is essential for strengthening national defense in an increasingly complex security environment.

How to cite: AM, M. T., Widjayanto, J., Pedrason, R., Taufiq, R. M., & Supriyadi, A. A. (2026). Restructuring National Defense Policy through the Integration of Artificial Intelligence for Strategic Decision-Making. *Jurnal Ilmiah Global Education*, *7*(2), 1862–1874. https://doi.org/10.55681/jige.v7i2.5767

INTRODUCTION

Artificial intelligence has become a strategic technology that influences how states understand threats, allocate defense resources, and organize military capabilities. In the defense sector, AI is no longer limited to automation or technical assistance. It increasingly functions as an enabling technology that shapes intelligence analysis, command and control, cyber defense, logistics, autonomous platforms, military training, and strategic planning. The growing importance of AI is closely related to the transformation of the contemporary security

environment, where threats emerge rapidly, information flows across multiple domains, and decision-makers are required to interpret complex data under significant time pressure.

The contemporary defense environment is marked by rapid information flows, cyber operations, autonomous systems, grey-zone activities, information warfare, and multidomain operations. These developments require states to build defense systems capable of collecting, integrating, and interpreting large volumes of heterogeneous data from satellites, sensors, cyber networks, open-source intelligence, unmanned systems, and field reports. In such conditions, conventional decision-making processes that rely mainly on sequential reporting and manual analysis are often too slow to support timely policy and operational responses. AI offers a means to process data at machine speed, detect patterns across multiple sources, and present decision options to human authorities. Therefore, the strategic value of AI lies not only in accelerating military operations, but also in improving the quality, consistency, and anticipatory capacity of defense policy decisions.

The emergence of AI also reflects a broader shift from platform-centric defense toward data-centric and algorithm-supported defense governance. Traditional defense modernization has often emphasized weapons systems, platforms, and physical infrastructure. However, the growing complexity of modern security threats requires defense institutions to treat data, algorithms, cloud infrastructure, and human-machine collaboration as strategic assets. Allen and Chan (2017) argue that AI has significant implications for national security because it affects military capability, intelligence systems, economic competitiveness, and strategic stability. Similarly, Horowitz (2018) explains that AI may influence international competition and the balance of power by changing the speed, scale, and diffusion of military innovation. These arguments show that AI adoption must be understood as part of defense policy restructuring, not merely as technology procurement.

Previous studies have emphasized that AI is increasingly relevant at the operational and strategic levels of war. Davis (2022) argues that AI can affect operational-level planning by supporting information processing, targeting analysis, and the synchronization of military functions. Meerveld (2023) adds that refusing to use AI in military organizations may become irresponsible when the volume and tempo of information exceed human analytical capacity. Choi (2021) highlights the importance of defense cloud infrastructure as a foundation for data integration and AI-enabled defense services. These studies indicate that AI is not merely a technical tool, but a policy issue that affects doctrine, command structure, resource management, and accountability.

Other studies also show that AI has become a central element of global military competition. Kania (2017) describes AI as an important factor in China's military modernization and future military power, particularly in relation to intelligentized warfare, autonomous systems, and decision-support technologies. Johnson (2019) further argues that AI-related innovations may affect international security by changing the character of warfare, increasing the speed of military interaction, and creating new vulnerabilities in crisis situations. These findings demonstrate that AI creates both opportunity and uncertainty. On the one hand, AI can enhance defense readiness and strategic responsiveness. On the other hand, it may intensify strategic rivalry if states adopt AI without adequate norms, verification mechanisms, and responsible governance.

At the operational level, AI may support several core defense functions. In intelligence, AI can assist in detecting anomalies, classifying objects, identifying threat patterns, and fusing information from multiple sources. In logistics, AI can improve forecasting, inventory management, maintenance planning, and resource allocation. In cyber defense, AI can support intrusion detection, malware analysis, and automated response to rapidly evolving attacks. In training and simulation, AI can generate adaptive scenarios that improve decision-making under uncertainty. The Defense Science Board (2016) notes that autonomy offers substantial operational benefits but also requires serious attention to testing, verification, human-machine teaming, and mission assurance. Cummings (2017) also emphasizes that military AI systems must be evaluated carefully because operational environments are often uncertain, adversarial, and difficult to model fully.

