Contemporary Readings in Law and Social Justice
ISSN: 1948-9137, e-ISSN: 2162-2752
Vol 15 (02), 2023
pp. 649 – 655

Legal analysis of the role of artificial intelligence in achieving and ensuring regional and international order and security

Shahriar Heidari Moghadam[1], Alireza Arashpour*[2]

1. Ph.D Student, Department of Public International Law, Najafabad Branch, Islamic Azad University, Najafabad, Iran.
2. Associate Professor, Department of Law, University of Isfahan, Isfahan, Iran. (Corresponding author).

Email: a.arashpour@ase.ui.ac.ir

Abstract

In the digital age, artificial intelligence (AI) plays a significant role as a transformative technology in various fields, including international security and human rights. With its predictive, data analysis, and crisis management capabilities, this technology can help improve the efficiency of international institutions, prevent conflicts, reduce security tensions, and promote the implementation of international law. The use of AI in the military, cybersecurity, and preventive diplomacy fields has been able to accelerate and make decision-making more efficient. However, the widespread use of AI has brought with it numerous legal and ethical challenges. These challenges include determining legal responsibility for actions resulting from algorithmic decisions, its impact on national sovereignty, the increased likelihood of algorithmic discrimination, and the risks of improper or uncontrolled use of this technology in armed conflicts. In addition, the lack of transparency in the decision-making process of AI and excessive dependence on it can weaken the fundamental principles of international law and reduce the role of governments and international institutions in ensuring order and security. This article uses an analytical-descriptive method and uses library resources and, with the aim of providing a comprehensive framework for regulating and monitoring the use of AI in international security, examines the applications of this technology, its legal and ethical challenges, and proposed solutions to ensure its responsible and sustainable use. In this regard, the role of international instruments, human rights principles, and monitoring mechanisms to reduce risks and enhance the effectiveness of the international legal system in dealing with AI is analyzed.

Keywords: Artificial Intelligence, International Law, World System

Received: 16 November 2023 **Revised:** 21 December 2023 **Accepted:** 29 December 2023

Introduction

In the contemporary world, artificial intelligence, as one of the most advanced technologies of the 21st century, has not only brought about profound changes in the economic, social and cultural spheres, but also plays a pivotal role in shaping international order and security. Artificial intelligence, defined as systems capable of performing tasks that usually require human intelligence, such as learning, decision-making and prediction, is now used in various fields including defense, surveillance, diplomacy and even cyber warfare. With its capabilities in processing big data and analyzing patterns, this technology can help to realize international order, but at the same time it also brings serious legal challenges. Legal analysis of the role of artificial intelligence in ensuring international security requires examining how this technology interacts with the principles of international law, including the sovereignty of states, human rights and humanitarian law. In this introduction, we first discuss the importance of artificial intelligence in today's world, then

examine its role in international security, and finally discuss the legal challenges and the need for regulatory regulation.

Artificial intelligence, which dates back to the 1950s, has become a strategic tool today thanks to advances in computing and machine learning algorithms. According to international reports, AI could increase global economic growth by 14 percent by 2030, but this growth comes with security risks. In the field of international security, artificial intelligence can act as a facilitator. For example, in defense systems, AI is able to predict threats and provide faster responses, such as using detection algorithms in border surveillance or analyzing satellite data to identify suspicious activities. The technology also plays a role in diplomacy; Where AI tools are used to analyze big data to make predictions about political crises. However, this role is dual: on the one hand, AI can enhance security, such as in the fight against terrorism by identifying behavioral patterns, and on the other, it can act as a tool to breach security.

