Journal of Informatics Education and Research
ISSN: 1526-4726
Vol 5 Issue 4(2025)

Artificial Intelligence and National Security: A New Approach in International Relations

[1]Djelloul Lakhdari
[1]University of Tissemsilt, (Algeria), Email: Djelloul.lakhdari@univ-tissemsilt.dz, ORCID: https://orcid.org/0009-0003-0495-5525

Received : *20-05-2025* ; Accepted : *08-08-2025* ; Published : *03-10*-2025

Abstract

The world is witnessing a fundamental transformation in the nature of security threats and the mechanisms for addressing them, driven by the rapid advancement of artificial intelligence technologies. AI is no longer merely an auxiliary tool; it has become a strategic actor that contributes to reshaping concepts of national security and international relations. This article examines the topic "Artificial Intelligence and National Security: A New Approach in International Relations" by analyzing how AI influences concepts of national security and its evolution into a strategic actor in international policy.

The article concludes that AI is no longer just a technical tool but has become a decisive element in shaping the security strategies of major states, through its role in security and military decision-making, data analysis, operational guidance, and predicting movements. At the same time, it raises unprecedented legal and ethical challenges that require the establishment of effective global governance frameworks. Therefore, understanding the dimensions of this transformation is essential for formulating more balanced security policies in the contemporary international environment.

Keywords: Artificial Intelligence, National Security, International Relations, Cyber Wars, Digital Sovereignty

INTRODUCTION

The international system has witnessed profound transformations in recent decades as a result of the rapid technological revolution, foremost among them artificial intelligence technologies. Artificial intelligence is no longer merely a technical tool that assists in data collection and analysis; it has become an active force influencing the dynamics of international relations and asserting itself as a central axis in shaping states' security and strategic policies. From my perspective, artificial intelligence has become one of the most significant factors reshaping the concept of national security including deterrence, sovereignty, and decision-making, as well as the management of conflicts, in addition to expanding the scope of warfare into the cyber and algorithmic domains.

What we observe today is that traditional actors in international relations are no longer the sole determinants of power balances; rather, they have been joined by "intelligent algorithms" that increasingly analyze, decide, and, in many cases, execute. This leads us to argue that artificial intelligence has become a point of convergence between technology and politics, between security and information, and between soft and hard power.

While artificial intelligence has made it possible to provide advanced capabilities for enhancing security systems, particularly for major powers, it has also raised a set of ethical and legal challenges. This, in turn, calls upon decision-makers to reconsider the limits of its uses. In light of the foregoing, it has become necessary to adopt a new analytical approach in order to understand how artificial intelligence has become a tool for reshaping and redefining traditional security concepts. Within the context of this transformation, it is therefore necessary to raise the following question:

Research Problem

To what extent has the use of artificial intelligence in the security policies of major powers led to a structural transformation in the concepts of national security, and to a reconfiguration of the logic of power and balance within international relations?

Hypotheses

1. Artificial intelligence contributes to shifting security power from its traditional military dimension to an algorithmic–digital dimension based on data and the speed of decision-making.
2. The use of artificial intelligence reinforces imbalances in international power relations in favor of digitally advanced states, rather than achieving a more balanced distribution of power.
3. The growing reliance on artificial intelligence generates unprecedented legal and ethical challenges related to responsibility for autonomous combat decision-making.

Objectives of the Study

This study aims to highlight the following elements:

1. To demonstrate the role of artificial intelligence in reshaping the concept of national security in light of current geopolitical and technological transformations.
2. To explain the role of artificial intelligence as a tool for formulating the security and military policies of major powers.
3. To analyze the political and strategic implications of the use of artificial intelligence in international relations, particularly in the context of crises.
4. To shed light on the legal and ethical challenges associated with the use of artificial intelligence in the security domain.

Methodology of the Study

This study adopts a descriptive–analytical approach to examine the impact of artificial intelligence on the reshaping of national security concepts and international relations, through describing the phenomenon and analyzing its political, security, and strategic dimensions. It also employs an interpretive and prospective dimension in order to understand the role of artificial intelligence in security and military decision-making, and to anticipate its future repercussions on power balances, as well as the legal and ethical challenges associated with its use.

The study relies on an analysis of the literature and secondary sources, including academic studies and strategic reports, with the aim of testing the research hypotheses and addressing the research problem concerning the extent to which artificial intelligence contributes to redefining traditional security concepts and reordering the features of the contemporary international system.

2. Artificial Intelligence and the Transformation of National Security Concepts

The concept of national security has long been associated with traditional dimensions confined to confronting external threats, protecting borders, and strengthening military power. With rapid technological development, the digital revolution, and the emergence of artificial intelligence technologies, the latter has become a decisive factor in security equations. All of this has imposed a radical transformation on the concept of national security. From this perspective, it can be argued that we are facing a transitional phase in which states have moved beyond merely defending their territory to entering a new phase in which they defend their data.

