USES OF ARTIFICIAL INTELLIGENCE IN THE SECURITY AND MILITARY FIELDS: BETWEEN THE DEMANDS OF INNOVATION AND THE LIMITS OF CRIMINAL LIABILITY

Kenza Belhocine *[1], Loubna Hachouf [2], Tahar Zouagri [3]

[1,2;3] Legal, Political and Shariaa research laboratory, University of Khenchela, (Algeria)

Emails : belhocine.kenza@univ-khenchela.dz [1] , loubna.hachouf@univ-khenchela.dz [2], zouagritahar@univ-khenchela.dz [3]

Received: 29/03/2025; Accepted: 12/05/2025; Published: 14/06/2025

Abstract

This research aims to analyze the growing uses of artificial intelligence (AI) in the security and military fields, focusing on balancing the demands of innovation with the limits of criminal liability. Artificial intelligence has become a crucial element in developing defense capabilities through autonomous combat systems, intelligent surveillance, and strategic data analysis. However, this technological advancement raises profound legal and ethical challenges related to determining liability in cases of errors or violations committed by autonomous systems.

The study concludes that traditional rules of criminal accountability are insufficient to address the specific nature of AI, which necessitates reformulating legal frameworks to ensure transparency and accountability. It also calls for the establishment of national and international legislation to regulate the use of such technologies and to strengthen international cooperation to align military innovation with humanitarian and legal principles.

Keywords: Artificial Intelligence, Security and Military Field, Criminal Liability

1. Introduction:

Amid the rapid technological transformations shaping the modern world, artificial intelligence (AI) has emerged as one of the most influential technologies in redefining the contours of human life, as well as the concepts of security and national sovereignty. AI has transcended civilian applications to enter more sensitive domains such as security and defense, where it is now employed in developing smart weapons, managing strategic systems, analyzing intelligence data, guiding military decisions, and even executing field operations of a combat nature. This evolution has raised profound legal and ethical questions regarding the limits of lawful use of such technologies and the scope of responsibility borne by their actors.

The use of AI in the security and military fields represents a double-edged sword: on one hand, it provides advanced analytical and operational capabilities that enhance efficiency, accuracy, and minimize human losses; on the other, it raises complex issues concerning the extent to which these uses align with established legal and humanitarian principles. When intelligent systems gain the capacity to make autonomous decisions — including target identification or the execution of strikes without direct human oversight — questions inevitably arise about who bears criminal responsibility in cases of serious violations or unlawful acts resulting from such automated decisions.

These transformations have created a new reality that exceeds the capacity of traditional legal frameworks to comprehend, particularly regarding the determination of criminal intent and free will — two essential pillars of criminal liability. Can an intelligent system be held accountable for its actions? Or should responsibility fall on the developer, operator, or deploying entity? How can the causal relationship be established between the harmful act and the system's autonomous decision? These are questions that place legal scholarship before unprecedented challenges in redefining the concepts of crime and punishment within a technologically evolving environment characterized by self-learning and autonomous decision-making.

Such issues acquire even greater sensitivity in the military context, given their direct implications for international peace and security. Unrestrained deployment of AI technologies in warfare and military control without precise legal regulation could lead to the exclusion of the human element from combat decision-making — a scenario that conflicts with the core principles of international humanitarian law, notably the principles of distinction between combatants and civilians, and proportionality in the use of force. Moreover, the potential for "intelligent machines" to commit acts that may constitute war crimes or crimes against humanity underscores the urgent need for legal frameworks ensuring accountability and transparency.

At the same time, states seek to strike a balance between the imperatives of innovation and military modernization, and the necessity of preserving legal safeguards that protect individuals and societies from the potential risks of such technologies. This underscores the need to develop specific national and international legislation governing the use of AI in security and defense, including clear definitions of responsibilities, oversight mechanisms, and operational standards that align with principles of justice and humanity.

In light of the foregoing, the central research question can be formulated as follows: **To what extent can technological innovation in the field of artificial intelligence be reconciled with the legal safeguards necessary to establish criminal liability for its use in the security and military domains?**

2. Definition of Artificial Intelligence.

According to the European Commission (2019), artificial intelligence refers to "systems that display intelligent behavior by analyzing their environment and taking actions with some degree of autonomy to achieve specific goals" (Daliou, 2023, pp. 209–210).

