National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

Navigating Modern Warfare: Indonesia's Strategic Efforts in Implementing Artificial Intelligence on the Nation's Defense Posture

Major Moris Pandjaitan

JCSP 51

Exercise Solo Flight

Disclaimer

Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission.

PCEMI n° 51

Exercice Solo Flight

Avertissement

Les opinons exprimées n'engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite.

Canada

CANADIAN FORCES COLLEGE - COLLÈGE DES FORCES CANADIENNES

JCSP 51 - PCEMI n° 51
2024 - 2025
Exercise Solo Flight – Exercice Solo Flight

Navigating Modern Warfare: Indonesia's Strategic Efforts in Implementing Artificial Intelligence on the Nation's Defense Posture

Major Moris Pandjaitan

Navigating Modern Warfare: Indonesia's Strategic Efforts in Implementing Artificial Intelligence on the Nation's Defense Posture

INTRODUCTION

The rapid evolution of advanced technologies has fundamentally reshaped the global security landscape, transforming how nations prepare for and respond to emerging threats. Technological innovations have become increasingly accessible and affordable, extending beyond powerful nations to a growing number of countries and even non-state actors. This widespread availability marks a pivotal shift, as cutting-edge capabilities are no longer limited to a handful of dominant powers.[1] As more states pursue technological advancements to strengthen their defense posture, the resulting security dilemma intensifies global tensions and threatens strategic stability. Rapid fluctuations in perceived power and threat perception further complicate this dynamic.[2] In this evolving environment, modern warfare is increasingly defined by the integration of technological sophistication, characterized by speed, data dominance, and autonomous systems, into national defense strategies.[3]

The dynamic global security landscape has profound implications for Indonesia. As the world's largest archipelagic nation, Indonesia occupies a geopolitically strategic location uniquely positioned between two oceans and two continents that shares land and maritime borders with ten neighboring countries. Although strategically advantageous, this geography simultaneously exposes Indonesia to a broad spectrum of security vulnerabilities, encompassing both military and non-military threats, as well as complex hybrid challenges.[4] Transition from conventional to non-traditional threats, driven by globalization and digitalization, has intensified the complexity of Indonesia's defense environment.[5] In response, the country must recalibrate its national defense strategy to prioritize rapid decision-making, technological agility, and integrated multi-domain capabilities. The Indonesian Defense White Paper underscores the importance of a total defense system mobilizing all national resources and encouraging civilian participation in a comprehensive effort to safeguard national interests.[6] Fulfilling this vision in today's volatile security climate necessitates a transformative approach anchored in innovation and technological resilience to effectively address the multidimensional threats of the digital era.

Among information and communication technology advancements, Artificial Intelligence (AI) ranks amongst the most transformative forces with the potential to redefine government operations, military strategies, and international power dynamics.[7] Significant advances in AI have already begun to reshape the character of warfare by enabling the deployment of intelligent

---

[1] Margaret E. Kosal and Heather Regnault, "Introduction," in *Disruptive and Game Changing Technologies in Modern Warfare: Development, Use, and Proliferation* (Switzerland: Springer International Publishing, 2020), 3.
[2] Ibid., 7.
[3] Goddy Uwa Osimen et al., "Artificial Intelligence and Arms Control in Modern Warfare," *Cogent Social Sciences* 10, no. 1 (December 31, 2024): 2, https://doi.org/10.1080/23311886.2024.2407514.
[4] Ministry of Defence of the Republic of Indonesia, ed., *Indonesian Defence White Paper 2015*, 3rd ed. (Jakarta: Departemen Pertahanan, Republik Indonesia, 2015), 1.
[5] Rizky Ramadhianto et al., "Implementation of Artificial Intelligence on Indonesia's Defense Intelligence Activities," *Jurnal Pertahanan: Media Informasi Ttg Kajian & Strategi Pertahanan Yang Mengedepankan Identity, Nasionalism & Integrity* 9, no. 2 (August 31, 2023): 351, https://doi.org/10.33172/jp.v9i2.14657.
[6] Ministry of Defence of the Republic of Indonesia, *Indonesian Defence White Paper 2015*, 29.
[7] Kosal and Regnault, "Introduction," 1.

systems capable of autonomous operations and real-time adaptability in complex environments. AI's military utility lies in its capacity to enhance decision-making, which directly contributes to improved strategic planning and operational precision.[8] In a defense context, AI bolsters critical functions such as intelligence gathering, autonomous system development, and cyber capabilities by delivering unprecedented levels of speed, accuracy, and strategic depth. Defense intelligence—defined as the critical knowledge essential for both civilian and military leadership to anticipate and mitigate security threats—relies heavily on timely, accurate information, a process that AI can significantly enhance through automation and pattern recognition.[9] This emphasis on intelligence aligns with Indonesia's total defense principle, which encourages the coordinated use of all national assets for collective security. Furthermore, AI-driven systems offer operational advantages such as rapid manoeuvrability, reduced personnel risk, and improved mission accuracy, which reinforce Indonesia's defense capacity.[10] As AI becomes increasingly central to modern military strategies globally, its thoughtful integration is imperative for Indonesia to maintain relevance and resilience in the shifting security landscape.[11]

Incorporation of AI into Indonesia's national defense posture is no longer a mere opportunity but a necessity. Effectively leveraging AI technologies bolsters the country's capacity to anticipate, deter, and respond to emerging security threats, while also reinforcing broader national objectives such as sovereignty, resilience, and regional stability. However, this integration must be guided by robust policy frameworks that ensure ethical governance, uphold legal accountability, and safeguard human rights.[12] This essay argues that, in response to evolving regional security threats, Indonesia must pursue a deliberate and strategic implementation of AI within its national defense posture to safeguard its territorial sovereignty.

TERMINOLOGY

The U.S. Joint Publication defines warfare as the efforts of engaging armed conflict against the adversary, shaped by evolving methods, technologies, and capabilities.[13] In the contemporary context, modern warfare is increasingly affected by unprecedented global interconnectedness, rapid and unpredictable change, and rising complexity driven by globalization and the information revolution.[14] As a result, modern warfare is characterized by the diversity of its actors, encompassing both traditional state forces and non-state entities, and by the hybrid nature of its conduct. The conduct of warfare has shifted away from conventional, state-on-state confrontations toward indirect engagements, increasingly defined by the use of political instruments, information warfare, and asymmetric strategies that exploit technological

