International Journal of Law and Public Policy
p-ISSN: 2721-6934, e-ISSN: 2721-6942

Research Paper

Integrating Artificial Intelligence into Indonesia's Defense Policy for Strategic Decision-Making

Faisal Yusman[1], Yuli Kartiningsih[1*], Alradix[1], Asep Adang Supriyadi[1]

[1] *Department Defense Science, Faculty Defense Science, Indonesia Defense University. Bogor, Indonesia.*

Article History
Received:
27.05.2025

Revised:
18.06.2025

Accepted:
30.06.2025

***Corresponding Author:**
Yuli Kartiningsih
Email:
yuli.kartiningsih@doctoral.idu.ac.id

Abstract: The transformation of Indonesia's national defense policy in the digital era requires the integration of Artificial Intelligence as a strategic instrument to enhance analytical and decision-making capabilities. This study aims to formulate an AI-based defense policy framework that is responsive to the dynamics of modern threats, as well as to identify the challenges and opportunities in its implementation. The research method used is a qualitative approach through document study and policy analysis that includes national regulations, academic literature, and global practices. The results of the study indicate that Indonesia still faces a number of fundamental obstacles, such as the absence of a national ethics framework for military AI, low institutional readiness, and weak regulations related to the control of autonomous systems. This study recommends the establishment of a defense AI ethics council, revision of the defense legal framework to include intelligent technology, and the development of a collaborative roadmap across ministries. It is expected that the resulting policy will not only be adaptive to technological disruption, but also guarantee accountability and national sovereignty in the use of AI for strategic defense interests.

Keywords: AI Defense Ethics, AI Governance, National Defense, Policy Reform, Strategic Decision-Making.

1. Introduction

The integration of Artificial Intelligence into national defense strategy marks a transformative paradigm shift, offering unlimited opportunities to strengthen decision-making processes and improve the overall security infrastructure [1]. The continued global expansion of AI capabilities in defense underscores the urgent need for a carefully designed ethical framework to regulate its implementation [2]. To ensure the ethical application of AI in national defense, this framework must carefully incorporate the principles of justified and reversible use, the establishment of fair and transparent systems and processes, a clear assertion of human moral responsibility, the maintenance of meaningful human control, and guarantees of AI system reliability [2]. The drive to consistently maintain technological superiority has driven advances in national defense strategies, especially in today's advanced information societies, with defense agencies around the world recognizing AI as a key technology to maintain an edge over adversaries [3].

AI capabilities, such as the ability to analyze large data sets, uncover patterns, and automate complex tasks, have positioned it as a transformative force capable of revolutionizing various aspects of national defense. From intelligence gathering and threat assessment to autonomous systems and cyber security, AI has the potential to fundamentally transform these domains [2]. As artificial intelligence and machine learning technologies advance, it is becoming increasingly important to understand their strategic implications for national security, particularly with regard to military applications, strategic imperatives, and renewed interest in AI's contribution to national security [1]. AI's diversity, combined with its capacity to process vast amounts of data and identify subtle trends, can provide valuable insights to decision-makers, enabling them to anticipate threats, assess risks, and formulate effective response strategies [4]. However, the integration of AI into national defense requires a comprehensive examination of the associated challenges, including ethical considerations, the need for robust oversight mechanisms, and the mitigation of risks associated with autonomous weapons systems.

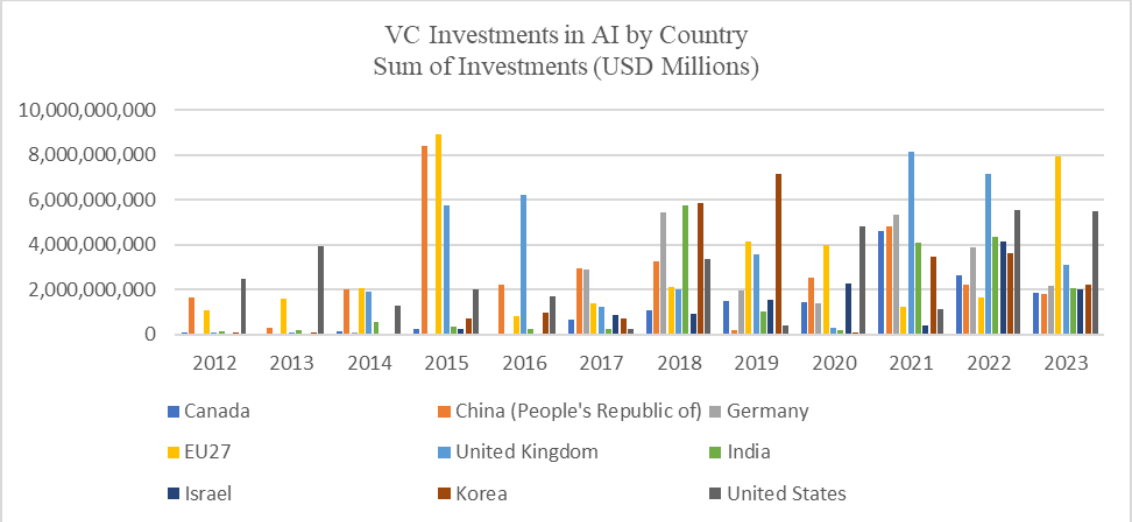
In the context of AI development for defense in Indonesia, leveraging this technology has become imperative in response to the increasingly complex and dynamic global defense environment [5]. The acceleration of science and technology has transformed the characteristics of threats, both military and non-military, thus requiring adjustments to the national defense strategy to maintain sovereignty and territorial integrity [6]. The implementation of artificial intelligence, particularly through unmanned aerial vehicles such as unmanned combat aerial vehicles and drones, has proven effective in physical conflicts, as well as crucial in the realm of non-physical warfare, including mapping conflict zones and securing cross-border areas [7]. AI integration has the potential to support the primary tasks of the state's defense equipment by reducing risks and increasing effectiveness and time efficiency, especially in long-range defense operations and anomaly detection for cybersecurity [5]. AI capabilities are also essential in surveillance and intelligence gathering, thanks to their ability to analyze large volumes of data and automatically identify dangerous activities.

However, the utilization of AI to support Indonesia's national defense still faces several obstacles, including the imperative for definitive regulations, adequate infrastructure, and the development of competent human resources [5]. Data released by the Central Statistics Agency in 2021 indicates a significant disparity in digital literacy and access to information technology across various regions of Indonesia, which implicitly affects the readiness to adopt advanced technologies such as AI in the defense context [8]. This underscores the urgency of drafting a comprehensive policy framework to ensure the responsible and ethical implementation of AI in Indonesia's defense sector, as well as integrating the protection of personal data and privacy as an integral part of that framework [5].

Extant data indicate that while the potential of AI is considerable, the digital infrastructure and workforce skills in Indonesia remain comparatively underdeveloped, thereby impeding the widespread adoption of this technology [9]. Despite a focus on technological advancements such as robotic marine vessels and drones, the utilization of AI in Indonesia's cyber defense is still in its nascent stages. It is anticipated that AI sensors will facilitate and expedite the analysis of increasingly sophisticated cyber threats [10]. By way of illustration, developed nations have extensively integrated AI into their weapon systems, thus rendering the development of AI capabilities for Indonesia's defense not merely an option but a strategic imperative to safeguard sovereignty and maintain a competitive advantage amidst the dynamics of global geopolitics [11].

According to data from the OECD AI Scoreboard in 2023, Indonesia ranks 38th out of 63 countries in terms of AI adoption and development, indicating a need for significantly increased investment in infrastructure and human resources to foster innovation and AI capabilities within the

defense sector [12]. The utilization of artificial intelligence by the Indonesian National Army constitutes a strategic imperative, given the continuously evolving and increasingly sophisticated nature of threats; consequently, this technology is highly relevant for ensuring the security of border regions [13]. Maximizing the application of AI is of paramount importance to guarantee the security of border regions and safeguard the integrity of the Unitary State of the Republic of Indonesia. Nevertheless, in comparison to other nations, particularly within the Southeast Asian region, Indonesia remains significantly behind in its preparedness for modernizing primary defense systems with AI integration, primarily due to limitations in the defense budget relative to those countries [9]. Therefore, augmenting investment in technological infrastructure is a primary priority to effectively realize the integration of AI into Indonesia's national defense system [14]. A study from Global Firepower in 2021 indicates that several major countries have integrated AI into their national defense systems, signifying a paradigm shift in global military strategies that Indonesia must address to avoid falling behind in the global defense technology competition [15].



