**Jurnal Praksis dan Dedikasi (JPDS)**
Oktober, 2025, Vol. 8, No. 2 hal. 361-377
http://dx.doi.org/10.17977/um022v8i22025p361-377

# Strengthening Indonesia's defense capability through AI-driven decision-making

**Alradix Djansena*, Asep Adang Supriyadi, Yuli Kartiningsih, Faisal Yusman, Basuki Rahmad Saleh**

*Corresponding author, Email: djansena@gmail.com

Universitas Pertahanan Republik Indonesia, FVFJ+G4H, IPSC Sentul, Sukahati, Citeureup, Bogor Regency, West Java, 16810, Indonesia

Paper received: 25-05-2025; revised: 10-07-2025; accepted: 24-08-2025; published: 10-10-2025

How to cite (APA Style): Djansena, A., Supriyadi, A. A., Kartiningsih, Y., Yusman, F., & Saleh, B. R. (2025). Strengthening Indonesia's defense capability through AI-driven decision-making. *Jurnal Praksis dan Dedikasi Sosial (JPDS), 8*(2), 361-377. DOI: 10.17977/um022v8i22025p361-377

## Abstract

The emergence of Artificial Intelligence (AI) in the Fourth Industrial Revolution has redefined the dynamics of modern military systems, especially in areas such as strategic decision-making, threat anticipation, and cybersecurity. While global powers like the United States, China, and the European Union have institutionalized AI within their defense doctrines, Indonesia is still in the developmental phase. This is particularly concerning given the intensifying security landscape and digital threats requiring an agile and intelligent defense framework. This study applies a qualitative methodology by integrating document-based analysis with cross-country comparative evaluation. It investigates how AI has been embedded into the defense architectures of leading countries and assesses the relevance and adaptability of these strategies for Indonesia's national security needs. AI technologies benefit defense systems, such as real-time decision support, automated logistics, and enhanced situational awareness through machine learning algorithms. Nonetheless, several challenges remain, including ethical issues, algorithmic bias, cyber vulnerabilities, Indonesia's limited digital infrastructure, and AI-specialized human capital. The U.S. emphasizes explainable AI (XAI) and operational integrity, China focuses on rapid militarization of AI, while the EU promotes regulation, ethics, and collaborative defense. Indonesia must accelerate the transformation of its defense policies by cultivating a national AI ecosystem, reinforcing its cybersecurity architecture, ensuring transparent and ethical governance, and prioritizing capacity building for AI professionals. A synergistic collaboration among the government, academic institutions, and defense industries is crucial to align AI deployment with Indonesia's national security goals. This research introduces a conceptual framework for AI policy reform tailored to Indonesia's geopolitical and technological context, offering an integrated model for ethical, scalable, and strategic AI implementation in the defense sector.

**Keywords:** explainable AI (XAI); defense technology innovation; military AI implementation

## INTRODUCTION

The rapid evolution of the Fourth Industrial Revolution has positioned Artificial Intelligence (AI) as a foundational element in shaping national security frameworks across the globe. In defense, AI plays a pivotal role in managing vast datasets, conducting advanced analytical operations, and supporting algorithm-based decision-making processes. These capabilities significantly enhance military performance, cybersecurity, and the overall effectiveness of defense infrastructure (Sarker et al., 2020). In this context, examining how different nations integrate AI into their defense strategies provides valuable insights for understanding its potential application in Indonesia.

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

Leading nations such as the United States, China, and the European Union have integrated AI into their strategic defense policies. This integration serves not only as a response to escalating digital threats but also as an effort to strengthen their geopolitical stance through technological superiority (Roberts et al., 2021). According to Li and Liu (2021), AI has been widely adopted to counter non-traditional threats, such as cyber intrusions and information warfare, by enabling more responsive and adaptive defense ecosystems. Conversely, Indonesia is still in the early stages of AI implementation in its military policies, despite facing increasingly complex geopolitical tensions and cyber vulnerabilities. Kasongo and Sun (2020) emphasize that deploying AI in the defense context can optimize border surveillance, streamline intelligence processing, and enhance simulation-based warfare planning.

Integrating AI in national defense presents several technical, ethical, and strategic challenges. One of the core issues is how AI can improve the quality and agility of decision-making in defense policy. Military and defense decisions often involve multifaceted political, technological, and strategic considerations. By leveraging machine learning and deep learning techniques, AI has the potential to assist military leaders in forecasting risks, evaluating strategic scenarios, and delivering data-driven, timely decisions (Roberts et al., 2021). However, Bavolar et al. (2024) warned that the absence of human oversight in AI-based decision-making could lead to critical errors and systemic bias, potentially undermining national security.

Cybersecurity threats further complicate AI adoption in defense. AI systems are increasingly targeted in cyber warfare operations, with the potential to disrupt defense infrastructure and manipulate sensitive algorithms (Ahmad et al., 2021). Attacks on these systems could result in data breaches, system hijacking, and even the loss of control over autonomous weapons. Moreover, the issue of decision transparency becomes paramount. Taddeo et al. (2021) note that the ethical dilemma surrounding delegating military authority to AI, especially in autonomous systems, poses fundamental questions about compliance with international humanitarian law.

Different countries have adopted distinct approaches to navigating these challenges. The United States has prioritized transparency and explainability in AI by developing Explainable AI (XAI) tools and institutions such as the Joint Artificial Intelligence Center (JAIC). Meanwhile, China pursues AI militarization aggressively, aiming for dominance across strategic domains, including autonomous drone operations and cyber-intelligence (Li & Liu, 2021). The European Union, on the other hand, has emphasized strict ethical frameworks, human rights protections, and international cooperation in AI governance (Taddeo et al., 2021). Drawing from these comparative perspectives, Indonesia can identify key lessons to guide the development of its own ethical, secure, and future-oriented AI defense framework.

For Indonesia, these global approaches offer valuable insights. Developing a resilient AI-based defense strategy requires establishing a robust digital infrastructure supporting AI integration, particularly where technological access and expertise remain uneven (Xiong et al., 2020). To keep pace with modern defense needs, Indonesia must accelerate the transformation of its defense policies, balancing innovation with ethical and legal safeguards. The goal is not only to harness the power of AI for strategic advantage but also to ensure its application is transparent, secure, and aligned with democratic principles and national interests.

With support for research, innovation, and strengthening human resources in AI, Indonesia has an excellent opportunity to utilize artificial intelligence as an integral part of the national defense system in the future (Yamin et al., 2021). However, to ensure its success, the integration of AI into defense policies must be supported by clear regulations, transparency in decision-making, and robust cybersecurity systems to avoid creating new risks that could be exploited by irresponsible parties (Taddeo et al., 2021). To address these opportunities and challenges, this study seeks to explore several key questions related to the role and implementation of AI in Indonesia's national defense policy.