However, AI does not eliminate the need for human judgment. Instead, it changes the structure of decision-making by creating a new relationship between human authorities and machine-generated recommendations. Scharre (2018) explains that autonomous weapons and military robotics raise difficult questions about control, responsibility, and the appropriate role of humans in decisions involving force. This issue is particularly important in strategic decision-making because military decisions often contain political, legal, ethical, and humanitarian consequences that cannot be reduced to algorithmic optimization. Therefore, AI should be positioned as a decision-support capability rather than a substitute for legitimate human command authority.

At the same time, research on the weaponization and governance of AI warns that technological adoption without policy control may create strategic and ethical risks. Burton and Soare (2019) identify the weaponization of AI as a source of uncertainty because autonomous and semi-autonomous systems may alter escalation dynamics and accountability in conflict. Jobin, Ienca, and Vayena (2019) show that global AI ethics guidelines converge around transparency, justice, non-maleficence, responsibility, and privacy, but differ in implementation mechanisms. Taddeo and Floridi (2018) also argue that ethical governance is necessary to ensure that AI remains beneficial while human control is preserved. The OECD Recommendation on Artificial Intelligence (2019), the U.S. Department of Defense Responsible AI Strategy and Implementation Pathway (2022), the Political Declaration on Responsible Military Use of AI and Autonomy (2023), and NATO's revised AI strategy (2024) also place strong emphasis on lawful, responsible, reliable, and human-controlled AI use in security and defense contexts.

The responsible integration of AI also requires a risk-management approach. AI systems may produce inaccurate outputs, amplify bias in training data, become vulnerable to adversarial manipulation, or generate recommendations that appear technically convincing but are strategically inappropriate. NIST (2023) emphasizes that AI risk management should address validity, reliability, safety, security, resilience, accountability, transparency, explainability, privacy, and fairness. ISO/IEC 23894:2023 also provides guidance for integrating AI-related risk management into organizational processes. In the defense sector, these principles are especially relevant because errors in AI-supported decision-making may affect national sovereignty, military operations, civilian safety, and international stability.

Security risks are also important because AI can be used not only for defense, but also for malicious purposes. Brundage et al. (2018) warn that AI may expand the threat landscape in digital, physical, and political domains by enabling more scalable cyberattacks, automated deception, surveillance, and manipulation. In military cyber defense, Kott et al. (2018) show that

autonomous intelligent cyber-defense agents may become necessary because future military networks will face sophisticated attacks that may exceed the reaction speed of human operators. These studies suggest that AI-based defense policy must include not only capability development, but also cyber resilience, data protection, adversarial testing, and safeguards against misuse.

For Indonesia and other developing defense systems, the integration of AI requires more than procurement of advanced technologies. Indonesia's National Strategy for Artificial Intelligence 2020–2045 provides a broad national direction through ethics and policy, talent development, infrastructure and data, research and industrial innovation, and priority-sector development. However, defense policy requires a more specific framework because military use of AI involves sensitive data, national sovereignty, command authority, cyber resilience, interoperability, classified information, and the possibility of force employment. This makes defense AI governance more complex than AI adoption in ordinary public administration or commercial sectors.

Indonesia's defense context also requires attention to institutional readiness. AI adoption depends on the availability of reliable data infrastructure, secure cloud architecture, skilled human resources, legal clarity, interagency coordination, and long-term research collaboration between government, defense industry, universities, and technology developers. Without these prerequisites, AI may remain fragmented across isolated projects and fail to support strategic decision-making. Therefore, the restructuring of national defense policy should include data governance, AI capability roadmaps, ethical standards, procurement mechanisms, testing and evaluation procedures, and human resource development. These elements are necessary to ensure that AI can strengthen national defense resilience while remaining under democratic, legal, and accountable control.

