JIGE 7 (2) (2026) 1821-1835
JURNAL ILMIAH GLOBAL EDUCATION
ejournal.nusantaraglobal.ac.id/index.php/jige
DOI: https://doi.org/10.55681/jige.v7i2.5764

# Artificial Intelligence-Based Reformulation of National Defense Policy for Strategic Decision-Making

**Ghazalie[1], Yusuf Ali[1], Aris Sarjito[1], Bambang Kustiawan[1], Asep Adang Supriyadi[1], Ceppi Hilmansyah[1], Wisnu Saputro[1], Katherine Erika[1]**

[1] Republic of Indonesia Defense University, Indonesia

*Correspondence: ghazalie@doktoral.idu.ac.id

## Article Info

***Article history:***

Received April 12, 2026
Approved May 18, 2026

***Keywords:***

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

**ABSTRACT**

*This study analyzes the reformulation of national defense policy through the integration of artificial intelligence (AI) as a strategic decision-support capability. The research is motivated by the increasing complexity of the contemporary security environment, including cyber threats, autonomous systems, information warfare, grey-zone operations, and multidomain military competition, which require faster and more reliable policy responses. Using a qualitative descriptive method based on literature review and policy analysis, this study examines scholarly publications, national defense policy documents, and international responsible-AI governance frameworks relevant to military decision-making, cybersecurity, ethics, and institutional readiness. The findings show that AI can strengthen national defense by improving intelligence analysis, predictive threat assessment, military simulation, logistics planning, cyber defense, and command-and-control support. However, AI integration also creates risks related to algorithmic bias, data security, accountability, interoperability, legal uncertainty, human oversight, and institutional capacity. The study proposes an AI-based defense policy reformulation model built on six pillars: legal mandate and doctrine, 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 be positioned not as a replacement for commanders or policymakers, but as a controlled decision-support instrument that strengthens strategic judgment. A responsible AI-based defense policy is therefore essential to ensure that technological innovation improves national defense effectiveness while remaining consistent with legal norms, ethical principles, humanitarian values, and national sovereignty.*



***How to cite:*** Ghazalie, G., Ali, Y., Sarjito, A., Kustiawan, B., Supriyadi, A. A., Hilmansyah, C., Saputro, W., & Erika, K. (2026). Reformulation of National Defense Policy Based on Artificial Intelligence Technology for Decision-Making . *Jurnal Ilmiah Global Education*, *7*(2), 1821–1835. https://doi.org/10.55681/jige.v7i2.5764

## INTRODUCTION

Artificial intelligence (AI) has become one of the most consequential technologies in the transformation of national defense. In the military and security sector, AI is no longer limited to technical automation, administrative efficiency, or digital modernization. It increasingly

functions as an enabling capability that supports intelligence analysis, cyber defense, logistics, surveillance, military simulation, autonomous systems, command and control, and strategic decision-making. The growing importance of AI is closely related to the changing character of contemporary security threats. Defense institutions today must operate in an environment marked by rapid information flows, geopolitical rivalry, cyber operations, disinformation campaigns, grey-zone activities, unmanned systems, and multidomain conflict. These conditions require defense decision-makers to process complex, heterogeneous, and time-sensitive data while maintaining accuracy, legal accountability, operational discipline, and strategic prudence.

The transformation of national defense in the AI era reflects a broader shift from platform-centric defense toward data-centric and decision-centric defense. Traditional defense policy has often emphasized military platforms, physical infrastructure, troop deployment, and conventional force posture. These elements remain important, but modern defense capability increasingly depends on the ability to collect, integrate, interpret, secure, and operationalize data. Defense institutions must be able to connect information from satellites, sensors, intelligence reports, cyber indicators, open-source intelligence, unmanned systems, border surveillance, logistics networks, and strategic assessments. In this context, AI offers the capacity to identify patterns, detect anomalies, support predictive assessment, accelerate information processing, and improve the quality of decision cycles. The strategic value of AI therefore lies not only in operational speed, but also in its potential to support evidence-based policy formulation, anticipatory planning, and adaptive defense governance.

The relevance of AI in national defense becomes more urgent when viewed against the acceleration of multidomain threats. Contemporary conflicts are no longer confined to land, sea, air, and conventional military confrontation. They increasingly involve cyber operations, space-based assets, electromagnetic disruption, information warfare, economic coercion, supply chain vulnerabilities, and psychological influence operations. Grey-zone strategies further complicate defense decision-making because adversaries often operate below the threshold of open armed conflict while still producing strategic effects. Such threats are difficult to assess through linear and conventional decision-making models. AI-supported systems may assist defense institutions by integrating fragmented indicators, identifying early warning signals, mapping threat patterns, and generating decision-support outputs. However, these benefits can only be achieved if AI is embedded within a clear policy framework that regulates data governance, institutional responsibility, human oversight, cybersecurity, procurement, interoperability, and ethical control.