Based on the above background, this research focuses on three central questions that guide the study. The first explores how Artificial Intelligence (AI) can enhance decision-making effectiveness in national defense policy. The second examines the main challenges in implementing AI within defense systems, particularly concerning cybersecurity and decision-making transparency. The third investigates how developed countries have adopted AI in their defense policies and how these approaches can be adapted to suit Indonesia's strategic and institutional context.

## METHOD

This study employs a qualitative research design to explore how AI can be systematically integrated into Indonesia's national defense policy framework. The approach focuses on understanding AI's theoretical underpinnings and practical applications in defense systems, particularly in enhancing strategic decision-making processes and strengthening cybersecurity readiness (Jensen et al., 2020; Han & Dunning, 2024). To achieve these research objectives, a qualitative approach is applied to provide an in-depth understanding of AI integration within Indonesia's defense policy framework.

The primary method used is document analysis, which involves a critical review of academic publications, policy documents, government reports, and strategic white papers related to the use of AI in military and security contexts. This analysis provides insight into global trends and challenges in adopting AI for defense purposes (Calderaro & Blumfelde, 2022; Taddeo et al., 2021). To complement this method, a comparative analysis is employed to provide a broader understanding of how leading nations have implemented AI in their defense strategies and what lessons can be drawn for Indonesia's context.

A comparative analysis was also conducted to enrich the findings. This technique evaluates how advanced countries, specifically the United States, China, and the European Union, have adopted and implemented AI technologies within their defense architectures. The selection of these countries is based on their leadership in AI development and distinctive strategic orientations. The United States emphasizes technological transparency and accountability through explainable AI (XAI); China prioritizes the rapid militarization of AI technologies; and the European Union takes a normative approach that centers on ethics, regulation, and collective defense principles (Roberts et al., 2021; Wood, 2024; Shaukat et al., 2020). This approach bridges global insights with Indonesia's context, ensuring the proposed strategies are practical and aligned with national defense priorities.

This study identifies key patterns, best practices, and policy gaps relevant to Indonesia by examining the similarities and contrasts among these models. These findings form the foundation for proposing a reform strategy tailored to Indonesia's geopolitical conditions and technological capabilities. The ultimate objective is to formulate actionable policy recommendations that support AI's ethical, secure, and effective integration into the Indonesian national defense system (Sætra, 2020; Yaacoub et al., 2023). In doing so, this study aims to contribute to the development of a forward-looking defense framework that leverages AI responsibly to strengthen Indonesia's national security.

## RESULTS AND DISCUSSION

### The Concept of AI in Defense Policy

#### *Machine Learning, Deep Learning, and Military Strategy Automation*

In recent decades, AI has become an essential pillar in the modernization of defense systems. Machine learning and deep learning have been widely adopted to enable autonomous systems to analyze large-scale data, identify threat patterns, and make operational decisions with minimal human intervention (Zhang & Li, 2020). These AI capabilities are pivotal in enhancing

battlefield responsiveness, automating intelligence processing, and refining tactical strategies in complex operational environments (Truong et al., 2020). As AI continues to advance, its growing role in autonomous military systems brings not only strategic advantages but also complex ethical challenges.

The integration of AI in modern military structures has gone beyond basic data processing and is now central to developing autonomous weapon systems. However, this evolution raises pressing ethical concerns. Specifically, delegating lethal decision-making to algorithms without human supervision has sparked global debate about autonomous warfare's moral and legal boundaries (Hoijtink & Muehlenhoff, 2020). Various international institutions have proposed frameworks to ensure that AI systems in defense operations remain accountable and aligned with humanitarian principles.

Moreover, AI is a cornerstone of cybersecurity strategies within defense organizations. Advanced machine learning algorithms detect anomalies in network traffic, identify intrusion attempts, and automatically execute mitigation protocols before threats escalate (Jensen et al., 2020). For example, AI-driven models are increasingly applied to recognize Distributed Denial of Service (DDoS) attacks and dynamically adapt countermeasures in real time, protecting critical digital infrastructure from disruption (Aljuhani, 2021). In this regard, the role of AI extends beyond autonomous systems to encompass critical functions in cybersecurity and digital defense operations.

Overall, the application of AI, particularly in machine learning and deep learning, has fundamentally transformed military strategy formulation and threat response capabilities. Nonetheless, the ethical, legal, and technical complexities surrounding this transformation must be continuously addressed to ensure responsible and secure use of these technologies in defense contexts.

### *Decision Making OODA Loop, Neural Networks, and Data-Based System Model*

AI is vital in enhancing real-time decision-making capabilities in military operations, particularly through frameworks like the OODA Loop (Observe, Orient, Decide, and Act) developed by military strategist John Boyd. This framework is increasingly supported by AI technologies that accelerate each stage of the cycle. AI systems can assimilate data from multiple sensors, interpret complex patterns using neural networks, and suggest optimal courses of action tailored to evolving battlefield conditions (Truong et al., 2020; Jensen et al., 2020). Building on this concept, neural network–based systems further enhance the OODA framework by enabling faster threat detection and more adaptive military responses.

Neural networks are integral to AI-driven decision support systems. These systems are designed to detect potential threats, forecast attack scenarios, and propose adaptive responses automatically. Predictive modeling enables military units to anticipate threats more accurately and respond more swiftly than traditional intelligence methods would allow (Cihon et al., 2021). However, the reliability of AI decisions is strongly influenced by data quality. As Schultze and Loschelder (2021) highlighted, the precision of numerical data fed into decision-making systems significantly affects the validity and credibility of resulting recommendations.

Beyond technical functionality, integrating AI into military decision-making also involves psychological and behavioral dimensions. Research by Horn and Freund (2022) reveals that individuals may vary in their perception of risks and rewards based on contextual cues and age, which may influence how AI-generated recommendations are interpreted or followed. Similarly, Ikink et al. (2024) demonstrate that uncertainty in time-sensitive scenarios can impact the consistency of decisions made under pressure, highlighting the need for AI systems to be aligned with human cognitive and emotional processing.

Moreover, as Neumann et al. (2022) emphasize, AI prediction models must carefully balance decision accuracy with user autonomy. Overreliance on automated systems may reduce

human agency, leading to ethical dilemmas, especially in high-stakes environments like defense. Therefore, successful deployment of AI in military decision-making requires advanced technical design and a nuanced understanding of the human factors that influence strategic choices.

### *Ethics and AI Regulation in the Military Regarding Issues of Transparency, Accountability, and Algorithmic Bias*

Despite the operational benefits of Artificial Intelligence (AI) in defense systems, its use introduces various ethical and regulatory challenges that cannot be overlooked. One critical concern is the lack of transparency in AI decision-making. Many AI algorithms function as "black boxes," generating outputs through complex processes for human users to interpret or audit. This opacity creates barriers to accountability, particularly when AI systems are involved in actions that may lead to fatal consequences in military contexts (Sætra, 2020). These concerns highlight the urgent need for clear accountability frameworks to ensure that the use of AI in defense remains transparent, ethical, and aligned with international law.