The main problem addressed in this article is the absence of an integrated policy framework that connects AI capability, defense governance, strategic decision-making, and responsible use. Much of the existing discussion focuses either on technological potential or on ethical risks, while the policy architecture needed to combine both aspects remains underdeveloped. This gap is important because defense AI cannot be managed effectively through technological modernization alone. It requires policy reformulation that connects strategic objectives, institutional design, legal authority, operational requirements, data infrastructure, and ethical safeguards.

Therefore, this article aims to analyze the role of AI in restructuring national defense policy and to formulate a responsible AI-based defense policy model for strategic decision-making. The contribution of this article lies in simplifying the discussion into a policy-oriented framework that can guide the integration of AI without reducing the authority of human decision-makers. By placing AI within a responsible governance framework, national defense institutions can use AI to improve decision speed, analytical accuracy, resource efficiency, and threat anticipation while maintaining human oversight, legal accountability, and strategic prudence.

METHODS

This study uses a qualitative literature review and policy analysis approach. The object of analysis is the integration of AI into national defense policy, particularly in relation to strategic decision-making. The study does not use field interviews or statistical testing; instead, it relies on

systematic reading, classification, and interpretation of relevant literature and policy documents. This method is appropriate because the topic concerns the relationship between emerging technology, institutional governance, and normative policy design.

The data sources consist of peer-reviewed journal articles, defense policy documents, international AI governance instruments, and selected national strategic documents published between 2018 and 2024. The literature was selected based on relevance to four themes: AI and military decision-making, AI-enabled defense capability, responsible and ethical AI governance, and institutional readiness for digital transformation. Sources that discussed AI in unrelated technical fields, such as health diagnostics or optical engineering, were excluded from the main analysis because they did not directly support the defense-policy argument.

The analysis was conducted in three stages. First, the relevant sources were mapped to identify AI functions that are most directly connected to defense decision-making, including intelligence analysis, cyber defense, logistics, command-and-control support, and training simulation. Second, the risks and governance challenges were categorized into ethical, legal, technical, institutional, and human-resource dimensions. Third, the findings were synthesized into a policy reformulation model that emphasizes responsible use, human oversight, secure infrastructure, and cross-sector collaboration. Validity was strengthened through source triangulation by comparing academic findings with official policy frameworks from defense and international organizations.

RESULTS AND DISCUSSION

This section presents the results of the qualitative literature review and policy analysis concerning the integration of artificial intelligence into national defense policy. The discussion is structured to explain the strategic relevance of AI not merely as a technological instrument, but as a policy capability that influences how defense institutions process information, formulate strategic options, allocate resources, and respond to complex security threats. In this regard, AI is examined as part of a broader transformation of defense governance, where data, algorithms, digital infrastructure, human expertise, and institutional accountability become interconnected elements of national defense readiness.

The findings indicate that the use of AI in defense cannot be understood only from the perspective of operational efficiency. Although AI can accelerate intelligence analysis, improve cyber-defense capability, optimize logistics, support command-and-control processes, and enhance military training simulations, its integration also raises important questions concerning legal authority, ethical responsibility, data security, human oversight, and institutional preparedness. Therefore, the discussion in this section balances the potential benefits of AI with the risks and governance challenges that must be addressed before AI can be responsibly embedded into national defense systems.

This section is divided into four main parts. The first part discusses AI as a strategic decision-support capability, emphasizing how AI can assist defense decision-makers in managing large-scale and multidomain information. The second part identifies the main challenges of AI integration, including accountability, cybersecurity, data governance, human-resource readiness, and interoperability. The third part formulates a policy reformulation model based on six key pillars: legal mandate and doctrine, responsible AI governance, secure data and infrastructure, human-AI teaming, accountable acquisition and testing, and cross-sector collaboration. The fourth part explains the broader policy implications for national defense,

particularly the need to treat AI adoption as a governance transformation rather than a single procurement or modernization project.

By organizing the discussion in this way, the article seeks to show that AI integration requires a careful connection between technological innovation and institutional control. AI can strengthen the speed and accuracy of strategic decision-making, but it must remain subject to human judgment, legal accountability, ethical safeguards, and national-security priorities. The central argument developed in this section is that the future of AI in defense depends not only on the sophistication of the technology itself, but also on the ability of defense institutions to build responsible governance mechanisms, secure digital ecosystems, and competent human resources capable of using AI critically and effectively.