---

[8] Kenneth Payne, *I, Warbot: The Dawn of Artificially Intelligent Conflict* (UK: Oxford University Press, 2021), 2.
[9] Richard L. Russell, "Strategic Intelligence and American Statecraft," in *Sharpening Strategic Intelligence: Why the CIA Gets It Wrong and What Needs to Be Done to Get It Right*, 1st ed. (Cambridge: Cambridge University Press, 2007), 5, https://doi.org/10.1017/CBO9780511509902.
[10] Stanislav Abaimov and Maurizio Martellini, *Cyber Arms: Security in Cyberspace* (Florida: CRC Press, 2020), xiii.
[11] Azizah Saffa, "AI Transforming Indonesia's Defence and Security," *OpenGov Asia*, March 15, 2024, https://opengovasia.com/2024/03/15/ai-transforming-indonesias-defence-and-security/.
[12] Charles Cohen, "AI in Defense: Navigating Concerns, Seizing Opportunities," *National Defense*, July 25, 2023, https://www.nationaldefensemagazine.org/articles/2023/7/25/defense-department-needs-a-data-centric-digital-security-organization.
[13] Joint Chiefs of Staff, "*Joint Warfighting*" (Joint Publication 1, Volume 1, August 27, 2023), II–5, https://keystone.ndu.edu/Portals/86/Joint%20Warfighting.pdf.
[14] David Jordan et al., *Understanding Modern Warfare*, 2nd ed. (Cambridge: Cambridge University Press, 2016), 438, https://doi.org/10.1017/CBO9781316460276.

vulnerabilities.[15] This evolution reflects a broader transformation in the strategic context, where the distinctions between war and peace, civilian and combatant roles, and physical and digital domains are becoming progressively obscured.

Artificial Intelligence (AI) refers to technologies that enable machines to replicate human cognitive functions and perform tasks aimed at achieving specific objectives. These systems demonstrate intelligent behavior through capabilities such as pattern recognition, natural language processing, strategic reasoning, and adaptive learning, enabling them to analyze environments, make decisions, and carry out actions traditionally requiring human intelligence.[16] The rapid advancement of AI continues to transform a wide range of fields and exerts a profound impact on the conduct of human affairs, particularly in the domains of defense and security operations.[17]

Pursuant to Law Number 3 of 2002 on National Defense of the Republic of Indonesia, the country adopts a Total Defense system, a comprehensive and integrated approach that involves the participation of all citizens and the mobilization of national resources. This system is implemented in a sustained and coordinated manner to uphold state sovereignty, maintain territorial integrity, and safeguard the entire nation against all forms of threats. The law designates the Indonesian National Armed Forces (TNI) as the principal component of national defense.[18] As an archipelagic country, the protection of Indonesia's vast geographic territory constitutes a strategic priority. The Indonesian Defense White Paper highlights the importance of developing a defense posture that is both agile and responsive to the impact of globalization and the evolving strategic environment. It emphasizes the need for adaptive national defense planning within a dynamic environment marked by complex security challenges that affect multiple aspects of national life.[19]

EVOLVING REGIONAL SECURITY THREATS AND INDONESIA'S STRATEGIC VULNERABILITY

Indonesia's security environment is becoming increasingly complex and multifaceted, particularly in its maritime domain. As a vast archipelagic state spanning two oceans, Indonesia relies heavily on its maritime space not only for natural resources and inter-island connectivity but also for access to vital international trade routes. However, this strategic geography simultaneously exposes the nation to a broad spectrum of vulnerabilities. Indonesia faces extensive maritime threats, ranging from terrorism and illegal fishing to transnational crimes and sovereignty disputes.[20] One of the most notable challenges has been securing the Malacca Strait, a vital shipping corridor that has experienced numerous incidents of piracy and armed robbery. Additionally, militant groups based in the southern Philippines have perpetrated cross-border

---

[15] Mary Kaldor, *New & Old Wars: [Organized Violence in a Global Era]*, 2nd edition, reprinted (Stanford, Calif.: Stanford University Press, 2010), 117.
[16] Stephan De Spiegeleire, Matthijs Maas, and Tim Sweijs, "Artificial Intelligence and the Future of Defense" (The Hague: The Hague Centre for Strategic Studies, 2017), 28.
[17] Osimen, Newo, and Fulani, "Artificial Intelligence and Arms Control in Modern Warfare," 2.
[18] "Law of the Republic of Indonesia Number 3 of 2002 on State Defense" (State Gazette of the Republic of Indonesia Number 3 of 2002, n.d.).
[19] Ministry of Defence of the Republic of Indonesia, *Defence White Paper 2015*, 9.
[20] Gilang Kembara, "Security Outlook of the Asia-Pacific Countries and Its Implications for the Defence Sector: Indonesia," in *Security Outlook of the Asia Pacific Countries and Its Implications for the Defense Sector*, vol. 16 (NIDS Joint Research Series, Japan: The National Institute for Defense Studies, 2018), 12.

kidnappings involving Indonesian and Malaysian citizens, further complicating regional maritime security.[21]

Illegal, unreported, and unregulated (IUU) fishing also represents a particular contentious issue for Indonesia, resulting in substantial economic losses. A critical hotspot is the South China Sea (SCS), where China's expansive territorial claims overlap with Indonesia's Exclusive Economic Zone near the Natuna Islands, one of Indonesia's outermost regions, abundant in fisheries and energy resources.[22] Recurrent incursions by Chinese fishing vessels and naval ships in these waters violate Indonesia's sovereign rights and escalate regional tensions.[23] Beyond the Natuna issue, Indonesia faces growing strategic pressures stemming from intensifying great power rivalries and regional militarization. As a key node in the Indo-Pacific, contested maritime zones and shifting alignments threaten Indonesia's strategic autonomy and freedom of manoeuvre.[24]

Indonesia's extensive maritime and land boundaries also contribute to recurring jurisdictional disputes with neighboring states. Notable maritime flashpoints include sea borders shared with Thailand, India, Malaysia, Vietnam, and Singapore, many of which lie in resource-rich and commercially significant waters.[25] The scattered geography and diverse topography of Indonesia's outermost islands further complicate border surveillance, demanding tailored defense capabilities.[26] These challenges are amplified by unresolved boundary claims, weak immigration controls, inadequate defense infrastructure in remote regions, and insufficient interagency coordination, all of which undermine Indonesia's ability to maintain sovereignty and secure its borders.

In parallel with these maritime and territorial challenges, Indonesia confronts a growing array of asymmetric and non-traditional security threats. Rapid technological advancement and increased information access have empowered non-state actors, shifting the security calculus away from purely conventional state-based threats. Terrorism remains a major concern, as Indonesia has experienced multiple attacks since the early 2000s linked to global jihadist networks such as Al-Qaeda. These groups not only endanger civilian lives but also engage in illicit activities, including arms trafficking, human smuggling, and drug trafficking, to fund their operations.[27]

Compounding these threats is the rapid escalation of cybersecurity threats. Indonesia ranks 24th globally and fifth in Southeast Asia on the Global Cybersecurity Index, lagging behind

