Journal of Social Work and Science Education
Volume 6 (1) 2025, 180-200
E-ISSN 2723-6919, P-ISSN 2746-0827

Reformulating National Defense Policy Through Artificial Intelligence: Enhancing Strategic Decision Making and Ethical Governance

Syarif Hidayatullah[1], Asep Adang Supriyadi[1], Ignatius Eko Djoko Purwanto[2], Guntur Eko Saputro[1]
[1]Universitas Pertahanan, West Java, Indonesia, [2]Research and Development Agency (Balitbang) of the Ministry of Defense of the Republic of Indonesia

Corresponding author e-mail: syarifnunky@gmail.com

Article History: Received on 7 February 2025, Revised on 13 April 2025, Published on 28 April 2025

Abstract: This study examines the role of artificial intelligence (AI) in reformulating national defense policy to enhance strategic decision making. Utilizing a qualitative, descriptive methodology supported by literature reviews and expert interviews, the research analyzes how AI can support data driven policy making, improve risk assessment, and optimize military resources. The research aims to examine how AI can improve operational efficiency, predictive analysis, and response capability against emerging threats. The study applies SWOT and Technology Readiness Level (TRL) frameworks to assess the strategic integration of AI in defense systems. Findings highlight both the opportunities and ethical concerns associated with AI adoption. The findings suggest that AI significantly supports data driven decision-making, enhances risk assessment, and optimizes military resource management. However, ethical and accountability concerns persist, necessitating the inclusion of explainable AI frameworks. The research proposes a structured model for ethical and inclusive AI governance and underscores the need for international cooperation in defense AI development.

Keywords: Artificial Intelligence, Defense Policy, Explainable AI, National Security, Strategic Decision Making

A. Introduction

The integration of advanced technologies in the defense sector is becoming increasingly significant in today's geopolitical landscape. The emergence of technologies such as artificial intelligence, machine learning, and the Internet of Things is transforming not only military operations but also the research and development processes within defense organizations. Artificial Intelligence (AI) is increasingly being recognized as a transformative capability in the global defense sector. The rapid advancement of AI technologies encompassing machine learning, neural networks, and big data analytics has profoundly altered how modern military organizations plan, operate, and respond to emerging threats. AI's ability to process

and analyze vast amounts of data in real time has significantly improved the effectiveness of surveillance systems, operational planning, and battlefield simulations. For instance, AI-driven platforms can autonomously evaluate complex threat scenarios and suggest optimal tactical responses, thereby enhancing situational awareness and decision-making precision (Kalogiannidis et al., 2024) ; (Shkalenko & Nazarenko, 2024). The geopolitical importance of AI is further illustrated by the strategic policies of leading military powers. The United States, for example, through its Department of Defense Joint Artificial Intelligence Center (JAIC), has implemented AI-based systems to support predictive maintenance, logistics, and cyber operations (Taddeo et al., 2021). Similarly, China's Civil Military Integration Strategy reflects its ambition to embed AI into both commercial and military ecosystems, aiming to leverage dual-use technologies for comprehensive national power (Wang et al., 2024). The United Kingdom and Australia have also launched national AI defense strategies, underlining the technology's relevance to future force structures and strategic doctrines (Zobi & Jarah, 2023). Beyond operational enhancements, AI's significance also lies in its potential to redefine command and control systems. AI is no longer merely a support tool; it functions as a co-analyst and, increasingly, a co decider in complex decision environments. This shift marks a strategic inflection point where technological superiority is directly linked to algorithmic capability, data infrastructure, and institutional readiness (Ho & O'Sullivan, 2019). As such, states that can effectively integrate AI into their defense frameworks are more likely to attain strategic advantage in a digitally contested global order.

Despite the growing adoption of artificial intelligence (AI) in military applications, the integration of AI into national defense policies remains fragmented and lacks a standardized ethical governance framework. Many national defense institutions still operate under hierarchical and bureaucratic policy models that are ill-suited to the rapid and adaptive nature of AI technologies. These rigid structures often fail to accommodate the complexities and unpredictability of contemporary threats, such as cyberwarfare, hybrid conflicts, and information operations (Weissmann, 2025). As a result, policy responses are frequently delayed, reactive, and misaligned with the capabilities offered by AI driven systems. Equally concerning is the ethical ambiguity surrounding AI use in defense. The reliance on opaque algorithms, often referred to as "black box" systems, raises significant accountability issues. When decisions are delegated to autonomous or semi-autonomous systems, the question of who bears responsibility for unintended consequences such as misidentification of targets or collateral damage remains unresolved (Vaassen, 2022); (Giubilini & Savulescu, 2017). This "responsibility gap" becomes even more critical in high stakes environments like military conflict zones, where decisions can result in loss of life or violations of international humanitarian law (Sio & Mecacci, 2021). Furthermore, algorithmic bias embedded in AI models can produce discriminatory or suboptimal decisions, especially if training data is incomplete, unrepresentative, or manipulated. Without transparency and explainability, stakeholders including policy makers, commanders, and the public may find it difficult to scrutinize or challenge the logic behind AI-

driven actions (Lepri et al., 2017). The lack of ethical oversight not only undermines democratic accountability but also erodes public trust in military institutions that deploy such technologies. To address these challenges, a comprehensive reform of defense policy is required one that prioritizes agility, ethical safeguards, and interdisciplinary collaboration. A key element of this reform is the integration of explainable AI (XAI) principles to ensure human oversight and institutional responsibility (Baum et al., 2022).

While the body of academic literature on artificial intelligence (AI) in military applications has grown significantly, most existing studies tend to focus on technical and operational aspects rather than policy oriented perspectives. A predominant share of AI research emphasizes algorithmic optimization, hardware software integration, and the development of autonomous weapon systems (Krügel et al., 2022);(Galliott & Wyatt, 2021). However, there remains a substantial gap in the scholarly exploration of how AI should be governed within strategic defense policymaking frameworks. In particular, issues related to ethics, legal accountability, and institutional readiness have not been thoroughly addressed within the defense policy literature. Moreover, research on AI deployment in defense often lacks integration with conceptual models of innovation governance and public policy. Few studies attempt to bridge the divide between technological readiness and strategic decision making mechanisms, such as those guided by national security doctrines or multilateral defense cooperation. As Ho and O'Sullivan note, the evolution of "smart systems" necessitates a parallel transformation in policy innovation and standardization, which current literature largely overlooks (Ho & O'Sullivan, 2019). This analytical void limits the practical utility of many technical studies when applied to real world defense governance contexts. There is also insufficient discussion around Technology Readiness Levels (TRL) and their strategic policy implications. Although TRL is widely used in defense research and development assessments, few publications apply it in tandem with strategic analysis tools like SWOT to evaluate policy viability (Chen et al., 2022). Similarly, the ethical governance of AI including the role of Explainable AI (XAI) and responsible innovation frameworks is often discussed in isolation from national security policy debates (Adobor & Yawson, 2022); (Baum et al., 2022). Addressing these gaps requires interdisciplinary research that merges technical sophistication with strategic policy insight, ensuring that AI integration into defense structures is both effective and ethically grounded.