2.1 Digital National Security

In light of the growing reliance on digital systems, national security is no longer limited to traditional dimensions such as border protection, military deterrence, or land and air threats. It has come to encompass the protection of cyberspace and digital infrastructure, given that artificial intelligence (AI)–enabled cyberattacks are capable of disrupting vital sectors such as energy, health, and transportation. Moreover, artificial intelligence has increased the complexity of this domain, as it has become an active element in building both offensive and defensive capabilities in the digital world.

This leads us to raise the following question: has national security transformed into digital security?

In the current context, digital security can be considered a natural extension of the traditional concept of national security; however, it goes beyond it in terms of the nature of the tools and the targeted domains. Artificial intelligence technologies are used to monitor cyber threats, predict them, and respond to them in real time. For example intelligent algorithms are employed to analyze patterns of cyberattacks and identify abnormal behaviors, enabling the early detection of threats before they actually materialize. Based on the foregoing, it can be argued that artificial intelligence does not merely protect systems; it also redefines the concepts of sovereignty and deterrence in the digital environment.

Digital national security is no longer simply an expansion of the scope of protection rather, it reflects a transformation in the very nature of security threats themselves. Risk has shifted from being a material event subject to geographic detection to an invisible process that takes shape within software architectures and data flows. This is evident in digital supply chain attacks, such as the SolarWinds attack, which targeted software relied upon by state institutions rather than their physical facilities, thereby confirming that the protection of digital systems has become an integral part of national security. Here, the importance of establishing international standards to govern the use of this technology within clear ethical and political frameworks becomes evident (Meleouni & Efthymiou, 2024:5).

2.2 Artificial Intelligence for Proactive Threat Detection

What distinguishes artificial intelligence is its ability to predict events before they occur by analyzing massive amounts of intelligence and field data, with the aim of identifying active or potential threats. In this context, it is noteworthy that the use of advanced technologies such as machine learning and deep learning has enabled security agencies to develop more effective proactive analytical systems. Instead of relying on delayed—and sometimes inaccurate—human reports, algorithms can anticipate early indicators of risk by analyzing open sources, monitoring social media platforms tracking the movements of suspicious individuals, and detecting threat signals before they escalate. This capability allows for rapid, real-time decision-making (Hoadley & Lucas, 2018:12).

In this context, artificial intelligence represents a shift from a reactive logic to a probabilistic risk management approach, where a threat is not defined by its actual occurrence but by its statistical likelihood. This is exemplified by some countries' use of predictive analytics systems to monitor unusual behavioral patterns, such as the behavioral analysis programs employed by Israel to detect potential security threats in sensitive areas. However, this shift raises a central issue regarding the reliance on "algorithmic suspicion" as a basis for security decision-making, given the

inherent risks of bias and predictive error. These capabilities also raise complex ethical and political questions related to privacy and the legitimacy of preemptive targeting.

2.3 Asymmetric Threats and Security Adaptation

The current reality indicates that asymmetric threats, such as cyberattacks or the exploitation of advanced technology by irregular groups, have become more complex due to the use of artificial intelligence. This shift has compelled states to redefine their security priorities. It also requires them to reconsider how to adapt to a security environment no longer governed by the traditional rules of warfare. Instead of focusing exclusively on armies, the emphasis has shifted to protecting systems, networks, and algorithms.

It is evident today that artificial intelligence tools are increasingly being exploited by non-state actors, such as terrorist organizations and actors supported by states or other entities, to carry out precise attacks in the digital space, thereby undermining the effectiveness of traditional deterrence models in the cyber environment.

In asymmetric wars that rely on artificial intelligence, adversaries are able to target structural vulnerabilities within national systems, such as electrical infrastructure or communication networks. Artificial intelligence has brought about a transformation in the nature of asymmetric threats in terms of effectiveness and time efficiency. In attacks similar to those that occurred in Ukraine in December 2015, malicious groups used industrial control software supported by automated analysis, which led to power outages affecting more than 230,000 homes.

According to a report by the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), this incident represents one of the clearest examples of targeting critical infrastructure through advanced cyber tools. These examples illustrate how non-state actors can exploit artificial intelligence in low-cost yet high-impact tactics, thereby undermining the effectiveness of traditional deterrence models and compelling states to reformulate their security adaptation mechanisms to encompass digital infrastructure and elements of political decision-making. From this perspective, national security becomes an issue that goes beyond the purely military dimension to include technical actors and political decision-makers (Johnson, 2019:9–14).