Source: OECD AI (Live data from OECD.AI - OECD.AI)

Figure 1. VC Investment in AI by Country

In alignment with this developmental trajectory, the Indonesian government, through Presidential Regulation Number 8 of 2021, has established a general defense policy direction that emphasizes the utilization of AI, concurrent with the launch of the National Artificial Intelligence Strategy. This strategic framework serves as a guideline for ministries and governmental organizations in the advancement of AI research operations within Indonesia [5]. Within this context, the government is actively promoting the adoption of advanced technologies such as AI to fortify the national defense and security sector, which is critical for the establishment of a more responsive and adaptive defense system [14], to realize national interests and global objectives through the Sustainable Development Goals [16].

The emergence of Artificial Intelligence as a force multiplier in the realm of national defense has catalyzed a paradigm shift in how countries conceptualize, formulate, and execute defense policies. With its ability to process vast datasets, detect hidden patterns, and automate high-risk operational tasks, AI is increasingly seen as critical for maintaining strategic superiority. However, in Indonesia, national defense policy has not yet significantly incorporated AI in a structured, ethical, and operationally viable manner. Consequently, this gap is particularly felt given the strategic implications of AI integration in defense systems, from enhancing surveillance and intelligence capabilities to improving efficiency in decision-making. This paper argues for the urgent need to reframe existing defense policies by integrating AI across the decision-making chain, addressing not only technological capabilities but also institutional, legal, and ethical readiness. Therefore, the main

objective of this research is to develop a comprehensive and forward-looking policy framework that enables Indonesia to adopt AI in its defense posture without compromising democratic accountability or strategic stability.

2. Literature Review

In recent decades, significant advancements in Artificial Intelligence have facilitated its widespread integration into various strategic sectors, most notably defense. Artificial Intelligence is progressively becoming a foundational element in the modernization of defense systems. Scharre, in his book Army of None, asserts that "AI-powered autonomous systems are reshaping tactical decision-making on the battlefield," thereby emphasizing an efficiency and speed unmatched by human capabilities in critical scenarios [17]. Furthermore, ethical frameworks and international regulations are deemed necessary to ensure the controlled and responsible application of AI within the military domain [2]. This highlights the imperative for a robust policy innovation framework that meticulously addresses the complexities of AI integration, while upholding ethical considerations and international norms.

A study accentuates the necessity of employing autonomous decision-making systems in military environments to expedite tactical and strategic responses. The study elucidates that AI algorithms possess the capability to assess myriad scenarios expeditiously, thereby substantially surpassing human proficiencies [18]. This is further corroborated by research, which posits that the integration of AI in a defense context not only augments operational efficiency but also fortifies system resilience when confronted with asymmetric threats and cyber incursions [19]. Such assimilation is indispensable for amplifying situational awareness and predictive analytics, enabling defense apparatuses to anticipate and neutralize threats with greater efficacy [20].

However, the employment of AI in strategic defense decisions presents notable ethical and policy-related challenges [21]. It is posited that over-reliance on algorithms may diminish human authority in consequential decision-making processes, particularly when AI systems exhibit opacity in their decision-making rationale. Consequently, the principles of "human-in-the-loop" and "explainable AI" are of paramount importance for ensuring accountability in AI-driven defense systems [22].

NATO and China offer examples of early adoption; however, Southeast Asian perspectives are notably underrepresented. Ethical considerations, regulatory methodologies, and institutional preparedness constitute core themes in contemporary literature. These themes are critical for establishing a balanced approach that leverages AI's transformative potential while mitigating its inherent risks, thus necessitating robust policy frameworks for responsible deployment in national defense [2]. Moreover, the proliferation of AI in military applications necessitates careful consideration of its implications for international stability and arms control, particularly concerning nuclear-armed states where AI could impact early-warning systems and command structures [23].

In Indonesia, the implementation of AI in the context of defense is still in the initiation phase. A study highlights those limitations including digital infrastructure, competent human resources, and a comprehensive regulatory framework are substantial obstacles in the effort to integrate AI into the national defense system [24]. Furthermore, the absence of a dedicated national AI policy specifically tailored for the defense sector hampers Indonesia's preparedness for digital transformation in this strategic domain [13].

Based on the literature review above, it can be concluded that while AI presents significant potential in strategic decision-making within the defense sector, there is an imperative need to develop normative, technological, and institutional frameworks that are adaptive to geopolitical challenges and dynamics. This research will construct a conceptual model that integrates technological, institutional, and policy dimensions to support the optimal utilization of AI in national defense decision-making. The Indonesian government recognizes the importance of AI, as evidenced by its national AI strategy, which aims to guide government agencies in AI research and development for national defense and security [13].

3. Methodology

This research adopts a qualitative and interpretive methodology using systematic literature reviews and comparative policy analysis. Main sources include peer-reviewed academic journals, government white papers, defense doctrine documents, and multinational AI ethics frameworks. The documents are analyzed using thematic content analysis to identify recurring policy themes such as ethical governance, accountability mechanisms, operational resilience, and civil-military innovation. The

literature selection criteria emphasize academic credibility, policy relevance, and timeframe, ensuring a solid foundation for policy synthesis.

This qualitative approach facilitates an in-depth exploration of the nuances and complexities inherent in the integration of AI into defense policies, which is crucial in the Indonesian context due to its unique geopolitical landscape and national security needs. The comparative policy review involves studying how various countries, particularly democracies with comparable strategic challenges, have incorporated AI into their defense architecture. The comparison focuses on policy formulation, technology acquisition, ethical safeguards, and operational deployment.

The comparative analysis will facilitate the identification of global best practices and lessons learned applicable to Indonesia, which will then be customized to the local context through stakeholder consultations and validation workshops. The research is conducted in phases: scoping review, data collection, data analysis, framework development, and validation. This structure helps in maintaining focus on the research objectives while allowing for flexibility in the selection of sources and adjustment of analytical methods. This structure helps in maintaining focus on the research objectives while allowing for flexibility in the selection of sources and adjustment of analytical methods. Data collection for this study primarily involved a literature review [25].

This involved synthesizing information from diverse academic databases, government publications, and relevant policy documents, with a focus on defense policy, AI strategy, and national security implications. The methodology employed also included a normative approach, analyzing legal frameworks and other valid sources to understand the regulatory landscape governing AI in Indonesia [26]. This comprehensive review of existing literature and policy documents facilitates a robust understanding of current AI integration efforts, while the normative analysis ensures the proposed framework aligns with Indonesia's unique legal and ethical considerations for AI governance. The comprehensive legal thinking regarding regulation is critical to addressing potential legal problems that may arise with the use of AI and technological developments in Indonesia, particularly concerning the potential for a legal vacuum in AI regulations [27]. This approach also involves an examination of the socio-technical implications, ensuring that the proposed framework not only addresses technological advancements but also considers the broader societal impact and ethical dimensions of AI deployment in defense [28].

4. Finding and Discussion

4.1. Finding

This research reveals that the integration of AI technology has great potential to significantly improve and revolutionize the national defense decision-making process. By leveraging advanced AI capabilities such as machine learning, natural language processing, and data analysis, defense organizations can access unparalleled levels of insight and intelligence, which can inform more strategic, data-driven, and informed decision-making across the spectrum of defense-related domains [29]. The implementation of AI systems can lead to optimal resource allocation, improved threat detection and response, and increased operational efficiency, ultimately strengthening overall national defense resilience and responsiveness [15]. However, the study also emphasizes the importance of addressing ethical considerations and potential risks associated with the use of AI in defense, including concerns about algorithmic bias, accountability challenges, and fierce debates surrounding autonomous weapon systems. In addition, this research highlights the critical need to create robust regulatory frameworks and guidelines to ensure the responsible, transparent, and ethical use of AI in the defense sector, while at the same time maximizing the potential benefits of AI to enhance national security and strategic decision-making [30].

4.1.1. Strategic Value of AI Integration

AI integration offers enhanced strategic value across several key defense decision-making domains. AI algorithms can analyze vast datasets from various sources to identify patterns and anomalies that human analysts are unlikely to detect [31]. AI systems can improve predictive capabilities, enabling policymakers to anticipate potential threats and proactively allocate resources [15]. AI-driven simulations and war games can provide decision-makers with a more nuanced understanding of the potential consequences of various actions [1]. AI-powered intelligence, surveillance, and reconnaissance systems can enhance situational awareness by automatically identifying and tracking potential threats in real-time [31]. Further enhancements can be achieved through AI-driven platforms that optimize resource allocation by dynamically adjusting deployment strategies based on real-time

threat assessments and logistical constraints, thus ensuring resources are strategically positioned for maximum impact [1].

