Transformation of Counter-Terrorism Strategies Based on Artificial Intelligence and Legal Challenges Regarding the use of Autonomous Weapons

Deden Rahmad Hidayat[1], Joko Setiono[2], Supardi Hamid[3]
[1]Sekolah Tinggi Ilmu Kepolisian, Indonesia, Baandungjuara2020@icloud.com
[2]Sekolah Tinggi Ilmu Kepolisian, Indonesia, joko_setiono@ymail.com
[3]Sekolah Tinggi Ilmu Kepolisian, Indonesia, supardihamid@gmail.com

Corresponding Author: Baandungjuara2020@icloud.com[1]

Abstract: The development of Artificial Intelligence (AI) has transformed various sectors, including national security and counter-terrorism strategies. The utilization of AI, particularly through intelligent surveillance systems and autonomous weapons systems (AWS), strengthens the state's capability to detect, analyze, and respond to potential terrorist threats swiftly and efficiently. However, the presence of this technology does not escape legal challenges, particularly concerning regulatory gaps and accountability for the use of autonomous weapons that can operate without human intervention. This study uses a normative juridical approach to examine the transformation of counter-terrorism strategies based on AI, as well as to analyze the absence of legal norms governing the use of AWS in Indonesia and within the context of international law. The findings show that national legal instruments such as Law No. 5 of 2018 on the Eradication of Criminal Acts of Terrorism and Law No. 3 of 2002 on State Defense are not yet adequate to address the new challenges posed by AI. On the other hand, international forums such as the Convention on Certain Conventional Weapons (UN CCW) are still debating the ethical and legal boundaries of AWS without producing a binding consensus. This research recommends the establishment of a new legal framework that is responsive to technological developments, ensuring the protection of human rights and the principle of accountability in the use of AI for security purposes. Without clear regulations, this transformation has the potential to result in abuse of power and serious violations of civil rights.

Keywords: Artificial Intelligence (AI), Autonomous Weapons System (AWS), counter-terrorism, legal gap, national security

Abstrak: Perkembangan Kecerdasan Buatan (AI) telah mengubah berbagai sektor, termasuk strategi keamanan nasional dan kontra-terorisme. Penggunaan AI, terutama melalui sistem pengawasan cerdas dan sistem senjata otonom (AWS), memperkuat kemampuan negara untuk mendeteksi, menganalisis, dan merespons ancaman terorisme potensial dengan cepat dan efisien. Namun, keberadaan teknologi ini tidak lepas dari tantangan hukum, terutama terkait celah regulasi dan pertanggungjawaban atas penggunaan senjata otonom yang dapat beroperasi tanpa campur tangan manusia. Studi ini menggunakan pendekatan yuridis normatif untuk

mengkaji transformasi strategi kontra-terorisme berbasis AI, serta menganalisis ketidakhadiran norma hukum yang mengatur penggunaan AWS di Indonesia dan dalam konteks hukum internasional. Temuan menunjukkan bahwa instrumen hukum nasional seperti Undang-Undang Nomor 5 Tahun 2018 tentang Pemberantasan Tindak Pidana Terorisme dan Undang-Undang Nomor 3 Tahun 2002 tentang Pertahanan Negara belum memadai untuk mengatasi tantangan baru yang ditimbulkan oleh AI. Di sisi lain, forum internasional seperti Konvensi tentang Senjata Konvensional Tertentu (UN CCW) masih mendiskusikan batas-batas etis dan hukum AWS tanpa menghasilkan konsensus yang mengikat. Penelitian ini merekomendasikan pembentukan kerangka hukum baru yang responsif terhadap perkembangan teknologi, memastikan perlindungan hak asasi manusia dan prinsip pertanggungjawaban dalam penggunaan AI untuk tujuan keamanan. Tanpa regulasi yang jelas, transformasi ini berpotensi menyebabkan penyalahgunaan kekuasaan dan pelanggaran serius terhadap hak-hak sipil.

Kata Kunci: Kecerdasan Buatan (AI), Sistem Senjata Otonom (AWS), kontra-terorisme, celah hukum, keamanan nasional

INTRODUCTION

The development of artificial intelligence (AI) has penetrated various sectors of human life, including the field of national security and defense (Putra, 2024). In this digital era, AI is not only used for commercial or industrial needs, but has also become an important part of complex defense systems (Rifky, 2024). Governments and security institutions utilize AI in various forms, ranging from video-based surveillance to data analysis systems for detecting potential threats (Sumarno, 2025). In the context of counter-terrorism, AI plays a significant role as a tool for processing massive and complex intelligence data. The use of this technology enables early detection of potential terrorist attacks, accelerates security responses, and increases the effectiveness of counter-terrorism operations (Nirmala, 2024).