1. AI as a Strategic Decision-Support Capability

The analysis shows that AI has the greatest defense value when it is treated as a decision-support capability rather than an autonomous substitute for commanders or policymakers. In strategic decision-making, AI can assist in collecting, filtering, integrating, and interpreting data from multiple sources, such as satellite imagery, sensors, intelligence reports, open-source information, cyber indicators, and logistics databases. This capability supports earlier threat detection and more accurate situational awareness.

AI can improve the defense decision cycle in at least five areas. First, in intelligence analysis, machine learning can help analysts identify patterns, anomalies, and correlations that may be difficult to detect manually. Second, in cyber defense, AI can support rapid detection of malware, intrusions, and abnormal network behavior. Third, in logistics, AI can improve stock estimation, route optimization, maintenance prediction, and resource allocation. Fourth, in training and simulation, AI can create adaptive scenarios that support realistic decision-making exercises. Fifth, in command-and-control support, AI can assist decision-makers by presenting alternative courses of action based on available data and operational constraints.

These benefits are strategic because they affect not only military operations but also defense policy formulation. Policy decisions on force posture, modernization priorities, personnel development, and defense budgeting increasingly depend on the ability to interpret complex data. AI can strengthen this process by reducing analytical delays and improving evidence-based planning. However, the final authority for policy and operational decisions must remain with accountable human officials.

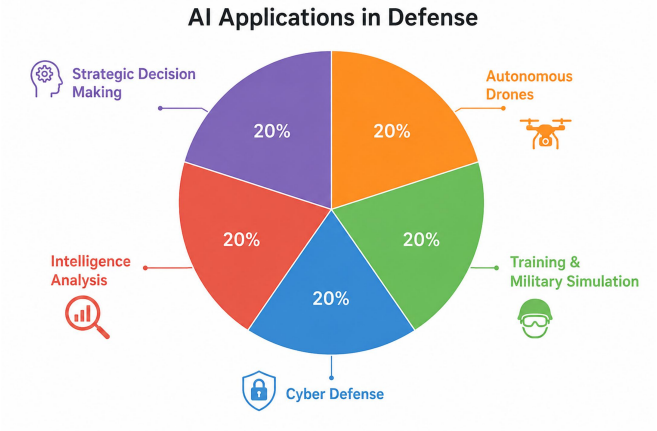

Figure 1. Illustrative Mapping of Artificial Intelligence Applications in Defense.

Figure 1 illustrates the main domains in which artificial intelligence can be applied to support defense functions. The figure presents five key areas: strategic decision-making, autonomous drones, training and military simulation, cyber defense, and intelligence analysis. Each area is shown with an equal proportion of 20%, indicating that these functions are conceptually interrelated and equally important in building an AI-enabled defense system.

Strategic decision-making refers to the use of AI to assist policymakers and defense commanders in processing complex information, identifying alternative courses of action, and improving the timeliness of decisions. Intelligence analysis represents the role of AI in detecting patterns, anomalies, and potential threats from large-scale data sources such as satellite imagery, sensor networks, intelligence reports, and open-source information. Cyber defense highlights AI's ability to detect abnormal network behavior, identify malware, support intrusion prevention, and strengthen digital resilience.

The figure also shows the relevance of AI in autonomous drones, particularly for surveillance, reconnaissance, and remote operational support. Meanwhile, training and military simulation demonstrate how AI can be used to create adaptive scenarios, improve operational readiness, and strengthen decision-making under pressure. Overall, the figure emphasizes that AI integration in defense should not be viewed as a single technological application, but as a multidimensional capability that supports intelligence, operations, cyber security, training, and strategic policy formulation. The percentages in the figure are illustrative and are used to show conceptual balance among the selected defense functions rather than to represent official statistical data.

The following figure provides an illustrative comparison of several AI application areas in defense, showing the relative prominence of intelligence analysis, autonomous drones, cyber defense, and military simulation.