AI's potential is realized through its computational and decision-making capabilities, enhancing the self-control and self-regulation of combat systems [31]. By implementing an AI-based defense strategy, Indonesia can optimize shipping routes, accurately plan supply needs, automate processes, and manage risks effectively [32]. Furthermore, the incorporation of AI facilitates the development of advanced autonomous defense systems capable of dynamically adapting to evolving threat landscapes, thereby enhancing the agility and effectiveness of the overall national defense strategy.

AI algorithms can be trained to identify subtle indicators of potential cyber attacks, enabling security teams to respond more quickly and effectively. AI can also automate many routine tasks associated with cybersecurity, such as threat detection and vulnerability scanning, freeing up human analysts to focus on more complex issues [33]. AI-driven cybersecurity platforms can continuously learn and adapt to new threats, providing defense organizations with stronger protection against evolving cyber risks. Furthermore, AI's capacity to evaluate large datasets and rapidly identify anomalies and suspicious patterns empowers AI/ML-driven defense systems [34]. By gaining insights into the strategies, methods, and protocols used by attackers, these systems can predict and defend against future attacks [35]. However, the implementation of AI in cybersecurity presents challenges, including the potential for sophisticated hackers to manipulate or bypass these systems and concerns about the lack of transparency in AI decision-making processes [36]. It is crucial to address these challenges through the development of robust validation techniques, ethical guidelines, and regulatory frameworks to ensure the responsible and effective use of AI in cybersecurity defense [37].

The integration of AI in autonomous weapons raises significant ethical concerns [38]. Therefore, it is important to develop an ethical framework that provides guidance for the use of AI in national defense [2]. This framework should address issues such as accountability, transparency, and potential unintended consequences [39]. The principles of just war theory, including proportionality and discrimination, must be incorporated into AI systems to ensure that they are used ethically and responsibly [2]. Most importantly, this ethical construct must operate in accordance with existing legal and regulatory provisions, serving to augment rather than replace established governance and oversight frameworks.

The application of AI in defense requires careful consideration of potential risks and challenges. One major concern is the possibility of attacks by adversaries on AI systems. Such attacks can manipulate AI algorithms to produce incorrect or biased results, potentially leading to flawed decision-making. Reliance on AI systems without incorporating robust human-in-the-loop validation mechanisms can inadvertently foster complacency, which in turn increases the risk of failing to detect emerging and unconventional threats that deviate from established patterns [35]. Successful adversarial attacks on AI systems can accelerate a series of detrimental effects, including the compromise of critical defense capabilities, exfiltration of sensitive data, or induction of systemic malfunctions, thus posing significant risks to national security [40].

AI utilization can enhance production efficiency through automation, machine maintenance forecasting, and supply chain optimization. AI's ability to analyze vast amounts of data, at speeds far exceeding human capabilities, transformatively improves intelligence efforts by identifying potential threats, uncovering hidden patterns in enemy activity, and providing enhanced situational awareness to decision-makers. The integration of AI-powered surveillance and reconnaissance systems can help automate threat recognition and facilitate faster responses [37]. AI can enhance training by simulating realistic combat scenarios, providing personalized feedback, and automating administrative tasks. Therefore, the development of comprehensive policies and guidelines is essential to maximize the benefits of AI while mitigating its risks [10].

4.1.2. Ethical, Legal, and Political Challenges

Ethical considerations surrounding AI in defense extend to potential algorithmic biases, which can disproportionately impact certain demographic groups, raising concerns about fairness and equality. Transparency and accountability in AI decision-making processes are crucial, particularly in lethal autonomous weapon systems, where delegating lethal decisions to machines raises fundamental questions about moral responsibility and legal liability [41]. Maintaining the use of AI requires the establishment of strict quality assurance protocols, fostering a sense of responsibility among AI practitioners, and embracing diverse perspectives in AI development [42]. Addressing legal and policy gaps is essential to ensure compliance with international humanitarian law and human rights

principles in the development and application of AI-supported defense systems [43]. Clear guidelines on AI decision-making processes, accountability for failures, and ensuring these systems do not perpetuate biases or violate individual rights are necessary [35]. Adhering to ethical standards and implementing reliable security measures are critical when using AI in cybersecurity.

Furthermore, the international security landscape introduces an additional layer of complexity, including concerns about data risks, system fragility, integration challenges, and potential misperceptions and misunderstandings [44]. Thus, developing norms and standards for the responsible use of AI in defense requires international cooperation to mitigate the risks of an AI arms race and ensure that AI is used to promote peace and stability. Regulatory uncertainty can also significantly hinder the development, implementation, and enforcement of AI policies, leading to gaps in oversight and governance [20] [45]. It is necessary to have ongoing dialogue with stakeholders, including employees, customers, regulators, and communities, to proactively identify and address ethical risks [46].

The potential for misuse and proliferation of AI technology poses a significant threat to international stability [47]. It is crucial to establish clear guidelines and regulations governing the development, deployment, and use of AI in defense to prevent unintended consequences and mitigate the risk of escalation [20]. The diffusion of AI capabilities to various actors could lead to deadly consequences [47]. It is essential to establish strict norms and protocols to regulate the export and transfer of AI technology, as well as to prevent misuse by non-state actors. Harmful misuses must be prevented through international dual-use aware policies and regulations.

International institutions can play an important role in regulating advanced AI systems, from supporting access to this technology to setting international safety standards [48]. International cooperation is essential to address the global challenges posed by AI, including the development of shared standards, norms, and regulations. Addressing regulatory gaps and promoting global cooperation can ensure that AI is developed and used responsibly, minimizing potential risks and maximizing benefits [49]. It is important to catalog and compare AI governance documents to identify points of difference and commonality [50].

Autonomous systems and predictive algorithms raise profound questions about moral responsibility, data bias, and legal compliance in the use of lethal force. Ensuring human-in-the-loop or human-on-the-loop oversight is crucial to maintaining accountability in AI-driven systems. The use of AI in defense requires careful consideration of ethical implications, legal frameworks, and strategic considerations to ensure that AI enhances, rather than undermines, human security and international stability [2]

The development of AI technology for military purposes has raised substantial ethical concerns, with an emphasis on the necessity of human oversight in decisions related to lethal force. In the discourse surrounding autonomous weapon systems, a broad consensus has formed regarding the need to maintain meaningful human control to prevent undesirable outcomes and ensure clear accountability. It is critical to implement robust safeguards and ethical frameworks to mitigate the risks associated with AI-supported weapons, including the potential for unintended escalation and the erosion of human control. The strategic implications of AI in defense are far-reaching, including AI's potential to alter the balance of power, accelerate the pace of conflict, and create new forms of strategic surprise [47].

4.1.3. Institutional Deficiencies

The case-by-case approach to addressing AI governance can lead to ambiguity and confusion. The urgency to address these challenges is reinforced by the increasing incorporation of AI into high-risk domains [51]. Existing governance initiatives lack the mechanisms and institutions to prevent misuse and recklessness and barely address autonomous systems [52]. The broad spectrum of existing AI governance initiatives manifests striking differences in methodology, breadth of application, and inherent legal force, creating a fragmented and potentially inconsistent regulatory landscape.

The lack of clarity in ethical principles and operational standards for the development and application of AI can lead to confusion and inconsistency among stakeholders [53]. A lack of technical capabilities and resources can hinder effective efforts to monitor and regulate AI systems. Gaps in expertise and resources can inhibit the understanding, assessment, and mitigation of risks and potential hazards associated with AI [54]. It is crucial to identify specific gaps in capabilities, policies, and resources that need to be addressed to ensure responsible AI development and deployment.

AI governance needs to consider the complex interactions of various factors, including ethical considerations, legal frameworks, and economic incentives. To effectively manage the risks associated with AI, especially in defense, policymakers must adopt a comprehensive approach that addresses the technical, ethical, and legal dimensions [42]. Addressing legal and policy gaps is essential to ensure compliance with international humanitarian law and human rights principles in the development and application of AI-supported defense systems [2].

As AI systems take on more complex tasks, including those involving military applications, questions of accountability become increasingly important. The absence of a clear accountability framework for AI decision-making can lead to a diffusion of responsibility and challenges in linking accountability for unintended harm. Establishing clear lines of responsibility and accountability for AI decision-making is critical to ensuring that individuals and organizations are held accountable for the consequences of their actions [55].