The Commission further defined artificial intelligence as "programs that use specific techniques and approaches to address contemporary issues such as intellectual property, focusing on tasks like predictions, recommendations, or decision-making that influence the environments with which they interact." This definition emphasizes the practical applications of artificial intelligence and its impact across various fields.

During the European Year of Youth (2022), the Commission provided a simplified definition, describing artificial intelligence as "a general term covering a range of technologies that enable machines or software to imitate human intelligence" (Daliou, 2023, pp. 209–210). This simplified version makes AI more accessible and easier to understand for the general public.

Accordingly, the following definition can be proposed:{Artificial Intelligence (AI) is an advanced branch of computer science aimed at designing and developing systems capable of simulating human intelligence and performing tasks that typically require complex reasoning—such as learning, analysis, and decision-making. AI involves the use of sophisticated algorithms and machine learning techniques that enable machines to process data, recognize patterns, and adapt to changing conditions. This field is distinguished by its ability to learn from experience and improve performance over time, making it a powerful tool across multiple domains}.

3. The Use of Artificial Intelligence in the Security and Military Fields.

There is no doubt that artificial intelligence represents one of the most significant technological transformations of the 21st century. It has become a strategic priority for states due to its advanced analytical and predictive capabilities, which bring about a qualitative shift across various sectors—particularly in the military field. AI has become a decisive factor in modernizing defense capabilities, developing weapon systems, enhancing operational efficiency, and even transforming the very concept of warfare.

Undoubtedly, major powers' interest in military technology is not new—it dates back to the 20th century, when Britain's development of radar technology during World War II marked a pivotal moment in the use of technology in warfare. With the advancement of AI, modern systems have become capable of performing complex functions that sometimes surpass human capabilities, ushering in a new revolution in the concepts of security and defense.

Below are the main applications of artificial intelligence in the military field:

A. Drone Swarms: Unmanned Aerial Vehicles (UAVs), commonly known as drones, are among the most prominent applications of AI in the military domain—especially when deployed in swarms. These drones are programmed to coordinate and cooperate autonomously, mimicking the behavior of social organisms such as bees.

The true power of drone swarms lies in their ability to exchange real-time information about targets—such as location, direction, wind speed, and threats—while making semi-autonomous decisions on the battlefield. This technology has been vividly demonstrated in the Russia–Ukraine conflict, where Russia employed Iranian-made Shahed drones, while Ukraine utilized Turkish Bayraktar TB2 drones, both serving as effective tools for reconnaissance and precision strikes (Ikram, 2024, pp. 184–188).

B. Algorithmic Bias as a Hidden Weapon: "Algorithmic bias" represents one of the most critical ethical and technical challenges in the use of AI—particularly in military contexts. It can be exploited as a tool for disinformation or to influence enemy decision-making.

The danger of this bias lies in the fact that AI systems may make crucial—or even lethal—decisions based on inaccurate or biased data, potentially leading to disastrous outcomes. Moreover, such systems can be harnessed for digital psychological warfare, amplifying certain narratives or sowing doubt within enemy ranks in preparation for subsequent operations.

C. Military Decision Support: AI plays a fundamental role in enhancing decision-making mechanisms in military environments that require rapid responses under complex and multidimensional information conditions. Through its ability to analyze massive datasets in record time, AI can provide precise recommendations to military leaders, helping to reduce the risks associated with human bias or information shortages.

Additionally, AI systems are used to simulate scenarios and evaluate potential alternatives before making field decisions—while maintaining human oversight as an essential component of the process (Nasreen N., 2025, p. 343).

D. Cybersecurity as a New Battlefield: Cybersecurity has become a core pillar of national security, as even the most advanced military systems are increasingly exposed to cyberattacks aimed at breaching or disabling their infrastructure.