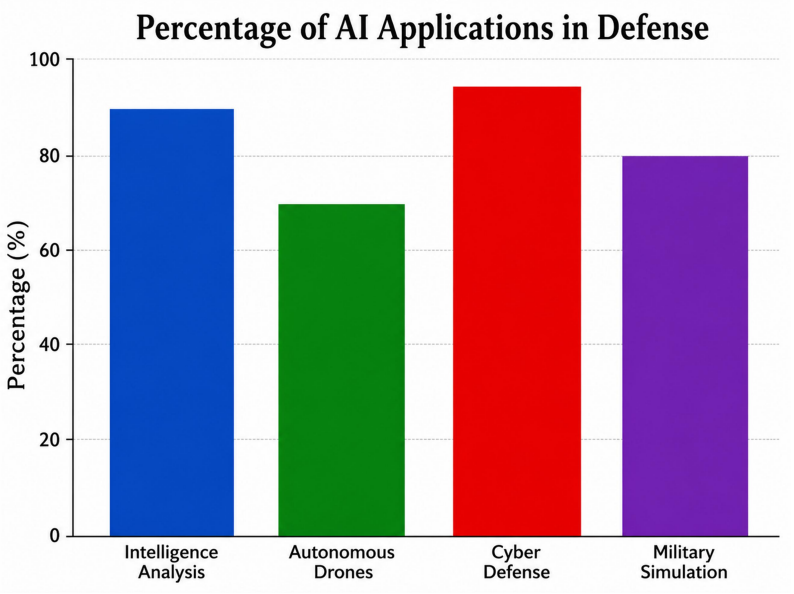

Figure 2. Illustrative Percentage of AI Applications in Defense.

2. Main Challenges in AI Integration

The integration of AI into defense policy faces several major challenges. The first challenge is accountability. AI systems may produce recommendations based on complex models that are difficult to explain. In a defense context, unclear accountability can become dangerous because decisions may involve sovereignty, the use of force, and the protection of civilian lives. Therefore, defense institutions must define who is responsible for AI design, data quality, system validation, operational use, and post-operation evaluation.

The second challenge is data governance and cybersecurity. AI systems depend on data quality, secure networks, and reliable digital infrastructure. Poor data can produce inaccurate recommendations, while cyber compromise can manipulate inputs or outputs. For this reason, AI integration must be linked to secure data architecture, access control, audit trails, encryption, and continuous cybersecurity testing. Defense AI cannot be separated from digital sovereignty and the protection of sensitive national-security information.

The third challenge is human-resource readiness. Defense personnel need AI literacy, data-analysis skills, and an understanding of the limits of algorithmic outputs. Without trained personnel, AI may either be rejected because it is not understood or overtrusted because it appears technologically advanced. Both conditions are risky. Human-AI teaming requires personnel who can question, validate, and use AI recommendations critically.

The fourth challenge is interoperability. AI systems must be compatible with existing command structures, intelligence processes, logistics systems, and legal procedures. If AI is introduced as an isolated technology, it may create fragmented systems rather than integrated defense capability. Policy reform must therefore address standards, data-sharing protocols, procurement rules, and institutional coordination.