Ethical concerns regarding military AI encompass accountability and human dignity, and the public strongly believes that human control over autonomous weapons is essential [47]. Maximizing the performance of AI technology must be balanced with legal constraints, particularly regarding transparency in weapon capabilities and adherence to international humanitarian law [56].

The development and use of AI in defense raise concerns about potential algorithmic bias, data privacy breaches, and the erosion of human control over critical decisions. A lack of transparency in AI systems can erode trust and confidence, especially in high-risk applications such as defense and security. It is essential to promote transparency and explainability in AI algorithms to enhance accountability and foster public trust [57].

AI systems must be designed to operate within established legal and ethical boundaries, incorporating human oversight and safeguards to prevent unintended harm. Legal risks associated with AI systems generally fall into two primary categories: safety risks and fundamental rights risks [58]. Addressing these risks requires interdisciplinary collaboration and ongoing dialogue among stakeholders, including policymakers, researchers, and civil society organizations [46]. The EU AI Act is a pioneering effort to establish a comprehensive legal framework for AI, addressing issues such as privacy, security, and ethical considerations [59].

The application of AI in strategic decision-making for national defense policy in Indonesia requires a multifaceted approach that combines ethical considerations, protection against bias, and the maintenance of human control. Transparency and accountability in AI systems are essential to building trust and ensuring alignment with humanitarian values. Developing a robust ethical and regulatory framework can help mitigate potential risks and ensure that AI is used responsibly and in alignment with national interests [60].

The integration of AI across Indonesian government institutions requires careful consideration of Indonesia's political landscape, marked by overlapping jurisdictions among various institutions, a challenge exacerbated by frequent personnel transitions. Addressing these shortcomings requires a multi-pronged approach that includes investing in education and training programs to develop a skilled AI workforce, fostering collaboration between government, industry, and academia to accelerate innovation, and establishing robust legal and ethical frameworks to guide AI development and deployment [13]. The development of adequate technology and infrastructure, along with clear and comprehensive regulations, is the foundation for ethical AI implementation. In Indonesia, the legal framework for information and electronic transactions, specifically Law Number 1 of 2024, is considered inadequate to address emerging crimes and privacy issues related to AI misuse. Further compounding this issue, the uncertain legal status of AI entities poses complexities in establishing responsibility and determining appropriate compensation in cases of harm or damage resulting from AI actions; this ambiguity necessitates a reevaluation of existing legal structures to accommodate the unique challenges posed by AI technology [26]. The Indonesian government has initiated cybersecurity measures by issuing legal products aimed at securing digital technology and safeguarding cyberspace, which serve as a foundation for AI-related strategic policies in national defense, ensuring the fulfillment of societal rights and obligations [13].

4.1.4. Benchmarking Global Best Practices

An evaluation of initiatives implemented by leading countries in the field of AI, such as the United States, China, and the European Union, can provide a valuable framework for Indonesia in developing its AI governance framework [13]. In the context of handling AI governance, a comparative analysis of the strategies implemented by various other countries reveals a spectrum of diverse approaches,

ranging from the establishment of comprehensive legal frameworks to the adoption of sector-specific regulations. Indonesia has the potential to gain valuable lessons from other countries' experiences in regulating AI, including from the European Commission's High-Level Expert Group on Artificial Intelligence [27]. In addition, several countries have implemented regulations related to text and data mining or data scraping for machine learning AI to mitigate potential copyright infringements arising from the use of datasets containing other people's creations as AI development material [61].

Singapura, for example, emphasizes human supervision, data governance, and fairness through initiatives such as "One Data Indonesia" and the Personal Data Protection Bill. In Southeast Asia, countries like Malaysia and the Philippines are developing national AI strategies with a focus on ethical considerations and regulatory frameworks. The United States prioritizes market-driven innovation with minimal regulatory constraints, while the European Union enforces a precautionary risk-based framework that emphasizes ethical protection [62].

Comparing AI governance in Asian countries such as India and Indonesia reveals unique approaches shaped by national priorities and challenges, emphasizing collaboration, adaptability, and ethical commitment. By comparing regulatory and ethical considerations in the US, EU, and Asia, Indonesia can create an adaptive AI governance framework [62]. Each of these examples illustrates the importance of adaptability and collaboration in AI governance and emphasizes the need for international harmonization to address the global implications of AI technology. An international cooperation framework is essential to align standards and ensure responsible AI development worldwide [60].

Examining AI governance models in the UK and Singapore provides valuable insights into building effective AI governance that encourages innovation while addressing ethical concerns. These models can offer insights for Indonesia to promote AI innovation and harness its positive potential [63]. Furthermore, understanding the cultural, social, and economic contexts that influence the development and application of AI technology is essential for tailoring governance frameworks to specific national circumstances.

Singapore's significant AI potential can be a cooperation opportunity with Indonesia in various potential sectors, such as research and industrial innovation. Singapore has also successfully established a National Artificial Intelligence Office as an institution that coordinates all efforts from various artificial intelligence actors. Indonesia can learn from countries like China, South Korea, and Singapore in developing personal data protection regulations [64].

4.1.5. Proposed Policy Innovation Framework

Developing a comprehensive AI governance framework tailored to Indonesia's specific legal and cultural context is crucial, requiring an examination of existing laws and regulations [13]. Indonesia's legal framework, including laws on electronic information, transactions, and personal data protection, needs to be strengthened to address AI-specific challenges such as accountability, ethics, and data protection [27] [65].

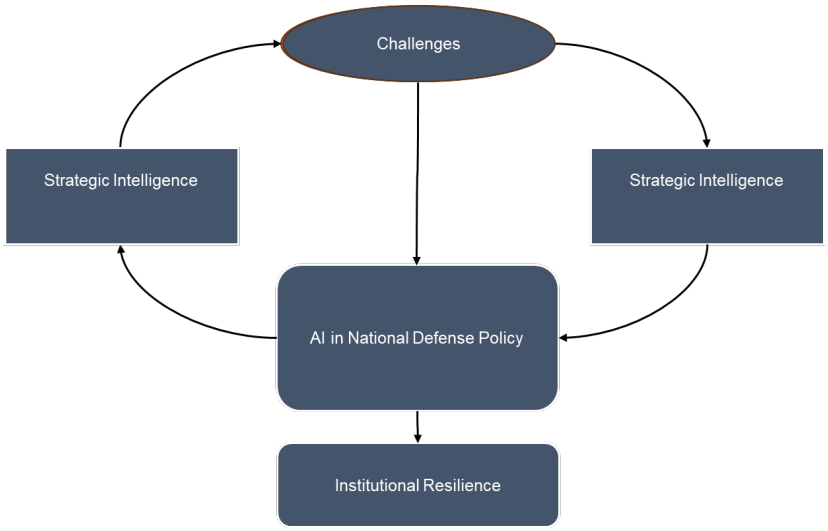
To create an AI regulatory framework that encourages innovation and protects public interests, Indonesia can learn from Singapore's sectoral approach and the European Union's risk-based approach. Indonesia's AI governance must ensure that AI systems operate ethically and legally, considering accountability, transparency, and human rights principles. Furthermore, Indonesia's approach may involve a combination of offensive and defensive strategies, focusing on adapting and strengthening existing laws such as the Personal Data Protection Law [26].

The proposed framework should include mechanisms for continuous monitoring, evaluation, and adaptation to address evolving challenges and opportunities in the field of AI, potentially drawing from the EU's General Data Protection Regulation as a model [66]. This includes the establishment of an independent AI ethics board tasked with providing guidance, oversight, and enforcement of ethical standards for AI development and deployment [27]. Furthermore, efforts to promote public awareness and understanding of AI technology are essential to foster trust, acceptance, and informed decision-making among citizens.

The Indonesian government can establish regulations at the ministerial level, such as ministerial regulations, as a medium-term option, while developing higher regulatory formats, such as presidential regulations or specific laws on AI [26]. A robust AI governance framework requires interdisciplinary collaboration, combining the knowledge and expertise of legal experts, computer scientists, ethicists, and policymakers to address the multifaceted challenges posed by AI. The

governance focus should extend beyond regulatory compliance to encompass broader considerations of social values, cultural norms, and human rights principles [53].