Previous studies have shown that AI is becoming a central factor in military modernization and international security competition. Allen and Chan (2017) argue that AI has broad implications for national security because it affects military power, intelligence capability, economic competitiveness, and strategic stability. Horowitz (2018) explains that AI can influence the balance of power by changing the speed, diffusion, and organizational requirements of military innovation. Kania (2017) further demonstrates that AI has become central to military modernization, particularly in the context of intelligentized warfare, autonomous systems, and decision-support technologies. Payne (2018) emphasizes that AI may create a revolution in strategic affairs by increasing speed, precision, autonomy, and complexity in military operations. Johnson (2019, 2020) also highlights that AI may influence future warfare and strategic stability, particularly when it is integrated into advanced conventional systems, nuclear-related command structures, and military decision-making processes. These studies

indicate that AI is not merely a technological instrument, but a strategic variable that affects defense policy, doctrine, force development, and institutional adaptation.

At the operational level, AI has been examined as a capability that supports planning, intelligence processing, and command decision-making. Davis (2022) argues that AI can be integrated into the operational level of war by supporting military planning, information processing, and the synchronization of operational functions while preserving human oversight. Meerveld et al. (2023) state that the refusal to use AI in military organizations may become irresponsible when the volume, velocity, and complexity of information exceed human analytical capacity. Probasco, Toner, Burtell, and Rudner (2025) also emphasize that AI-enabled decision-support systems can assist military commanders, especially at the operational level, where large volumes of information must be assessed quickly and accurately. These findings suggest that AI should not be understood only as an autonomous weapon issue. Its broader significance lies in its ability to support human decision-makers across the military decision-making process, including intelligence preparation, threat assessment, logistics forecasting, resource allocation, scenario simulation, and strategic planning.

Nevertheless, the effectiveness of AI in defense does not depend solely on algorithmic sophistication. It also depends on data quality, institutional infrastructure, cloud architecture, cybersecurity, organizational culture, human expertise, and governance mechanisms. AI systems require reliable data pipelines, secure digital infrastructure, interoperable platforms, clear access control, and continuous monitoring. Without these foundations, AI may produce misleading outputs, reinforce poor-quality data, increase cyber vulnerabilities, or create false confidence among decision-makers. The U.S. Department of Defense (2023) emphasizes that data, analytics, and AI adoption must be treated as an integrated capability rather than as isolated technological projects. Similarly, ISO/IEC 23894:2023 highlights the need for AI-specific risk management, while ISO/IEC 42001:2023 provides requirements for establishing, implementing, maintaining, and improving an AI management system. These frameworks show that AI adoption requires institutional readiness, not merely technological acquisition.

The integration of AI into defense systems also raises serious ethical, legal, and governance challenges. Burton and Soare (2019) warn that the weaponization of AI may create strategic uncertainty because autonomous and semi-autonomous systems can alter escalation dynamics and accountability in conflict. Scharre (2018) emphasizes that the use of autonomous weapons requires clear rules regarding human control, responsibility, and the decision to use force. Jobin, Ienca, and Vayena (2019) show that global AI ethics guidelines commonly emphasize transparency, justice, non-maleficence, responsibility, and privacy, although implementation mechanisms vary across jurisdictions and institutions. In the military context, these principles become more urgent because AI-supported decisions may affect national sovereignty, civilian protection, proportionality, distinction, accountability, and compliance with international humanitarian law. Thus, responsible AI in defense must be designed to preserve meaningful human judgment, especially in decisions involving the use of force.

Recent international developments demonstrate that AI governance has become a strategic policy priority. The OECD Recommendation on Artificial Intelligence emphasizes inclusive growth, human-centered values, transparency, robustness, safety, and accountability. UNESCO's Recommendation on the Ethics of Artificial Intelligence provides global ethical principles related to human rights, dignity, transparency, fairness, privacy, and human oversight. The European Commission's High-Level Expert Group on AI (2019) stresses trustworthy AI,

while the EU Artificial Intelligence Act establishes a risk-based regulatory framework for AI systems. NIST (2023) provides the AI Risk Management Framework to help organizations govern, map, measure, and manage AI risks. The U.S. Department of Defense (2022) Responsible Artificial Intelligence Strategy and Implementation Pathway emphasizes responsible, equitable, traceable, reliable, and governable AI. NATO's Revised Artificial Intelligence Strategy (2024) further stresses responsible use, interoperability, resilience, strategic foresight, and alliance-wide coordination. These frameworks show that AI adoption in defense must be guided by legal clarity, ethical safeguards, risk management, technical assurance, and institutional accountability.