---

[21] Ibid., 10.
[22] Andrias Darmayadi and Ervina Nabilah Purnamasari, "The Indonesia – China Relations in the Natuna Sea Dispute Resolution: Struggle for Sovereignty," *Journal of Eastern European and Central Asian Research (JEECAR)* 9, no. 1 (February 4, 2022): 45, https://doi.org/10.15549/jeecar.v9i1.870.
[23] Aisya Muyassara Wisnugroho, "South China Sea Conflict: Indonesia's Goals and Strategies Through the 'ABC Triangle Conflict Model,'" *Modern Diplomacy*, June 22, 2024.
[24] Evan A. Laksmana, "Stuck in Second Gear: Indonesia's Strategic Dilemma in the Indo-Pacific," *ISEAS-Yusof Ishak Institute*, no. 170 (2021): 3.
[25] Siti Ruhana and Tun Abdul Karim, "Indonesia vs. Malaysia: The Battle for Border Territory Resolved," *International Law Discourse in Southeast Asia* 3, no. 1 (January 31, 2024): 5, https://doi.org/10.15294/ildisea.v3i1.78889.
[26] Diah Ayu Permatasari, "An Overview of the Indonesian Security Outlook," *Jurnal Keamanan Nasional* 1, no. 1 (April 27, 2015): 16, https://doi.org/10.31599/jkn.v1i1.1.
[27] Kembara, "Security Outlook of the Asia-Pacific Countries and Its Implications for the Defence Sector: Indonesia," 12.

regional peers such as Singapore and Malaysia.[28] Recent cyberattacks, including significant data breaches in 2023 and a disruptive ransomware attack on public services in June 2024, have exposed serious vulnerabilities within Indonesia's digital domain. Furthermore, cyber networks have become central battlefields, exploited for disruption and utilized by non-state actors for recruitment, propaganda dissemination, and coordination. The diffusion of digital capabilities has thus enabled the proliferation of cybercrime, targeting both state institutions and the broader population.[29]

The shifting character of contemporary threats has introduced greater fragility in the conduct of warfare, increasingly blurring the lines between peace and conflict. Alongside rapid technological sophistication, asymmetric and non-traditional threats have significantly eroded the effectiveness of conventional defense mechanisms. The integration of advanced weapon systems, the growing reliance on cyber tools, and the emergence of non-state actors employing irregular tactics have reshaped the battlespace, making speed, adaptability, and precision critical to effective national defense.[30] For Indonesia, these challenges are intensified by limited surveillance infrastructure, particularly across its extensive and fragmented border regions. With ninety-two outermost islands and diverse geographical conditions, Indonesia's archipelagic terrain requires tailored and adaptive defense approaches to ensure territorial integrity and enhance deterrence.[31] The rising complexity of this security environment underscores the urgent need to move beyond traditional paradigms and embrace strategies grounded in innovation, agility, and technological integration.

The advancement of modern technologies offers significant opportunities for states to enhance their defense posture by enabling the development of sophisticated military capabilities aligned with the demands of modern warfare.[32] In response to an increasingly challenging security environment, Indonesia has acknowledged the urgency of military modernization and embedded this priority within its national defense vision and strategic planning documents. Contemporary defense strategies increasingly emphasize the integration of AI into weapons systems and operational frameworks, reflecting a broader transition toward technology-driven military capabilities. AI holds significant promise in defense applications, particularly in streamlining operations, enhancing decision-making, and increasing the accuracy and effectiveness of military missions.[33] For Indonesia, AI integration can bolster critical military functions, most notably by enhancing maritime domain awareness and surveillance, strengthening cyber defense capabilities, and improving deterrence against potential adversaries.

---

[28] Arief Isdiman Saleh and Muhammad Danu Winata, "Indonesia's Cyber Security Strategy: Problems and Challenges," in *Proceedings of the International Joint Conference on Arts and Humanities 2023 (IJCAH 2023)*, ed. Ali Mustofa et al., vol. 785, Advances in Social Science, Education and Humanities Research (Paris: Atlantis Press SARL, 2023), 1675–96, https://doi.org/10.2991/978-2-38476-152-4_169.

[29] Kembara, "Security Outlook of the Asia-Pacific Countries and Its Implications for the Defence Sector: Indonesia," 16.

[30] Pieter Pandie, "Indonesia: New Wings, Old Woes," *International Politics and Society*, January 13, 2025, https://www.ips-journal.eu/topics/foreign-and-security-policy/new-wings-old-woes-8017/.

[31] Permatasari, "An Overview of the Indonesian Security Outlook," 17.

[32] Ramadhianto et al., "Implementation of Artificial Intelligence on Indonesia's Defense Intelligence Activities," 351.

[33] Irvan Arianto Randa Lembang et al., "Indonesia Military Research and Development in Dealing with the Sixth Generation Warfare : The Use of Artificial Intelligence in War Operations," *East Asian Journal of Multidisciplinary Research* 2, no. 2 (February 28, 2023): 654, https://doi.org/10.55927/eajmr.v2i2.3263.

STRATEGIC BENEFITS OF AI INTEGRATION IN NATIONAL DEFENSE

AI is rapidly reshaping how military institutions address complex, high-speed, and multi-domain threats. In an era defined by information-centric warfare, the capacity to process vast and diverse data streams, adapt to dynamic operational conditions, and make rapid decisions has become an essential determinant of military effectiveness.[34] AI technologies support these capabilities by accelerating analytical processes, increasing decision-making precision, and enhancing operational agility, which are especially critical in countering asymmetric and non-traditional security challenges.[35] For Indonesia, a geographically dispersed archipelagic state with growing exposure to maritime and cyber vulnerabilities, AI integration offers a strategic pathway to modernize its defense posture, extend its operational reach, and improve national readiness amid escalating regional instability.

AI delivers substantial operational advantages across a range of military functions.[36] One of its most transformative contributions lies in the enhancement of Intelligence, Surveillance, and Reconnaissance (ISR) capabilities. AI facilitates the rapid processing and analysis of large volumes of data from diverse sources, including satellite imagery, radar, and electronic signals, to detect anomalies, identify patterns, and generate actionable intelligence.[37] This real-time intelligence capability significantly improves persistent situational awareness, a critical asset in monitoring national borders, maritime corridors, and strategic zones. For Indonesia, a nation with vast terrain and widespread territory, AI-enabled ISR tools offer the potential to fill critical surveillance gaps and accelerate threat detection and response.[38] In particular, the application of AI in information and communication technologies to enhance data collection, area mapping, and interoperability would significantly improve maritime surveillance capabilities in critical zones such as the Malacca Strait. Furthermore, AI integration supports the development of real-time early warning and rapid response systems, which are essential for countering transnational crimes, terrorism, and other asymmetric maritime threats.[39]

In addition to ISR, AI strengthens decision-making by providing commanders with advanced decision-support systems. Through machine learning algorithms and real-time data fusion, AI can generate predictive models, risk assessments, and scenario-based forecasts. These tools reduce human cognitive burden and support faster, more accurate decision-making in high-pressure operational environments.[40] In missile defense, for example, AI can track incoming threats and recommend optimal interception trajectories faster than human operators, dramatically improving response time.[41]

---

[34] Forrest Morgan et al., *Military Applications of Artificial Intelligence: Ethical Concerns in an Uncertain World* (California: RAND Corporation, 2020), 18, https://doi.org/10.7249/RR3139-1.
[35] Osimen, et al., "Artificial Intelligence and Arms Control in Modern Warfare," 5.
[36] Morgan et al., *Military Applications of Artificial Intelligence*, 8.
[37] Morgan et al., 13.
[38] Kembara, "Security Outlook of the Asia-Pacific Countries and Its Implications for the Defence Sector: Indonesia," 17.
[39] Rudy Ag Gultom, et al., "Interoperable Defense Systems for the Malacca Strait: A Military-Civilian Approach Using Sensing Technology," *World Journal of Advanced Research and Reviews* 20, no. 2 (November 30, 2023): 471, https://doi.org/10.30574/wjarr.2023.20.2.2286.
[40] Morgan et al., *Military Applications of Artificial Intelligence*, 18.
[41] Mir Moin Uddin Hasan and Md Suzon Islam, "The Role of Artificial Intelligence in Military Systems: Impacts on National Security and Citizen Perception" (Engineering, September 30, 2024), 2, https://doi.org/10.20944/preprints202409.2328.v1.