Accountability becomes even more problematic when AI systems operate with partial or complete autonomy. For example, determining responsibility becomes ambiguous if an AI-driven system initiates a strike on the wrong target. This raises serious questions about the chain of command and legal liability within autonomous warfare environments (Jensen et al., 2020). The inability to trace and explain how an AI system reached its decision threatens to erode trust and reduce the perceived legitimacy of military operations.

Additionally, AI systems are susceptible to adversarial attacks, deliberate manipulations of input data that can deceive algorithms into making erroneous decisions. Such attacks are especially dangerous in the defense sector, where misinformation or system compromise can have catastrophic outcomes (Zhang & Li, 2019). These vulnerabilities can be exploited to misdirect automated defense responses, leading to operational failures or even conflict escalation (Karatas et al., 2020). Thus, strong human oversight and clear regulations are essential to ensure AI strengthens defense while upholding safety and ethics.

In light of these risks, it is essential to establish comprehensive regulatory frameworks that govern the use of AI in military applications. These frameworks must address explainability, data integrity, operational oversight, and ethical constraints. Ensuring that AI remains under meaningful human control is a core principle many international defense and ethics scholars advocate for. Continuous innovation, robust cyber defenses, and transparent governance mechanisms are necessary to ensure that AI contributes positively to national security without introducing unacceptable risks or undermining humanitarian norms.

## AI Implementation in National Defense System

### *Machine learning for Intrusion Detection and Automated Response*

AI, particularly machine learning, has become critical in strengthening cybersecurity within modern defense systems. Its ability to process large volumes of data in real time enables military organizations to identify anomalies, detect potential cyber intrusions, and automate high-efficiency response mechanisms (Johnson, 2023). As digital threats grow increasingly sophisticated, adopting AI has transformed national defense from reactive to predictive.

Cyber threats pose one of the most persistent and dangerous challenges to national security infrastructures. Sobb et al. (2020) emphasize that the proliferation of interconnected systems, particularly within the Supply Chain 4.0 ecosystem, has created new vulnerabilities that malicious actors can exploit. AI-powered security systems are now being deployed to continuously monitor network traffic, detect deviations from normal behavior, and activate mitigation protocols before an attack can escalate.

Machine learning algorithms are especially valuable in intrusion detection systems (IDS), where they are trained to recognize specific patterns associated with cyberattacks. These algorithms can automatically flag suspicious activity and initiate defensive measures without human intervention. Kong et al. (2021) argue that such capabilities are vital for reducing response times and containing threats in dynamic digital environments.

Moreover, many nations have begun integrating neural network-based detection models into their military communication infrastructures. These models can analyze threat signals in milliseconds, offering a strategic advantage in protecting critical data and ensuring the integrity of command-and-control operations (Knutsen, 2022). For example, the United States and the European Union have already deployed these systems to defend strategic assets and minimize the risk of cyber sabotage.

In addition to cybersecurity, AI plays an increasingly prominent role in drone navigation and unmanned military operations. Hodge et al. (2021) highlight that deep reinforcement learning has enabled drones to adaptively navigate hazardous terrain with greater autonomy and decision-making efficiency than traditional systems. These advancements underscore the importance of integrating AI into surveillance and defense networks and field-level tactical operations. Ultimately, the success of machine learning in defense depends not only on technical sophistication but also on the ability to align AI models with the evolving threat landscape and operational needs. A proactive cybersecurity posture powered by AI is indispensable for defending modern military systems against increasingly complex digital threats.

### *AI in Information Warfare Strategy*

Information warfare has emerged as a key dimension in modern conflict, where AI is increasingly utilized to combat disinformation, digital propaganda, and manipulate public perception. AI-powered systems have proven effective in monitoring online narratives, detecting anomalies in information dissemination, and identifying the coordinated spread of falsehoods to undermine political and social stability (Rieker, 2022). In this context, AI plays a crucial role in strengthening digital resilience by detecting and countering disinformation that threatens national stability.

AI can analyze complex data sets from social media and digital platforms through machine learning and deep learning techniques to trace how disinformation spreads and where it originates. Al Garadi et al. (2021) emphasize that this capability allows for early detection of coordinated information attacks, which can be used to manipulate public opinion or destabilize government credibility. These systems can classify content, recognize bot-generated communication, and evaluate the credibility of information sources in real time.

AI systems used in information warfare are designed to detect fake news and assess the intent and reach of such campaigns. By comparing linguistic patterns, propagation speed, and the interconnectedness of suspicious sources, AI can uncover disinformation networks and identify hostile actors, both state and non-state, that leverage information as a weapon (Li & Liu, 2021). Furthermore, the application of AI in this domain raises essential legal and ethical concerns. The use of AI to counter digital propaganda must be balanced with respect for freedom of expression and privacy rights. Therefore, developing AI strategies for information warfare should be accompanied by strict legal frameworks and transparent oversight mechanisms to prevent misuse.

In summary, AI is critical in strengthening a nation's cognitive security by identifying and neutralizing digital threats in the information domain. As adversaries become more adept at exploiting the digital environment, integrating AI into information warfare strategies becomes essential for maintaining political stability, safeguarding public discourse, and protecting national interests.

### *AI in the Optimization of Military Logistics and Resources*

AI is increasingly recognized as a transformative force in optimizing military logistics and resource management. By leveraging advanced data analytics, AI can forecast operational requirements, streamline supply chains, and enhance the maintenance of military assets with higher efficiency and precision (Johnson, 2023). This optimization ensures readiness in high-stakes environments where time-sensitive decisions are vital. AI systems can analyze historical data and real-time battlefield information to predict logistical demands such as fuel, ammunition, and equipment needs. These predictive models help reduce wastage and ensure timely resource availability. For example, algorithms can detect patterns indicating potential equipment failure, allowing preventive maintenance actions to be taken before malfunctions occur, thereby minimizing operational downtime and improving mission continuity (Cihon et al., 2021).

Beyond resource management, AI also plays a significant role in operational simulations and tactical planning. Reinforcement learning algorithms are increasingly used to simulate complex battle scenarios and generate optimal strategy recommendations. These simulations assist commanders in evaluating multiple tactical options and provide adaptive responses based on changing threat variables (Atanassova-Cornelis & Sato, 2022). Incorporating AI into logistics also enhances military organizations' ability to adapt under dynamic and uncertain conditions. AI-assisted decision-making allows for real-time resource reallocation, automated supply routing, and intelligent inventory control, thereby increasing resilience and reducing human error in logistics coordination. Taken together, AI enables defense organizations to move from reactive logistics to proactive and predictive systems. The integration of AI into logistics not only improves operational efficiency and resource utilization and supports strategic military goals by ensuring sustained supply lines, agile maneuverability, and battlefield readiness.