Furthermore, AI policies must align with global standards, including the UNESCO Recommendation on the Ethics of AI, and incorporate principles such as proportionality, "do no harm," and human oversight [67]. The development of legal and ethical guidelines for AI requires a comprehensive framework that aligns with international norms while addressing Indonesia's specific needs, bridging the gap between global standards and local implementation. Ethical considerations should be embedded throughout the AI lifecycle, from design and development to deployment and evaluation, to ensure that AI systems align with societal values and norms [68]. Indonesia can establish comprehensive and adaptable AI governance by learning from global experiences and engaging diverse stakeholders [69].



Figures 2. Conceptual Framework

Next, the researchers present a table of policy gaps and recommendations that highlights five key policy areas, the existing shortcomings in Indonesia, and solution-oriented recommendations for each. This table provides a comprehensive overview of the existing policy challenges and proposed solutions to improve AI governance in Indonesia.

Table1. AI Defense Policy Gaps and Recommendation

Policy Area	Current Gap in Indonesia	Recommendation
AI Integration Focus	No structured AI deployment in defense systems	Integrate AI into ISR, cyber-defense, and logistics
Ethical & Legal Safeguards	No legal framework for AI use in military ops	Create legislation for AI ethics and accountability
Institutional Structure	No centralized AI Defense Council	Establish a National AI Defense Council
Global Benchmarking Focus	Limited alignment with global AI practices	Adopt elements from NATO/JAIC/China AI models
Cross-Sector Collaboration	Weak public-private-academic R&D linkages	Facilitate joint AI R&D initiatives across sectors

4.1.5. Strategy for Leveraging AI for Strategic Decision-Making in National Defense

This systematic approach facilitates a clear understanding of the necessary interventions to bridge the current regulatory and implementation gaps in Indonesia's AI ecosystem. Indonesia's national defense strategy can be significantly enhanced through the judicious integration of AI, offering capabilities for advanced threat detection, predictive analytics, and optimized resource allocation [16]. This strategic leverage necessitates a robust policy framework that addresses ethical considerations, data security, and the integration of AI within existing defense infrastructures.

The implementation of AI in defense must also consider the unique challenges and opportunities within Indonesia's legal and ethical landscape. The legal framework surrounding AI in Indonesia is currently general, lacking specific regulations on accountability, ethics, and data protection, which necessitates the establishment of new laws to keep pace with technological advancements [27]. A normative legal research approach, incorporating legislative and comparative analyses, reveals that while the global adoption of AI in national defense is accelerating, Indonesia's utilization and regulatory framework remain suboptimal, necessitating specific regulations for AI integration [13]. This includes addressing the risks of misuse, such as autonomous weapons operating without human intervention, and developing robust cybersecurity measures to counter enhanced threats and potential AI-enabled terrorist activities [13] [26].

The government must develop adequate policies, laws, and regulations as a fundamental basis for AI integration, alongside strengthening intelligence capabilities to understand and overcome AI-related threats [5]. This strategic imperative is underscored by Indonesia's current stage of AI adoption within its defense sector, which, while promising, requires substantial development to reach parity with global leaders [13]. Future conflicts will increasingly rely on smaller, highly effective combat units augmented by autonomous, unmanned military systems with high levels of autonomy, emphasizing the need for advanced AI in defense [5].

The application of AI in national defense is not merely a technical upgrade but a transformative shift that necessitates a parallel evolution in legal and ethical frameworks to ensure responsible and effective deployment [13]. A robust national defense strategy must incorporate comprehensive AI integration to optimize intelligence gathering, threat assessment, and operational efficiency, leveraging AI's capacity for rapid data processing and pattern recognition [5]. These technological advancements will play a crucial role in enhancing Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) frameworks within Indonesia's defense architecture [27].

The current general legal framework for AI in Indonesia, particularly concerning accountability and data protection, is inadequate for the specific requirements of national defense applications and necessitates new, specialized legislation to govern the use of AI in this critical sector [26]. The strategic integration of AI into Indonesia's defense apparatus offers substantial improvements in maritime monitoring, operational efficiency, and international collaboration, despite facing challenges such as high initial costs, infrastructure deficits, and data security concerns. The higher accuracy afforded by AI in threat detection and monitoring significantly contributes to increased situational awareness and more informed decision-making for operational leaders within the Indonesian Navy [70].

AI's potential in national defense is vast, encompassing logistical support, simulation, target recognition, and threat monitoring, which significantly enhances a nation's ability to protect its interests and people [13]. Indeed, the complexity of operations and the dynamic maritime environment surrounding Indonesia demand swift responses, necessitating robust and integrated information systems for effective monitoring, analysis, and strategic decision-making. Thus, AI-powered systems can serve as a foundational element for fostering effective collaboration among various stakeholders, ensuring the collective security and sovereignty of global maritime territories [70].

The urgency for comprehensive AI regulation in Indonesia's defense sector is paramount given the rapid global advancements in AI-driven military capabilities and the current suboptimal integration of AI within the national defense system [13]. This includes bolstering the ship information systems of the Indonesian Navy with AI, which can dramatically enhance maritime surveillance and threat detection capabilities through the integration of advanced sensors and real-time data analysis [70]. These advancements are crucial for maintaining national security and sovereignty in an increasingly complex geopolitical landscape, particularly given Indonesia's vast maritime territory and strategic location. The enhanced capabilities include identifying potential dangers and analyzing data from

diverse sources to recognize threat patterns, thereby enabling faster and more accurate decision-making for operational leaders.

Within the framework of leveraging AI in strategic decision-making, this research endeavors to establish an analytical framework employing the PMESII methodology to ensure a comprehensive evaluation of political, military, economic, social, information, and infrastructural factors. This framework is designed to facilitate a holistic understanding of how AI can be integrated into defense strategies, thereby optimizing resource allocation and enhancing overall strategic foresight. Furthermore, the framework directly addresses the critical need for Indonesia to overcome existing limitations in AI adoption, including deficiencies in workforce skills and infrastructural investment, to fully capitalize on AI's potential in national security [9].

Table 2. PMESII Analysis

PMESII Aspects	Impact AI Integration
Politics	enhances defense legitimacy through greater transparency and accountability in military operations
Military	strengthen defense systems automatically, enable early detection, and enhance capabilities in cyber defense
Economic	involves budget efficiency and reduced personnel costs in managing national defense through logistics optimization and predictive maintenance.
Social	requires mitigating public concerns regarding weapon autonomy through the development of a strong ethical framework and transparent public communication
Infrastructure	highlights the need for modernizing digital infrastructure and ensuring adequate cybersecurity to support AI defense systems, as well as improving C4ISR systems
Information	enhance C4ISR systems in collecting and analyzing intelligence data in real-time, which will increase situational awareness and enable rapid decision-making, thereby allowing for more adaptive responses to threats

4.2. Discussion on AI-Driven Transformation in National Defense Strategy

The integration of AI into Indonesia's national defense strategy presents transformative opportunities to enhance capabilities, optimize resource allocation, and improve decision-making processes. This incorporation should commence with the strategic development of AI systems engineered for advanced threat detection, sophisticated intelligence analysis, and robust cyber defense, all of which are crucial for fortifying the national security infrastructure [13]. The capacity of AI to process vast quantities of data in real-time can furnish decision-makers with actionable insights, thereby enabling proactive responses to potential threats and minimizing vulnerabilities across critical infrastructure.

AI enhances military readiness through predictive maintenance of defense equipment, optimizes logistics, and automates routine tasks, allowing personnel to focus on strategic activities [15]. AI-based simulations and training programs offer realistic scenarios for military personnel, improving readiness and decision-making skills under pressure, which enhances the overall effectiveness of the national defense strategy [29].

By analyzing data on security threats, AI facilitates cross-agency and international collaboration, enabling coordinated responses to challenges like smuggling [70]. Furthermore, the implementation of AI-based systems for real-time situational awareness involves advanced integration of diverse data streams, including satellite imagery, signals intelligence, and sensor data in the field, thus providing a comprehensive and integrated operational picture that drastically improves the accuracy and effectiveness of military operations, resulting in better strategic outcomes [71].

Indonesia needs to invest in research and development and build capacity to utilize AI in national defense [13]. This investment can improve real-time threat monitoring and detection, enhancing situational awareness and decision-making for TNI Angkatan Laut leaders [70]. This also requires investment in human resources to effectively manage and oversee AI systems in a military context.

Addressing challenges through strategic budget allocation, infrastructure development, personnel training, and the formulation of ethical regulations is crucial for the successful integration of AI into national defense [70]. In recognition of AI's potential, the Indonesian government has undertaken initial initiatives to explore its application across various sectors, including the formulation of a National Strategy for Artificial Intelligence in 2020, marking a fundamental step toward integrating AI into the nation's development agenda [13]. Moreover, AI's role in augmenting national defense capabilities extends beyond conventional military applications to encompass cybersecurity, border protection, and disaster response.