The use of AI in counter-terrorism encompasses various aspects, from tracking the movement of suspected individuals, analyzing patterns of digital communication, to predicting actions based on historical data and machine learning algorithms (Astuti, 2024). The advantage of AI lies in its ability to process large amounts of information quickly and accurately, which is impossible to do manually. This technology also plays a role in identifying terrorist networks more broadly through social network analysis and relationships between individuals. Globally, developed countries have integrated AI into their national security systems, creating systems capable of making automatic decisions under certain conditions (Farid, 2023). However, this advancement also raises legal and ethical challenges that cannot be ignored.

One of the most controversial forms of AI implementation is the use of autonomous weapons, which are weapon systems capable of selecting and attacking targets without direct human involvement (Sianturi, 2023). These autonomous weapons raise concerns about human control over lethal force and the risk of decision-making errors that may endanger civilians (Sidauruk, 2019). The use of this technology in the context of counter-terrorism raises serious questions about legal responsibility in the event of violations or targeting errors. The international community is also divided in responding to the use of autonomous weapons, as although operationally efficient, this technology is highly prone to misuse. Indonesia, as a state governed by law, needs to respond to this development critically and cautiously.

The main challenge faced is the legal gap in regulating the use of AI technology, particularly in the form of autonomous weapons (Wahyudi, 2025). The existing legal system has yet to explicitly regulate the limits or legal responsibilities in the use of such technology in the context of national security (Najwa, 2024). Law No. 5 of 2018, which serves as the legal foundation for counter-terrorism, does not contain provisions on the use of AI or autonomous

weapons (Paamsyah, 2023). Similarly, Law No. 3 of 2002 on State Defense still adopts a traditional approach in addressing threats and national defense (Puslatpur, 2023). This mismatch indicates that Indonesian regulations are not yet capable of accommodating advanced technological developments that have significant implications for human rights and global security.

In addressing this challenge, legal theory that is responsive to technological developments becomes highly relevant as a framework (Majid, 2021). This theory emphasizes the importance of an adaptive and progressive legal system in responding to rapid social and technological change (Pramono, 2021). The law is not only a tool to stabilize society but must also be able to facilitate innovation without sacrificing fundamental principles of justice and human rights. This approach aligns with the concept of legal tech, in which the law must not lag in regulating the use of digital technology, including AI (Mania, 2023). Legal thinking must evolve in parallel with technology so that legal protection remains effective and not merely symbolic.

Artificial intelligence in the context of national security is not just a technical tool but has become an integral part of defense strategy. AI is used to detect, analyze, and respond to various forms of threats, whether domestic or foreign (Gaire, 2023). In this case, AI does not stand alone but is integrated into a broader security system, including communication, logistics, and operational systems (Zhang, 2021). This development creates a need to reevaluate the boundaries between human and machine roles in strategic decision-making. Artificial intelligence is not merely a tool, but a new actor that can determine the direction of security policy if not properly regulated.

One important aspect of this discourse is the distinction between fully autonomous weapons and semi-autonomous weapons. Semi-autonomous weapons still rely on human authorization in final decision-making, while fully autonomous weapons can carry out missions independently based on specific algorithms (Riani, 2025). This distinction is crucial because it concerns legal responsibility in case of violations. In the context of international humanitarian law, clarity in the chain of command and responsibility is essential to ensure accountability (Sarjito, 2023). However, when algorithms become the main decision-makers, these principles become blurred and difficult to apply.

Existing national legal instruments are currently insufficient to regulate the role of AI in the defense context. The ITE Law, for example, mainly regulates electronic transactions and personal data protection, and does not cover the operational aspects of AI use in military or security contexts (Respati, 2024). The Law on the Management of National Resources also focuses more on human and material resources, without specifically addressing the role of autonomous technology. The absence of legal norms regulating AI as part of security strategy creates a grey area that is vulnerable to abuse. This is a strong signal for lawmakers to begin formulating legal instruments that are appropriate to the challenges of the digital era.