At the international security level, AI in the military domain has also become a subject of multilateral concern. The Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy (2023) seeks to build international norms for responsible state behavior in developing, deploying, and using military AI. The Responsible AI in the Military Domain (REAIM) Blueprint for Action (2024) emphasizes responsible development, human accountability, risk assessment, and international cooperation. The United Nations General Assembly Resolution 79/239 on artificial intelligence in the military domain affirms the relevance of international law, including the United Nations Charter, international humanitarian law, and international human rights law. These developments indicate that military AI is no longer only a domestic defense modernization issue. It has become part of global security governance, strategic stability, arms control debates, and international legal accountability.

For Indonesia, AI-based defense policy reform is highly relevant to the broader agenda of national technological transformation and defense modernization. Indonesia's National Strategy for Artificial Intelligence 2020–2045 provides a general direction for AI development through ethics and policy, infrastructure and data, talent development, research and innovation, and priority sectors. However, the defense sector requires a more specific policy framework because military AI involves classified information, sovereignty, command authority, cyber resilience, interoperability, strategic intelligence, defense procurement, and the potential use of force. AI in defense cannot be treated as ordinary public-sector digitalization because it is directly related to national security, state survival, strategic autonomy, and the protection of national interests.

The need for a defense-specific AI framework is also consistent with Indonesia's legal and policy architecture. Law Number 3 of 2002 concerning National Defense defines national defense as all efforts to defend state sovereignty, territorial integrity, and the safety of the nation. Presidential Regulation Number 8 of 2021 concerning the General Policy of National Defense 2020–2024 provides policy direction for the management of the national defense system. These legal foundations require defense policy to respond to the development of strategic threats, including technological disruption, cyber threats, and multidomain security challenges. Therefore, the integration of AI into national defense should be framed as a strategic governance issue that connects technology, doctrine, law, ethics, human resources, infrastructure, and institutional readiness.

The urgency of this research lies in the need to bridge the gap between technological potential and policy preparedness. Many discussions on AI in defense focus either on operational benefits, such as speed, automation, surveillance, and intelligence processing, or on ethical risks, especially autonomous weapons and human control. However, fewer studies provide an integrated policy framework that connects AI capability, responsible governance, strategic decision-making, procurement, infrastructure, and national defense reform. Without

such a framework, AI adoption may become fragmented, reactive, vendor-dependent, and weakly integrated into doctrine and institutional planning. It may also create accountability gaps, cybersecurity vulnerabilities, interoperability problems, and operational risks if AI systems are deployed before adequate governance mechanisms are established.

This policy gap is particularly important for countries that are still developing defense AI ecosystems. AI adoption requires not only advanced technology, but also data governance, skilled personnel, secure infrastructure, ethical review mechanisms, procurement standards, testing and evaluation protocols, and institutional learning. Defense organizations must ensure that AI systems are explainable enough for operational use, traceable enough for accountability, reliable enough for mission-critical environments, and governable enough to prevent unintended escalation or misuse. They must also prevent automation bias, data poisoning, model drift, adversarial manipulation, and overdependence on foreign technology providers. In this sense, AI defense policy is not only about adopting new tools, but also about building sovereign capability, institutional resilience, and responsible decision-making architecture.

Based on this background, this study aims to analyze the role of AI in national defense decision-making and to formulate a policy reformulation model that enables responsible AI integration. The article focuses on three main questions: first, how AI contributes to strategic defense decision-making; second, what challenges arise from AI implementation in defense policy; and third, what policy model can guide responsible AI adoption in national defense. The contribution of this study is a structured reformulation model that aligns technological innovation with legal mandate, ethical governance, secure infrastructure, human-AI teaming, accountable acquisition, testing and evaluation, and cross-sector collaboration. By doing so, this research seeks to strengthen the conceptual and practical foundation for AI-based national defense policy reform that is adaptive, accountable, and aligned with Indonesia's strategic interests.