AI's role in logistics and predictive maintenance significantly enhances operational efficiency. By analyzing sensor data and historical performance records, AI can anticipate equipment failures, optimize maintenance schedules, and streamline supply chains. This advancement reduces system downtime, improves platform availability, and ensures that personnel and materials are in favorable condition. In large, decentralized archipelagic operations such as Indonesia's, this level of logistical precision is essential to sustain military readiness. Beyond logistics, AI is increasingly utilized in training and simulation environments. When integrated with virtual and augmented reality systems, AI can deliver adaptive training tailored to individual performance. AI-enabled virtual wargaming also allows military personnel to rehearse complex scenarios in immersive settings, enhancing preparedness and reducing overall training costs.[42]

Furthermore, AI contributes to threat detection beyond conventional battlefield applications. In the era of information superiority, AI plays a pivotal role in both offensive and defensive cyber operations by enhancing the analysis of intelligence within the digital domain. In cybersecurity, AI supports the development of resilient networks and mitigates denial-of-service attacks by identifying vulnerabilities and automating defensive responses.[43] By analyzing patterns from intrusion attempts, AI enables defense systems to anticipate and counter future attacks more effectively.[44] Machine learning significantly augments this capability by allowing systems to learn from previous breaches and detect anomalies that may indicate emerging, unknown threats. This capability constitutes a proactive first line of defense, bolstering incident management and long-term risk mitigation strategies.[45] Moreover, AI's capacity to process real-time data and analyze vast information streams enables more rapid and precise identification of hidden threat vectors.[46] Ultimately, these AI-driven functions enhance force protection and accelerate national responses to unconventional, digital-age threats.

One of the most transformative applications of AI in defense is the development of Autonomous Weapons Systems (AWS), which are capable of independently identifying and engaging targets with minimal or no human oversight. These systems integrate AI, machine learning algorithms, and advanced sensor technologies to operate effectively in complex operational settings, enabling faster and more precise responses than conventional systems. The emergence of AWS represents a significant evolution in the character of warfare, offering unprecedented levels of speed, accuracy, and operational reach.

The deployment of AWS in the military has penetrated across all domains. In the aerial domain, Unmanned Aerial Vehicles (UAVs), such as the MQ-9 Reaper, are equipped with advanced targeting systems and autonomous navigation capabilities, enabling them to conduct extended surveillance missions and execute precision strikes with minimal human intervention. In the maritime domain, autonomous surface vessels like the U.S. Navy's Sea Hunter are capable

---

[42] Kurtis H. Simpson et al., "Militarizing AI: How to Catch the Digital Dragon?," *On Track*, National Security in the Age of AI and Robotics, 35 (January 2025): 11.
[43] Simpson et al., 12.
[44] Greg Allen and Taniel Chan, "Artificial Intelligence and National Security" (Cambridge: Harvard Kennedy School Belfer Center for Science and International Affairs, July 2017), 19.
[45] Ramanpreet Kaur, et al., "Artificial Intelligence for Cybersecurity: Literature Review and Future Research Directions," *Information Fusion* 97 (April 7, 2023): 16, https://doi.org/10.1016/j.inffus.2023.101804.
[46] Fauzi Abdurrachman et al., "Building the Tni's Defense Posture in Cyberspace: Strategies for Dealing with Cyber Warfare in the Digital Era," *International Journal of Progressive Sciences and Technologies (IJPSAT)* 48, no. 1 (December 1, 2024): 457.

of patrolling vast oceanic expanses, supporting anti-submarine and reconnaissance missions without risking crew safety.[47] The growing integration of these systems into military strategies promise to reduce human casualties and operational risks in future conflicts, while maintaining persistent situational awareness. The strategic advantages of AWS are particularly relevant for Indonesia, given its vast maritime domain, dispersed islands, and limited access in remote areas. Autonomous drones can reinforce surveillance in sensitive regions such as the South China Sea, where territorial disputes and IUU present ongoing security concerns. The CH-4B UAVs currently deployed by the Indonesian Air Force in the Natuna Airbase are a practical example of this capability. These systems enhance maritime domain awareness, enable timely reconnaissance, and reduce personnel risks in contested or hazardous environments.[48]

Beyond operational reach, AWS offer notable advantages in persistence and precision. Unlike human operators, autonomous systems do not suffer from fatigue and can sustain missions over extended periods. Their ability to rapidly process sensor input and execute responses independently makes them highly effective in dynamic, time-sensitive scenarios, such as cross-border incursions or missile interception. Additionally, their deployment in hostile environments, such as dense jungles, remote islands, or wide maritime expanses, enables sustained presence without compromising personnel safety.[49]

Nonetheless, the integration of AWS also introduces critical operational and ethical considerations. Key issues include command responsibility, legal accountability, and the risks of overreliance on machine-driven decision-making.[50] These concerns underscore the importance of establishing clear national doctrines, legal frameworks, and ethical safeguards. For Indonesia, this means developing responsible governance mechanisms that uphold accountability, transparency, and compliance with international law. When supported by robust oversight and ethical design, AWS can serve as strategic force multipliers, extending Indonesia's defensive reach, improving battlefield survivability, and reinforcing its deterrence posture in an increasingly contested Indo-Pacific region.[51]

The global landscape offers critical insights into how leading military powers are operationalizing AI across strategic, operational, and tactical levels. These examples provide Indonesia with valuable models for adaptation, particularly in areas aligned with its geostrategic vulnerabilities and modernization priorities. The U.S. has spearheaded AI integration through initiatives such as Project Maven.[52] The Project utilizes machine learning to process and recognize massive volumes of data to support targeting decision-making with enhanced precision

---

[47] Damilola Bartholomew Sholademi, "The Role of Autonomous Systems in Modern Warfare," *International Research Journal of Modernization in Engineering Technology and Science* 6, no. 10 (October 2024): 524, https://www.doi.org/10.56726/IRJMETS62073.