In this context, artificial intelligence provides sophisticated tools for detecting attack patterns and identifying cyber threats at their early stages, allowing for the development of more effective defensive strategie. AI is also employed to predict future attacks by uncovering security vulnerabilities and analyzing abnormal network behavior, thereby strengthening overall cyber defense readiness (Mohamed D., 2023, pp. 604–606).

The significance of this issue was underscored by the "Pager Incident" in Lebanon, September 2024, which represented a complex cyberattack with intelligence and military objectives.

E. Multi-Task Military Robots: Military robots are AI-powered autonomous units designed to perform combat or logistical tasks without exposing soldiers to direct danger.

These include:

- Ground combat robots such as the Russian "Uran-9",
- Robots specialized in explosive ordnance disposal (EOD),
- Reconnaissance robots conducting surveillance missions in hazardous environments.

These machines are distinguished by their ability to navigate difficult terrain and make real-time decisions based on field data (Nasreen S, 2024, p. 870).

F. Robotic Combat Dogs: Robotic combat dogs are among the latest innovations in military robotics, designed to mimic real dogs in movement and intelligence while being equipped with advanced sensors and high combat capabilities.

Notably, the "Spot" robot has entered active service in both the U.S. and French armies, while China showcased its "Robodogs" during the Golden Dragon exercises in May 2024. These robotic dogs are capable of maneuvering, running, climbing, and identifying targets and threat in complex environments (Mahmoud Kamal Al-Bahnasawi, 2025).

G. Autonomous Submarines: Unmanned autonomous submarines represent a leading innovation in maritime artificial intelligence, operating independently underwater without human crews, which both reduces risks and enhances operational efficiency.

The United States pioneered this field with the launch of the "Sea Hunter" in April 2016—an autonomous submarine capable of sailing continuously for months, tracking hostile submarines, and providing accurate intelligence data to command units for strategic decision-making (Mahmoud Kamal Al-Bahnasawi, 2025).

4. The International Legal Framework for Artificial Intelligence in International and Regional Conventions.

International human rights law constitutes an integrated system of international legal norms aimed at protecting and promoting human rights worldwide. These rules are grounded in binding international treaties and conventions that oblige states to respect and safeguard individual rights. They entail legal commitments requiring states to take specific measures to ensure these rights, both in times of peace and during conflict. The principles of international human rights law—especially those of a peremptory (jus cogens) nature—are binding upon all states and cannot be violated under any circumstances. These include fundamental rights such as the right to life, freedom from torture, and protection against discrimination.

The importance of these norms is reflected in international texts affirming the responsibility of states to protect individuals, including preventing potential violations by governmental and non-governmental actors alike. The acknowledgment of these rules by states serves as evidence of their commitment to the international legal order and enhances their international legitimacy.

In this context, international legal accountability for human rights violations gains particular significance amid the growing challenges posed by artificial intelligence (AI). AI technologies increasingly threaten some of the fundamental human rights, such as privacy, non-discrimination, and equality before the law. Experience has shown that certain AI systems—especially those relying on complex algorithms and big data—may lead to automated decisions that lack transparency, thereby perpetuating discrimination or social exclusion.

In the face of these challenges, there is a renewed need to develop legal frameworks ensuring the safe and ethical use of AI technologies. This requires states and the international community to adopt effective regulatory mechanisms consistent with universal human rights values, providing legal protection against the risks associated with irresponsible AI use—particularly in sensitive areas such as security, criminal justice, employment, and public services.

Within this framework, key international instruments such as the Universal Declaration of Human Rights (1948), the International Covenant on Civil and Political Rights (1966), and the International Covenant on Economic, Social and Cultural Rights (1966) have established the foundational reference for protecting human dignity. These documents laid the groundwork for numerous subsequent international agreements with a specialized focus, including those concerning the rights of women, children, persons with disabilities, refugees, and migrant workers.

Regional human rights charters also play a complementary and equally vital role, such as the European Convention on Human Rights, the American Convention on Human Rights, and the African Charter on Human and Peoples' Rights. These instruments provide legal tools for regional judicial and human rights oversight, thereby reinforcing adherence to principles of dignity and freedom in the face of modern technological threats.