## METHODS

This study employs a qualitative descriptive approach through literature review and policy analysis. The method is appropriate because the research examines the relationship between emerging technology, defense governance, and strategic decision-making rather than measuring a single empirical variable. The object of analysis is the reformulation of national defense policy based on AI technology, particularly in relation to decision-support capability, responsible governance, and institutional readiness.

The data sources consist of peer-reviewed journal articles, books, policy documents, official defense strategies, and international AI governance frameworks. The sources were selected purposively based on their relevance to four themes: AI and military decision-making, AI-enabled defense capability, responsible AI governance, and defense policy reform. Academic sources were used to build the theoretical and analytical foundation, while policy documents were used to understand how governments and international organizations regulate responsible AI in defense and security contexts.

The selection process followed clear inclusion and exclusion criteria. Sources were included when they discussed AI in national security, military operations, cyber defense, autonomous systems, strategic stability, AI ethics, defense innovation, or institutional readiness. Sources were excluded when they discussed AI in unrelated sectors without direct relevance to defense policy. This criterion was applied to ensure that the analysis remains focused on the

research problem and avoids excessive discussion of AI applications outside the defense and security domain.

The analysis was carried out in four stages. First, the literature was mapped to identify the main defense functions supported by AI, including intelligence analysis, predictive threat assessment, military simulation, cyber defense, logistics planning, and command-and-control support. Second, the challenges of AI adoption were classified into technical, legal, ethical, institutional, and human-resource dimensions. Third, findings from academic studies were compared with official policy frameworks, including responsible AI principles, risk management guidelines, and military AI governance documents. Fourth, the results were synthesized into a policy reformulation model that can guide responsible AI integration in national defense.

Source triangulation was used to strengthen the validity of the analysis. Academic findings were compared with policy frameworks from government institutions and international organizations. This triangulation is important because AI-based defense policy involves both empirical technological capability and normative governance principles. The study also applies a systemic perspective, drawing from Soft Systems Methodology (SSM), to understand the interaction between technology, policy, military organizations, legal norms, and security actors. Through this approach, AI integration is analyzed not as a stand-alone procurement issue, but as a broader transformation of defense governance.

Table 1. Research Analysis Framework

| Analytical Stage | Main Focus | Expected Output |
|---|---|---|
| **Literature mapping** | AI functions in defense decision-making | Identification of key AI application areas |
| **Challenge classification** | Technical, legal, ethical, institutional, and human-resource risks | Structured risk categories |
| **Policy comparison** | Responsible AI principles and defense governance frameworks | Policy gaps and governance requirements |
| **Model synthesis** | Integration of AI capability with responsible governance | AI-based defense policy reformulation model |

## RESULTS AND DISCUSSION

This section presents the results of the literature review and policy analysis concerning the integration of AI 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 AI 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, 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.

***Artificial Intelligence as a Strategic Decision-Support Capability***

The analysis shows that AI has its greatest defense value when it is positioned as a strategic decision-support capability. Strategic defense decisions require the interpretation of complex data, the assessment of alternative courses of action, and the consideration of political, legal, operational, and ethical consequences. AI can support this process by processing large-scale information, detecting hidden patterns, generating predictive assessments, and presenting analytical options to decision-makers. However, the final authority to decide must remain with accountable human actors.

In intelligence analysis, AI can support the fusion of information from satellites, sensors, cyber networks, open-source intelligence, and field reports. Machine learning systems can identify anomalies, classify objects, and detect patterns that may be difficult for human analysts to observe manually. This capability is important because contemporary threats often emerge across multiple domains and may involve ambiguous actors, cyber operations, or disinformation campaigns. When integrated into a secure intelligence architecture, AI can reduce analytical delay and improve early warning capacity.

In cyber defense, AI can help detect malware, suspicious network behavior, unauthorized access, and abnormal system activity. Djenna (2023) emphasizes that AI-based malware detection can improve the ability to identify and mitigate digital threats. Kott et al. (2018) also argue that autonomous and intelligent cyber-defense agents may become necessary because future military networks will face sophisticated threats that exceed the reaction speed of human operators. These findings indicate that AI is particularly relevant to cyber resilience, where speed and pattern recognition are central to defense effectiveness.

AI also contributes to logistics and resource allocation. Military logistics depends on accurate forecasts, inventory management, route optimization, maintenance schedules, and supply-chain resilience. AI can support predictive maintenance by identifying equipment failure patterns before they disrupt operations. It can also improve the allocation of resources in crisis situations by integrating operational requirements, location data, and available supply. In this sense, AI contributes not only to combat operations, but also to the sustainability of defense readiness.