2.4 Redefining the Enemy

In light of the development of artificial intelligence technologies, the concept of the “enemy” in the contemporary strategic environment has moved beyond traditional perceptions. It has come to be embodied in autonomously intelligent algorithms, invisible digital networks, and even internal breaches that threaten security from within. This transformation necessitates a reconfiguration of the state’s strategic outlook encompassing the concepts of deterrence, sovereignty, and security. States that fail to keep pace with this shift will face serious difficulties in asserting their sovereignty and ensuring their stability.

In this context, the threat becomes more ambiguous, as the state may not know the source of the attack, who is behind it, or even its ultimate objectives. From this perspective, this ambiguity can be considered a fundamental challenge for security decision-makers, as the response process becomes more complex and the effectiveness of traditional deterrence is weakened.

Recent reports have indicated that artificial intelligence is capable of concealing the traces of digital attacks and generating digital behaviors that are difficult to detect or attribute to a specific actor, thereby complicating processes of strategic understanding and analysis. This raises the

following question: how can the enemy be identified in an environment where algorithms simulate human action and conceal the identity of the adversary (Russell et al., 2024:9)?

The NotPetya attack in June 2017 provides a clear example of this transformation. The malware employed intelligent algorithms that spread automatically across companies and states, causing global losses exceeding ten billion US dollars, according to the World Economic Forum, without the ability to attribute the attack to a specific actor. This reality illustrates how artificial intelligence can redefine the very notion of the enemy and make it necessary for states to adopt technical and proactive security strategies based on the analysis of digital patterns and the assessment of intangible threats, rather than relying solely on traditional responses.

In light of the foregoing, it can be said that artificial intelligence has fundamentally altered the nature of national security. It has not only changed the tools of national security but has also touched its very essence. Concepts such as threat and enemy have been redefined. Therefore, the future of national security depends on the extent to which states can build their strategies and security approaches based on technological proactive, and transparent foundations, supported by artificial intelligence technologies capable of keeping pace with the era of algorithmic threats.

3. Artificial Intelligence as a Strategic Actor in International Relations

Until recently, the influential actors in international relations were limited to states international organizations, and some multinational corporations. However, in the context of accelerated digital transformation, artificial intelligence has emerged as a new actor. It no longer merely serves as a tool used to achieve strategic objectives rather it has begun to participate in shaping choices and guiding decisions, making it an invisible strategic actor in the equation of power and influence.

3.1 Artificial Intelligence and the Transformation of Decision-Making

Decision-making in international relations has long been associated with human analysis, relying on the judgments of political elites and their assessments of national interest. However, the integration of artificial intelligence into analytical processes and security and military decision-making has profoundly altered this equation. In my estimation, we are facing a fundamental turning point, where information is no longer merely a tool to support decisions; rather, its production and analysis are governed by algorithmic logic, which asserts itself as a partner—and sometimes even as a substitute—for the human mind in the processes of analysis and decision-making.

What we observe today is that artificial intelligence increasingly contributes to supporting security decision-making through advanced analytical systems that rely on big data and predictive algorithms, especially in situations characterized by uncertainty and complex crises. For instance, in the United States, the Department of Defense has developed platforms based on artificial intelligence to identify threat patterns and make proactive decisions (Hoadley & Lucas, 2018:21).

The integration of artificial intelligence into decision-making represents a genuine strategic transformation. In 2019, DARPA reports indicated that AI-based predictive analysis platforms in the U.S. military were capable of processing millions of data points daily to provide security options with accuracy surpassing that of traditional human teams, thereby contributing to faster decision-making during war exercises. This example reflects how artificial intelligence is no longer merely an auxiliary tool but an invisible actor that asserts itself at the core of strategic analysis, redefining the nature of political and military thinking in moments of crisis.

According to a study conducted by the "Carnegie" Foundation, artificial intelligence may reduce

human hesitation in moments of crisis; however, it may also increase the likelihood of misjudgment due to its high speed of interaction and lack of political and ethical context (Chivvis & Kavanagh, 2024:5). From this, we can conclude that artificial intelligence not only alters decision-making mechanisms but also the very nature of the thinking that produces decisions.

3.2 Artificial Intelligence as a Tool of Power Balance

Today, major states view artificial intelligence as a "strategic resource," no less important than possessing energy or nuclear superiority. Consequently, having advanced capabilities in artificial intelligence grants states stronger negotiating positions and greater deterrence capacity. The question that now arises is: has artificial intelligence become an element of the balance of power in the international system?

Artificial intelligence has become an unconventional strategic weapon that reshapes the balance of power among major states, particularly amid the escalating competition between China and the United States. Pentagon reports indicate that this race in the field of artificial intelligence constitutes one of the foremost emerging threats to U.S. national security (Allen & Chan, 2018:13).