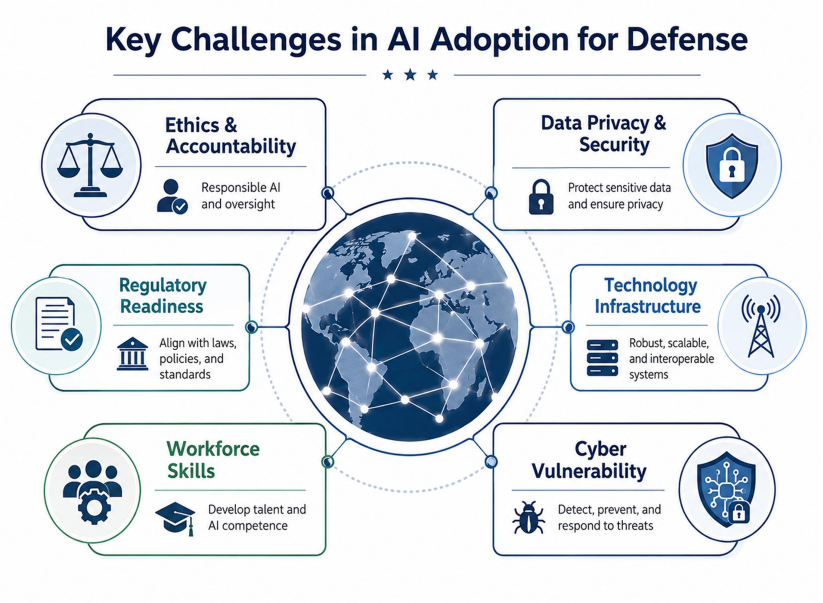

Figure 3. Key Challenges in AI Adoption for Defense Policy.

3. Model of AI-Based Defense Policy Reformulation

Based on the literature and policy analysis, AI-based defense policy reformulation should be organized around six mutually connected pillars. These pillars simplify the earlier broad discussion and translate it into a more operational policy model.

Table 1. AI-Based Defense Policy Reformulation Model

Policy Pillar	Core Requirement	Expected Contribution
Legal mandate and doctrine	Authorized uses, limits, and command responsibility.	Doctrinal clarity and lawful use.
Responsible AI governance	Accountability, transparency, reliability, fairness, privacy, and human oversight.	Ethical control and public trust.
Secure data and infrastructure	Data standards, secure cloud, audit trails, and cyber controls.	Reliable outputs and data protection.
Human-AI teaming	AI literacy, review protocols, and critical validation by users.	Informed human judgment.
Accountable acquisition and testing	Validation, red-teaming, lifecycle monitoring, and vendor accountability.	Safer deployment of AI systems.
Cross-sector collaboration	Coordination among government, industry, universities, and research institutions.	Faster defense innovation.

The proposed model places governance before deployment. This sequence is important because AI systems can affect high-risk decisions before institutions fully understand their limitations. A defense institution should therefore begin with policy architecture, data readiness, and ethical safeguards before moving toward large-scale operational implementation. Pilot projects should be limited to decision-support functions that allow human review, such as intelligence triage, logistics planning, training simulation, and cyber monitoring.

The model also emphasizes that AI adoption must be incremental. In the short term, defense institutions should conduct data audits, identify priority use cases, and develop responsible AI guidelines. In the medium term, they should build secure infrastructure, train personnel, and establish testing and certification procedures. In the long term, AI can be integrated into broader defense planning and command-support systems, provided that human oversight, explainability, and accountability mechanisms remain active.

4. Policy Implications for National Defense

The policy implication of this analysis is that national defense institutions should not treat AI as a single procurement project. AI integration is a governance transformation that affects doctrine, organization, personnel, infrastructure, regulation, and cooperation with external actors. A fragmented approach will produce isolated tools, while an integrated approach can produce a coherent AI-enabled defense ecosystem.

The first implication is the need for a defense-specific responsible AI framework. General national AI strategies are useful, but defense requires additional safeguards because of the sensitivity of military information and the consequences of strategic decisions. The second implication is the need to strengthen data governance. Without standardized and trusted data, AI cannot produce reliable recommendations. The third implication is the need to develop an AI-literate defense workforce. Human decision-makers must remain able to interpret AI outputs and challenge them when necessary.

Finally, AI policy must be adaptive. Technology develops faster than formal regulation, and security threats change continuously. For that reason, defense AI policy should include periodic review, performance evaluation, ethical audit, and lessons learned from pilot projects. Such adaptive governance will allow defense institutions to benefit from innovation while minimizing uncontrolled risks.

5. Synthesis of Findings

The discussion above shows that the integration of artificial intelligence into national defense policy should be understood as a strategic governance issue rather than a purely technological agenda. AI has the potential to strengthen defense decision-making by improving the speed, accuracy, and integration of information across intelligence, cyber defense, logistics, training simulation, and command-and-control processes. These functions are particularly important in a security environment characterized by rapid information flows, multidomain threats, cyber operations, autonomous systems, and strategic uncertainty. In this context, AI can help defense institutions move from reactive decision-making toward more anticipatory and evidence-based policy formulation.