At the international level, various agreements and conventions have sought to regulate the use of technology in armed conflict, one of which is the Geneva Convention and its Additional Protocols. Principles such as proportionality, distinction between combatants and civilians, and the obligation to avoid unnecessary suffering remain the main foundation in the use of military force. However, these instruments have not explicitly regulated new technologies such as autonomous weapons. Debates at the UN regarding LAWS indicate that the international community is still seeking a meeting point between technological progress and humanitarian protection. Indonesia needs to be active in these forums to ensure that national interests and humanitarian principles are preserved.

The discourse on AI and autonomous weapons in the context of counter-terrorism cannot be separated from the principles of International Humanitarian Law (IHL) and International Human Rights Law (IHRL). These two legal regimes form the basis for assessing the legitimacy of state actions in responding to threats with armed force. The use of AI that

potentially violates the right to life and the principle of non-discrimination must be critically examined through the lens of international law (Lush, 2023). Commitment to human rights and humanitarian law serves as the moral and juridical filter that determines whether a technological innovation can be justified within the modern legal system. Indonesia, as a country that upholds humanitarian values, must ensure that the use of AI in defense remains within a just and responsible legal framework.

METHOD

This research uses a normative juridical method, which emphasizes the analysis of applicable positive legal norms and legal literature relevant to the research topic. This method is used to examine how national legislation and international legal instruments respond to the development of artificial intelligence technology, particularly in the context of counter-terrorism and the use of Autonomous Weapons Systems (AWS). This study examines the legal substance of laws such as Law No. 5 of 2018 on the Eradication of Criminal Acts of Terrorism, Law No. 3 of 2002 on State Defense, Law No. 11 of 2008 in conjunction with Law No. 19 of 2016 on Information and Electronic Transactions, and Law No. 23 of 2019 on the Management of National Resources. In addition, this study also refers to international legal provisions, including the principles of International Humanitarian Law and discourse in forums such as the United Nations Convention on Certain Conventional Weapons (UN CCW). The data collection technique is carried out through library research, referring to legal documents, scientific journals, international organization reports, and academic publications that discuss the technological, ethical, and legal aspects of AI and AWS. Data analysis is conducted qualitatively with a systematic approach to legal structures and regulatory gaps, in order to formulate coherent and in-depth arguments on the urgency of legal reform in facing technological disruption in the national security sector.

RESULT AND DISCUSSION

Transformation of Counter-Terrorism Strategies through Artificial Intelligence

Indonesia's counter-terrorism strategy was initially rooted in a conventional approach based on law enforcement and open military operations. After the 2002 Bali Bombing, this approach was reinforced by the establishment of the Special Detachment 88 Anti-Terror Unit, which combined militaristic and intelligence elements. Repressive actions became the main characteristic, supplemented by social and religious deradicalization efforts. However, with the development of technology-based terrorism tactics, this traditional approach began to face limitations in reaching cyberspace and highly dynamic global networks. The counter-terrorism strategy then began to shift toward digital methods, utilizing information technology and data analytics in efforts to prevent and respond early to threats.

A major change in this approach is evident in the use of data mining and big data as primary tools for collecting and analyzing information from various sources, including social media and digital communications. Patterns of communication, online behavior, and relationships among individuals in terrorist networks can be mapped and modeled using artificial intelligence. Machine learning algorithms can be trained to detect signs of radicalization or potential attacks based on historical data sets. The use of this technology enables early detection of individuals or groups displaying involvement patterns in terrorist activities. This paradigm shift creates a strategic advantage for the state in responding to threats that are no longer linear or merely physical in nature.

The application of AI in national security strategy includes various forms and mechanisms. One of the most prominent is the integration of AI in public surveillance systems, such as facial recognition-based CCTV, which can identify individuals in a crowd with high precision. AI is also used in tracking online activities, especially in monitoring extremist

content spread across the internet and social media. This technology works automatically to filter, flag, and even report suspicious activities to law enforcement. These systems are not only passive but can also provide early warnings and predict attack patterns based on real-time data. This accelerates the decision-making process and response to potential threats.

Several institutions in Indonesia have already begun applying AI technology in their operations. The National Counter-Terrorism Agency (BNPT), for example, has collaborated with other ministries and institutions to monitor terrorist propaganda in digital media. The State Intelligence Agency (BIN) is known to have developed AI-based automatic detection systems to anticipate threats from radical groups, both domestic and those connected to transnational networks. Regionally, Indonesia is also involved in technology-based intelligence cooperation with ASEAN countries, including sharing information obtained through intelligent surveillance systems. This collaboration strengthens Indonesia's position in addressing cross-border threats that are digital and decentralized in nature.