The integration of AI into Indonesia's defense strategies marks a critical evolution, driven by the need to adapt to modern warfare and address evolving security challenges [13]. Integrating AI with advanced sensors like radar, sonar, and thermal cameras enhances the accuracy of real-time monitoring, allowing for the identification of suspicious activities. This integration enables faster and more precise responses, strengthening maritime security. The development of AI should focus on multidisciplinary approaches that bridge the gap between technological capabilities and practical applications, ensuring that AI-driven solutions are tailored to Indonesia's specific defense needs and strategic objectives [70].

Indonesia's national defense faces challenges such as external threats and internal security issues, necessitating the adoption of advanced technologies like AI to address these challenges effectively [13]. Contemporary military strategies increasingly rely on the synergistic integration of AI with other advanced technologies, such as the Internet of Things for enhanced sensor networks, Cyber-Physical Systems for autonomous control of defense systems, and Big Data analytics for actionable intelligence [72]. Given the increasing reliance on AI-integrated technologies in contemporary warfare, it is crucial for the TNI to proactively adapt by modernizing its defense infrastructure, integrating advanced AI capabilities throughout its operational framework, and adjusting its strategic approach to effectively counter emerging threats and safeguard national interests [9] [70].

Indonesia can leverage AI to improve early threat detection for threats like terrorism or other crimes, with machine learning algorithms analyzing behavioral patterns in public areas to identify anomalies and alert authorities before critical situations arise. Additionally, AI-supported systems can enhance cybersecurity capabilities by automatically detecting and responding to cyber threats, protecting critical government infrastructure and data from cyber attacks [37]. The implementation of the Smart Defense 5.0 concept heavily relies on the integration of AI into the technological infrastructure, which requires a comprehensive architecture that includes robust communication networks, secure and scalable data storage systems, and edge computing technologies that enable real-time data processing and analysis near the source [14].

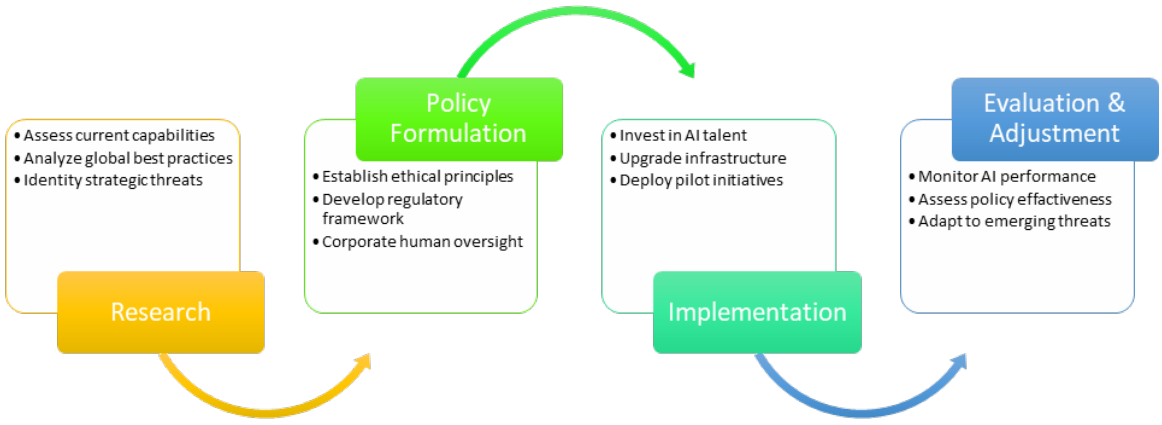
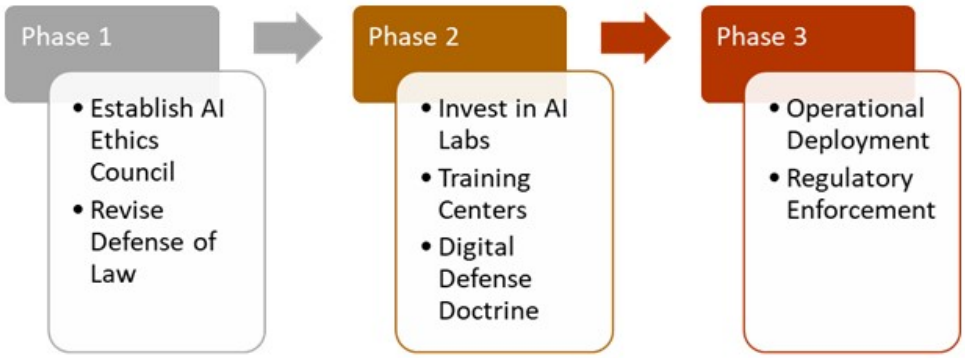


Figure 3. Roadmap for AI-Driven National Defense Policy in Indonesia

To maintain technological sovereignty in AI, Indonesia must prioritize the development of domestic AI capabilities, reducing reliance on foreign technologies and ensuring that AI systems align with national values and security imperatives. Indonesia should also adopt a proactive approach to address ethical considerations in AI development by establishing comprehensive guidelines and frameworks. This includes ensuring transparency in AI algorithms, protecting privacy rights, and preventing bias in AI decision-making processes [2]. Indonesia also should foster collaboration between government, academia, and the private sector to accelerate AI innovation and develop solutions tailored to Indonesia's unique needs [14] [73]. Such collaboration enables resource sharing, knowledge transfer, and the creation of a robust AI ecosystem that drives economic growth and improves public services.

Reframing Indonesia's National Defense Policy via AI integration can offer competitive advantages, improve decision-making, and accelerate digital transformation. Indonesia should actively participate in international forums and collaborations to shape global AI governance frameworks, promote responsible AI development, and safeguard its interests in the evolving AI landscape [74]. By strategically integrating AI into its national defense framework, Indonesia can achieve these goals while maintaining its sovereignty and promoting regional stability. To remain competitive in the digital age and safeguard its national interests, Indonesia must embrace AI-driven innovation and develop strategies to mitigate risks while maximizing benefits. Indonesia can enhance transparency and accountability in governance by deploying AI-driven systems that monitor financial transactions, detect anomalies, and reduce corruption [75].



Figures 4. AI Implementation in National Defense Policy

5. Conclusion

Indonesia is currently at a critical juncture, where failure to adapt to the transformative impact of AI on security could lead to strategic marginalization. By strategically revising its national defense policies to incorporate AI, Indonesia has the opportunity to enhance its strategic review, operational effectiveness, and ethical accountability. This paper puts forward five core policy recommendations:

- Form a National AI Defense Council under the Ministry of Defense to coordinate AI strategies and implementation across the defense sector. This council will ensure unified direction and efficient resource allocation.
- Codify the use and accountability of AI in military operations through legislation, establishing clear limitations and safeguards for the application of AI in defense scenarios. The legal framework will address ethical considerations and potential risks associated with AI technology.
- Create AI ethics training and certification programs for defense personnel to promote responsible AI usage and minimize biases in AI systems. The training will equip personnel with the knowledge to handle AI technologies ethically and effectively.
- Promote cross-sector AI R&D collaboration through public-private-academic partnerships, fostering innovation and ensuring that AI solutions are tailored to Indonesia's unique defense needs. Collaborative efforts will leverage diverse expertise and resources to accelerate AI development.

- Implement mandatory Human-in-the-Loop / Human-on-the-Loop protocols in all AI weapon systems to maintain human oversight and control, preventing unintended consequences. HITL/HOTL protocols will ensure that critical decisions are made with human judgment and accountability.

Future research should focus on operational pilot studies within Indonesia's defense apparatus and the development of AI ethics indicators tailored to Indonesia's constitutional and cultural values, ensuring that AI technology aligns with national identity and ethical standards. Creating a comprehensive and adaptive AI strategy is crucial not only for strengthening Indonesia's national defense but also for proactively shaping its strategic role in an era increasingly defined by technological advancements.