## Case Study on AI Implementation in Global Defense

In recent years, AI has become one of the main technologies in modernizing national defense systems. Several major countries, such as the United States, China, and the European Union, have adopted AI in their defense, ranging from innovative missile systems to cyber defense strategies.

### *The Use of AI in Missile Defense Systems and Cybersecurity in the United States*

The United States has established itself as a global leader in adopting AI for defense innovation, particularly in missile defense systems and cybersecurity. With significant budget allocations channeled through the Department of Defense, the U.S. continues to prioritize the integration of AI to enhance the performance and reliability of its strategic military infrastructure (Johnson, 2023). One of the most prominent applications of AI is in ballistic missile interception systems. For instance, the Ground-Based Midcourse Defense (GMD) system utilizes machine learning and big data analytics to detect, track, and neutralize incoming intercontinental ballistic missiles (ICBMs). AI enhances these systems by processing data in real time and adjusting interception parameters with high accuracy (Taddeo et al., 2021).

The United States has also developed Explainable Artificial Intelligence (XAI) systems to ensure the transparency and accountability of AI decision-making in defense. These systems are designed to produce decision outputs that can be interpreted by human operators, maintaining human oversight and reducing the risk of opaque or erroneous decisions (Wood, 2024). This aligns with the broader U.S. strategy to integrate AI as a decision-support tool rather than a fully autonomous agent.

In cybersecurity, AI plays a vital role in threat detection and mitigation. Through deep learning and generative adversarial networks (GANs), the U.S. military employs AI systems capable of identifying attack patterns, predicting cyber threats, and initiating defensive measures before breaches occur (Kandhro et al., 2023). These tools have become essential in protecting critical infrastructure, including military communication systems and command networks.

Despite these advancements, integrating AI in U.S. defense systems is challenging. One major concern is the risk of adversarial attacks that can manipulate AI models into making false predictions. Ren et al. (2020) emphasize the growing need for robust AI defenses that can withstand data poisoning and model exploitation tactics often used in cyber warfare. To address these risks, the Pentagon actively invests in developing resilient AI systems and has implemented regulatory measures to govern their use. These efforts reflect a dual commitment to innovation and accountability, reinforcing the United States' position at the forefront of AI-driven military transformation.

### *AI Strategies in the Militarization and Strengthening of Defense Infrastructure in China*

China has aggressively positioned Artificial Intelligence (AI) as a strategic asset within its broader agenda for military modernization. As part of its national initiative, the Next Generation Artificial Intelligence Development Plan and consistent with the industrial vision outlined in Made in China 2025 China has made large-scale investments in AI research and development, with a clear emphasis on its application in defense systems (Roberts et al., 2021; Fajar & Ismail, 2020).

One of the most prominent manifestations of this strategy is the deployment of autonomous military drones capable of executing reconnaissance and strike missions with minimal human intervention. These systems rely on deep learning algorithms to identify targets, assess environmental variables, and adjust combat behavior in real time, offering a significant advantage in high-speed tactical scenarios (Roberts et al., 2020).

In addition to combat capabilities, AI is critical in China's defense infrastructure, particularly in surveillance and information control. The Chinese government has developed sophisticated AI-enabled monitoring systems that allow for real-time analysis of digital communications, social behavior, and cyber anomalies. These tools serve a dual purpose: enhancing national security and consolidating internal control over sensitive information (Roberts et al., 2020).

China has also demonstrated significant progress in AI-based cybersecurity, including using adversarial machine learning models to anticipate, adapt to, and neutralize evolving cyber threats. These systems are integrated into national digital defense platforms, enabling proactive responses to complex intrusion attempts (Yamin et al., 2021). However, the rapid militarization of AI in China has drawn international concern, particularly regarding the ethical dimensions and lack of regulatory transparency. While technological advancement is undeniable, China has yet to establish widely accepted ethical standards governing AI in military applications. This raises questions about the unchecked use of autonomous systems, the potential for human rights violations, and the risk of escalation in conflict zones where AI operates without human intervention.

In summary, China's AI strategy reflects an ambition to achieve global dominance in defense technology. By integrating AI across military, cyber, and surveillance domains, China continues to blur the boundaries between technological innovation and state power projection, often at the expense of ethical oversight and regulatory safeguards.

### *AI Approach to Collective Defense and Digital Security in the European Union*

Unlike the United States and China, which prioritize AI's operational and militaristic applications, the European Union (EU) adopts a more normative and regulatory approach. The EU's defense AI strategy is grounded in ethical governance, transparency, and the preservation

of international law, particularly about human rights and humanitarian standards (Taddeo et al., 2021). Integrating AI into cyber defense systems through strict oversight and legal frameworks is central to the EU's approach. The EU has invested in developing AI-based threat detection systems that utilize machine learning algorithms to monitor, assess, and respond to cyber threats in real time. These systems are particularly effective in securing military communication networks and safeguarding sensitive digital infrastructure across member states (Yaacoub et al., 2023).

In support of transparency, the European Union also emphasizes using Explainable Artificial Intelligence (XAI) in defense settings. XAI systems are engineered to provide clear, interpretable reasoning for AI-generated decisions, ensuring that automated defense responses remain accountable and understandable to human operators (Wood, 2024). This is especially important in autonomous systems scenarios where decision clarity is essential to preventing misuse or unintended escalation. Beyond its internal defense infrastructure, the EU actively promotes global collaboration on AI governance in the security sector. Through diplomatic and regulatory initiatives, the EU seeks to establish international norms that regulate the development and deployment of AI for military purposes. This includes advocating for multilateral agreements on the ethical use of autonomous weapons and preventing AI-driven escalation in armed conflicts (Shaukat et al., 2020).

The EU's strategy reflects its broader identity as a security community grounded in collective responsibility and shared values. Rather than prioritizing dominance through militarization, the EU aims to position itself as a global leader in responsible AI use, where innovation is aligned with legal compliance, ethical imperatives, and multilateral cooperation. In essence, the European Union's AI approach in defense represents a balancing act between technological advancement and normative constraint. Its focus on regulation, ethical deployment, and international engagement contrasts with other global powers' aggressive AI strategies. It offers a model of governance-oriented innovation in the realm of military technology.

## Challenges and Obstacles in the Implementation of AI in Defense

The biggest challenge AI faces in the defense sector is the cybersecurity of AI systems. AI used in defense systems can become targets for exploitation by malicious actors, either in the form of attacks on the AI model itself or using AI for their nefarious purposes (Taddeo et al., 2021). Here are the challenges and obstacles in the implementation of AI:

### *The Use of AI-Powered Malware*

The implementation of AI in defense systems is increasingly challenged by the emergence of AI-powered malware, an advanced form of malicious software capable of adapting and evading detection. Unlike conventional cyber threats, AI-enhanced malware can analyze its environment, mimic legitimate user behavior, and evolve its attack patterns to bypass security protocols, particularly in highly sensitive military networks (Yamin et al., 2021). This class of malware utilizes machine learning techniques to blend into regular data traffic, making detection by traditional rule-based intrusion detection systems far more difficult. As highlighted by Truong et al. (2020), these attacks often exploit system vulnerabilities through behavioral deception, allowing them to propagate stealthily across interconnected defense platforms without triggering alarms. Such adaptive threats reflect a fundamental shift in cyber warfare, where offense becomes increasingly intelligent, autonomous, and resilient.