This study aims to offer a comprehensive and policy-relevant framework for integrating artificial intelligence (AI) into national defense strategy. In response to the literature gaps identified, the primary objective is to evaluate how AI can be systematically embedded within defense policy making to improve strategic decision-making, enhance operational efficiency, and uphold ethical governance. Unlike prior research that isolates technical development from institutional application, this study bridges that divide by employing a dual framework approach combining SWOT analysis and Technology Readiness Level (TRL), assessment to simultaneously

examine strategic positioning and technological maturity (Chen et al., 2022) ; (Xu et al., 2024). The SWOT analysis enables a holistic examination of internal and external factors influencing AI adoption in defense, identifying strengths such as data driven responsiveness and weaknesses like algorithmic opacity (Lepri et al., 2017). Meanwhile, the TRL framework provides a structured evaluation of the developmental stages of AI technologies, ensuring that only mature, secure, and scalable systems are recommended for deployment (Chen et al., 2022). This dual-method approach is critical for aligning policy recommendations with both innovation potential and institutional capability. In addition to its analytical contribution, the study introduces an ethical lens grounded in the principles of Explainable AI (XAI), which emphasizes transparency and human oversight in automated decision making processes (Baum et al., 2022). By integrating XAI into defense policy discourse, the study addresses accountability challenges and reinforces institutional trust. The study's findings are intended to serve not only academic interests but also practical needs of policymakers, defense strategists, and AI developers. It offers a roadmap for creating inclusive, adaptive, and innovation-driven defense ecosystems through cross sector collaboration engaging government, academia, and the private sector (Whetsell et al., 2019); (Adobor & Yawson, 2022). Ultimately, this research contributes to the emerging field of AI governance in national security, ensuring that technological advancement supports rather than undermines strategic, ethical, and democratic principles.

This research also highlights the need to increase the capacity of defense institutions in terms of digital and technological literacy to optimally manage the risks and opportunities arising from AI integration (Alaja & Sorsa, 2020). Thus, this study not only contributes to the formulation of technology based defense policies but also strengthens the perspective on public policy and technology ethics in the face of the digital revolution. The findings of this study are expected to be a reference for policy makers, academics, and defense practitioners in designing a more responsive, intelligent, and globally competitive national strategy. The research question that is the focus of this study is, How can artificial intelligence be effectively integrated into national defense policies to improve strategic decision making while maintaining ethical accountability and operational security?

B. Methods

This study employed a qualitative descriptive approach supported by policy analysis and a systematic literature review. The selection of this method aligns with the conceptual and interdisciplinary nature of the research topic, the reformulation of national defense policy through the integration of artificial intelligence (AI). Given the complexity of technological and institutional dynamics, this design allows for a comprehensive exploration of ethical, strategic, and technological implications (Adobor & Yawson, 2022); (Taddeo et al., 2021).

The research was carried out in six main stages. First, key issues were identified based on global AI defense developments. Second, a conceptual framework was developed from academic and policy literature (Makridis et al., 2024). Third, data were collected from secondary sources, including peer reviewed journals, government defense strategy documents, and international publications on AI governance (O'Shaughnessy et al., 2022). In the fourth stage, data were categorized thematically across four domains: AI integration, ethics and accountability, policy governance, and the TRL and SWOT frameworks (Lepri et al., 2017). Fifth, the data were analyzed using thematic analysis and narrative synthesis to uncover policy patterns and governance gaps (Paglieri, 2024). Sixth, conclusions were drawn and recommendations formulated for adaptive and ethical AI-based defense policies (Guardia et al., 2020).

Key informants included Ministry of Defense officials, defense university scholars, and national defense industry experts, interviewed using semi-structured guides based on SWOT and TRL indicators (Giubilini & Savulescu, 2017). Field research was conducted in Jakarta and Bandung, selected for their relevance to national policy formulation and AI research and development (Mitrović, 2021). To ensure validity, the study employed source and theory triangulation, literature synthesis matrices, and policy document analyses (Naeem & Hauser, 2024); (List, 2021). The research adhered strictly to academic ethical standards throughout.

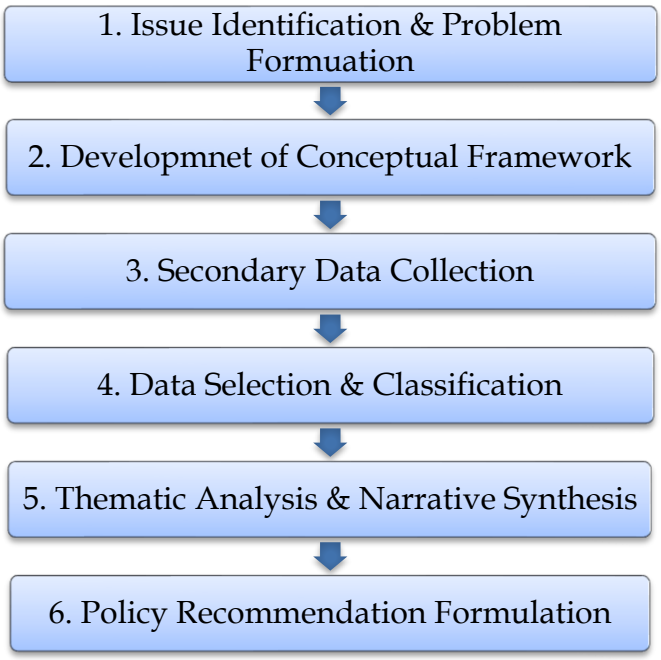

Figure 1. Research Method Flowchart

C. Results and Discussion

Data Driven Policy Development for Defense AI

The adoption of artificial intelligence (AI) in national defense requires a paradigm shift toward data driven policy development. Traditional defense policy making, often reliant on hierarchical decision making and static threat assessments, is increasingly inadequate in addressing the dynamic and multifaceted nature of contemporary security threats. AI systems, characterized by their capacity for real time data analysis, predictive modeling, and pattern recognition, offer transformative opportunities for enhancing the responsiveness and precision of defense policies (Nallakaruppan et al., 2024). Data driven policy development emphasizes the integration of empirical insights into strategic decision making processes. In the defense sector, this entails utilizing AI generated analytics to inform threat assessments, resource allocation, and operational planning. As Nallakaruppan et al., illustrate through the application of Explainable AI (XAI) models in regulatory frameworks, transparency and data interpretability are crucial for ensuring that AI driven insights can be translated into actionable and accountable policies (Nallakaruppan et al., 2024).