In military training and simulation, AI can create adaptive scenarios that reflect changing threat environments. Cummings (2017) notes that military AI must be evaluated carefully because operational environments are uncertain and adversarial. The Defense Science Board (2016) similarly emphasizes testing, verification, human-machine teaming, and mission assurance, while Boulanin and Verbruggen (2017) underline the importance of mapping autonomy in weapon systems before deployment. AI-enabled simulation allows defense personnel to test tactical and strategic decisions in controlled environments while reducing cost and operational risk. This capability is valuable for preparing commanders and personnel to make decisions under pressure, especially in multidomain scenarios involving land, sea, air, space, and cyber dimensions.

AI can also support command-and-control processes by presenting alternative courses of action, evaluating operational constraints, and improving situational awareness. Davis (2022) explains that AI can influence operational-level planning through information processing and synchronization of military functions. However, AI-generated recommendations must be interpreted critically. Strategic decisions cannot be reduced to technical optimization because they involve political objectives, legal rules, humanitarian consequences, and national interests. Therefore, AI should strengthen human judgment rather than replace it.

Table 2. AI Application Areas and Their Defense Policy Relevance

| AI Application Area | Defense Function | Policy Relevance |
|---|---|---|
| **Intelligence analysis** | Data fusion, anomaly detection, threat pattern recognition | Improves situational awareness and early warning |
| **Cyber defense** | Malware detection, intrusion monitoring, automated response support | Strengthens cyber resilience and digital sovereignty |
| **Logistics and maintenance** | Route optimization, inventory forecasting, predictive maintenance | Supports resource efficiency and operational readiness |
| **Training and simulation** | Adaptive scenarios and decision-making exercises | Improves preparedness and reduces training risk |
| **Command-and-control support** | Alternative courses of action and decision recommendations | Enhances timeliness and evidence-based planning |

***Main Challenges in Implementing AI in Defense Policy***

The implementation of AI in defense policy creates several challenges that must be addressed before large-scale deployment. The first challenge is accountability. AI systems may produce recommendations based on complex models that are difficult to explain. In defense, unclear accountability can become dangerous because decisions may involve sovereignty, the use of force, and the protection of civilian lives. Defense institutions must clearly define who is responsible for data quality, system design, algorithm validation, operational use, and post-operation evaluation.

The second challenge is data governance and cybersecurity. AI systems depend on the quality, integrity, and security of data. If the data used to train or operate AI systems are incomplete, biased, or manipulated, the resulting recommendation may be unreliable. Brundage et al. (2018) warn that AI can expand the threat landscape by enabling scalable cyberattacks, automated deception, and manipulation. Therefore, defense AI must be linked to secure data architecture, access control, encryption, audit trails, and continuous cyber testing. The protection of AI systems is inseparable from the protection of national-security information.

The third challenge is human oversight. AI systems can accelerate decision-making, but speed alone does not guarantee strategic wisdom. Scharre (2018) argues that autonomous weapons and military robotics raise difficult questions about human control and responsibility. This issue is especially important when AI is used in systems related to targeting, surveillance, or

the use of force. Responsible defense policy must ensure meaningful human control, especially for decisions that may produce lethal or irreversible consequences.

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 capability. Interoperability also includes compatibility among agencies, military branches, allies, and technology providers. Choi (2021) emphasizes that defense cloud strategy is important because data integration is a foundation for AI-enabled defense services. Without interoperability, AI cannot support coherent defense decision-making.

The fifth challenge is human-resource readiness. Defense personnel must understand both the potential and the limitations of AI. Without adequate AI literacy, personnel may either reject AI because they do not trust it or overtrust AI because it appears advanced and objective. Both conditions are risky. Human-AI teaming requires personnel who can question, validate, and interpret AI outputs. Therefore, defense policy must include training programs for commanders, intelligence analysts, cyber-defense personnel, procurement officials, and legal advisers.

The sixth challenge is legal and ethical uncertainty. Jobin et al. (2019) show that AI ethics guidelines often agree on broad principles but differ in practical implementation. This gap becomes more serious in defense because military AI may affect strategic stability, escalation control, humanitarian law, and civilian protection. Burton and Soare (2019) argue that the weaponization of AI can create uncertainty in conflict. Therefore, national defense policy must translate general responsible-AI principles into clear operational rules, review mechanisms, and accountability standards.