In addition to stealth and adaptability, AI-powered malware can employ deepfake technology to execute sophisticated social engineering attacks. By simulating military leaders' voice, appearance, or communication style, attackers can inject misinformation or manipulate internal communications to destabilize command structures. Wood (2024) notes that these tactics are especially dangerous when used to impersonate trusted personnel, leading to potential breaches of secure systems or even unauthorized activation of defense mechanisms.

Another development that is concerning is the use of model extraction and data poisoning techniques. Through model extraction, adversaries can replicate AI models deployed in defense settings and analyze their weaknesses. Chaalan et al. (2024) emphasize that this can lead to the development of targeted counter-AI strategies that degrade or mislead the system. Meanwhile, poisoning attacks involve subtly manipulating the training data of AI systems to cause them to learn incorrect patterns, potentially rendering their threat detection or decision-making capabilities unreliable. These emerging threats underscore AI's dual-use nature: while strengthening defense capabilities, it simultaneously equips adversaries with tools for sophisticated digital sabotage. The proliferation of AI-driven attacks demands a comprehensive security strategy that includes developing adversarially robust AI models, real-time threat intelligence, and enhanced cybersecurity collaboration between the government and defense sectors.

In short, as AI becomes embedded in the fabric of national defense, safeguarding it from exploitation is no longer optional it is imperative. Failing to anticipate and counter AI-powered malware could compromise strategic assets, disable critical infrastructure, and undermine national security from within.

### *The Regulatory and Ethical Constraints in AI-Based Decision Making*

Deploying AI in military decision-making processes raises profound regulatory and ethical dilemmas. As AI development accelerates, existing legal frameworks often lag, leaving significant oversight, accountability, and risk mitigation gaps. One primary concern lies in the absence of standardized international norms that define the permissible boundaries of AI use in military operations, especially regarding autonomous weapon systems (Calderaro & Blumfelde, 2022). The ethical complexity intensifies when AI is granted decision-making authority in life-or-death scenarios. Without clear regulations, there is a risk that these systems could operate beyond moral or legal boundaries, particularly when accountability mechanisms are unclear or absent. The ambiguity surrounding who is responsible when an AI system makes a critical error, such as misidentifying a target or triggering an unintended escalation, remains a persistent challenge (Jensen et al., 2020).

In technologically advanced militaries, AI is increasingly integrated into Internet of Things (IoT)-based platforms, creating additional vulnerabilities. Butun et al. (2019) emphasize that while these systems can improve efficiency and situational awareness, they are also susceptible to cyberattacks, data breaches, and unauthorized manipulation. The convergence of AI with IoT technologies necessitates a regulatory framework that governs AI behavior and secures the broader digital ecosystem in which it operates. Moreover, the weaponization of AI by both state and non-state actors has transformed the nature of geopolitical competition. In the United Kingdom, for instance, AI is central to strategic doctrines such as “Global Britain in the Grey Zone,” which outlines the role of AI in hybrid conflict environments that blur the line between peace and war (Strachan, 2021; Rauta & Monaghan, 2021). These developments reveal a trend where AI is not only a tool for national defense but also an instrument of influence in ambiguous, non-traditional warfare settings.

Given these realities, nations must adopt comprehensive AI governance models that ensure transparency, legal accountability, and compliance with international humanitarian law. This includes the need for human-in-the-loop or human-on-the-loop mechanisms to maintain ethical oversight, particularly in autonomous systems. Failure to regulate AI adequately could result in uncontrolled escalation, violation of human rights, or misuse of lethal technologies. Thus, as defense establishments worldwide continue to adopt AI, a simultaneous effort must be made to establish enforceable ethical and legal boundaries that safeguard humanity from the unintended consequences of algorithmic warfare.

### *Limitations of Infrastructure and Human Resources in AI Implementation in Developing Countries*

One of the most pressing obstacles facing developing countries in adopting AI for defense is the lack of robust digital infrastructure and a shortage of skilled human resources. In contrast to technologically advanced nations that have invested heavily in AI ecosystems, countries like Indonesia are still in the early stages of developing the necessary support systems for AI research, deployment, and maintenance (John Deva Prasanna et al., 2024).

Integrating AI into military systems demands high-performance computing infrastructure, secure data centers, and access to large, high-quality datasets. Without these fundamental components, the effectiveness of AI algorithms in real-world defense applications is significantly diminished. Moreover, developing AI systems for strategic environments requires a collaborative research ecosystem involving defense institutions, academia, and industry, an ecosystem that remains underdeveloped in many emerging economies (Sætra, 2020).

Another significant limitation lies in the lack of qualified personnel. Operating, training, and maintaining AI systems in defense contexts requires data science, machine learning, cybersecurity, and systems engineering expertise. Unfortunately, the talent pool in these domains remains shallow in many developing nations. Investment in education, scholarships, and specialized military training programs is, therefore, crucial to ensure the sustainable integration of AI into national defense policies (Han & Dunning, 2024).

Comparative studies also highlight stark differences in funding allocations. While countries like the United States invest billions annually in AI defense research, and the European Union provides structured support through the European Defence Fund (EDF), Indonesia's investment in defense-related AI research remains limited. Without substantial public and private sector investment, the AI gap between Indonesia and more developed defense powers may widen (Calderaro & Blumfelde, 2022). To address these challenges, Indonesia must prioritize the development of its digital infrastructure, expand support for AI-focused education, and encourage cross-sector collaboration. Strategic partnerships with foreign defense industries, technology firms, and research institutions can accelerate knowledge transfer and support domestic capacity-building.

In conclusion, while AI holds transformative potential for defense modernization, its success in developing countries hinges on overcoming foundational constraints. Only through long-term investment, policy commitment, and human capital development can nations like Indonesia harness AI's benefits for national security in a rapidly evolving global environment.

## *AI-Based Defense Policy Reformulation Strategy for Indonesia*

The development of AI in national defense systems requires a comprehensive approach based on a strong ecosystem. According to Rosa et al. (2020), a country's military policy is not only determined by national power alone but also by internal stability, the state's capacity to extract resources, and the level of elite consensus. In developed countries, national security policies are beginning to integrate energy transition strategies to enhance defense resilience (Kivimaa & Sivonen, 2021). Therefore, building a solid AI ecosystem becomes the first step in reformulating national defense policy, among other things, as follows:

## *Improvement of Research and Development Capacity*

Enhancing the capacity for research and development (R&D) is a foundational step in building an AI ecosystem for national defense. For Indonesia, establishing a robust R&D infrastructure is essential to reducing dependence on foreign technologies and developing indigenous AI solutions tailored to the country's strategic environment. Lessons from countries like the United States and China demonstrate that breakthroughs in military AI are often driven by well-funded, collaborative ecosystems that involve universities, research centers, defense industries, and government agencies (Han & Dunning, 2024).