The effectiveness of AI in counter-terrorism can be seen from several international case studies. Countries such as the United States, the United Kingdom, and Israel have utilized AI to proactively detect terror networks before actions are carried out. Programs like Palantir in the US are capable of analyzing data from various agencies to build risk models and provide operational recommendations to security forces. In Europe, AI algorithms are used to detect individuals showing signs of digital radicalization before they commit actual attacks. Findings from these cases show that AI can enhance predictive and responsive capabilities compared to conventional reactive methods. These systems have also proven effective in significantly reducing the number of attacks in the medium term.

In the context of counter-radicalization, AI also plays a promising role. This technology is used to map extremist narratives and compare them with deradicalization content to assess the effectiveness of digital campaigns. This approach allows relevant institutions to tailor deradicalization messages more precisely based on measurable data. For example, through sentiment analysis and content distribution networks, AI can identify key target groups and monitor the spread of radical ideologies within online communities. This data-based approach makes counter-radicalization programs more strategic and evidence-based, rather than merely normative or assumption-driven.

The use of AI is also crucial in cyber surveillance, particularly in detecting cyberattacks designed to spread terror doctrines or recruit members online. Many terrorist groups today use social media platforms or the dark web to conceal their communications. AI is used to read anomalies in data traffic, detect the use of certain codes or ciphers, and track suspicious transactions that may lead to terrorist financing. This surveillance is not only aimed at preventing attacks but also at identifying the digital ecosystem that supports the existence of radical groups. This technology serves as a vital bridge between the virtual world and law enforcement actions in the real world.

Although AI offers great potential in combating terrorism, there are serious challenges that must be considered to ensure its use remains within legal and ethical boundaries. One major challenge is the accuracy of algorithms, which can still be biased or erroneous in identifying individuals, potentially causing misidentification and human rights violations. In addition, AI systems require vast and sensitive data, which, if not managed properly, could lead to privacy breaches. The security of the AI systems themselves must also be guaranteed to prevent exploitation by malicious actors for the opposite purpose. Despite its advanced technology, final decisions must still lie in human hands as a form of legal accountability.

The digital transformation in counter-terrorism strategy opens new opportunities to safeguard national security with a more precise and measurable approach. The integration of AI into security systems is no longer an option but a necessity, in line with the increasing complexity of threats that are difficult to predict manually. The human role remains essential

as the main decision-maker and controller of the autonomous systems being developed. The combination of technology and strategic thinking becomes the key to creating a defense system that is not only technically robust but also grounded in legal and humanitarian principles. Indonesia must continue to build adequate capacity and regulation to ensure that this transformation proceeds fairly, efficiently, and responsibly.

Legal Gap Issues in the Use of Autonomous Weapons System (AWS)

Autonomous weapons systems (AWS) are weapon systems capable of selecting and attacking targets independently, without direct human involvement in the final decision-making process. This technology is designed with complex algorithms and artificial intelligence that enable the weapon to assess battlefield situations, identify threats, and execute military actions automatically. In the context of military or counter-terrorism operations, this capability brings unprecedented operational efficiency. However, major legal concerns arise regarding who is legally responsible if an AWS makes an error, attacks civilian targets, or causes disproportionate harm. The question of accountability becomes increasingly complex when no human directly gives the order to attack.

In Indonesia, there is no legal regulation that specifically addresses the development or use of AWS. Law No. 3 of 2002 on State Defense and Law No. 5 of 2018 on the Eradication of Criminal Acts of Terrorism still operate within the framework of conventional threats. These regulations do not anticipate the use of AI-based weapons systems capable of acting independently, including in emergency contexts or without a direct connection to an operator. The absence of clear norms creates a significant legal vacuum, particularly in procedural aspects and accountability if AWS is deployed in warfare or counter-radicalization operations. This opens the door to inconsistent legal interpretations and potential violations of fundamental rule-of-law principles.

The mismatch between national legal norms and military technological developments is also evident in the absence of rules that explain the technical limitations of automated systems in armed conflict or internal security. The Defense Law only outlines basic principles of national defense without addressing technical aspects such as weapon system autonomy. Meanwhile, the Terrorism Law tends to emphasize human actions and conspiracies between individuals, not artificial entities acting independently. This situation creates a gap in legal responsibility if violations occur through AWS usage, including when the technology is deployed in domestic terrorism responses. Legal updates are needed that are not only responsive to technological developments but also proactive in establishing ethical and legal boundaries.