Among the most pressing challenges posed by AI are its military applications, which may lead to the development of autonomous weapons or independent combat systems. These raise fundamental questions regarding compliance with international humanitarian law (IHL), as the use of such technologies in armed conflicts could result in grave violations of the laws of war and undermine legal protection for individuals.

Therefore, the international community is today called upon to reconsider the legal frameworks governing the use of AI—both in peacetime and wartime—and to strengthen coordination between international humanitarian law and international human rights law. Such an approach is essential to ensure respect for human dignity and to mitigate the risk of AI being employed in ways that violate fundamental humanitarian principles, particularly in military contexts (Haswa, n.d., pp. 141–148).

5. The Relationship Between the Uses of Artificial Intelligence in the Security and Military Fields and State Sovereignty: Between Power Enhancement and the Risks of Breach

Artificial intelligence (AI) is one of the most revolutionary technologies that has reshaped the concepts of power and sovereignty in contemporary international relations. The development and use of these technologies have become a fundamental measure of a state's capacity to safeguard its vital interests, preserve its national security, and strengthen its position within the international system. Consequently, the prudent and regulated use of AI is now considered an essential component of the state's **technological sovereignty**, which constitutes an extension of the principle of sovereignty enshrined in the Charter of the United Nations, reinforcing national decision-making independence and control over defense and security instruments.

Conversely, the growing reliance on intelligent systems in military and security domains—such as weapons systems management, intelligence monitoring, and strategic data analysis—enhances the state's ability to protect its borders and interests. However, any failure to secure these systems, or weakness in the digital infrastructure, may lead to a **breach of state sovereignty** through cyberattacks, algorithmic manipulation, or targeting of sensitive sovereign data. From the standpoint of international law, such actions constitute a violation of the principle of non-intervention in the internal affairs of states and a direct infringement upon their right to determine their own technological destiny.

Moreover, artificial intelligence raises significant legal challenges regarding the determination of international responsibility in cases of harm resulting from the misuse of autonomous systems or their deviation from human control. The absence of a clear international legal framework regulating the use of AI in the military sphere opens the door to potential developments that may threaten international peace and security. This calls for the establishment of a specific international legal regime for AI governance that ensures its peaceful and responsible use within the bounds of legitimate sovereignty.

Accordingly, the relationship between artificial intelligence and state sovereignty rests on a delicate balance: the greater a state's ability to develop and legally and technically secure its AI systems, the stronger its sovereignty and independence become; whereas neglecting protection or legal oversight increases the risks that may lead to breaches of sovereignty and the undermining of its very foundations. (Crootof, R., & Ard, B., 2021, pp. 215–260).

6. The Challenges of Criminal Liability for the Use of Artificial Intelligence in Security and Military Fields

The application of criminal liability within the context of artificial intelligence (AI) raises unprecedented legal and ethical challenges that transcend the traditional boundaries of criminal law. These challenges stem from the unique nature of AI systems, which are characterized by their capacity for self-learning and autonomous decision-making. This autonomy necessitates a reconsideration of key legal concepts such as intent, mens rea (criminal intent), and causation under the prevailing legal frameworks.

A. Challenges Related to the Elements of Crime

Crimes involving artificial intelligence represent one of the most significant challenges facing modern legal systems. Such crimes raise complex issues concerning the application of traditional elements of criminal responsibility, particularly given the distinct characteristics of AI systems. The central challenge lies in assessing whether existing legal principles are adequate to address this rapidly evolving technological reality, as traditional components of crime may prove insufficient to encompass the unique aspects of AI-related offenses.

-Difficulty in Determining the Mental Element (Mens Rea) in AI Crimes:

One of the most profound challenges in addressing AI-related crimes lies in determining the mental element—or criminal intent—required for liability. Traditional legal systems are built upon the premise of human will and intent, yet AI systems lack conventional volition or mens rea. Moreover, AI systems can make independent decisions without direct human intervention (Mohamed, A., 2023, pp. 45–46).

The complexity of algorithms and the opacity of decision-making processes in deep learning systems further complicate the attribution of criminal responsibility. In addition, the self-learning and adaptive capabilities of certain AI systems can lead to unforeseen or unintended outcomes, making it even more difficult to establish liability (Redouane, 2024, pp. 353–354).