Indonesia can emulate this approach by fostering stronger ties between its academic institutions, government research bodies, and the domestic defense industry. Saxi (2022) argues that such cross-sectoral cooperation is a proven model for generating military innovations that are not only technologically advanced but also operationally relevant. An integrated R&D strategy would allow Indonesia to develop AI applications suited for national security challenges, including surveillance systems, autonomous platforms, and decision-support tools for military planning.

Furthermore, the growing prevalence of data poisoning attacks and model extraction threats, where malicious actors attempt to corrupt or replicate AI systems, emphasizes the urgency of advancing secure AI development. Chaalan et al. (2024) highlight that without robust R&D capacity, countries risk deploying vulnerable systems that adversaries can exploit in high-stakes scenarios. Therefore, investments must focus not only on innovation but also on cybersecurity resilience. Indonesia should introduce fiscal incentives to attract private investment into AI defense research to accelerate progress. Tax benefits, research grants, and public-private co-funding schemes can help catalyze innovation and reduce financial barriers for startups and tech firms in the defense sector. Establishing a national AI research institute with a defense technology focus could serve as a central hub for coordinating innovation efforts and supporting the creation of next-generation military systems.

According to Mallapaty (2025), sustainable research funding and bold strategic planning are critical in supporting AI innovation in defense. Schneider (2024) adds that large language models (LLMs) and explainable AI (XAI) have demonstrated high potential in enhancing decision-making capabilities in military command structures. These insights highlight Indonesia's need to invest in defense-specific R&D infrastructures that integrate predictive models and operational AI tools.

As Ali and Choi (2020) note, AI development must be accompanied by frameworks that address deployed systems' security, scalability, and adaptability. Hence, Indonesia's R&D agenda must go beyond basic experimentation to include rigorous testing, validation, and ethical assessments, ensuring that the resulting AI technologies can be safely and effectively integrated into defense operations.

In summary, strengthening R&D capacity is not merely a technical imperative but a strategic necessity. Indonesia can lay the groundwork for self-reliant and secure AI integration in its national defense apparatus through focused investment, institutional collaboration, and innovation-driven policy.

### *Integration of AI in the National Cybersecurity System*

The growing complexity of cyber threats has elevated cybersecurity to a central priority in national defense, and Artificial Intelligence (AI) has become a vital tool in this domain. Integrating AI into Indonesia's cybersecurity infrastructure is a strategic step to strengthen national resilience against conventional and asymmetric digital attacks. Yamin et al. (2021) underscore that AI's capabilities in detecting, predicting, and neutralizing cyber threats provide a decisive advantage in maintaining digital sovereignty.

AI-powered cybersecurity systems rely on machine learning and deep learning models to monitor network behavior, identify anomalies, and automate responses to potential threats. These systems can detect irregular patterns in traffic or activity that may indicate an intrusion, even before a full-scale attack occurs. Han and Dunning (2024) argue that such predictive capabilities are crucial in modern defense environments where cyberattacks originate from multiple sources and escalate rapidly.

AI has increasingly enabled rapid anomaly detection and proactive defense responses against evolving cyber threats (Schmitt, 2024). Springer (2024) cautions that the weaponization of AI, particularly in the form of adversarial malware, presents novel challenges, requiring Indonesia to adopt adaptive and resilient AI-enabled cybersecurity systems.

Building a national AI-driven cybersecurity framework in Indonesia should begin with fortifying the military's digital infrastructure. This includes developing intelligent intrusion detection systems (IDS), automated firewall management, and threat intelligence platforms that can operate in real time. Madsen et al. (2023) emphasize that defense cybersecurity protects sensitive data and ensures operational continuity in military communications and telehealth logistics during missions. Furthermore, an integrated cybersecurity strategy must involve coordination across military and civilian agencies. As Rieker (2022) points out, siloed approaches to digital defense limit situational awareness and hinder rapid response. Therefore, interoperability between TNI, cyber intelligence units, and national ICT regulators is essential to creating a unified and adaptive cyber defense structure.

Adopting AI in cybersecurity requires strengthening technical personnel and institutional capacity. Training programs for military cyber units, certification of ethical hackers, and partnerships with universities specializing in computer science and information security can accelerate the development of a skilled cybersecurity workforce. In parallel, policy frameworks must be established to regulate AI use, data governance, and incident response protocols, ensuring that AI-driven cybersecurity adheres to ethical and legal standards. In conclusion, integrating AI into national cybersecurity systems offers Indonesia a proactive and dynamic defense posture. Through intelligent automation, predictive analytics, and cross-sectoral coordination, AI can help secure the country's digital landscape and support the operational effectiveness of its broader defense strategy.

### *Strengthening AI Regulation and Governance in Defense Policy*

The need for robust regulatory and governance frameworks grows increasingly urgent as AI becomes more deeply embedded in defense systems. Regulation is a safeguard against misuse and a foundation for ethical and transparent integration of AI into national security structures. Sætra (2020) stresses that AI applications in military settings without clearly defined legal boundaries risk operating outside acceptable norms, potentially causing unintended harm or policy overreach.

Indonesia’s national defense framework must therefore evolve to include a legal architecture that governs the deployment and oversight of AI technologies. These regulations should address key issues such as decision accountability, transparency in algorithmic processes, risk assessment procedures, and limits on the autonomy of AI-powered weapons systems. Han and Dunning (2024) highlighted that such legal clarity ensures that AI does not bypass democratic oversight, especially in force or surveillance operations.

Beyond legislation, governance mechanisms are essential to monitor AI development and deployment. This includes establishing dedicated oversight bodies or interagency task forces responsible for evaluating the ethical, technical, and strategic implications of AI use in defense. Rebholz et al. (2024) emphasize that an effective governance structure must incorporate multiple perspectives, ranging from military command to data ethics experts, to ensure well-rounded policy formulation and enforcement.

Drawing from international practices, several developed countries have already instituted AI governance models that integrate privacy protections, data integrity standards, and ethical use principles in military applications. Kusev et al. (2022) point out that these frameworks often require AI systems to be explainable, auditable, and subject to human control—features that enhance both operational accountability and public trust. Indonesia should aim to adopt similar principles when crafting its national defense AI guidelines.