Moreover, systematic data analysis methodologies, as exemplified in banking supervision studies (Guerra & Castelli, 2021), can be adapted to the defense context to enhance oversight and reduce decision making errors. By adopting machine learningbased risk management techniques, defense institutions can move beyond reactive strategies toward proactive threat anticipation and mitigation (Paglieri, 2024). However, the integration of AI into defense policy frameworks must be carefully managed to prevent overreliance on algorithmic outputs. Human judgment remains indispensable, particularly in interpreting complex data environments where sociopolitical nuances cannot be fully captured by machine learning models. Therefore, the development of data driven defense policies must be accompanied by robust governance structures that balance automation with ethical oversight, ensuring that empirical data serves to augment rather than replace strategic human decisionmaking. In sum, data driven policymaking represents a foundational shift in defense strategy, positioning AI not merely as a technological tool but as an enabler of adaptive, anticipatory, and ethically sound national security frameworks.

Thematic Frameworks for AI-Based National Defense Policy.

The formulation of AI-based defense policy must begin with a comprehensive understanding of geopolitical dynamics. National security strategies are invariably shaped by the international system, where the distribution of power, regional alliances, and strategic rivalries dictate the scope and urgency of defense innovation. Mitrović, emphasizes that countries situated within competitive geopolitical environments, such as Southeast Asia or Eastern Europe, must align AI adoption with broader national interest frameworks that anticipate external threats and regional

instability (Mitrović, 2021). The increasing militarization of AI by great powers such as the United States, China, and Russia further underscores the need for smaller or developing states to recalibrate their defense posture through AI enhanced strategic alignment. Artificial intelligence enables states to simulate conflict scenarios, monitor adversarial movements, and enhance their strategic forecasting capacities. When integrated with geopolitical intelligence, AI acts as a multiplier of strategic advantage provided it is guided by clear political objectives and institutional alignment. Without such alignment, AI risks being treated as an isolated technological investment rather than as an embedded instrument of national defense doctrine.

AI driven defense policy must embed ethical governance principles at its core to ensure legitimacy, accountability, and compliance with international humanitarian law. The rapid deployment of autonomous systems in military contexts raises questions about moral responsibility, civilian harm, and decision opacity. As Taddeo et al. argue, AI must be governed by normative frameworks that protect human rights while enabling national security objectives (Taddeo et al., 2021). The inclusion of ethical constraints is not a limiting factor but a stabilizing force, ensuring that AI systems are implemented within boundaries that are politically acceptable and legally sound. Explainable AI (XAI) is a necessary condition for ethical oversight. Systems that lack interpretability cannot be audited or held accountable, and this compromises both transparency and trust in defense institutions (Baum et al., 2022). In this regard, ethical governance must go beyond code of conduct guidelines and evolve into institutional mechanisms that monitor and evaluate AI behavior in real time. Embedding these mechanisms into national policy ensures that AI remains a strategic asset rather than an ungoverned liability.

The successful integration of AI into national defense policy also requires a robust innovation ecosystem built on multisectoral collaboration. The National Innovation System (NIS) framework provides a useful lens through which governments, academic institutions, and private technology firms can cooperate to advance dual-use technologies (Alaja & Sorsa, 2020). AI innovations developed in the civilian domain often serve as foundational elements for military adaptation, especially in areas such as cyber defense, logistics automation, and command and control systems. Collaboration enhances not only the technical quality of defense systems but also their adaptability and long term sustainability. Naeem and Hauser stress that cross sector governance models are essential for translating AI research into real world applications, particularly in the face of evolving security threats (Naeem & Hauser, 2024). Moreover, inclusive stakeholder engagement encourages public trust, regulatory coherence, and shared responsibility three factors critical to sustaining an AI informed defense strategy.

Trends in modern defense policy strategy

Modern defense policy is characterized by an evolving strategy that responds to a range of challenges and opportunities, particularly in the wake of significantly changing global dynamics and technological advancements. This analysis looks at salient trends in contemporary defense policy strategies drawn from relevant literature highlighting key changes and emerging practices. Developed nations have recognized the potential of AI and are actively developing policies that leverage this technology for military applications. This integration not only improves operational efficiency and decision making but also reshapes strategic planning to include considerations of cyber warfare and autonomous systems.

Ethical Considerations and Policy Frameworks: With the adoption of advanced technologies such as AI and cyber security measures, defense policies increasingly need to embed ethical considerations into their frameworks. The need for ethical governance arises from concerns about accountability, transparency, and potential bias in AI-driven systems. Ho and O'Sullivan discuss how standard frameworks are emerging to address these challenges, suggesting that governments will play a critical role in ensuring the responsible adoption of innovative technologies in the defense context (Radičić & Pugh, 2016). This trend reflects a broader recognition that ethical guidelines are critical in balancing national interests with moral imperatives.

Innovation and Technology Adaptation. The concept of innovation systems has gained traction in developing effective national defense policies. Alaja and Sorsa highlight how the idea of programmatic policy has shifted toward fostering an environment conducive to innovation in military operations (Alaja & Sorsa, 2020). This system not only encourages collaboration between different sectors but also focuses on the dual-purpose nature of technology, where innovations can be used for both civilian and military applications. Transparency and Open Policy Analysis: Another emerging trend is the push for transparency in defense policy formulation. Advocates for evidence based policy making call for the incorporation of transparent processes that involve the participation of diverse stakeholders in defining and implementing defense strategies (Guardia et al., 2020). This approach ensures that defense policy is subject to scrutiny that encourages greater trust and collaboration among the public and relevant organizations.

Artificial Intelligence in Decision Making.