In international forums, the use of AWS has triggered extensive debates regarding the morality and legality of its use, especially within the scope of international humanitarian law. The Convention on Certain Conventional Weapons (CCW) under the United Nations has become the primary platform for global discussions on banning or restricting AWS. Many countries are pushing for a moratorium or a new international agreement to regulate the use of such systems, given the lack of a binding global consensus. Some argue that the use of AWS without direct human control could violate basic humanitarian principles that underpin the laws of war. Issues of "machine accountability" and potential violations of international law have become focal points in numerous conferences and joint statements by member states.

International humanitarian law principles such as distinction, proportionality, and precaution face significant challenges in the context of AWS use. The system's ability to differentiate between combatants and non-combatants remains highly questionable, especially in urban warfare or asymmetric conflicts. Target misidentification by autonomous systems can lead to civilian deaths and large-scale destruction of civilian infrastructure. Furthermore, ensuring that AWS actions are always proportional to the actual threat is difficult, especially

since decision-making algorithms are not transparent. This raises serious questions about how international legal principles can be applied to non-human entities.

The use of AWS also carries high risks to human rights, particularly the right to life and the right to protection from arbitrary treatment. In non-conflict contexts such as domestic counter-terrorism, the deployment of AWS may violate civilian rights if the technology executes fatal actions based on inaccurate data or assumptions. Additionally, there is concern that such systems could be used as repressive tools by states against specific groups without public oversight or accountability. The situation becomes even more complex if there is no strict control mechanism over the use of such technology in civilian contexts. The issue is not only about the potential for human rights violations but also the absence of legal avenues for victims to seek justice.

The potential dysfunction of AI in autonomous weapon systems is both a technical and ethical problem that cannot be ignored. AI systems can misread data, suffer algorithmic failures, or be subject to cyberattacks that alter their behavior into aggression without justification. In such situations, there is no guarantee that the system will comply with applicable orders or legal norms. The lack of human oversight in the decision-making process renders AWS systems inherently unaccountable. This creates unpredictable risks that could have widespread impacts on societal stability and security.

AWS also presents a moral dilemma in both military and civil legal contexts. When weapons have full autonomy to decide when and whom to attack, concerns arise about the removal of humanity from conflict. The decision-making process concerning life and death should be a human responsibility, not that of a machine. Delegating this responsibility to an algorithm undermines the fundamental values of justice and human dignity that form the foundation of both international and national law. Machines lack empathy, moral judgment, and awareness of the consequences of their actions.

Regulations governing AWS must be anticipatory, not merely reactive. Such regulations need to establish technical, procedural, and legal parameters to ensure that the use of this technology remains within the boundaries of humanity and public interest. Indonesia, as a democratic country that upholds human rights and the rule of law, has a vested interest in formulating clear and comprehensive policies regarding AWS. These policies must include aspects of accountability, oversight, and limitations in its use, both in conflict situations and in counter-terrorism operations. The formulation of such legal norms is essential to ensure that technological advancement does not compromise the legal values that serve as the nation's guiding compass.

CONCLUSION

The transformation of counter-terrorism strategies through artificial intelligence has ushered in a new era in national security, characterized by efficiency, speed, and precision in addressing terrorist threats. Artificial intelligence has proven capable of strengthening intelligence systems, expanding surveillance reach, and enhancing predictive capabilities related to potential radicalization and attacks. However, the use of advanced technologies such as autonomous weapons systems also brings significant challenges, particularly in the legal domain. The absence of clear norms and regulations in both national and international law creates gaps that can be exploited without control, potentially harming civil rights, undermining humanitarian legal principles, and weakening institutional accountability. This development demands the formulation of legal policies that are not only adaptive but also grounded in the principles of humanity and the rule of law.

The legal gaps accompanying the use of AI and AWS in national security must be addressed through a visionary normative approach. The Indonesian government needs to update and harmonize legal instruments, both by revising relevant laws and by formulating

implementing regulations that explicitly govern the limits, responsibilities, and oversight mechanisms of autonomous technology. Furthermore, active participation in international forums related to AWS regulation is essential to advocate for accountability and humanitarian principles within the global framework. Collaboration among the state, academia, and civil society is also crucial to ensure that technological sophistication does not become a tool of uncontrolled violence, but rather functions as an instrument of protection, justice, and peace. Through a responsive and ethical legal approach, the use of artificial intelligence can be directed toward a more humane and responsible future in counter-terrorism efforts.

REFERENCES

Astuti, S. A. (2024). Literasi Kemanfaatan Teknologi terhadap Cyber Terrorism di Era Disrupsi dengan AI (Artificial Intelligence). *Indonesian Journal of Criminal Law and Criminology (IJCLC), 5(3)*.