Evans (2024) and Maas (2024) underscore the urgent need for legal accountability in autonomous military operations, especially in lethal force scenarios. Islam and Wasi (2024) propose a human rights-based framework for AI policy to prevent humanitarian law violations in developing countries. Meanwhile, Cools and Maathuis (2024) emphasize the necessity of building

trust in autonomous weapon systems through technical transparency. Furthermore, Schneider (2024) and Jagers et al. (2025) call for international standards and certification schemes to regulate military AI technologies. Floridi (2024) and Trusilo & Danks (2024) highlight the normative trade-offs and moral responsibilities associated with dual-use AI systems, which apply in civilian and military contexts. These insights align with Indonesia's need to ensure that AI deployment is effective and ethically defensible.

Public perception is another vital dimension. Maas (2024) notes that societal trust in AI depends on inclusive policy discussions and public oversight. Indonesia must, therefore, embed democratic values and accountability into its AI defense governance. In the Indonesian context, this would also entail formulating standard operating procedures (SOPs) for AI deployment, implementing audit trails for high-risk algorithms, and introducing mandatory testing phases before field use. These mechanisms minimize operational errors and contribute to building a secure, responsible, and transparent AI ecosystem within the national defense apparatus.

In conclusion, AI regulation and governance are not ancillary to defense strategy because they are central to it. By establishing legal and ethical guardrails around AI implementation, Indonesia can ensure that technological advancement is aligned with its constitutional principles, international obligations, and the broader goal of upholding security with integrity.

### *Enhancing Human Resource Capacity in the Field of AI*

One of the most critical enablers of AI adoption in the defense sector is the availability of skilled human capital. While technological infrastructure and regulatory frameworks are essential, their effectiveness largely depends on the competence and preparedness of personnel who design, implement, and operate AI systems. In many developing countries, including Indonesia, a shortage of AI-literate professionals remains a significant barrier to the strategic integration of this technology (Ali & Choi, 2020).

To address this gap, Indonesia must invest heavily in AI-focused education and capacity-building initiatives tailored to defense needs. This includes expanding military academic curricula to incorporate subjects such as machine learning, data ethics, algorithmic decision-making, and cybersecurity. As highlighted by Yaacoub et al. (2023), the presence of cross-disciplinary knowledge, combining military tactics with data science and engineering, is vital for preparing personnel to manage and supervise intelligent systems effectively.

Beyond formal education, continuous professional training is equally important. Specialized training programs for defense engineers, intelligence analysts, and operational commanders should be institutionalized to ensure they remain up-to-date with the latest AI innovations and security protocols. Collaborations with domestic universities and international defense education institutions can further enrich these programs by bringing in global best practices and technical expertise (Han & Dunning, 2024).

The government should also establish incentive mechanisms to attract AI talent into defense-related roles. Competitive salaries, career advancement pathways, and research grants can encourage young professionals and academics to contribute to the national defense AI ecosystem. Moreover, creating AI research fellowships or exchange programs with allied nations may facilitate knowledge transfer and enhance global collaboration in defense technology development (Roberts et al., 2021). Another priority is fostering a culture of innovation and ethical responsibility within military institutions. Human resource strategies must emphasize technical competence, critical thinking, ethical judgment, and an understanding of the strategic implications of AI deployment in conflict environments. As Madsen et al. (2023) assert, human oversight remains irreplaceable in ensuring that AI serves its intended defensive purpose without compromising moral or legal standards.

Even the most advanced AI defense systems risk becoming ineffective or dangerous without a well-prepared and continuously trained human workforce. Enhancing human capital is

thus not a secondary concern but a strategic necessity that underpins the successful and ethical adoption of AI in Indonesia's national defense policy.

## CONCLUSION

The integration of Artificial Intelligence (AI) into Indonesia's defense sector represents both an urgent necessity and a transformative opportunity. Learning from the strategies of global powers such as the United States, China, and the European Union, Indonesia must pursue a balanced approach that aligns technological advancement with ethical responsibility. The nation's AI-driven defense transformation should be anchored on four interrelated pillars: strengthening domestic research and development to reduce technological dependency, embedding AI in cybersecurity systems to counter evolving digital threats, establishing robust ethical and regulatory frameworks to ensure accountability, and investing in human capital to build an AI-literate defense workforce. Together, these components form a comprehensive foundation for responsible innovation and operational resilience. Ultimately, Indonesia's embrace of AI in defense must transcend mere technological adoption—it requires institutional readiness, cross-sector collaboration, and long-term strategic vision. When implemented effectively, AI will not only reinforce Indonesia's defense capabilities and sovereignty but also position the nation as a forward-looking, resilient actor in the global security landscape.

## REFERENCES

Al Garadi, M. A., Mohamed, A., Al-Kabsi, A. M., et al. (2021). Fighting propaganda and fake news using AI: A survey. *Information Processing & Management, 58*(1), 102567. https://doi.org/-10.1016/j.ipm.2020.102567

Ali, H. M., & Choi, T. (2020). Artificial intelligence applications in the military: Current developments and outlook. *Journal of Defense Studies, 16*(2), 123–139.

Anneken, M., et al. (2025). Ethical considerations for the military use of artificial intelligence in visual reconnaissance. *Defense Technology Review, 15*(1), 33–47.

Atanassova-Cornelis, E., & Sato, Y. (2022). Emerging technologies and security policy: Strategic competition in the Indo-Pacific. *Asia-Pacific Review, 29*(2), 123–144.

Butun, I., Österberg, P., & Song, H. (2019). Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures. *IEEE Communications Surveys & Tutorials, 22*(1), 616–644.

Calderaro, A., & Blumfelde, L. (2022). Artificial intelligence governance and cybersecurity in the global South. *Global Policy, 13*(3), 389–400. https://doi.org/10.1111/1758-5899.13106

Chaalan, A., Shashika, G., & Ahmad, I. (2024). Robust adversarial training for deep neural networks in defense applications. *Defense Technology, 20*(1), 55–68.

Cihon, P., Maas, M. M., & Kemp, L. (2021). Should artificial intelligence governance be centralised? Design lessons from history. *Journal of AI Research and Policy, 12*(3), 85–102.

Cools, K., & Maathuis, C. (2024). Trust or bust: Ensuring trustworthiness in autonomous weapon systems. *Journal of Autonomous Systems, 9*(3), 150–165.

Evans, N. (2024). Command responsibility in military AI contexts: Balancing theory and practice. *AI & Society, 39*(2), 123–137.

Fajar, A. N., & Ismail, N. (2020). China's AI strategy: Military modernization through civil–military fusion. *Strategic Trends in Asia, 8*(1), 77–90.

Floridi, L. (2024). Normative tradeoffs for principle to practice guidance in military AI ethics. *AI & Society, 39*(4), 250–265.

Grand-Clément, S. (2023). *Artificial intelligence beyond weapons: Application and impact of AI in the military domain*. UNIDIR. https://unidir.org/publication/artificial-intelligence-beyond-weapons

Han, M., & Dunning, T. (2024). Artificial Intelligence and national security policy in Southeast Asia: Capabilities and constraints. *Asian Security Studies, 17*(1), 44–67.