In the legal context, the role of AI in international security is tied to the fundamental principles of international law. Public international law, which is based on the UN Charter and the Geneva Conventions, emphasizes the maintenance of peace and security. AI, entering military arenas, raises challenges such as accountability in the use of autonomous weapons. Legal analyses show that the lack of adequate regulation in this area can lead to violations of human rights, including the right to privacy, freedom of expression and non-discrimination. In the European Union, AI legislation has attempted to regulate high-risk systems, but national security exemptions have created loopholes that could lead to human rights abuses. In addition, AI has profound geopolitical implications. The competition between great powers such as the United States, China and Russia to master AI technology has become a "new Cold War". Leaders such as Vladimir Putin have asserted that the country that dominates AI will rule the world. This competition has not only led to an AI arms race, but also highlights the need for international legal frameworks. Reports from the 2023 AI Security Summit at Bletchley Park, attended by 30 countries, stress the need for risk assessment and ongoing oversight. From a legal perspective, this requires updating existing institutions such as the United Nations, where efforts to ban autonomous weapons have so far failed. AI can also undermine global security through asymmetric threats, such as use by terrorist groups for biological or cyber attacks. Key legal challenges in this area include a lack of transparency, accountability and governance. AI often acts as a "black box", where its decision-making process is unclear, making it difficult to attribute responsibility in cases of violations of international law. For example, if an AI system causes a cyberattack, it will be complex to determine whether this action violates the principle of non-interference in the internal affairs of States (Article 2(4) of the UN Charter). Comparative analyses show that national approaches, such as those in Israel, which focus on innovation but lack binding mechanisms, can undermine regional security.

Internationally, efforts are underway to regulate AI. The Council of Europe Convention on AI, which focuses on human rights but excludes national security systems, demonstrates a weakness in comprehensive coverage. The European Union has classified systems by risk with its AI law and banned the use of real-time biometric systems in public spaces, but security exceptions remain. China, with an approach focused on national security, has enacted specific laws for AI, which focus on security content. In the United States, the federal approach emphasizes safety and security, but varies under different governments. Organizations such as the OECD and the G7 have provided guiding principles, such as safety, transparency, and accountability, that could form the basis for international law. The need for legal analysis in this area stems from the fact that AI is not only a tool, but also has the potential to change the global power structure. This technology can help to shape international order, such as in anticipating environmental crises or managing migration, but without strong legal frameworks, its risks – including the erosion of sovereignty and the rise of inequalities – could threaten global security. This analysis will therefore focus on examining the role of AI within the framework of international law, highlighting the need for new treaties similar to the Nuclear Non-Proliferation Treaty.

Theoretical foundations and research background

Artificial Intelligence (AI), as one of the most advanced technologies of the 21st century, is playing an increasing role in shaping international relations. This technology not only provides new tools for

surveillance, decision-making and military operations, but can also strengthen or weaken international order and security. A legal analysis of the role of AI in achieving and ensuring international order and security requires an examination of the theoretical foundations, existing legal frameworks and challenges ahead. This article examines this issue based on authoritative legal sources and international reports. The aim is to provide a comprehensive analysis that shows how AI can act as a dual tool: on the one hand, a enhancer of peace and security, and on the other, a source of new threats. (SIPRI, 2025).

International order refers to the set of rules, institutions and relationships that regulate the interactions of states, while international security focuses on preventing threats to global peace. AI, with its capabilities such as machine learning, big data analytics, and automated decision-making, has the potential to transform these areas. However, the lack of comprehensive legal frameworks for AI has raised concerns about its misuse.

Artificial Intelligence in International Law

The theoretical foundations of AI in international law are rooted in general principles such as state sovereignty, non-intervention, and human rights. As a dual technology, AI has both peaceful and military applications. From a legal perspective, AI can be analyzed under existing frameworks such as the Treaty on the Non-Proliferation of Nuclear Weapons (NPT) or the Biological Weapons Convention, but require specific provisions (UN High Commissioner for Human Rights, 2023).

One key foundation is the concept of "State responsibility" in international law. According to Article 1 of the Statute of the International Court of Justice, states are responsible for their actions, but with AI, the attribution of actions to states becomes complicated. For example, if an automated AI system causes harm, is the state liable? Analysis shows that AI can disrupt sovereignty, particularly in the areas of lawmaking and law enforcement (OUP, 2025).

In international relations theories, realism emphasizes that AI can change the balance of power, as in the nuclear arms race. Liberalism focuses on international cooperation to regulate AI, such as initiatives by the OECD and UNESCO, which also examine the role of AI in shaping social norms, where AI can amplify disinformation and threaten security (Al-Kindi Publishers, 2025).