Farid, I. R. (2023). Pemanfaatan Artificial Intelligence Dalam Pertahanan Siber. *Nusantara: Jurnal Ilmu Pengetahuan Sosial, 10(2)*, 779-788.

Gaire, U. S. (2023). Application of artificial intelligence in the military: An overview. *Unity Journal, 4(01)*, 161-174.

Lush, E. (2023). The view through a different lens: Increasing respect for international humanitarian law through the use of the international human rights law framework. *Journal of International Humanitarian Legal Studies, 14(1)*, 95-129.

Majid, A. (2021). Studi tentang Wacana Hukum Responsif dalam Politik Hukum Nasional di Era Reformasi. *Dinamika Hukum, 12(1)*.

Mania, K. (2023). Legal technology: assessment of the legal tech industry's potential. *Journal of the Knowledge Economy, 14(2)*, 595-619.

Najwa, F. R. (2024). Analisis Hukum Terhadap Tantangan Keamanan Siber: Studi Kasus Penegakan Hukum Siber di Indonesia. *AL-BAHTS: Jurnal Ilmu Sosial, Politik, dan Hukum, 2(1)*, 8-16.

Nirmala, A. Z. (2024). Pre-Crime dan Teknologi: Mengantisipasi Terorisme Sebelum Terjadi di Indonesia. *Jurnal Kompilasi Hukum, 9(2)*, 169-177.

Paamsyah, J. I. (2023). Upaya Penanggulangan Tindak Pidana Terorisme Di Indonesia. *Innovative: Journal Of Social Science Research, 3(6)*, 2973-2985.

Pramono, B. (2021). Law Enforcement of Indonesian National Army (TNI) Soldiers with a Progressive Legal Approach. *Hang Tuah Law Journal*, 30-42.

Puslatpur, P. P. (2023). Kedudukan Dan Fungsi Komponen Cadangan Dalam Memperkuat Sistem Pertahanan Negara Ditinjau Dari Uu Nomor 3 Tahun 2002 Tentang Pertahanan Negara. *LEX PRIVATUM, 11(5)*.

Putra, M. A. (2024). INTEGRASI KECERDASAN BUATAN DALAM BERBAGAI SEKTOR: DAMPAK, PELUANG, DAN TANTANGAN. *Jurnal Cakrawala Ilmiah, 3(12)*, 3831-3838.

Respati, A. A. (2024). Reformulasi UU ITE terhadap Artificial Intelligence Dibandingkan dengan Uni Eropa dan China AI Act Regulation. *JURNAL USM LAW REVIEW, 7(3)*, 1737-1758.

Riani, E. A. (2025). IMPLIKASI ETIS PENGGUNAAN KECERDASAN BUATAN DALAM SISTEM SENJATA OTONOM: TANTANGAN DAN TANGGUNG JAWAB MORAL DI ERA PERANG MODERN. *NUSANTARA: Jurnal Ilmu Pengetahuan Sosial, 12(1)*, 256-262.

Rifky, S. K. (2024). *Artificial Intelligence: Teori dan Penerapan AI di Berbagai Bidang*. Jambi: PT. Sonpedia Publishing Indonesia.

Sarjito, A. (2023). Sinkronisasi Kebijakan Pertahanan dalam Operasi Militer dengan Hak Asasi Manusia. *Journal of Governance and Policy Innovation, 3(2)*, 17-41.

Sianturi, D. M. (2023). Tantangan Penggunaan Artificial Intelligence Dalam Hybrid Warfare. *Innovative: Journal Of Social Science Research, 3(5)*, 9984-9996.

Sidauruk, S. M. (2019). Penggunaan Autonomous Weapons System Dalam Konflik Bersenjata Internasional menurut Hukum Humaniter Internasional. *Diponegoro Law Journal, 8(2)*, 1489-1505.

Sumarno, I. A. (2025). *Manajemen Pertahanan Modern: Tantangan Modernisasi Militer dan Integrasi AI.* Bandung: Indonesia Emas Group.

Wahyudi, B. R. (2025). Tantangan Penegakan Hukum terhadap Kejahatan Berbasis Teknologi AI. *Innovative: Journal Of Social Science Research, 5(1)*, 3436-3450.

Zhang, C. &. (2021). Study on artificial intelligence: The state of the art and future prospects. *Journal of Industrial Information Integration, 23*, 100224.