Collectively, these factors underscore the urgent need to develop new legal frameworks that align with the nature of AI technologies, ensuring that criminal responsibility is determined in a fair and effective manner.

-The Problem of Causation Between the Operator’s Act and AI-Generated Harm:

Establishing the causal link between the operator’s conduct and harm caused by AI presents one of the most fundamental challenges to the application of traditional criminal liability principles. The autonomy inherent in AI systems makes it difficult to attribute harmful outcomes directly to the operator’s commands. Moreover, the interplay of multiple contributing factors—such as input data, environmental conditions, and system interactions with other technologies—further complicates the determination of responsibility.

Additional difficulties arise from the technical complexity faced by courts and legal experts in understanding how AI systems function and in pinpointing specific failures. The continuous updates and evolution of these systems make it nearly impossible to identify the precise moment an error occurred, thereby obscuring causation.

Taken together, these issues challenge traditional legal theories of causation and call for a re-examination of this concept. There is a pressing need to develop new legal frameworks capable of addressing the distinctive features of AI and accommodating its evolving technological dynamics (Redouane, 2024, pp. 353–354).

B. Challenges Related to the Nature of Criminal Liability

With the rapid advancement of artificial intelligence (AI) technologies and their growing use in security and military domains, new legal challenges have emerged concerning the very nature of criminal liability. Addressing these challenges requires a comprehensive reassessment of traditional legal concepts of responsibility, to adapt them to the distinctive characteristics of AI systems—particularly their self-learning and autonomous decision-making capabilities. Among the key issues in this context are:

-Expanding the Scope of Liability to Include Supervision of AI Systems:

Given the legal and ethical complexities arising from the deployment of AI in security and defense, legal systems must adopt a more comprehensive approach to defining criminal responsibility. This approach should expand the scope of liability to include those responsible for the supervision and operational management of AI systems, while reinterpreting the concept of responsibility within a modern technological framework.

In this regard, the principle of supervisory liability can be applied, whereby individuals and entities responsible for the operation and oversight of AI systems bear the duty of continuous monitoring to ensure their safe performance. Developers and operators could also be subject to a legal duty of care, requiring them to implement all necessary measures to guarantee the safety and reliability of their systems.

Furthermore, liability could be extended to corporations and institutions that design, produce, or employ AI systems, encouraging them to adopt stricter compliance and oversight policies. Regular auditing and review mechanisms for AI systems should be mandated to ensure ongoing conformity with ethical and legal standards.

Collectively, these mechanisms could form a balanced legal framework that reconciles technological innovation with legal accountability, while accommodating the dynamic and evolving nature of AI systems (Al-Zahraa, 2023, p. 97).

-The Principle of Precaution and Due Diligence in Managing AI Technologies:

The application of the precautionary principle and due diligence represents a pivotal step toward establishing a legal framework that ensures the safe and responsible use of AI technologies. Originally derived from environmental and public health law, this principle can be effectively adapted to govern AI-related risks.

Within this framework, risk assessment emerges as a fundamental component: developers and users must conduct thorough analyses of potential hazards prior to deploying any AI system, thereby enhancing preventive measures and minimizing possible harm. Transparency is equally crucial—entities must disclose how their systems operate and make decisions to facilitate accountability and strengthen public trust.

Moreover, continuous training and capacity building for personnel operating AI systems are essential to ensure competent and secure use. Establishing effective response mechanisms for emergencies or system failures is also necessary to mitigate damage and enable swift remediation.

This holistic approach to implementing the precautionary and due diligence principles provides a balanced legal framework that both encourages innovation and guarantees legal and security protection for society. It could also serve as a foundation for future specialized legislation regulating artificial intelligence (Redouane, 2024, p. 355).