Hoijtink, M., & Muehlenhoff, H. L. (2020). The militarisation of artificial intelligence: Governance challenges and policy implications. *Journal of International Relations and Development, 23*(4), 888–910.
Horn, S. S., & Freund, P. A. (2022). Age-related differences in risk perception and AI trust in military contexts. *Military Psychology, 34*(2), 115–130.
Ikink, E., Meijer, F., & Steenbeek, W. (2024). Stress and uncertainty in AI-based combat simulations. *AI & Society, 39*(1), 88–104.
Islam, M. R., & Wasi, A. T. (2024). Balancing power and ethics: A framework for addressing human rights concerns in military AI. *Journal of Military Ethics, 23*(4), 211–225.
Jagers, N., et al. (2025). In search of a global governance mechanism for Artificial Intelligence. *AI & Society, 40*(1), 1–15.
Jensen, C., Michaels, R., & Tang, L. (2020). Trust and accountability in artificial intelligence military applications. *Defence Studies, 20*(3), 264–285.
Johnson, M. (2023). Next-gen AI for defense: Cybersecurity and logistics revolution. *Journal of Strategic Technology, 8*(1), 11–26.
Kandhro, S., Qureshi, K., & Qadir, R. (2023). Artificial intelligence and generative adversarial networks in military cybersecurity. *Cyber Defense Review, 9*(2), 134–153.
Karatas, S., Kantarci, B., & Mouftah, H. T. (2020). A survey on artificial intelligence and adversarial machine learning in cybersecurity. *IEEE Access, 8*, 222984–223012.
Knutsen, K. (2022). AI and predictive logistics in NATO missions. *European Journal of Military Studies, 4*(2), 77–94.
Kong, Z., Zhang, R., & Yu, Y. (2021). Deep learning-based intrusion detection in military wireless sensor networks. *Security and Privacy, 4*(1), e104.
Kusev, P., Purser, H., & Ayton, P. (2022). Decision accountability in human–AI collaboration. *AI Ethics, 2*(3), 99–116.
Li, X., & Liu, Y. (2021). China's AI-powered defense modernization: Strategic implications and policy debates. *East Asian Security Review, 9*(1), 22–40.
Maas, J. (2024). Public perceptions of the use of artificial intelligence in defence. *AI & Society, 39*(3), 200–215.
Maas, J. (2024). The ethics of military AI: Responsibility, control and moral judgement. *Ethics and Information Technology, 26*(1), 89–102.
Madsen, T., Reiersen, E., & Tømte, C. (2023). *Digital defense readiness: Strengthening AI education in armed forces*. Norwegian Defense University Press.
Mallapaty, S. (2025). *'Boggles the mind': US defence department slashes research on emerging threats*. Nature. https://www.nature.com/articles/d41586-025-00671-9
Neumann, R., Jang, Y., & Keller, K. (2022). AI-enabled military decisions: Trust, bias, and human control. *Technology in Society, 68*, 101884.
Priyandita, G. (2024). *When regulating AI, ASEAN should remain committed to responsible behaviour*. Fulcrum. https://fulcrum.sg/when-regulating-ai-asean-should-remain-committed-to-responsible-behaviour/
Rebholz, S., Glauner, P., & Holzinger, A. (2024). Building trustworthy military AI: The need for auditability and governance. *Defense Policy Journal, 14*(1), 45–62.
Ren, J., Li, Z., & Zhou, X. (2020). Adversarial attacks and defenses in deep learning: A survey. *IEEE Access, 8*, 77742–77773.
Rieker, P. (2022). Cognitive security in the age of AI: Combating disinformation in the digital battlespace. *European Journal of Information Warfare, 3*(1), 56–73.
Roberts, H., Cowls, J., Morley, J., Taddeo, M., Wang, V., & Floridi, L. (2021). The Chinese approach to artificial intelligence: An analysis of policy and regulation. *Nature Machine Intelligence, 3*(5), 433–435.
Sætra, H. S. (2020). AI in defense: Normative dilemmas and the future of military ethics. *AI & Society, 35*(3), 595–607.
Saxi, H. L. (2022). Strategic defense R&D partnerships: Learning from US–NATO cooperation. *Security & Defence Quarterly, 40*(1), 33–52.
Schmitt, M. (2024). Integrating AI-based and conventional cybersecurity measures into defense systems. *Journal of Cybersecurity, 12*(3), 45–60.
Schmitt, M. (2024). Standardization and certification for military AI systems. *Journal of Defense Technology, 14*(2), 99–113.

Schneider, T. (2024). Enhancing trust in Large Language Models for streamlined decision-making in military operations. *Journal of Military Decision Systems, 8*(3), 120–135.
Schneider, T. (2024). Explainable AI in the military domain. *Ethics and Information Technology, 26*(2), 145–158.
Shaukat, K., Luo, S., Varadarajan, V., & Hameed, I. A. (2020). AI policies in defense and human rights. *Ethics and Information Technology, 22*(4), 291–304.
Springer, M. (2024). The weaponization of artificial intelligence in cybersecurity. *Cyber Defense Journal, 10*(1), 77–89.
Strachan, H. (2021). AI in hybrid conflict: The UK's evolving strategy in grey zone warfare. *RUSI Journal, 166*(5), 56–70.
Taddeo, M., Floridi, L., & Santoni de Sio, F. (2021). Ethical governance of AI in military applications. *Nature Communications, 12*, 5951. https://doi.org/10.1038/s41467-021-26244-w
Truong, N. B., Lee, G. M., Askoxylakis, I., Hoang, D. T., & Dang, H. L. (2020). Data protection and artificial intelligence in military operations. *Computer Law & Security Review, 37*, 105420.
Trusilo, D., & Danks, D. (2024). Commercial AI, conflict, and moral responsibility: Dual-use implications. *AI & Ethics, 12*(2), 98–112.
Wood, D. (2024). Explainable AI for national security: Ethics, design, and deployment. *Journal of Defense Ethics, 2*(1), 13–28.
Xiong, X., Song, Y., & Wang, Q. (2020). Digital infrastructure development in emerging economies: Challenges and opportunities for AI implementation. *Asian Development Policy Review, 12*(3), 151–168.
Yaacoub, J. P. A., Noura, H., Salman, O., & Chehab, A. (2023). Cybersecurity risk assessment and mitigation in AI systems: Trends and challenges. *Computers & Security, 115*, 102610.
Yamin, M. M., Katt, B., & Gkioulos, V. (2021). Cybersecurity challenges and solutions in smart defense systems. *Journal of Information Security and Applications, 58*, 102703.
Zhang, Y., & Li, Z. (2019). Artificial intelligence-enhanced malware attacks and defenses. *Journal of Network and Computer Applications, 125*, 1–16.