Table 3. Major Risks and Governance Responses in Defense AI Integration

| Risk Area | Potential Impact | Required Governance Response |
|---|---|---|
| **Algorithmic bias** | Inaccurate or discriminatory recommendations | Data validation, fairness testing, and human review |
| **Cyber compromise** | Manipulated inputs, disrupted systems, or intelligence leakage | Encryption, red-teaming, access control, and continuous monitoring |
| **Accountability gap** | Unclear responsibility for AI-supported decisions | Legal mandate, audit trails, and defined command responsibility |
| **Overreliance on AI** | Reduced human judgment and strategic prudence | Human-AI teaming and critical validation protocols |
| **Interoperability failure** | Fragmented systems and ineffective coordination | Standards, data-sharing rules, and integrated architecture |
| **Regulatory uncertainty** | Inconsistent use and possible violation of humanitarian norms | Responsible AI doctrine and compliance review |

***AI-Based Reformulation of National Defense Policy***

Based on the findings above, AI-based defense policy reformulation should be built on a governance-first approach. This means that defense institutions should not begin with technology procurement alone. They must first establish policy architecture, legal mandate, data governance, ethical safeguards, and institutional readiness. This sequence is important because AI systems may affect high-risk decisions before institutions fully understand their limitations. Governance must therefore precede deployment.

The first pillar is legal mandate and doctrine. Defense institutions must define the authorized uses, limits, and command responsibilities associated with AI. This includes determining which AI functions may be used for decision support, which require human approval, and which are prohibited or require special review. Legal mandate is essential to ensure that AI use remains consistent with national defense law, command responsibility, and international humanitarian obligations.

The second pillar is responsible AI governance. This pillar includes accountability, transparency, reliability, fairness, privacy, and human oversight. The U.S. Department of Defense (2022) emphasizes responsible, equitable, traceable, reliable, and governable AI. NIST (2023) further highlights validity, safety, security, resilience, accountability, explainability, and privacy as core dimensions of AI risk management. These principles should be translated into defense-specific guidelines that regulate AI development, testing, deployment, and review.

The third pillar is secure data and digital infrastructure. AI requires reliable data, secure cloud systems, interoperability standards, audit trails, and cyber controls. Defense AI cannot operate effectively if data are fragmented or vulnerable to manipulation. Secure data infrastructure is also necessary to protect classified information and maintain digital sovereignty. For Indonesia, this pillar is particularly important because AI adoption must be aligned with national data governance, cyber resilience, and defense modernization priorities.

The fourth pillar is human-AI teaming. AI should assist commanders and policymakers, not replace them. Human-AI teaming requires personnel who understand how to interpret AI outputs, identify uncertainty, challenge automated recommendations, and apply legal and ethical judgment. Training should therefore include AI literacy, data analysis, cyber risk awareness, and operational validation. This pillar ensures that human judgment remains central in strategic defense decisions.

The fifth pillar is accountable acquisition and testing. Defense institutions should establish validation, red-teaming, lifecycle monitoring, and vendor accountability before deploying AI systems. Testing must examine not only technical performance, but also resilience against adversarial manipulation, explainability, bias, interoperability, and mission relevance. AI procurement should include clear standards for data protection, system auditability, and post-deployment evaluation.

The sixth pillar is cross-sector collaboration. AI innovation often emerges from universities, research institutions, private technology companies, and defense industries. Defense policy must create mechanisms for collaboration while protecting national security and sensitive data. Kivimaa (2022) notes that innovation policy must adapt to global security contexts. In the defense sector, this means building partnerships that support innovation, talent development, research, and responsible technology transfer.

Table 4. Six Pillars of Responsible AI Integration in Defense Policy

| 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 and responsible defense innovation |

***Policy Implications for Indonesia***

The proposed model has several implications for Indonesia's national defense policy. First, Indonesia needs a defense-specific AI policy framework that translates the National Strategy for Artificial Intelligence 2020–2045 into the military and defense context. The national AI strategy provides a useful foundation, but defense AI requires additional safeguards due to the sensitivity of classified data, command authority, cyber resilience, and the possible use of force. A defense-specific framework would help define priority use cases, ethical boundaries, procurement requirements, and institutional responsibilities.

Second, Indonesia should begin AI integration through low-risk but high-value decision-support functions. Early implementation can focus on intelligence triage, cyber monitoring, logistics planning, disaster-related defense support, maritime surveillance, and training simulation. These areas allow AI to improve analytical capacity while maintaining human review. More sensitive applications, such as autonomous weapons or targeting support, should only be considered after stronger legal, ethical, and technical safeguards are established.