Artificial Intelligence (AI) is rapidly changing the landscape of strategic decision-making across domains, including national defense. The application of AI in this context encompasses a range of concepts and methodologies that enhance decision making processes, increase efficiency, and address ethical dilemmas. Predictive Analytics and Risk Assessment AI's capacity for predictive analytics is one of its most significant contributions to strategic decision making. Kalogiannidis et al. show how

AI technologies enhance predictive risk assessment, enabling organizations to more accurately anticipate potential operational risks (Kalogiannidis et al., 2024). By analyzing historical data and identifying patterns, AI systems can provide insights that inform proactive strategies, increasing resilience in dynamic environments. This concept is particularly relevant in the defense context, where timely and accurate predictions can lead to improved operational readiness.

Automated Decision Making The shift toward automated decision making presents both opportunities and challenges. The concept of an "Artificial Moral Advisor," as discussed by Giubilini and Savulescu, suggests that AI can assist leaders in making ethical decisions by evaluating complex moral dilemmas (Giubilini & Savulescu, 2017). However, this automated approach also poses risks, as reliance on AI for significant social decisions can lead to a "responsibility gap," where accountability becomes unclear (Taylor, 2024). This highlights the need for a clear framework governing the use of AI in critical decision-making processes, particularly in defense, where decisions often have profound implications.

Explainable Artificial Intelligence (XAI) The demand for explainability and transparency in AI applications has led to the emergence of Explainable Artificial Intelligence (XAI), which emphasizes the need for AI systems to provide understandable reasons for their outputs. Baum et al. argue that XAI is critical to maintaining trust and accountability in AI-assisted decision-making (Baum et al., 2022). In military applications, where decisions can have lifeor death consequences, ensuring that AI recommendations can be easily interpreted and justified is critical to fostering human oversight and ethical governance.

Collective Responsibility and Governance With the increasing delegation of decision-making to AI systems, critical questions arise regarding collective responsibility. The concept of group agency in AI decision-making suggests that moral accountability should not rest solely with individuals but can extend to AI systems and the organizations that implement them (List, 2021). This perspective requires a re-evaluation of existing governance structures to ensure that accountability mechanisms are robust enough to address the complexities introduced by the use of AI in a strategic context. Ethical and Moral Implications The ethical implications of the application of AI in decision-making are profound. Aleksandrova et al. highlight behavioral changes caused by AI applications that can result in significant economic and social impacts, including potential job losses due to automation (Aleksandrova et al., 2023). In defense scenarios, the ethical consequences of using AI in surveillance, targeting, and warfare raise pressing questions about human rights, accountability, and the ethical use of technology.

Interdisciplinary Approaches to AI Ethics A key concept in the literature is the need for interdisciplinary collaboration in formulating ethical frameworks for AI applications. O'Shaughnessy et al. emphasize the importance of integrating diverse

cultural values and inputs into AI governance to ensure inclusive and responsible deployment of the technology (O'Shaughnessy et al., 2022). This approach is relevant in the field of national defense, where international cooperation can lead to more comprehensive strategies that reflect shared ethical standards.

Relevant AI models for national defense applications.

Several models and concepts demonstrate how AI can be effectively implemented in defense applications. The following is a synthesis of relevant AI models and their implications for national defense, supported by literature references.

1. AI driven Decision Support Systems (DSS) play a critical role in national defense by enabling military planners and decision makers to analyze large amounts of data and make informed choices. These systems use AI algorithms to assimilate real-time data from multiple sources, enhancing situational awareness. Taddeo et al. emphasize the potential of AI to support decision-making frameworks in the defense context, highlighting the importance of developing advanced analytical capabilities to support military strategy (King et al., 2020).
2. Autonomous systems powered by machine learning algorithms are increasingly being integrated into defense capabilities, including surveillance drones and robotic systems. Krügel et al. discuss the implications of AI in creating autonomous decision making tools, emphasizing the importance of trust in these systems by military personnel (Krügel et al., 2022). This reflects a growing trend in the use of AI to improve military efficiency and reduce the risks associated with placing personnel in dangerous situations.
3. Explainable Artificial Intelligence (XAI) is critical in the defense sector, where the stakes of decision-making are high. XAI aims to make AI decision making processes understandable to human users. Owens et al. recognize the importance of using XAI to build trust between military personnel and machine based decision making tools, enhancing effective integration of AI into operations while ensuring accountability (Owens et al., 2022). This transparency is critical to maintaining ethical standards in military decisions that rely on AI recommendations.
4. Human AI Cognitive Cooperation The concept of human-AI cognitive cooperation involves developing collaboration between AI systems and human operators to improve decision-making outcomes. Vold's research highlights that effective cognitive cooperation can lead to better strategic decisions regarding military interventions (Vold, 2024). AI assists human operators by providing analytical capabilities that complement human intuition and judgment, ultimately improving the quality of decisions in critical defense scenarios.
5. Governance and Ethics Models As AI technologies develop in the defense context, the ethical and governance implications of these technologies become increasingly important. Szewczyk points to the need for a framework that ensures the ethical application of AI in military applications, with an eye toward accountability, transparency, and responsibility (Sio & Mecacci, 2021). This

balance of innovation with ethical considerations is critical to fostering public trust and maintaining compliance with international standards.

6. Cybersecurity and Risk Management AI models focused on cybersecurity and risk management are critical to protecting military assets from cyber threats. Rahman et al. propose the use of AI and blockchain technologies to enhance cybersecurity frameworks, improve incident response, and risk assessment capabilities (Rahman et al., 2024). This dual approach not only protects military assets but also ensures operational continuity against evolving cyber threats, making AI a key asset in contemporary defense strategies.

Implementation of AI in National Security.

United States Military AI Initiatives The United States has been at the forefront of integrating AI into defense. The Department of Defense (DoD) has initiated the Joint Artificial Intelligence Center (JAIC) to accelerate the delivery of AI capabilities to its military forces. According to Taddeo et al., the DoD strategy emphasizes the development of AI technologies for a variety of applications, including predictive maintenance, logistics, and operational planning (Taddeo et al., 2021). JAIC aims to streamline collaborative AI efforts across the military branches with a focus on the ethical use of AI and promoting transparency in the decision making process.

China has embraced AI as a core component of its military modernization. The National Civil Military Integration Strategy launched in 2015 is an example of the country's approach to facilitating the dual use of technologies developed for civilian purposes in the military. Research by Wang et al. suggests that this policy enhances military capabilities by integrating advanced technologies, including AI-driven surveillance and reconnaissance systems, although it does not significantly impact innovation outcomes (Wang et al., 2024). The strategy aims to encourage greater collaboration between civilian companies and military organizations, reflecting a comprehensive approach to national defense.