[48] Muhammad Rayhan Faqih Syahfa and Gufron Gozali, "Drones: A 'Mad Thing' For Indonesian Future's Armaments – OpEd," *Eurasia Review*, May 29, 2024, https://www.eurasiareview.com/29052024-drones-a-mad-thing-for-indonesian-futures-armaments-oped/.

[49] Sholademi, "The Role of Autonomous Systems in Modern Warfare," 528.

[50] Morgan et al., *Military Applications of Artificial Intelligence*, 30.

[51] Saffa, "AI Transforming Indonesia's Defence and Security."

[52] Michael Zequeira, "Artificial Intelligence as a Combat Multiplier Using AI to Unburden Army Staffs," *Military Review Online Exclusive*, September 2024, 2, https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/Online-Exclusive/2024/AI-Combat-Multiplier/AI-Combat-Multiplier-UA1.pdf.

and speed.[53] This effort was able to assist in intelligence gathering in actual operational use in the fight against non-state actors. Another U.S. program, the U.S. Air Force's Loyal Wingman, illustrates human-machine teaming in which one piloted aircraft controls several AI-enabled UAVs to execute missions autonomously, especially to perform dangerous tasks.[54]

At the same time, the People's Republic of China (PRC) has implemented substantial reforms to its military strategic guidelines, motivated by a growing recognition of the transformative impact of technological and industrial revolutions in securing information superiority in modern warfare. Within this framework, China is implementing a phased roadmap aimed at becoming the global leader in AI by 2030.[55] This strategy emphasizes military-civil fusion, the development of advanced combat capabilities, and the promotion of research, education, and training. As part of its efforts, the PRC is upgrading its defense systems by integrating AI to develop intelligent weapons, automate battlefield functions, and enhance human-machine collaboration within its newly established Strategic Support Force.[56] In addition, China prioritizes civil-military integration by leveraging the private sector in cyber innovation and placing significant emphasis on cultivating skilled personnel through education and training programs. Its overarching ambition is to achieve cyber domain superiority, an area where traditional boundaries are increasingly blurred and non-state actors play a central role.[57]

Russia has increasingly prioritized AI as a critical component of its military modernization, viewing it as essential to preserving national sovereignty and achieving technological parity with global powers like the U.S. and China. Moscow has directed significant investment toward integrating AI into robotics, command and control systems, ISR, and unmanned systems across land, maritime, and aerial domains to address manpower shortages and boost battlefield effectiveness.[58] Notably, the development of advanced combat drones like Okhotnik and Altius, which are reportedly equipped with AI-enabled C4ISR capabilities, illustrates Russia's shift toward autonomous warfare. In the ongoing conflict in Ukraine, Russia has deployed loitering munitions and AI-assisted drones to enable real-time object recognition and dynamic targeting, thereby increasing tactical adaptability. Additionally, Russia's extensive use of cyber campaigns, including disinformation efforts and cyberattacks against Ukrainian infrastructure, underscores the increasing salience of AI in non-kinetic cyber operations below the threshold of open conflict.[59] These examples illustrate how AI can be weaponized to achieve strategic effects without direct confrontation.

---

[53] Michael C. Horowitz et al., "The Future of Military Applications of Artificial Intelligence: A Role for Confidence-Building Measures?," *Orbis* 64, no. 4 (2020): 531, https://doi.org/10.1016/j.orbis.2020.08.003.
[54] Morgan et al., *Military Applications of Artificial Intelligence*, 54.
[55] Horowitz et al., "The Future of Military Applications of Artificial Intelligence," 531.
[56] Yatsuzuka Masaaki, "PLA's Intelligentized Warfare: The Politics on China's Military Strategy," *Security & Strategy* 2 (January 2022): 29, https://www.nids.mod.go.jp/english/publication/security/pdf/2022/01/05.pdf.
[57] Elsa B. Kania and John K. Costello, "The Strategic Support Force and the Future of Chinese Information Operations," *Cyber Defense Review*, July 31, 2018, 110, https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/1589125/the-strategic-support-force-and-the-future-of-chinese-information-operations/.
[58] Anna Nadibaidze, "Russian Perceptions of Military AI, Automation, and Autonomy," *Foreign Policy Research Institute*, January 2022, 16, https://www.fpri.org/wp-content/uploads/2022/01/012622-russia-ai-.pdf.
[59] Samuel Bendett, "The Role of AI in Russia's Confrontation with the West," *CNAS Transatlantic Security*, May 3, 2024, 6, https://www.cnas.org/publications/reports/the-role-of-ai-in-russias-confrontation-with-the-west.

The strategic trajectories of the United States, China, and Russia in integrating AI into defense systems offer valuable insights for Indonesia's military modernization agenda. The U.S. experience highlights the strategic utility of AI in enhancing decision superiority, ISR capabilities, and autonomous coordination, particularly in joint operations and real-time threat detection.[60] This underscores the need for Indonesia to prioritize AI integration into early warning systems and battlefield automation, especially across its maritime and air defense components, to bolster border security. China's model, characterized by strong civil-military fusion, aggressive investment in AI research and education, and robust coordination between public and private sectors, exemplifies the effectiveness of a whole-of-nation approach.[61] As stipulated in Law No.3/2002 and reinforced in Indonesia's Defense White Paper, the Total Defense doctrine mandates the mobilization of all national resources, both civilian and military, in the defense of national sovereignty. Leveraging this framework, Indonesia can adapt China's approach by fostering AI collaboration among the Ministry of Defense, research institutions, defense industries, and civilian technology sectors. Meanwhile, Russia's focus on integrating AI into operational capabilities and cyber operations illustrates AI's potential in amplifying asymmetric responses and strategic deterrence. The deployment of UAVs, radar, signal-based systems, and AI-integrated weapon platforms should become a priority for Indonesia, not only to enhance territorial defense but also to minimize personnel risks in challenging terrains.[62] Moreover, learning from Russia's use of AI-driven cyber capabilities, Indonesia must urgently develop robust cyber defense tools, supported by a national cyber doctrine, interagency coordination, and civil-military collaboration. These measures are crucial to securing Indonesia's digital sovereignty and enhancing resilience in the face of rising asymmetric threats.[63]

As a geographically dispersed archipelagic state facing persistent surveillance demands and growing cyber vulnerabilities, Indonesia must treat AI-driven autonomy, data fusion, and real-time operational responsiveness not as optional innovations but as strategic imperatives. Developing a clear doctrine, investing in human capital, and establishing ethical and legal frameworks for AI use will be essential to ensure that AI integration efforts uphold democratic values while bolstering national resilience in an increasingly volatile Indo-Pacific security landscape, in alignment with Indonesia's Total Defense doctrine.