However, the findings also indicate that the benefits of AI are inseparable from significant governance challenges. The adoption of AI in defense creates risks related to accountability, data integrity, cyber vulnerability, institutional readiness, human-resource capacity, interoperability, and ethical control. These risks become more serious because defense decisions may involve sovereignty, the use of force, classified information, and the protection of civilian lives. Therefore, AI cannot be integrated into defense policy without clear legal authority, responsible governance standards, secure infrastructure, and mechanisms for human oversight.

A central finding of this article is that AI should be positioned as a controlled decision-support capability. It should assist commanders, policymakers, and defense planners, but it should not replace human judgment or institutional responsibility. The role of AI is to process complex information, identify patterns, generate analytical options, and support timely decisions. The authority to interpret AI outputs, evaluate strategic consequences, and make final decisions must remain with accountable human actors. This principle is essential to maintain legal responsibility, ethical legitimacy, and strategic prudence in national defense.

The proposed six-pillar policy model provides a structured pathway for responsible AI integration in defense. Legal mandate and doctrine are needed to define the permitted scope and limits of AI use. Responsible AI governance is required to ensure transparency, reliability, fairness, privacy, and accountability. Secure data and digital infrastructure are necessary to protect sensitive information and produce reliable outputs. Human-AI teaming strengthens the capacity of personnel to use AI critically and effectively. Accountable acquisition and testing ensure that AI systems are validated before deployment and monitored throughout their lifecycle.

Cross-sector collaboration enables defense institutions to benefit from innovation developed by universities, research institutions, defense industries, and technology companies.

Overall, the synthesis suggests that successful AI adoption in national defense depends on the balance between innovation and control. AI can improve strategic decision-making only when technological development is aligned with doctrine, law, ethics, institutional capacity, and human competence. Without this balance, AI may create fragmented systems, unclear responsibility, and new vulnerabilities. With proper governance, however, AI can become an important instrument for strengthening national defense resilience in an increasingly complex and data-driven security environment.

CONCLUSION

AI has significant potential to restructure national defense policy by improving the speed, accuracy, and integration of strategic decision-making. Its main value lies in supporting intelligence analysis, cyber defense, logistics management, training simulation, and command-and-control processes. However, AI should not be understood as a substitute for human judgment. In defense policy, human authority remains essential because strategic decisions involve legal responsibility, ethical consequences, and national sovereignty.

The study finds that the successful integration of AI into defense policy depends on institutional readiness, responsible governance, secure data infrastructure, trained personnel, and accountable testing mechanisms. The proposed model consists of six pillars: legal mandate and doctrine, responsible AI governance, secure data and infrastructure, human-AI teaming, accountable acquisition and testing, and cross-sector collaboration. These pillars provide a practical basis for reformulating defense policy so that AI can strengthen national defense without undermining accountability or public trust.

Future research should examine the implementation of this model through empirical case studies in defense institutions, including interviews with policymakers, military officers, cyber-defense personnel, and technology developers. Such research would provide stronger evidence on institutional readiness, operational constraints, and the most feasible pathway for responsible AI adoption in national defense.

REFERENCES

Allen, G., & Chan, T. (2017). Artificial intelligence and national security. Belfer Center for Science and International Affairs, Harvard Kennedy School.

Badan Pengkajian dan Penerapan Teknologi. (2020). Strategi Nasional Kecerdasan Artifisial Indonesia 2020-2045. Jakarta: BPPT.

Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., Dafoe, A., Scharre, P., Zeitzoff, T., Filar, B., Anderson, H., Roff, H., Allen, G. C., Steinhardt, J., Flynn, C., hÉigeartaigh, S. Ó., Beard, S. J., Belfield, H., Farquhar, S., ... Amodei, D. (2018). The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. Future of Humanity Institute, University of Oxford.

Burton, J., & Soare, S. R. (2019). Understanding the strategic implications of the weaponization of artificial intelligence. Cybersecurity and Defense Conference. https://doi.org/10.23919/CYCON.2019.8756866

Choi, S. O. (2021). National defense cloud strategy. IEEE SNPD Winter Conference. https://doi.org/10.1109/SNPDWinter52325.2021.00026

Cummings, M. L. (2017). Artificial intelligence and the future of warfare. Chatham House.