The UK's defence strategy includes a commitment to AI to enhance military capabilities and improve decision-making. The AI for Defence Strategy, launched alongside the UK's national AI strategy, highlights focus areas such as autonomous systems, predictive analytics for threat assessment and data sharing, although specific reference to the impact of the strategy would enhance this section. At present, there is insufficient evidence from the references provided to support the claims made about the UK's approach to AI (Taddeo et al., 2021).

Australia's Defence AI Strategy Australia's Defence AI Strategy emphasises the importance of AI in achieving national security objectives. The strategy outlines targeted investments in AI to enhance operational capability and improve workforce efficiency. While ethical governance and responsible use of AI technology are essential to ensuring public trust in defence applications, claims made about scientific support

for these ideas lack relevant references (Zobi & Jarah, 2023). Thus, further evidence on this ethical issue is needed.

Estonian Cybersecurity Innovation Estonia is a case study in leveraging AI for cybersecurity in the defense domain. The country has invested significantly in digital infrastructure and innovative cybersecurity policies. The Cyber Defense League uses AI to detect potential cyber threats and automate responses to cyber incidents. While the proactive approach to cybersecurity is commendable, claims about its protective capabilities and potential as an international model lack strong supporting evidence from the references provided (Jauernig et al., 2022). This requires further research and clear citation.

The application of AI to defense policy is a dynamic and evolving landscape characterized by innovation in military technology, strategic planning, and ethical governance. Case studies from the United States, China, the United Kingdom, Australia, Estonia, and international collaborations illustrate the transformative potential of AI to enhance national security. As countries continue to refine their strategies around AI and defense, a balanced approach that combines ethical considerations and intergovernmental cooperation will be critical to the success of AI integration.

The successes and failures of AI-driven defense strategies.

The primary success of an AI-driven defense strategy is increased operational efficiency and decision making capabilities. AI can process large amounts of data quickly, providing military leaders with actionable insights that can improve situational awareness on the battlefield. For example, automated data analysis can facilitate intelligence gathering missions by integrating multiple intelligence sources, including satellite imagery and open source intelligence (OSINT) (Kotaridis & Benekos, 2023). Such capabilities are particularly important in the Ukraine - Russia conflict, where integrated intelligence operations significantly increase responsiveness and adaptability to fast-moving developments (Kotaridis & Benekos, 2023). This illustrates the potential of AI to transform defense operations into a proactive rather than a reactive paradigm, as detailed in a study focused on the impact of AI on intelligence and strategic decision making processes (Kotaridis & Benekos, 2023); (Holmes & Wheeler, 2024).

Galliott and Wyatt highlight that current AI technologies, such as autonomous weapons systems (AWS), carry intrinsic risks, including incorrect command decisions based on overconfidence in algorithmic outputs. They note that AI systems can misinterpret data from critical domains such as computer vision and pattern recognition, which can lead to catastrophic operational failures if not adequately supervised (Galliott & Wyatt, 2021). Therefore, while AI can enhance operational capacity, it simultaneously creates vulnerabilities due to potential misjudgments

rooted in algorithmic limitations. AI integration must consider the ethical implications of automated decision-making that can override human judgment, potentially leading to unintended consequences in complex combat scenarios. Furthermore, the potential for AI systems to operate with bias requires the implementation of transparency and accountability mechanisms to mitigate disparities and enforce ethical standards in military operations (Lepri et al., 2017); (Dowding & Taylor, 2024). AI also poses challenges related to accountability for decisions made in defense settings. As automated systems become more autonomous, understanding who is responsible for failures or errors of judgment becomes more complicated. Sio and Mecacci discuss this "responsibility gap," where accountability may not lie entirely with the human operator or the AI system, raising concerns about trust in these technologies (Sio & Mecacci, 2021).

A large number of references use qualitative methodologies to explore the nuances of integrating AI into defense strategies. For example, Weissmann's study investigates the impact of technological advances, particularly AI and machine learning, on modern threats through qualitative analysis, assessing the strategic implications for intelligence and security services in the context of hybrid warfare (Weissmann, 2025). Similarly, Galliott and Wyatt discuss the design factors of autonomous weapon systems qualitatively, emphasizing human factors and uncertainty in the decision-making process associated with military leadership (Galliott & Wyatt, 2021). Additionally, Jauernig et al. address the reluctance toward algorithms in ethical decision making, applying qualitative methodology to determine public sentiment and concerns regarding algorithm mediated judgments in high stakes situations (Jauernig et al., 2022).

Data Collection. The following sources can be categorized based on their methodology, policy reports, expert interviews, and secondary analysis. Each type of data source provides different insights and rigor to the research landscape around this important topic. Policy reports provide valuable insights derived from comprehensive analyses conducted by governmental and non-governmental organizations. Such reports reflect the operational needs and strategic insights required for effective policymaking in the defense sector. In addition, Mustonen Ollila et al. apply a grounded theory approach to studying the components of defense strategy in the contemporary information society environment by emphasizing qualitative data collected through empirical research to understand the underlying dynamics (Makridis et al., 2024). This type of report enriches the existing policy framework by exploring the interrelationships among defense components, revealing important insights for strategic defense in a complex information space.

Leveraging expert interviews is an important technique for gathering experiential insights into AI applications in defense. For example, Bodnieks used semi-structured interviews to explore the legal basis of defense strategies related to hybrid warfare in Latvia. The study adopted both qualitative and quantitative approaches, using

document analysis along with content analysis derived from expert opinions to inform legal strategies in the military context (Lepri et al., 2017). Secondary analysis offers a methodology for synthesizing existing data and literature to derive new conclusions. For example, Ciarli et al. present a comprehensive review of quantitative forecasting techniques related to the future of technology, focusing on existing data while classifying these methods based on their description, utilization, and characteristics (Ruiter, 2021).

This methodology emphasizes the importance of using pre-existing data to address contemporary issues, facilitating informed decisions regarding risk management in military applications. When developing an analytical framework for assessing AI-driven defense strategies, a variety of models can be used, including SWOT analysis, Technology Readiness Level (TRL) assessments, and data driven policy analysis. Each framework offers unique insights and methodological approaches to evaluating the effectiveness, challenges, and readiness of AI technologies in defense applications. SWOT analysis is a strategic planning tool that can be used to analyze internal and external factors that influence the application of AI technologies in defense strategies. By categorizing strengths, weaknesses, opportunities, and threats, military planners can determine their strategic capabilities and potential barriers. For example, strengths may include the increased operational efficiency and superior data processing capabilities of AI systems. However, weaknesses may arise from algorithmic bias and ethical issues associated with autonomous decision-making (Alrabiah & Drew, 2020); (Nallakaruppan et al., 2024). Opportunities for AI applications may involve increasing situational awareness on the battlefield, while threats may come from enemy technological advances and the potential for misuse of AI (Xu et al., 2024).