IMPLEMENTING AI RESPONSIBLY — CHALLENGES AND POLICY IMPERATIVES

While AI offers significant advantages in strengthening defence capabilities, it also presents profound legal, ethical, and institutional barriers. Addressing these issues demands a deliberate and well-regulated approach that aligns with democratic principles and Indonesia's Total Defense doctrine, which mandates the coordinated mobilization of all national resources for the preservation of sovereignty.[64]

A central legal concern in military AI use is compliance with International Humanitarian Law, particularly the Law of Armed Conflict (LOAC). Fully autonomous weapon systems may

[60] Horowitz et al., "The Future of Military Applications of Artificial Intelligence," 531.
[61] Kania and Costello, "The Strategic Support Force and the Future of Chinese Information Operations," 114.
[62] Lembang et al., "Indonesia Military Research and Development in Dealing with the Sixth Generation Warfare," 657.
[63] Abdurrachman et al., "Building the Tni's Defense Posture in Cyberspace: Strategies for Dealing with Cyber Warfare in The Digital Era," 457.
[64] Saffa, "AI Transforming Indonesia's Defence and Security."

struggle in adhering to the principles of distinction and proportionality under the LOAC, particularly in asymmetric conflicts, where the system may fail to distinguish between combatants and civilians. Moreover, AI-powered cyber capabilities, which often traverse civilian infrastructure, raise substantial risks for privacy, human rights, and personal data protection.[65]

Indonesia currently lacks a comprehensive legal framework governing the application of AI in national defense. While existing regulations, such as the Law on Electronic Information and Transactions and the Law on Personal Data Protection, provide partial coverage, they do not adequately address the unique military and ethical dimensions of AI deployment in defense contexts.[66] This regulatory gap stands in contrast to frameworks like the European Union's AI Act, which enforces strict oversight and risk-based controls on AI systems. Accordingly, Indonesia urgently needs to develop a national AI defense roadmap that integrates legal, ethical, and governance mechanisms to ensure the secure, accountable, and responsible adoption of AI in military applications.

Accountability is a critical concern in AI-enabled operations. When autonomous systems cause harm, particularly in lethal engagement or cyber operations, identifying responsibility becomes difficult. This ambiguity not only weakens command responsibility but also risks undermining legal deterrence.[67] Studies have emphasized the necessity of embedding ethical AI frameworks, enhancing human oversight, and enforcing transparency in military AI operations to reduce civilian casualties, privacy violations, and systemic misuse.[68]

Indonesia's efforts to integrate AI into its defense posture face significant structural and institutional barriers. The Indonesian Armed Forces (TNI)'s current infrastructure, particularly in border surveillance, real-time threat detection, and data integration, remains underdeveloped. Simultaneously, there is a significant shortage of personnel trained in AI technologies, exacerbated by a lack of military education programs centered on digital transformation. To overcome these limitations, Indonesia must cultivate military academic competencies. The Ministry of Defense and the TNI must initiate AI literacy and competency programs, while building collaboration with national research agencies, universities, and tech industries. This will reduce reliance on foreign dependency and leverage national resilience.[69] This approach aligns with Indonesia's Total Defense doctrine through encouraging civil-military fusion.

Cybersecurity is another strategic frontier where AI offers significant advantages. As TNI increasingly relies on AI-assisted tools for digital defense, it must contend with operational difficulties and vulnerabilities in protecting classified data. This capability requires technical proficiency, secure digital infrastructure, and robust cyber doctrine to ensure operational effectiveness and safety. Moreover, the lack of dedicated AI training programs and the absence of centralized oversight for AI deployment compound these risks.[70] Addressing these gaps requires not

---

[65] Morgan et al., *Military Applications of Artificial Intelligence*, 31.
[66] Ichsan Perwira Kurniagung and Andreas Christian Hamonangan Panggabean, "Navigating Indonesia's Emerging AI Regulations," *FKNK Law Firm*, September 5, 2024, https://navigating-indonesias-emerging-ai-regulations-fknk-lawfirm-tok8c/.
[67] Morgan et al., *Military Applications of Artificial Intelligence*, 33.
[68] Uddin Hasan and Islam, "The Role of Artificial Intelligence in Military Systems," 13.
[69] Lembang et al., "Indonesia Military Research and Development in Dealing with the Sixth Generation Warfare," 655.
[70] Tri Wahyu Asmoro Putro, "Implementasi Big Data dan Artificial Intelligence Untuk Meningkatkan Kemampuan Intelijen TNI," *Ranah Research : Journal of Multidisciplinary Research and Development* 6, no. 6 (September 2024): 2868, https://doi.org/10.38035/rrj.v6i6.

only capacity building but also regulatory harmonization and sustained evaluation mechanisms to ensure implementation effectiveness.

Indonesia's reliance on foreign defense technology presents another structural limitation. While international cooperation is necessary for knowledge transfer and system integration, Indonesia must invest in domestic research and development and establish public-private partnerships to support the development of a sustainable defense structure. Given the urgent nature of security threats ranging from transnational crime and territorial violations in the border areas, the South China Sea, and the Malacca Strait, these efforts must not be delayed, as surveillance gaps, maritime incursions, and asymmetric threats continue to jeopardize national interests.[71]

Comparative experiences offer valuable lessons. For instance, Canada's Department of National Defence and Canadian Armed Forces have introduced a comprehensive AI strategy outlining five core principles: effective governance, agile innovation, ethical and legal compliance, talent development, and external collaboration.[72] By combining these insights with its own strategic doctrines, Indonesia can responsibly integrate AI while upholding democratic values, national sovereignty, and adherence to international norms. Below are key recommendations for AI implementation in Indonesia's defense system:

- Develop a National AI Defense Roadmap to institutionalize governance, legal frameworks, ethical guidelines, and interoperability across military and civilian stakeholders.
- Invest in AI-based infrastructure for surveillance and threat response, particularly in outer islands, border areas, and maritime chokepoints.
- Build human capital through military-academic collaboration, AI-focused training programs, and simulation exercises to enhance adaptability in high-tech environments.
- Establish an AI Military Oversight Committee for centralized auditing, ethical review, and operational accountability in AI-enabled defense systems.

CONCLUSION

In conclusion, the rapid evolution of AI has brought about significant shifts in global defense strategies, compelling countries, including Indonesia, to re-evaluate their military preparedness. As demonstrated in this essay, the strategic integration of AI into Indonesia's defense posture is not only essential for enhancing technological capabilities but also a national imperative. Amid regional threats, intensifying superpower competition, asymmetric challenges, and the rapid transformation of warfare, AI offers capabilities that can significantly enhance Indonesia's decision-making speed, operational reach, and national resilience.

Indonesia's geographic vulnerability as an archipelagic nation, spanning two oceans and at the crossroads of major geopolitical rivalries, necessitates a highly adaptive defense strategy. From the ongoing conflict in the Natuna Sea to increasingly sophisticated cyberattacks on national infrastructure, Indonesia faces a complex security environment where traditional defense instruments are insufficient. In this context, AI emerges as a strategic enabler. Its capacity to automate intelligence collection, support predictive maintenance, optimize logistics,

[71] Pandie, "Indonesia: New Wings, Old Woes."
[72] Department of National Defence, *The Department of National Defence and Canadian Armed Forces Artificial Intelligence Strategy*, [D2-633/2024E-PDF] (Ottawa: National Defence, 2024), 24.

and power autonomous surveillance and weapons platforms allows it to address critical gaps in national defense, particularly across Indonesia's vast and fragmented territory.