Davis, S. I. (2022). Artificial intelligence at the operational level of war. Journal of Strategic Studies, 45(1), 1-23. https://doi.org/10.1080/14751798.2022.2031692

Defense Science Board. (2016). Summer study on autonomy. Office of the Under Secretary of Defense for Acquisition, Technology and Logistics.

Department of Defense. (2022). Responsible Artificial Intelligence Strategy and Implementation Pathway. Washington, DC: U.S. Department of Defense.

Department of Defense. (2023). Data, Analytics, and Artificial Intelligence Adoption Strategy. Washington, DC: U.S. Department of Defense.

Djenna, A. (2023). Artificial intelligence-based malware detection, analysis, and mitigation. Symmetry, 15(3), 677. https://doi.org/10.3390/sym15030677

European Commission, High-Level Expert Group on Artificial Intelligence. (2019). Ethics guidelines for trustworthy AI. European Commission.

Horowitz, M. C. (2018). Artificial intelligence, international competition, and the balance of power. Texas National Security Review, 1(3), 36–57.

ISO/IEC. (2023). ISO/IEC 23894:2023: Information technology—Artificial intelligence—Guidance on risk management. International Organization for Standardization.

Jobin, A., Ienca, M., & Vayena, E. (2019). Artificial intelligence: The global landscape of ethics guidelines. Nature Machine Intelligence, 1, 389-399. https://doi.org/10.1038/s42256-019-0088-2

Johnson, J. (2019). Artificial intelligence and future warfare: Implications for international security. Defense & Security Analysis, 35(2), 147–169. doi:10.1080/14751798.2019.1600800

Kania, E. B. (2017). Battlefield singularity: Artificial intelligence, military revolution, and China's future military power. Center for a New American Security.

Kivimaa, P. (2022). Transforming innovation policy in the context of global security. Environmental Innovation and Societal Transitions, 43, 55-67. https://doi.org/10.1016/j.eist.2022.03.005

Kott, A., Théron, P., Drašar, M., Rzadca, K., LeBlanc, B., Pihelgas, M., Mancini, L., & Panico, A. (2018). Towards an active, autonomous and intelligent cyber defense of military systems: The NATO AICA reference architecture. 2018 International Conference on Military Communications and Information Systems.

Kurnia, R. (2023). Management of human resources in national defense depends on defense economics point of view. International Journal of Society and Economics in Action, 13(1). https://doi.org/10.35335/ijosea.v13i1.201

Meerveld, H. W. (2023). The irresponsibility of not using AI in the military. AI & Society. https://doi.org/10.1007/s10676-023-09683-0

Mori, S. (2018). US defense innovation and artificial intelligence. Asia-Pacific Review, 25(2), 16-44. https://doi.org/10.1080/13439006.2018.1545488

National Institute of Standards and Technology. (2023). Artificial intelligence risk management framework (AI RMF 1.0). U.S. Department of Commerce.

National Security Commission on Artificial Intelligence. (2021). Final report. National Security Commission on Artificial Intelligence.

NATO. (2024). Summary of NATO's revised Artificial Intelligence (AI) Strategy. Brussels: North Atlantic Treaty Organization.

OECD. (2019). Recommendation of the Council on Artificial Intelligence. OECD/LEGAL/0449. Paris: Organisation for Economic Co-operation and Development.

Scharre, P. (2018). Army of none: Autonomous weapons and the future of war. W. W. Norton & Company.

State Department. (2023). Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy. Washington, DC: U.S. Department of State.

Taddeo, M., & Floridi, L. (2018). How AI can be a force for good. Science, 361(6404), 751–752. doi:10.1126/science.aat5991

Tarasenko, S., Karintseva, O., & Syed, W. (2023). Awareness and readiness to use artificial intelligence by the adult population: Survey results. Problems and Perspectives in Management, 22(4). https://doi.org/10.21511/ppm.22(4).2024.01

UNESCO. (2021). Recommendation on the ethics of artificial intelligence. United Nations Educational, Scientific and Cultural Organization.