The TRL framework provides a systematic approach to assessing the maturity of AI technologies for use in defense applications. Technologies are rated on a scale of 1 to 9, with lower levels indicating fundamental research and higher levels indicating proven systems ready for deployment. Chen et al. emphasize the importance of TRL in aviation safety by noting that technologies must undergo rigorous testing and validation before certification (Chen et al., 2022). By implementing TRL assessments, defense organizations can identify where AI technologies are in their development and prioritize investment and research efforts accordingly. This approach aligns resources with the specific growth stage of AI applications, ensuring a smoother transition from development to operational deployment. SWOT analysis of Artificial Intelligence (AI) integration in National Defense Policy Reformulation.

Table 1. SWOT Analysis

Factor	Description
Strength	1. Increase efficiency in strategic decision making Enable predictive analysis of threats
	2. Accelerate intelligence data processing
	3. Reduce dependence on human personnel in routine operations
Weakness	1. Dependence on sophisticated technological infrastructure
	2. Risk of bias in AI algorithms
	3. Challenges in transparency and accountability of AI-based decisions
	4. Potential cyber attacks that could exploit AI
Opportunity	1. Increased investment in defense AI research and development
	2. Potential for international cooperation in cybersecurity and defense AI
	3. Increased effectiveness of military operations through autonomous systems
	4. Utilization of AI in efficient management of defense resources
Threat	1. Global competition for military AI supremacy
	2. Risk of misuse of AI by state and non-state actors
	3. Potential failure of AI systems in critical situations
	4. Uneven regulations and policies at the global level

SWOT Analysis Data Calculation

To obtain a quantitative picture of the impact of AI on defense policy, using the SWOT weighting and rating approach.

Table 2. SWOT Analysis Data Calculation

Factor	Weight (%)	Rating (1-5)	Final Score
Strength (S)	35%	4.5	1,575
Weakness (W)	25%	3.0	0.75
Opportunity (O)	20%	4.0	0.8
Threat (T)	20%	3.5	0.7
Total	**100%**		**3.825**

Data Interpretation:
A score of 3.825 indicates that the integration of AI in defense policy has strong strategic potential. AI's strengths in efficiency and data analysis have the largest weighting (35%), indicating its significant impact. Threats and weaknesses have significant impact but can be addressed through regulation and supervision.

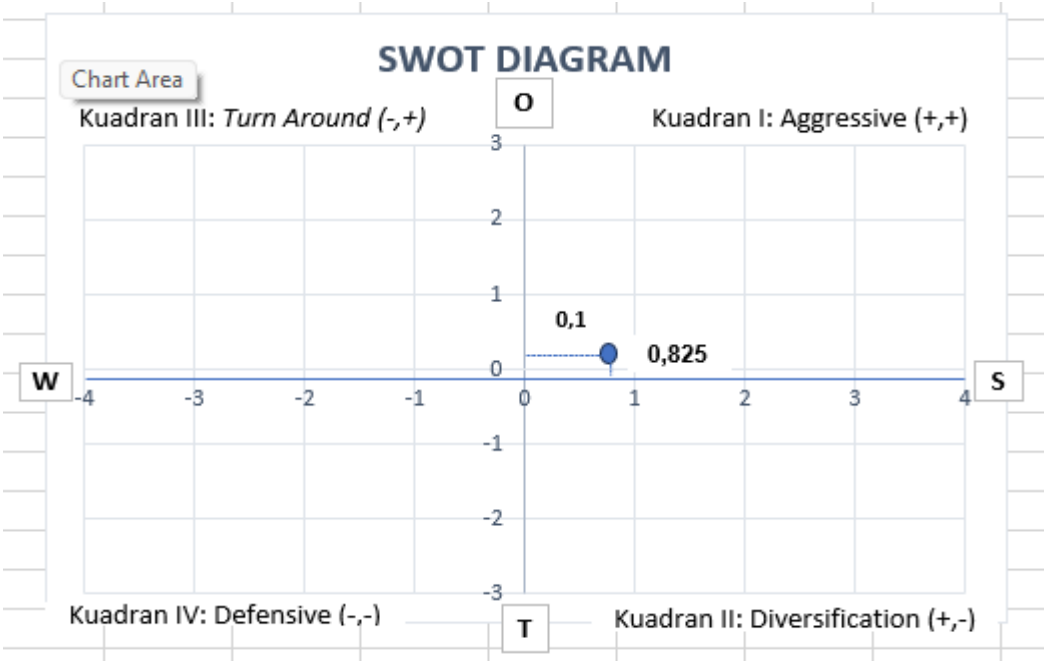

Figure 2. SWOT Diagram

Information:
S → O : Harnessing the power of AI to seize investment and collaboration opportunities.
S → T : Reduce threats by improving AI security.
W → O : Overcoming weaknesses with research and development.
W → T : Mitigating weaknesses so that they are not exacerbated by global threats.

Interpretation and Policy Implications

The use of AI in national defense has high potential, but still requires strict regulation and supervision to avoid bias and cyber threats. Investment is needed in strengthening AI infrastructure, including policies to ensure transparency in AI based decision making. International collaboration in cybersecurity is essential, especially in mitigating the threat of AI used by non state actors. The development of explainable AI (XAI) is a priority, in order to increase accountability in military decision-making.

The results of the study show that artificial intelligence (AI) contributes significantly to the reformulation of national defense policy by strengthening the strategic decisionmaking process, increasing operational efficiency, and expanding the capacity of predictive analysis of evolving threats. The integration of AI into defense policy allows for resource optimization, increased situational awareness, and simplified risk assessment processes through faster and more accurate data processing capabilities (Kalogiannidis et al., 2024). Based on the results of the literature review and dialogue with experts, it was found that AI plays an important role in changing the paradigm

of strategic planning from a reactive approach to a predictive approach. AI is able to simulate various threat and response scenarios that enable the government to design more adaptive defense policies. As stated by Baum et al., an AI system designed with the principle of explainability can bridge human limitations in processing the complexity of strategic data, as well as increase accountability in decision making (Baum et al., 2022).