Third, defense institutions should conduct data-readiness and infrastructure audits before deploying AI at scale. AI systems require clean, secure, and interoperable data. Without reliable data, AI outputs may be misleading. Data audits should examine data ownership, classification, access rights, storage security, interoperability, and quality control. Infrastructure audits should assess secure cloud readiness, communication networks, backup systems, cyber protection, and continuity planning.

Fourth, Indonesia needs to develop AI-literate defense personnel. Human-resource development should be integrated into defense education, staff colleges, cyber units, intelligence training, and procurement institutions. AI literacy does not mean that all military personnel must become programmers. Rather, commanders and policymakers must understand what AI can and cannot do, how uncertainty appears in AI outputs, how to question automated recommendations, and how to maintain human responsibility in decision-making.

Fifth, Indonesia should strengthen cross-sector and international cooperation. AI development requires collaboration among government institutions, defense industry, universities, research centers, and technology developers. International cooperation is also important to learn from responsible AI frameworks, interoperability standards, and cyber-defense practices. However, such cooperation must be balanced with national sovereignty, data protection, and control over sensitive defense technologies.

Finally, AI policy must be adaptive. Technology develops faster than formal regulation, while security threats continue to evolve. Therefore, defense AI policy should include periodic review, ethical audits, performance evaluation, lessons learned from pilot projects, and revision mechanisms. Adaptive governance will allow defense institutions to benefit from innovation while reducing uncontrolled risks.

***Synthesis of Findings***

The discussion above shows that the integration of AI into national defense policy should be understood as a strategic governance issue rather than a purely technological agenda. AI can improve defense decision-making by strengthening intelligence analysis, cyber defense, logistics, military simulation, and command-and-control support. These functions are important in a security environment marked by rapid information flows, multidomain threats, cyber operations, 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 benefits of AI are inseparable from governance risks. AI adoption in defense creates challenges related to accountability, data integrity, cyber vulnerability, institutional readiness, human-resource capacity, interoperability, and ethical control. These risks are serious because defense decisions may involve sovereignty, the use of force, classified information, and the protection of civilians. Therefore, AI cannot be integrated responsibly without legal authority, secure infrastructure, human oversight, and transparent accountability mechanisms.

A central finding of this study is that AI should be positioned as a controlled decision-support capability. AI should assist commanders, policymakers, and defense planners by processing complex information, identifying patterns, and generating analytical options. However, 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.

Overall, successful AI adoption depends on the balance between innovation and control. AI can improve national defense effectiveness 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, AI can become an important instrument for strengthening national defense resilience in an increasingly complex and data-driven security environment.

## CONCLUSION

This study concludes that AI-based reformulation of national defense policy is necessary to respond to the increasing complexity of contemporary security threats. AI can strengthen strategic decision-making by improving intelligence analysis, predictive threat assessment, cyber defense, logistics planning, military simulation, and command-and-control support. Its main contribution lies in helping defense institutions process large-scale information more quickly and accurately, thereby improving the timeliness and quality of policy and operational decisions.

However, AI integration also creates significant risks. These risks include algorithmic bias, data manipulation, cybersecurity vulnerabilities, unclear accountability, weak human oversight, limited interoperability, legal uncertainty, and uneven institutional readiness. Therefore, AI must not be positioned as a replacement for commanders or policymakers. It should be used as a controlled decision-support instrument that remains subject to human judgment, legal responsibility, ethical principles, and national-security priorities.

The study proposes a six-pillar model for responsible AI integration in defense policy: 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 framework for ensuring that AI strengthens national defense without undermining accountability, sovereignty, or humanitarian values. For Indonesia, the implementation of this model should begin with policy clarification, data readiness, pilot projects in decision-support functions, AI literacy development, and secure collaboration among defense institutions, academia, industry, and technology providers.

Future research should examine the empirical implementation of this model in specific defense institutions through interviews, case studies, and operational readiness assessments. Such research would provide stronger evidence regarding institutional constraints, priority use cases, and feasible pathways for responsible AI adoption in national defense.

## REFERENCES


Allen, G. C., & 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*. BPPT.

Boulanin, V., & Verbruggen, M. (2017). *Mapping the development of autonomy in weapon systems*. Stockholm International Peace Research Institute.

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. In *The 11th International Conference on Cyber Conflict: Silent Battle*. https://doi.org/10.23919/CYCON.2019.8756866

Choi, S. O. (2021). National defense cloud strategy. In *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. *Defense & Security Analysis, 38*(1), 74–90. https://doi.org/10.1080/14751798.2022.2031692

Defense Innovation Board. (2019). *AI principles: Recommendations on the ethical use of artificial intelligence by the Department of Defense*. Defense Innovation Board.