From a legal perspective, AI in international security can be used as a tool to predict conflicts. AI models can identify threat patterns by analyzing big data, but this raises privacy issues. The CNAS (2018) report notes that AI can strengthen anti-money laundering operations and improve international financial security.

In addition, theoretical foundations include the ethics of AI. Principles such as transparency, fairness, and accountability are highlighted in international documents such as the UNESCO Recommendation on the Ethics of AI (2021). These principles can be the basis for ensuring an international order where AI becomes a tool for peace rather than a threat.

The role of AI in realizing international order:

The international order is based on the principles of the UN charter, such as maintaining peace and cooperation. AI can play a positive role in realizing this order. For example, in the field of diplomacy, AI provides tools such as sentiment analysis to predict crises. The Stanford Report (2025) shows that AI can enhance intelligence analysis in the space domain and report on space threats.

In foreign policy, AI is changing geopolitical structures. Countries such as China and Russia have national AI strategies that affect the balance of power. Putin has stated that leadership in AI means governing the world. It can replace open political systems and push governments towards digital strategies.

In addition, AI in global institutions such as the UN can be used to monitor compliance with treaties. For example, AI can analyze satellite data to detect violations of nuclear treaties. This role in achieving order is associated with reducing the risk of conflict, but requires international consensus.

In the economic sphere, AI can facilitate international trade, but it creates challenges such as inequality. Legal analysis suggests that AI can help resolve trade disputes through predictive models, but WTO regulations need to be updated.

The role of AI in human rights is also key. AI can improve the monitoring of war crimes, but its misuse can violate rights. The European Union has attempted to ban high-risk applications, such as social scoring systems, with the AI Act (2024) (PJ Criminology, 2024).

The Role of Artificial Intelligence in Ensuring International Security

International security encompasses military, cyber, and non-traditional threats. AI in ensuring security can provide advanced defensive tools. For example, AI systems in cybersecurity can predict and repel attacks. The CNAS report emphasizes that AI can enhance counterterrorism operations (CNAS, 2018).

In the military domain, autonomous weapons (AWS) can reduce human risk, but they also create threats such as lack of control. In the war in Ukraine, AI has been used to make autonomous decisions. International humanitarian law (IHL) distinguishes between civilians and combatants, but AI can make mistakes.

AI also plays a role in biosecurity. AI tools can design viruses, which are a threat to global security. The low cost of these tools (e.g. $100,000 to recreate a virus) empowers terrorists (Al-Kindi Publishers, 2025).

Globally, the US-China competition in AI is shaping security. China has an advantage in data, while Russia focuses on weapons. The SIPRI report (2025) points to the need to manage the risks of military and civilian AI.

AI could help in space AI, where it analyzes space-based threats (Stanford, 2025). This role in ensuring security comes with benefits such as early warning.

Legal challenges and proposed regulations

Legal challenges to AI include a lack of adequate regulation in national security and the private sector (PJ Criminology, 2024). These gaps allow unchecked use.

Transparency and accountability are key. AI reduces transparency in automated decision-making. Recommendations include mandatory human oversight and stakeholder engagement.

At the international level, initiatives such as the AI Safety Summit (2023) and the independent AI Security Report provide a basis for policy (Al-Kindi Publishers, 2025). International law prohibits AI from violating sovereignty (Just Security, 2025.(

Another challenge is the impact on human rights. AI can enable mass surveillance and create discrimination. The Council of Europe Convention emphasizes human rights, but its implementation is optional.

In recent years, the role of artificial intelligence (AI) in international legal areas, especially in realizing and ensuring global order and security, has attracted the attention of scholars. This technology not only provides new tools for monitoring and anticipating threats, but also raises new legal challenges such as accountability, the rule of international law, and security risks.

The technology not only provides new tools for monitoring and predicting threats, but also raises new legal challenges such as accountability, the rule of international law, and security risks.