The SWOT analysis conducted shows that the main strengths of AI lie in its ability to manage big data, detect hidden patterns in military intelligence, and provide precise tactical advice. The main weaknesses include the risk of algorithmic bias, dependence on digital infrastructure, and limited system transparency (Lepri et al., 2017); (Dowding & Taylor, 2024). Strategic opportunities arise from increasing global investment in AI technologies for the military, international collaboration on cybersecurity systems, and increasing technological literacy among policymakers (Whetsell et al., 2019). The identified threats include global AI supremacy competition that creates an imbalance in military power, the risk of misuse of AI by non-state actors, and regulatory fragmentation that can undermine international cooperation (Sio & Mecacci, 2021);(Wang et al., 2024). Thus, defense policy reformulation must include strategies to mitigate system vulnerabilities and the integration of a strong ethical framework. This study also found that the successful integration of AI into defense policy is highly dependent on the existence of inclusive and value-based governance. According to Ho and O'Sullivan, the government has an important role in creating standards for responsible AI implementation and encouraging public participation in technology policy making (Ho & O'Sullivan, 2019).

D. Conclusions

Integrating artificial intelligence (AI) into national defense policy is a critical step toward enhancing the effectiveness and responsiveness of strategic decision making in an era marked by complex and unpredictable threats. This study finds that AI has the capacity to strengthen national defense by enabling predictive analysis, improving operational efficiency, and enhancing situational awareness. AI facilitates early detection of threats such as cyberattacks, information warfare, and hybrid conflicts, allowing for timely and data-informed responses. The findings highlight that AI technologies are quite mature for policy-level integration, but their success depends on the presence of ethical safeguards, institutional readiness, and transparent governance structures. For AI to serve as a reliable tool in defense strategy, it must function in a way that is explainable, accountable, and aligned with national security objectives. This calls for a deliberate and inclusive approach involving collaboration among policymakers, defense institutions, academic researchers, and the technology industry. Reforming defense policy through AI also requires the development of oversight mechanisms to evaluate risk, ensure operational integrity, and prevent unintended consequences. AI should be seen not as a replacement for human judgment but as a strategic partner that enhances decision quality while preserving

ethical standards and human oversight. A comprehensive and adaptive policy framework is needed to guide the sustainable application of AI in defense, one that reflects national values and is capable of evolving alongside technological advancements. Ultimately, successful integration of AI into defense policy will depend on a balanced approach that combines innovation with responsibility, enabling a more resilient and future-ready national defense posture.

E. Acknowledgement

Thank you to our family who always provide support, the lecturers who provide guidance and direction in writing the journal.

References

Adobor, H., & Yawson, R. M. (2022). The Promise of Artificial Intelligence in Combating Public Corruption in the Emerging Economies: A Conceptual Framework. *Science and Public Policy*, *50*(3), 355–370. https://doi.org/10.1093/scipol/scac068

Alaja, A., & Sorsa, V. (2020). The Evolution of the National Innovation System as Programmatic Policy Idea in Finland. *Science and Public Policy*, *47*(6), 834–843. https://doi.org/10.1093/scipol/scaa045

Aleksandrova, A., Ninova, V., & Zhelev, Z. (2023). A Survey on AI Implementation in Finance, (Cyber) Insurance and Financial Controlling. *Risks*, *11*(5), 91. https://doi.org/10.3390/risks11050091

Alrabiah, A., & Drew, S. (2020). Proactive Management of Regulatory Policy Ripple Effects via a Computational Hierarchical Change Management Structure. *Risks*, *8*(2), 49. https://doi.org/10.3390/risks8020049

Baum, K., Mantel, S., Schmidt, E., & Speith, T. (2022). From Responsibility to Reason-Giving Explainable Artificial Intelligence. *Philosophy & Technology*, *35*(1). https://doi.org/10.1007/s13347-022-00510-w

Chen, L., Alwi, H., Edwards, C., & Sato, M. (2022). Flight Evaluation of an LPV Sliding Mode Observer for Sensor FTC. *Ieee Transactions on Control Systems Technology*, *30*(3), 1319–1327. https://doi.org/10.1109/tcst.2021.3096946

Dowding, K., & Taylor, B. R. (2024). Algorithmic Decision-Making, Agency Costs, and Institution-Based Trust. *Philosophy & Technology*, *37*(2). https://doi.org/10.1007/s13347-024-00757-5

Galliott, J., & Wyatt, A. (2021). Considering the Importance of Autonomous Weapon System Design Factors to Future Military Leaders. *Australian Journal of International Affairs*, *76*(2), 219–244. https://doi.org/10.1080/10357718.2021.1940093

Giubilini, A., & Savulescu, J. (2017). The Artificial Moral Advisor. The "Ideal Observer" Meets Artificial Intelligence. *Philosophy & Technology*, *31*(2), 169–188. https://doi.org/10.1007/s13347-017-0285-z

Guardia, F. H. de la, Grant, S., & Miguel, E. (2020). A Framework for Open Policy

Analysis. *Science and Public Policy*, *48*(2), 154–163. https://doi.org/10.1093/scipol/scaa067

Guerra, P., & Castelli, M. (2021). Machine Learning Applied to Banking Supervision a Literature Review. *Risks*, *9*(7), 136. https://doi.org/10.3390/risks9070136

Ho, J., & O'Sullivan, E. (2019). Addressing the Evolving Standardisation Challenges of 'Smart Systems' Innovation: Emerging Roles for Government? *Science and Public Policy*, *46*(4), 552–569. https://doi.org/10.1093/scipol/scz008

Holmes, M., & Wheeler, N. J. (2024). The Role of Artificial Intelligence in Nuclear Crisis Decision Making: A Complement, Not a Substitute. *Australian Journal of International Affairs*, *78*(2), 164–174. https://doi.org/10.1080/10357718.2024.2333814

Jauernig, J., Uhl, M., & Walkowitz, G. (2022). People Prefer Moral Discretion to Algorithms: Algorithm Aversion Beyond Intransparency. *Philosophy & Technology*, *35*(1). https://doi.org/10.1007/s13347-021-00495-y

Kalogiannidis, S., Kalfas, D., Papaevangelou, O., Giannarakis, G., & Chatzitheodoridis, F. (2024). The Role of Artificial Intelligence Technology in Predictive Risk Assessment for Business Continuity: A Case Study of Greece. *Risks*, *12*(2). https://doi.org/10.3390/risks12020019