However, this potential is not without risk. Integrating AI into defense systems raises critical legal, ethical, and institutional concerns. Despite their operational advantages, fully autonomous systems challenge international law, particularly concerning the principles of distinction and proportionality under the Law of Armed Conflict. Moreover, the lack of clear attribution in AI-enabled cyber or kinetic incidents raises serious accountability dilemmas, potentially eroding trust, undermining deterrence, and blurring chains of command. At present, Indonesia lacks a comprehensive legal framework to regulate the military use of AI, leaving significant governance, oversight, and public protection gaps. This institutional void must be addressed with urgency.

Equally pressing are infrastructure and human capital challenges. As this analysis has shown, Indonesia's defense technology ecosystem remains underdeveloped. The TNI still struggles with real-time data integration, effective border surveillance, and digital resilience—critical components for practical AI applications. Furthermore, the limited number of defense professionals with AI expertise hampers meaningful adoption. Addressing these challenges requires a long-term strategy for institutional transformation, including investment in research and development (R&D), digital infrastructure across remote regions, and robust human resource development through military-academic collaboration and professional AI training.

AI implementation in national defense also aligns with Indonesia's Total Defense doctrine, which emphasizes mobilizing civilian and military resources. A whole-of-nation approach, inspired by civil-military fusion models seen in countries such as China and Canada, is essential for embedding AI within Indonesia's broader security architecture. This integration can support joint innovation, ensure regulatory alignment, and prevent overdependence on foreign technologies—a current strategic vulnerability. Comparative case studies such as Canada's *Responsible AI Strategy for Defence* and the U.S. Project Maven show that ethical and operational integration of AI can succeed when guided by transparent governance, accountability, and legal safeguards.

To meet these goals, Indonesia must establish a National AI Defense Roadmap that outlines short- and long-term priorities, from enhancing maritime surveillance to cultivating a self-reliant defense AI industry. A Military AI Oversight Committee should be created to enforce ethical usage and conduct regular audits. In parallel, partnerships with trusted international allies and the domestic private sector should be strengthened to ensure knowledge transfer, reduce foreign dependency, and accelerate local innovation.

In short, adopting AI in defense must be strategic and responsible. If approached holistically—accounting for doctrine, infrastructure, human capital, and governance—Indonesia can transform its defense posture to meet the demands of modern warfare. By doing so, it will safeguard its sovereignty and territorial integrity and assert its strategic autonomy amid increasing instability in the Indo-Pacific. The time for decisive action is now—before the pace of change exceeds the nation's ability to respond.

BIBLIOGRAPHY

Abaimov, Stanislav. *Cyber Arms: Security in Cyberspace*. Milton, UNITED KINGDOM: CRC Press, 2020.

Abdurrachman, Fauzi, Bambang Suharjo, and Yudhi Biantoro. "Building The Tni's Defense Posture In Cyberspace: Strategies For Dealing With Cyber Warfare In The Digital Era." *International Journal of Progressive Sciences and Technologies (IJPSAT)* 48, no. 1 (December 1, 2024): 451–61.

Allen, Greg, and Taniel Chan. "Artificial Intelligence and National Security." Cambridge: Harvard Kennedy School Belfer Center for Science and International Affairs, July 2017.

Bendett, Samuel. "The Role of AI in Russia's Confrontation with the West." *CNAS Transatlantic Security*, May 3, 2024, 1–31. https://www.cnas.org/publications/reports/the-role-of-ai-in-russias-confrontation-with-the-west.

Cohen, Charles. "AI in Defense: Navigating Concerns, Seizing Opportunities." *National Defense*, July 25, 2023. https://www.nationaldefensemagazine.org/articles/2023/7/25/defense-department-needs-a-data-centric-digital-security-organization.

Darmayadi, Andrias, and Ervina Nabilah Purnamasari. "The Indonesia – China Relations in the Natuna Sea Dispute Resolution: Struggle for Sovereignty." *Journal of Eastern European and Central Asian Research (JEECAR)* 9, no. 1 (February 4, 2022): 41–48. https://doi.org/10.15549/jeecar.v9i1.870.

De Spiegeleire, Stephan, Matthijs Maas, and Tim Sweijs. "Artificial Intelligence and the Future of Defense." The Hague: The Hague Centre for Strategic Studies, 2017.

Department of National Defence. *The Department of National Defence and Canadian Armed Forces Artificial Intelligence Strategy*. [D2-633/2024E-PDF]. Ottawa: National Defence, 2024.

Horowitz, Michael C., Lauren Kahn, and Casey Mahoney. "The Future of Military Applications of Artificial Intelligence: A Role for Confidence-Building Measures?" *Orbis* 64, no. 4 (2020): 528–43. https://doi.org/10.1016/j.orbis.2020.08.003.

Irvan Arianto Randa Lembang, Romie Oktavianus Bura, and R Djoko Andreas Navalino. "Indonesia Military Research and Development in Dealing With The Sixth Generation Warfare : The Use of Artificial Intelligence in War Operations." *East Asian Journal of Multidisciplinary Research* 2, no. 2 (February 28, 2023): 649–60. https://doi.org/10.55927/eajmr.v2i2.3263.

Joint Chiefs of Staff. "Joint Warfighting." Joint Publication 1, Volume 1, August 27, 2023. https://keystone.ndu.edu/Portals/86/Joint%20Warfighting.pdf.

Jordan, David, James D. Kiras, David J. Lonsdale, Ian Speller, Christopher Tuck, and C. Dale Walton. *Understanding Modern Warfare*. 2nd ed. Cambridge: Cambridge University Press, 2016. https://doi.org/10.1017/CBO9781316460276.

Kaldor, Mary. *New & Old Wars: [Organized Violence in a Global Era]*. 2nd edition, Reprinted. Stanford, Calif.: Stanford University Press, 2010.

Kania, Elsa B., and John K. Costello. "The Strategic Support Force and the Future of Chinese Information Operations." *Cyber Defense Review*, July 31, 2018. https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/1589125/the-strategic-support-force-and-the-future-of-chinese-information-operations/.

Kaur, Ramanpreet, Dušan Gabrijelčič, and Tomaž Klobučar. "Artificial Intelligence for Cybersecurity: Literature Review and Future Research Directions." *Information Fusion* 97 (April 7, 2023): 101804. https://doi.org/10.1016/j.inffus.2023.101804.

Kembara, Gilang. "Security Outlook of the Asia-Pacific Countries and Its Implications for the Defence Sector: Indonesia." In *Security Outlook of the Asia Pacific Countries and Its Implications for the Defense Sector*, 16:151. Japan: The National Institute for Defense Studies, 2018.

Kosal, Margaret E., ed. *Disruptive and Game Changing Technologies in Modern Warfare: Development, Use, and Proliferation*. 1st ed. 2020. Cham: Springer International Publishing : Imprint : Springer, 2020.