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

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.

European Commission. (2024). *Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence*. European Union.

Helmer, D., Boardman, M., Conroy, S. K., Hepworth, A. J., & Harjani, M. (2024). *Human-centred test and evaluation of military AI*. arXiv. https://arxiv.org/abs/2412.01978

Horowitz, M. C. (2018). Artificial intelligence, international competition, and the balance of power. *Texas National Security Review, 1*(3), 36–57. https://doi.org/10.15781/T2639KP49

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

International Organization for Standardization. (2023b). *ISO/IEC 42001:2023 Artificial intelligence — Management system*. ISO.

Jobin, A., Ienca, M., & Vayena, E. (2019). The global landscape of AI 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. https://doi.org/10.1080/14751798.2019.1600800

Johnson, J. S. (2020). Artificial intelligence: A threat to strategic stability. *Strategic Studies Quarterly, 14*(1), 16–39.

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. In *2018 International Conference on Military Communications and Information Systems*.

Maas, M. M. (2019). How viable is international arms control for military artificial intelligence? Three lessons from nuclear weapons. *Contemporary Security Policy, 40*(3), 285–311. https://doi.org/10.1080/13523260.2019.1576464

Maslej, N., Fattorini, L., Perrault, R., Gil, Y., Parli, V., Kariuki, N., Capstick, E., Reuel, A., Brynjolfsson, E., Etchemendy, J., Ligett, K., Lyons, T., Manyika, J., Niebles, J. C., Shoham, Y., Wald, R., Walsh, T., Hamrah, A., Santarlasci, L., Betts Lotufo, J., Rome, A., Shi, A., & Oak, S. (2025). *Artificial Intelligence Index Report 2025*. Stanford Institute for Human-Centered Artificial Intelligence.

Meerveld, H. W., Lindelauf, R. H. A., Postma, E. O., & Postma, M. (2023). The irresponsibility of not using AI in the military. *Ethics and Information Technology, 25*, Article 14. 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.

North Atlantic Treaty Organization. (2021). *NATO Artificial Intelligence Strategy*. NATO.

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

OECD. (2019). *Recommendation of the Council on Artificial Intelligence*. Organisation for Economic Co-operation and Development.

Payne, K. (2018). Artificial intelligence: A revolution in strategic affairs? *Survival, 60*(5), 7–32. https://doi.org/10.1080/00396338.2018.1518374

Probasco, E. S., Toner, H., Burtell, M., & Rudner, T. G. J. (2025). *AI for military decision-making: Harnessing the advantages and avoiding the risks*. Center for Security and Emerging Technology, Georgetown University.

Republic of Indonesia. (2002). *Law Number 3 of 2002 concerning National Defense*.

Republic of Indonesia. (2021). *Presidential Regulation Number 8 of 2021 concerning the General Policy of National Defense 2020–2024*.

Responsible AI in the Military Domain. (2024). *REAIM Blueprint for Action*. REAIM Summit.

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

Scharre, P., & Lamberth, M. (2022). *Artificial intelligence and arms control*. Center for a New American Security.

Simmons-Edler, R., Badman, R., Longpre, S., & Rajan, K. (2024). *AI-powered autonomous weapons risk geopolitical instability and threaten AI research*. arXiv. https://arxiv.org/abs/2405.01859

Simmons-Edler, R., Dong, J., Lushenko, P., Rajan, K., & Badman, R. P. (2025). *Military AI needs technically informed regulation to safeguard AI research and its applications*. arXiv. https://arxiv.org/abs/2505.18371

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

UNESCO. (2021). *Recommendation on the Ethics of Artificial Intelligence*. United Nations Educational, Scientific and Cultural Organization.

United Nations General Assembly. (2024). *Resolution 79/239: Artificial intelligence in the military domain and its implications for international peace and security*. United Nations.

United Nations Office for Disarmament Affairs. (2024). *Governance of artificial intelligence in the military domain*. UNODA.

U.S. Department of Defense. (2022). *Responsible Artificial Intelligence Strategy and Implementation Pathway*. Department of Defense.

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

U.S. Department of State. (2023). *Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy*. U.S. Department of State.

Zhou, W., & Greipl, A. R. (2024). Artificial intelligence in military decision-making: Supporting humans, not replacing them. *International Committee of the Red Cross Humanitarian Law & Policy Blog*.