One key study in this area is examining the impact of AI on international law and global power. Maas (2019) argues that AI can lead to legal development (i.e., the creation of new laws), legal displacement (replacing existing laws), or even the destruction of international legal structures, as AI's characteristics, such as lack of transparency and rapid development, make it difficult to enforce traditional laws. This analysis suggests that AI may create global gaps and highlight the need to adapt international law.

In the area of international security, Horowitz et al. (2018) examine the applications of AI in defense, intelligence, homeland security, and diplomacy. They emphasize that AI can enhance state instruments, but

also bring risks such as economic disruption and political instability, which require integrated strategies to ensure global security. This study focuses on the role of AI in changing the global balance of power.

Puscas (2023) presents a taxonomy of AI risks to international peace and security, analyzing technical risks (such as safety and cybersecurity) and global risks (such as miscalculation and escalation of conflicts). He suggests that international confidence-building measures are necessary to mitigate these risks, which strengthens the legal aspect of ensuring global order.

Bexheti (2025) examines the role of AI in foreign policy and international security, emphasizing its impact on geopolitical structures. Referring to initiatives such as the EU's Artificial Intelligence Law, he argues that AI can ensure security, but requires international cooperation to prevent misuse.

Dias and Sagoo (2024) introduce international law as a starting point for AI in times of uncertainty. They emphasize that human rights principles and public international law can regulate AI, without the need for new treaties, and that this approach can protect the global order from AI risks such as disinformation and cyberattacks.

Finally, Dulka (2023) analyzes the application of AI in international human rights and examines its benefits and risks in monitoring rights violations. He proposes a cost-benefit framework for assessing the use of AI, which can help ensure global security and order from a legal perspective.

This background suggests that AI has the dual potential to enhance and threaten international order and security, and its legal analysis requires multifaceted approaches.

This background suggests that AI has the dual potential to enhance and threaten international order and security, and its legal analysis requires multi-pronged approaches.

Proposals include extending registration and oversight to the private sector, eliminating double standards (such as the EU's ban on AI exports), and establishing binding ethical principles.

AI has great potential to bring about international order and ensure security, but its legal challenges require urgent action. By developing international frameworks, the benefits can be maximized and the risks minimized. The future of AI in security depends on global cooperation.

Research Methodology

This research aims to conduct a legal analysis of the role of artificial intelligence (AI) in realizing and ensuring international order and security. The research topic is in the field of international law and focuses on examining the legal impacts, challenges and opportunities of AI in areas such as cybersecurity, autonomous weapons, international monitoring and treaty enforcement. The research methodology is based on standard approaches in legal research, which include a combination of descriptive, analytical and comparative methods. These methods have been selected based on a review of the existing literature in the field of AI and international law (such as reports from the United Nations, the European Union and academic articles.

Research Findings

The research on the legal analysis of the role of artificial intelligence (AI) in realizing and ensuring international order and security, based on a review of legal sources, international reports and academic articles, shows the dual impact of this technology. AI, as a transformative tool, can increase the efficiency of international institutions, but at the same time it poses serious legal and security challenges. The following is a summary of the key findings based on positive aspects, risks and legal implications:

.1The positive role of AI in strengthening international security and order:

o AI provides predictive capabilities, big data analytics, and crisis management that help prevent conflicts, reduce security tensions, and better enforce international law. For example, in the military, cybersecurity, and preventive diplomacy domains, AI makes decision-making faster and more efficient. Also, the

application of AI to traditional weapons systems and cyber operations improves performance and can be used in predictive tools or large language models for more accurate information.

o In the context of human rights and global security, AI can help protect fundamental rights, such as monitoring violations or anticipating humanitarian crises, but this requires compliance with the principles of international humanitarian law (IHL.(

.2Security and legal challenges and risks:

o Technological and operational risks: AI faces risks such as safety (failure in unexpected circumstances), cyber (data poisoning or adversarial attacks) and human-machine interaction (such as automation bias or overconfidence). These risks can lead to miscalculation, escalation of conflicts (such as in nuclear systems) and proliferation of weapons (convergence with biology or chemistry to design pathogens). Also, in armed conflicts, AI transforms the traditional structure of warfare and creates challenges such as identifying the use of force in cyberspace, respecting the principles of separation, proportionality and necessity.