Kurniagung, Ichsan Perwira, and Andreas Christian Hamonangan Panggabean. "Navigating Indonesia's Emerging AI Regulations." *FKNK Law Firm*, September 5, 2024. https://navigating-indonesias-emerging-ai-regulations-fknk-lawfirm-tok8c/.

Laksmana, Evan A. "Stuck in Second Gear: Indonesia's Strategic Dilemma in the Indo-Pacific." *ISEAS-Yusof Ishak Institute*, no. 170 (2021).

"Law of the Republic of Indonesia Number 3 of 2002 on State Defense." State Gazette of the Republic of Indonesia Number 3 of 2002, n.d.

Masaaki, Yatsuzuka. "PLA's Intelligentized Warfare: The Politics on China's Military Strategy." *Security & Strategy* 2 (January 2022): 17–36. https://www.nids.mod.go.jp/english/publication/security/pdf/2022/01/05.pdf.

Ministry of Defence of the Republic of Indonesia, ed. *Indonesian Defence White Paper 2015*. 3rd ed. Jakarta: Departemen Pertahanan, Republik Indonesia, 2015.

Morgan, Forrest, Benjamin Boudreaux, Andrew Lohn, Mark Ashby, Christian Curriden, Kelly Klima, and Derek Grossman. *Military Applications of Artificial Intelligence: Ethical Concerns in an Uncertain World*. California: RAND Corporation, 2020. https://doi.org/10.7249/RR3139-1.

Nadibaidze, Anna. "Russian Perceptions of Military AI, Automation, and Autonomy." *Foreign Policy Research Institute*, January 2022, 1–29. https://www.fpri.org/wp-content/uploads/2022/01/012622-russia-ai-.pdf.

Osimen, Goddy Uwa, Oluwamurewa Newo, and Oluwakemi Morola Fulani. "Artificial Intelligence and Arms Control in Modern Warfare." *Cogent Social Sciences* 10, no. 1 (December 31, 2024): 1–16. https://doi.org/10.1080/23311886.2024.2407514.

Pandie, Pieter. “Indonesia: New Wings, Old Woes.” *International Politics and Society*, January 13, 2025. https://www.ips-journal.eu/topics/foreign-and-security-policy/new-wings-old-woes-8017/.

Payne, Kenneth. *I, Warbot: The Dawn of Artificially Intelligent Conflict*. Oxford Scholarship Online Political Science. London: Hurst & Company, 2021. https://doi.org/10.1093/oso/9780197611692.001.0001.

Permatasari, Diah Ayu. “An Overview of the Indonesian Security Outlook.” *Jurnal Keamanan Nasional* 1, no. 1 (April 27, 2015): 1–26. https://doi.org/10.31599/jkn.v1i1.1.

Putro, Tri Wahyu Asmoro. “Implementasi Big Data dan Artificial Intelligence Untuk Meningkatkan Kemampuan Intelijen TNI.” *Ranah Research : Journal of Multidisciplinary Research and Development* 6, no. 6 (September 2024): 2864–72. https://doi.org/10.38035/rrj.v6i6.

Ramadhianto, Rizky, Tahan Samuel Lumban Toruan, Susaningtyas Nefo Handayani Kertopati, and Hikmat Zakky Almubaroq. “Implementation of Artificial Intelligence on Indonesia’s Defense Intelligence Activities.” *Jurnal Pertahanan: Media Informasi Ttg Kajian & Strategi Pertahanan Yang Mengedepankan Identity, Nasionalism & Integrity* 9, no. 2 (August 31, 2023): 350–65. https://doi.org/10.33172/jp.v9i2.14657.

Rudy Ag Gultom, Aris Poniman, and Syachroel. “Interoperable Defense Systems for the Malacca Strait: A Military-Civilian Approach Using Sensing Technology.” *World Journal of Advanced Research and Reviews* 20, no. 2 (November 30, 2023): 468–73. https://doi.org/10.30574/wjarr.2023.20.2.2286.

Ruhana, Siti, and Tun Abdul Karim. “Indonesia vs. Malaysia: The Battle for Border Territory Resolved.” *International Law Discourse in Southeast Asia* 3, no. 1 (January 31, 2024). https://doi.org/10.15294/ildisea.v3i1.78889.

Russell, Richard L. “Strategic Intelligence and American Statecraft.” In *Sharpening Strategic Intelligence: Why the CIA Gets It Wrong and What Needs to Be Done to Get It Right*, 1st ed., 1–28. Cambridge: Cambridge University Press, 2007. https://doi.org/10.1017/CBO9780511509902.

Saffa, Azizah. “AI Transforming Indonesia’s Defence and Security.” *OpenGov Asia*, March 15, 2024. https://opengovasia.com/2024/03/15/ai-transforming-indonesias-defence-and-security/.

Saleh, Arief Isdiman, and Muhammad Danu Winata. “Indonesia’s Cyber Security Strategy: Problems and Challenges.” In *Proceedings of the International Joint Conference on Arts and Humanities 2023 (IJCAH 2023)*, edited by Ali Mustofa, Ima Widiyanah, Binar K. Prahani, Imami A. T. Rahayu, Moh. Mudzakkir, and Cicilia D. M. Putri, 785:1675–96. Advances in Social Science, Education and Humanities Research. Paris: Atlantis Press SARL, 2023. https://doi.org/10.2991/978-2-38476-152-4_169.

Sholademi, Damilola Bartholomew. “The Role of Autonomous Systems in Modern Warfare.” *International Research Journal of Modernization in Engineering Technology and Science* 6, no. 10 (October 2024): 523–38. https://www.doi.org/10.56726/IRJMETS62073.

Simpson, Kurtis H., Raphael Racicot, Samuel Paquette, Samuel Villanove, and Adam MacDonald. “Militarizing AI: How to Catch the Digital Dragon?” *On Track*, National Security in the Age of AI and Robotics, 35 (January 2025): 56.

Syahfa, Muhammad Rayhan Faqih, and Gufron Gozali. “Drones: A ‘Mad Thing’ For Indonesian Future’s Armaments – OpEd.” *Eurasia Review*, May 29, 2024. https://www.eurasiareview.com/29052024-drones-a-mad-thing-for-indonesian-futures-armaments-oped/.

Uddin Hasan, Mir Moin, and Md Suzon Islam. “The Role of Artificial Intelligence in Military Systems: Impacts on National Security and Citizen Perception.” Engineering, September 30, 2024. https://doi.org/10.20944/preprints202409.2328.v1.

Wisnugroho, Aisya Muyassara. “South China Sea Conflict: Indonesia’s Goals and Strategies Through the ‘ABC Triangle Conflict Model.’” *Modern Diplomacy*, June 22, 2024.

Zequeira, Michael. “Artificial Intelligence as a Combat Multiplier Using AI to Unburden Army Staffs.” *Military Review Online Exclusive*, September 2024. https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/Online-Exclusive/2024/AI-Combat-Multiplier/AI-Combat-Multiplier-UA1.pdf.