7. Conclusion:

Artificial intelligence (AI) has become one of the most transformative technologies redefining the notions of power and sovereignty in the 21st century—particularly within the security and military spheres. Its ability to analyze massive data sets, make autonomous decisions, and execute complex operations has revolutionized conflict management and defense strategy. However, this technological advancement has also introduced profound legal and ethical challenges, especially concerning the determination of criminal liability for actions committed by intelligent systems, given their relative autonomy and the difficulty of controlling their decision-making processes. Thus, there is an urgent need to strike a delicate balance between the imperatives of technological innovation—driven by global military competition—and the legal constraints designed to safeguard human values and ensure accountability.

A. Findings:

- The study revealed that the uses of AI have gone far beyond logistical support or data analysis, extending to autonomous combat systems, cybersecurity defense, and intelligence management, making AI a foundational pillar of modern security architectures.
- Despite the existence of general principles within international humanitarian law, these are insufficient to regulate emerging AI-driven military applications, particularly due to the challenge of identifying responsibility for decisions made without direct human intervention.
- The findings confirmed that the main challenge lies in establishing mens rea (criminal intent) and causality, as it is difficult to determine intent when AI systems commit harmful or lethal acts. The autonomy of such systems weakens the applicability of traditional accountability frameworks.
- The study also showed that the growing integration of AI enhances military efficiency, yet simultaneously raises the risk of violating human rights and humanitarian principles, underscoring the need for a new legal approach balancing innovation with responsibility.
- It concluded that the rapid evolution of AI technologies necessitates dynamic legal frameworks capable of adapting to technological change by incorporating principles of transparency, precaution, and accountability into national legislation while promoting international cooperation for binding regulatory standards.
- the relationship between artificial intelligence and state sovereignty rests on a delicate balance: the greater a state’s ability to develop and legally and technically secure its AI systems, the stronger its sovereignty and independence become; whereas neglecting protection or legal oversight increases the risks that may lead to breaches of sovereignty and the undermining of its very foundations.

B. Recommendations:

- States should adopt national laws clearly defining the scope of AI use in security and military operations, including restrictions on fully autonomous systems capable of making independent combat decisions.
- A new legal principle should be established to impose joint liability on both developers and operators of AI systems for damages resulting from their use, ensuring accountability and preventing impunity.

- It is recommended to create an international committee or an additional protocol to the Geneva Conventions dedicated to regulating AI use in warfare, setting unified legal standards to guarantee compliance with international humanitarian law.
- Governments and manufacturers must implement pre-deployment risk assessment mechanisms and disclose the operational characteristics of AI systems used in security and defense sectors to ensure responsible and ethically compliant use.

8. References

- Daliou, F. (2023). Contemporary Issues: From Intellectual Property to Artificial Intelligence. Algiers: Houma Publishing House.
- Belbay, A. (2024). Artificial Intelligence in International Law: A Study of Concepts, Frameworks, and Applications. Algiers: Legal Book Foundation and Ibn Al-Nadim for Publishing and Distribution.
- Dahmani, M. (2023). Artificial Intelligence as a Mechanism to Enhance Cybersecurity. Journal of Legal and Political Thought, 7(2).
- Al-Zahraa, F. (2023). Issues in Determining Criminal Liability in Artificial Intelligence Crimes: Toward a New Legal Framework. Arab Journal of Legal and Judicial Studies, Naif Arab University for Security Sciences, 6(3).
- Redouane, L. S. (2024). Criminal Liability of Company Managers in the Era of Artificial Intelligence: New Legal Challenges and Prospects. Journal of Legal and Economic Studies, University Center of Barika, 7(2).
- Bahi, A. Sh. A. (n.d.). The Legal Regulation of Artificial Intelligence under International Human Rights Law. University of Menoufia, Egypt.
- Salem, N. (2024). The Impact of Employing Artificial Intelligence Technologies Militarily: A Study of the Variables of Wars and Conflicts. Journal of Law and Interdisciplinary Sciences, 3(1).
- Mahmoud, M. K. (2025). The Military Turn Toward Artificial Intelligence and Its Impact on the Traditional Arms Race. Berlin: The Arab Democratic Center.
- Crootof, R., & Ard, B. (2021). Structuring Tech Sovereignty: AI, Cybersecurity, and the Future of State Power. Yale Journal of International Law, 46(2).