King, T. C., Aggarwal, N., Taddeo, M., & Floridi, L. (2020). Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions. In *Science and Engineering Ethics* (Vol. 26, Issue 1). Springer Netherlands. https://doi.org/10.1007/s11948-018-00081-0

Kotaridis, I., & Benekos, G. (2023). Integrating Earth Observation IMINT With OSINT Data to Create Added-Value Multisource Intelligence Information: A Case Study of the Ukraine–Russia War. *Security and Defence Quarterly*, *43*(3), 1–21. https://doi.org/10.35467/sdq/170901

Krügel, S., Ostermaier, A., & Uhl, M. (2022). Zombies in the Loop? Humans Trust Untrustworthy AI-Advisors for Ethical Decisions. *Philosophy & Technology*, *35*(1). https://doi.org/10.1007/s13347-022-00511-9

Lepri, B., Oliver, N., Letouzé, E., Pentland, A., & Vinck, P. (2017). Fair, Transparent, and Accountable Algorithmic Decision-Making Processes. *Philosophy & Technology*, *31*(4), 611–627. https://doi.org/10.1007/s13347-017-0279-x

List, C. (2021). Group Agency and Artificial Intelligence. *Philosophy & Technology*, *34*(4), 1213–1242. https://doi.org/10.1007/s13347-021-00454-7

Makridis, C., Borkowski, A., & Alterovitz, G. (2024). Perspectives on Advancing Innovation and Human Flourishing Through a Network of AI Institutes. *Science and Public Policy*, *51*(3), 557–562. https://doi.org/10.1093/scipol/scad088

Mitrović, M. (2021). Assessments and Foreign Policy Implementation of the National Security of Republic of Serbia. *Security and Defence Quarterly*, *34*(2), 7–19. https://doi.org/10.35467/sdq/135592

Naeem, H., & Hauser, J. (2024). Should We Discourage AI Extension? Epistemic Responsibility and AI. *Philosophy & Technology*, *37*(3). https://doi.org/10.1007/s13347-024-00774-4

Nallakaruppan, M. K., Chaturvedi, H., Grover, V., Balusamy, B., Jaraut, P., Bahadur,

J., Meena, V. P., & Hameed, I. A. (2024). Credit Risk Assessment and Financial Decision Support Using Explainable Artificial Intelligence. *Risks*, *12*(10), 164. https://doi.org/10.3390/risks12100164

O'Shaughnessy, M., Schiff, D., Varshney, L. R., Rozell, C. J., & Davenport, M. A. (2022). What Governs Attitudes Toward Artificial Intelligence Adoption and Governance? *Science and Public Policy*, *50*(2), 161–176. https://doi.org/10.1093/scipol/scac056

Owens, E., Sheehan, B., Mullins, M., Cunneen, M., Ressel, J., & Castignani, G. (2022). Explainable Artificial Intelligence (XAI) in Insurance. *Risks*, *10*(12), 230. https://doi.org/10.3390/risks10120230

Paglieri, F. (2024). Expropriated Minds: On Some Practical Problems of Generative AI, Beyond Our Cognitive Illusions. *Philosophy & Technology*, *37*(2). https://doi.org/10.1007/s13347-024-00743-x

Radičić, D., & Pugh, G. (2016). R&D Programmes, Policy Mix, and the 'European Paradox': Evidence From European SMEs. *Science and Public Policy*, scw077. https://doi.org/10.1093/scipol/scw077

Rahman, M. M., Pokharel, B. P., Sayeed, S. A., Bhowmik, S., Kshetri, N., & Eashrak, N. (2024). riskAIchain: AI-Driven IT Infrastructure—Blockchain-Backed Approach for Enhanced Risk Management. *Risks*, *12*(12), 206. https://doi.org/10.3390/risks12120206

Ruiter, A. de. (2021). The Distinct Wrong of Deepfakes. *Philosophy & Technology*, *34*(4), 1311–1332. https://doi.org/10.1007/s13347-021-00459-2

Shkalenko, A. V, & Nazarenko, A. (2024). Integration of AI and IoT Into Corporate Social Responsibility Strategies for Financial Risk Management and Sustainable Development. *Risks*, *12*(6), 87. https://doi.org/10.3390/risks12060087

Sio, F. S. d., & Mecacci, G. (2021). Four Responsibility Gaps With Artificial Intelligence: Why They Matter and How to Address Them. *Philosophy & Technology*, *34*(4), 1057–1084. https://doi.org/10.1007/s13347-021-00450-x

Taddeo, M., McNeish, D., Blanchard, A., & Edgar, E. (2021). Ethical Principles for Artificial Intelligence in National Defence. *Philosophy and Technology*, *34*(4), 1707–1729. https://doi.org/10.1007/s13347-021-00482-3

Taylor, I. (2024). Collective Responsibility and Artificial Intelligence. *Philosophy & Technology*, *37*(1). https://doi.org/10.1007/s13347-024-00718-y

Vaassen, B. (2022). AI, Opacity, and Personal Autonomy. *Philosophy & Technology*, *35*(4). https://doi.org/10.1007/s13347-022-00577-5

Vold, K. (2024). Human-AI cognitive teaming: using AI to support state-level decision making on the resort to force. *Australian Journal of International Affairs*, *78*(2), 229–236. https://doi.org/10.1080/10357718.2024.2327383

Wang, S., Xia, M., Shi, X., Hou, B., & Lu, S. (2024). China's Distinctive Civil–military Integration Policy and Firm Innovation. *Science and Public Policy*, *51*(5), 761–779. https://doi.org/10.1093/scipol/scae013

Weissmann, M. (2025). Future Threat Landscapes: The Impact on Intelligence and Security Services. *Security and Defence Quarterly*. https://doi.org/10.35467/sdq/197248

Whetsell, T. A., Leiblein, M. J., & Wagner, C. S. (2019). Between Promise and Performance: Science and Technology Policy Implementation Through Network Governance. *Science and Public Policy*, *47*(1), 78–91. https://doi.org/10.1093/scipol/scz048

Xu, Z., Chu, B., Geng, H., Nian, X., & Zhang, C. (2024). Model-Guided Learning for Wind Farm Power Optimization. *Ieee Transactions on Control Systems Technology*, *32*(2), 428–439. https://doi.org/10.1109/tcst.2023.3315547

Zobi, M. K. A., & Jarah, B. A. F. (2023). The Role of Internal Auditing in Improving the Accounting Information System in Jordanian Banks by Using Organizational Commitment as a Mediator. *Risks*, *11*(9), 153. https://doi.org/10.3390/risks11090153