o State responsibility and legal challenges: International state responsibility is defined based on attributable conduct and breach of obligations (such as the prohibition on the use of force in Article 2, paragraph 4 of the UN Charter). But in AI-based cyberattacks, (agent identification) is difficult and can lead to violations of sovereignty, non-interference or human rights. Challenges such as algorithm transparency, algorithmic discrimination and over-reliance on AI undermine the principles of international law.

o Impact on human rights and job security: AI has adverse effects such as threatening the job security of vulnerable groups, violating privacy and increasing inequalities. In the field of counter-terrorism, the use of AI should be accompanied by sensitivity to rights such as freedom of expression and association.

.3Existing legal frameworks and the need for development:

o Public international law, humanitarian law and customary law (such as treaties and general principles) apply to AI, but there are gaps such as lack of transparency, the speed of technological development and geopolitical competition. For example, the US and the EU have different approaches: the US focuses on voluntary assessments, while the EU has established more extensive regulations. International organizations such as the United Nations play a pivotal role in setting standards and cooperation.

Conclusion

Artificial intelligence has great potential to strengthen international order and security by improving decision-making, crisis prevention and law enforcement, but its risks – including conflict escalation, accountability challenges and human rights violations – require responsible legal approaches. The lack of transparency and dependence on AI could diminish the role of states and lead to global instability. Therefore, the international community should develop new frameworks, including specific treaties for AI in cyberwarfare, confidence-building measures (such as transparency and information exchange), maintaining human control in critical decision-making and multilateral cooperation through the United Nations. This will not only reduce risks, but also ensure the equitable use of AI and help maintain global security. Ultimately, international law should be the starting point for AI governance to strike a balance between innovation and protection.

Resources

1. SIPRI. (2025). Artificial intelligence and international peace and security. Retrieved from https://www.sipri.org/yearbook/2025/12
2. OUP. (2025). Governance Disruption: How AI Changes International Law. Retrieved from https://academic.oup.com/book/61416/chapter/533870916
3. Al-Kindi Publishers. (2025). The Role of Artificial Intelligence in Foreign Policy and International Politics. Retrieved from https://al-kindipublishers.org/index.php/ijlps/article/download/10953/9933/30513

4. PJ Criminology. (2024). Comparative Legal Analysis of the Role of Artificial Intelligence. Retrieved from https://www.pjcriminology.com/wp-content/uploads/2024/05/58-Comparative-Legal-Analysis-of-the-Role.pdf
5. Stanford. (2025). Leveraging Artificial Intelligence to Empower Intelligence Analysis in the Space Domain. Retrieved from https://law.stanford.edu/2025/08/22/leveraging-artificial-intelligence-to-empower-intelligence-analysis-in-the-space-domain/
6. CNAS. (2018). Artificial Intelligence and International Security. Retrieved from https://www.cnas.org/publications/reports/artificial-intelligence-and-international-security
7. Just Security. (2025). Governing AI Agents Globally. Retrieved from https://www.justsecurity.org/121990/governing-ai-agents-globally/
8. Horowitz, M., Scharre, P., Allen, G. C., Frederick, K., Cho, A., & Saravalle, E. (2018). Artificial Intelligence and International Security. Center for a New American Security (CNAS.(
9. Puscas, I. (2023). AI and International Security: Understanding the Risks and Paving the Path for Confidence-Building Measures. United Nations Institute for Disarmament Research (UNIDIR.(
10. Maas, M. M. (2019). International Law Does Not Compute: Artificial Intelligence and the Development, Displacement or Destruction of the Global Legal Order. Melbourne Journal of International Law.
11. Bexheti, M. S. (2025). The Role of Artificial Intelligence in Foreign Policy and International Security. International Journal of Law and Political Sciences.
12. Dias, T., & Sagoo, R. (2024). AI Governance in the Age of Uncertainty: International Law as a Starting Point. Just Security.
13. Dulka, A. (2023). The Use of Artificial Intelligence in International Human Rights Law. Stanford Technology Law Review.