References

[1] D. I. Mikhailov, "Artificial Intelligence and Machine Learning in National Security," pp. 1–5, Mar. 2023.
[2] M. Taddeo, D. McNeish, A. Blanchard, and E. Edgar, "Ethical Principles for Artificial Intelligence in National Defence," *Philos Technol*, vol. 34, no. 4, pp. 1707–1729, Mar. 2021.
[3] A. King, "Digital Targeting: Artificial Intelligence, Data, and Military Intelligence," *Journal of Global Security Studies*, vol. 9, no. 2, Jun. 2024.
[4] M. Yazdi, E. Zarei, S. Adumene, and A. Beheshti, "Navigating the Power of Artificial Intelligence in Risk Management: A Comparative Analysis," *Safety*, vol. 10, no. 2, Jun. 2024.
[5] A. N. Rahmatika, "Strategi Pertahanan Negara Indonesia Dalam Menghadapi Ancaman Artificial Intelligence," vol. 8, no. 2, Mar. 2022.
[6] Y. Sutrasna, "Strategi Pertahanan Indonesia dalam Menghadapi Ancaman Militer dan Non Militer Melalui Prespektif Ekonomi Pertahanan," *Syntax Literate: Jurnal Ilmiah Indoensia*, vol. 8, no. 7, p. 2023, Jul. 2023.
[7] M. F. Ridwansyah and A. Zuhra, "Penggunaan Artificial Intelligence Dalam Perang Dari Aspek Prinsip Pembedaan," *terAs Law Review: Jurnal Hukum Humaniter dan HAM*, vol. 4, no. 1, pp. 15–32, Oct. 2022.
[8] F. Boentolo, C.-C. C. R. Manu, O. G. Saragih, and S. Zalukhu, "Peran Guru Memanfaatkan Ai Dalam Membangun Generasi Unggul Menuju Indonesia Emas 2045," *Aletheia Christian Educators Journal*, vol. 5, no. 1, pp. 42–48, May 2024.
[9] S. C. Islam Taufik, R. Rismayanti, D. R. Sopian, and A. A. Dede Saputra, "The Influence Of The Development Of Artificial Intelligence Technology In The Industrial Field," *Jurnal Indonesia Sosial Teknologi*, vol. 4, no. 8, pp. 1186–1199, Aug. 2023.
[10] M. Schmitt and P. Koutroumpis, "Cyber Shadows: Neutralizing Security Threats with AI and Targeted Policy Measures," *IEEE Transactions on Artificial Intelligence*, Mar. 2025.
[11] R. A. E. Wahyuni, S. D. Waluyo, and H. Simatupang, "Strengthening The Cyber Defense Center Of The Ministry Of Defence Of The Republic Of Indonesia (Pusdatin Kemhan) To Support The Indonesian Defense Diplomacy In Cyber Defense Security Cooperation In Asean," *Jurnal Pertahanan*, vol. 7, no. 3, pp. 511–525, 2021.
[12] P. L. Gaol, "Implementation of Performance Management in Artificial Intelligence System to Improve Indonesian Human Resources Competencies," in *IOP Conference Series: Earth and Environmental Science*, IOP Publishing Ltd, Apr. 2021.
[13] I. A. Pangestu, A. Thorik, M. R. Fadhlillah, and N. Mozin, "The Urgency of Artificial Intelligence Regulation in Supporting the National Defence System," *Jambura Journal Civic Education*, vol. 2, no. 1, pp. 82–89, May 2022.
[14] H. Putra, B. Eko Mulyono, and S. TNI Corresponding Author, "Smart Defense 5.0 Concept to Protect the Indonesian Capital City (IKN)," *Indonesian Journal of Interdisciplinary Research in Science and Technology (MARCOPOLO)*, vol. 2, no. 11, pp. 1479–1486, 2024.
[15] Y. Lee, T. Park, Y. Kang, J. Kim, and J. Kang, "ROK Defense M&S in the Age of Hyperscale AI: Concepts, Challenges, and Future Directions," *Law*, p. 7, Jan. 2025.
[16] A. D. W. Sumari, "The Contributions of Artificial Intelligence in Achieving Sustainable Development Goals: Indonesia Case," *IOP Conf Ser Mater Sci Eng*, vol. 982, no. 1, Dec. 2020.
[17] P. Scharre, *Army of None: Autonomous Weapons and the Future of War*. New York: W.W. Norton & Company, 2020.

[18] T. Araujo, N. Helberger, S. Kruikemeier, and C. H. de Vreese, "In AI we trust? Perceptions about automated decision-making by artificial intelligence," *AI Soc*, vol. 35, no. 3, Mar. 2020.
[19] R. Montasari, *Artificial Intelligence and National Security*. Cham Springer Nature Switzerland, 2023.
[20] H. Taylor, "The Impact of Artificial Intelligence on Defense Strategies," *International Journal of Defence And Strategic Studies (Ijdss)*, vol. 1, no. 1, pp. 42–50, Oct. 2023.
[21] A. Cunningham, "Integrated Warfare: How U.S. Special Operations Forces Can Counter AI-Equipped Chinese Special Operations Forces," 2024.
[22] J. Boulent *et al.*, "Scaling whale monitoring using deep learning: A human-in-the-loop solution for analyzing aerial datasets," *Front Mar Sci*, vol. 10, 2023, doi: 10.3389/fmars.2023.1099479.
[23] V. Chernavskikh, "Nuclear Weapons and Artificial Intelligence: Technological Promises and Practical Realities," Sep. 2024. [Online]. Available: https://www.sipri.org/sites/default/files/2024-09/bp_2409_ai-nuclear.pdf. [Accessed: Jun. 27, 2025].
[24] K. B. Prasetyo, J. Mahroza, and H. Z. Al-Mubaroq, "Implementation of Good Governance in Indonesia's Defense and Security Sector Reform Facing the Dynamic of Globalization," *Jurnal Kewarganegaraan*, vol. 7, no. 1, 2023.
[25] Francisca and A. Saptomo, "Legal Framework for the Application of Pancasila-Based Artificial Intelligence Technology to Minimize Risks and Optimize Benefits Towards Indonesia Emas 2045," *Asian Journal of Engineering, Social and Health*, vol. 3, no. 4, pp. 903–912, 2024.
[26] I. Maria, "Artificial Intelligence Governance Strategy in the Indonesian Regulation System, Offensive or Defensive?" *Journal Islamic Economic Minangkabau Sharia Oikonomia Law Journal*, vol. 2, no. 4, 2024.
[27] A. D. C. Firza, K. Samudera, and A. hira, "Legal Arrangement of Artificial Intelligence in Indonesia: Challenges and Opportunities," *Universitas Negeri Semarang, Indonesia VOLUME*, vol. 1, no. 2, pp. 14–30, 2023.
[28] D. Olivia, "Legal Aspects of Artificial Intelligence on Automated Decision-Making in Indonesia: Lessons from the European Union, the United States, and China," *Lentera Hukum*, vol. 7, no. 3, pp. 301–318, Nov. 2020.
[29] D. H. Hagos and D. B. Rawat, "Recent Advances in Artificial Intelligence and Tactical Autonomy: Current Status, Challenges, and Perspectives," *Sensors*, vol. 22, no. 24, Dec. 2022.
[30] A. Anand and H. Deng, "Towards Responsible Ai In Defence A Mapping And Comparative Analysis Of Ai Principles Adopted By States," Geneva, Switzerland, 2023. Available: https://unidir.org/files/2023-02/Brief-ResponsibleAI-Final.pdf. [Accessed: Jun. 27, 2025].
[31] A. Bin Rashid, A. K. Kausik, A. Al Hassan Sunny, and M. H. Bappy, "Artificial Intelligence in the Military: An Overview of the Capabilities, Applications, and Challenges," 2023, *Wiley-Hindawi*.
[32] S. Octaviana, Manajemen Logistik Pertahanan Era Society 5.0 Shoraya Lolyta Octaviana Cv. Aksara Global Akademia 2024. Garut: Cv. Aksara Global Akademia, 2024.
[33] Geraldine O Mbah and Achudume Nkechi Evelyn, "AI-powered cybersecurity: Strategic approaches to mitigate risk and safeguard data privacy," *World Journal of Advanced Research and Reviews*, vol. 24, no. 3, pp. 310–327, Dec. 2024.
[34] J. Kinyua and L. Awuah, "Ai/ml in security orchestration, automation and response: Future research directions," *Intelligent Automation and Soft Computing*, vol. 28, no. 2, pp. 527–545, 2021.
[35] M. Roshanaei, M. R. Khan, and N. N. Sylvester, "Navigating AI Cybersecurity: Evolving Landscape and Challenges," *Scientific Research Publishing*, vol. 16, no. 3, pp. 155–174, Mar. 2024.
[36] K. Achuthan, S. Ramanathan, S. Srinivas, and R. Raman, "Advancing cybersecurity and privacy with artificial intelligence: current trends and future research directions," 2024, *Frontiers Media SA*.
[37] M. Roshanaei, M. R. Khan, and N. N. Sylvester, "Enhancing Cybersecurity through AI and ML: Strategies, Challenges, and Future Directions," *Journal of Information Security*, vol. 15, no. 03, pp. 320–339, 2024.
[38] R. G. IEEA SA, *A Framework for Human Decision-Making through the Lifecycle of Autonomous and Intelligent Systems in Defense Applications*. New York, NY: IEEE SA, 2024. [Online]. Available: https://www.ieee.org/about/corporate/governance/p9-26.html. [Accessed: Jun. 27, 2025].

[39] M. Narayanan and C. Schoeberl, "Issue Brief A Matrix for Selecting Responsible AI Frameworks," 2023.
[40] D. S. Hoadley and N. J. Lucas, "Artificial Intelligence and National Security," Apr. 2018. [Online]. Available: www.crs.govR45178. [Accessed: Jun. 27, 2025].
[41] A. Blanchard and M. Taddeo, "Autonomous weapon systems and jus ad bellum," *AI Soc*, vol. 39, no. 2, pp. 705–711, Apr. 2024.
[42] S. M. Williamson and V. Prybutok, "The Era of Artificial Intelligence Deception: Unraveling the Complexities of False Realities and Emerging Threats of Misinformation," *Information (Switzerland)*, vol. 15, no. 6, Jun. 2024.
[43] C. Velasco, "Cybercrime and Artificial Intelligence. An overview of the work of international organizations on criminal justice and the international applicable instruments," *ERA Forum*, vol. 23, no. 1, pp. 109–126, May 2022.
[44] S. A. Alexandrovich, "Artificial Intelligence and International Security," *IEEE Explorer*, vol. 70, no. 5, Mar. 2024.
[45] D. Araya and M. King, "The Impact of Artificial Intelligence on Military Defence and Security," 2022.
[46] M. Maiti, P. Kayal, and A. Vujko, "A study on ethical implications of artificial intelligence adoption in business: challenges and best practices," *Future Business Journal*, vol. 11, no. 1, p. 34, Mar. 2025.
[47] F. Morgan *et al.*, *Military Applications of Artificial Intelligence: Ethical Concerns in an Uncertain World*. RAND Corporation, 2020.
[48] L. Ho *et al.*, "International Institutions for Advanced AI," *Law (Cornell University)*, Jul. 2023.
[49] E. Zaidan and I. A. Ibrahim, "AI Governance in a Complex and Rapidly Changing Regulatory Landscape: A Global Perspective," *Humanit Soc Sci Commun*, vol. 11, no. 1, Dec. 2024.
[50] J. Correia, "Military capabilities and the strategic planning conundrum," *Security and Defence Quarterly*, vol. 24, no. 2, pp. 21–50, Jun. 2019.
[51] C. Cath, "Governing artificial intelligence: Ethical, legal and technical opportunities and challenges," Nov. 28, 2018, Royal Society Publishing.
[52] Y. Bengio *et al.*, "Managing extreme AI risks amid rapid progress," *Science (1979)*, vol. 384, no. 6698, pp. 842–845, 2024.
[53] M. Pflanzer, Z. Traylor, J. B. Lyons, V. Dubljevic, and C. S. Nam, "Ethics in human–AI teaming: principles and perspectives," *AI and Ethics*, vol. 3, no. 3, pp. 917–935, Mar. 2022.
[54] A. Reuel *et al.*, "Open Problems in Technical AI Governance," *Law (Cornell University)*, Apr. 2025.
[55] J. Davidovic, "On the purpose of meaningful human control of AI," *Front Big Data*, vol. 5, Jan. 2023.
[56] J. Kwik and T. Van Engers, "Algorithmic fog of war: When lack of transparency violates the law of armed conflict," *Journal of Future Robot Life*, vol. 2, no. 1–2, pp. 43–66, Mar. 2021.
[57] A. Dhopte and H. Bagde, "Smart Smile: Revolutionizing Dentistry with Artificial Intelligence," *Cureus*, vol. 15, no. 6, pp. 1–10, Mar. 2023.
[58] M. J. Okuno and H. G. Okuno, "Legal frameworks for AI service business participants: a comparative analysis of liability protection across jurisdictions," 2025, *Springer Science and Business Media Deutschland GmbH*.
[59] D. Korobenko, A. Nikiforova, and R. Sharma, "Towards a Privacy and Security-Aware Framework for Ethical AI: Guiding the Development and Assessment of AI Systems," in *ACM International Conference Proceeding Series*, Association for Computing Machinery, Jun. 2024.
[60] S. M. Ibrahim, M. A. Alshraideh, M. Leiner, I. M. Aldajani, and B. Ouarda, "Artificial intelligence ethics: ethical consideration and regulations from theory to practice," *IAES International Journal of Artificial Intelligence*, vol. 13, no. 3, pp. 3703–3714, Sep. 2024.
[61] R. J. Alam Wibowo, "Ciptaan dan Invensi Hasil Kecerdasan Buatan dalam Perspektif Hak Cipta dan Paten," *Jurnal Ilmiah Kebijakan Hukum*, vol. 17, no. 3, p. 269, Nov. 2023.
[62] V. Kulothungan and D. Gupta, "Towards Adaptive AI Governance: Comparative Insights from the U.S., EU, and Asia," *Law*, 2025.
[63] L. Lestari and U. Nur, "The Use Of Artificial Intelligence In Governance Through Online Media Evaluation," *Jurnal Trias Politika*, vol. 7, no. 2, pp. 183–204, 2023.

[64] D. Setiawati, H. A. Hakim, and F. A. H. Yoga, "Optimizing Personal Data Protection in Indonesia: Lesson Learned from China, South Korea, and Singapore," *Indonesian Comparative Law Review*, vol. 2, no. 2, 2020.

[65] N. Ishak, "Guarantee of Information and Communication Technology Application Security in Indonesia: Regulations and Challenges?" *ACLJ*, vol. 4, no. 2, pp. 108–117, 2023.

[66] D. Lewis, M. Lasek-Markey, D. Golpayegani, and H. J. Pandit, "Mapping the Regulatory Learning Space for the EU AI Act," May 2025, [Online]. Available: http://law.org/abs/2503.05787. [Accessed: Jun. 27, 2025].

[67] C. Huang, Z. Zhang, B. Mao, and X. Yao, "An Overview of Artificial Intelligence Ethics," *IEEE Transactions on Artificial Intelligence*, vol. 4, no. 4, pp. 799–819, Aug. 2023.

[68] B. P. Singh and A. Joshi, "Ethical considerations in AI development," in *The Ethical Frontier of AI and Data Analysis*, IGI Global, 2024, pp. 156–179.

[69] T. Saheb, "Mapping Ethical Artificial Intelligence Policy Landscape: A Mixed Method Analysis," *Sci Eng Ethics*, vol. 30, no. 2, Apr. 2024.

[70] A. Purja, E. Sulistyadi, A. Sudiarso, M. Asvial, and R. A. Gultom, "The Prospect of Using Artificial Intelligence in TNI Ship Information Systems as a Manifestation of a Resilient Maritime Defense Industry", *IJHESS*, vol. 3, no. 3, Dec. 2023.

[71] P. Nunes, A. Correia, and M. F. Teodoro, "Information gathering, management and transferring for geospatial intelligence - A conceptual approach to create a spatial data infrastructure," in *AIP Conference Proceedings*, American Institute of Physics Inc., Jun. 2017.

[72] U. S. Gaire, "Application of Artificial Intelligence in the Military: An Overview," *Unity Journal*, vol. 4, no. 01, pp. 161–174, Feb. 2023.

[73] M. A. Khan, "Understanding the Impact of Artificial Intelligence (AI) on Traditional Businesses in Indonesia," *Journal of Management Studies and Development*, vol. 3, no. 02, pp. 146–158, Jun. 2024.

[74] I. Susilowati, K. Nadirah, and L. A. Aanisah, "Artificial Intelligence (AI) as a Digital Strategy for National Defence in the Era of Global Politics," *'ADALAH Buletin Hukum & Keadilan*, vol. 8, no. 6, pp. 19–35, 2024.

[75] V. Chilukuri and R. Scanlon, "Countering the Digital Silk Road: Indonesia About the Technology and National Security Program," Mar. 2025.