The 2020 Pentagon report shows that U.S. investment in military artificial intelligence aims to maintain superiority in smart weapons systems, while China is intensifying its efforts to develop predictive analysis platforms and intelligent drones reflecting a digital race that is reshaping traditional power balances. A practical example is China’s use of AI-based military command systems to enhance response speed in naval maneuvers, giving it a relative advantage over conventional powers. This reality confirms that artificial intelligence is no longer merely a support tool but has become a central strategic element in the redistribution of power and deterrence in the international system.

Some researchers argue that artificial intelligence may become an important factor in the redistribution of power in the international system, not only in favor of conventional powers but also for non-state actors or even rising states, provided it is invested wisely (Sultan & Jamy, 2024:9). From this perspective, it can be said that artificial intelligence not only serves technological superiority but is also used as a means of strategic leverage.

3.3 Shaping State Behavior in Crises

The use of artificial intelligence is not limited to peacetime in risk analysis and threat assessment; its role deepens during crises in shaping state behavior. In situations of acute tension, algorithms assist in outlining potential scenarios and evaluating available options based on criteria of effectiveness, cost, and legitimacy. In my view, artificial intelligence has become an influential (invisible) actor in decision-making, reshaping states’ strategic responses and profoundly affecting how they act under pressure.

The experience of the 2021 U.S. military exercises demonstrates the integration of artificial intelligence into command and control (C2) systems, where algorithms helped evaluate over 500,000 scenarios within 72 hours to provide rapid strategic recommendations regarding troop movements, according to the 2022 RAND Corporation report. This illustrates how artificial intelligence has become an invisible actor guiding state behavior in crises, increasing the accuracy of military decisions while simultaneously exposing decision-makers to the risk of unintended escalation when interpreting adversaries’ hostile activities within automated models that lack full political context.

A study by the RAND Corporation indicates that some states have already begun integrating artificial intelligence technologies into command and control (C2) systems during crises, aiming to reduce decision-making time and enhance the accuracy of targeting and military response (Russell et al., 2024:13). However, this rapidity in interaction may produce adverse effects, as it increases the likelihood of unintended escalation, especially if the adversary's behaviors are interpreted within automated analytical models that lack precise political reading.

We also observe that the use of artificial intelligence in analyzing the intentions of other states may lead to an overreliance on technical predictions rather than political understanding and analysis, which could result in misinterpretation or erroneous assessments (Johnson, 2019:160). From this, we can conclude that, despite its technical advantages, artificial intelligence increases the complexity of crises due to its automated interpretations, which may lack contextual and political understanding.

3.4 Redefining the Concept of Sovereignty

One of the most prominent transformations imposed by artificial intelligence in international relations is the reshaping of the concept of sovereignty. Sovereignty is no longer measured solely by control over land and borders; it has become linked to the ability to possess data, direct algorithms, and control cross-border digital systems.

In this context, the concept of "digital sovereignty" has emerged, representing a state's ability to protect its citizens' data, prevent its leakage to foreign entities, and control the flow of information across its electronic borders (Ishkhanyan, 2025:3). However, the challenge lies in the fact that the digital space, by its nature, does not recognize borders which undermines states' ability to assert their traditional sovereignty.

I believe that states today face a strategic dilemma: they are required to maintain their sovereignty while relying on digital tools and algorithms that are not entirely under their control. From this emerges the urgent need to establish international regulatory mechanisms for the use of artificial intelligence, taking into account that future sovereignty will be hybrid, combining political decision-making with technological dominance.

As digital governance frameworks indicate, the absence of standardized norms in this field opens the door to subtle foreign interventions through artificial intelligence whether in elections, shaping public opinion, or even in economic decision-making. A case in point is the 2018 Cambridge Analytica scandal, where the data of millions of Facebook users was used to influence the U.S. presidential election, highlighting the vulnerability of states' digital sovereignty to foreign interference via AI tools. Reports indicated that the data of approximately 87 million users was exploited without their consent. In light of the foregoing, it appears that the traditional concept of sovereignty is no longer capable of encompassing the complexities of the current digital environment (Zaidan & Ibrahim, 2024:11).

From what has been discussed, it is evident that artificial intelligence has transcended the limits of a mere technical tool to become a strategic actor in international relations. It reshapes decision-making processes, redraws power balances, guides state behavior in crises, and poses fundamental challenges to the concept of sovereignty. From this perspective, I believe that this transformation necessitates a thorough reexamination of traditional theories in international relations (realism and liberalism) to align them with this "non-human actor."

4. Applications of Artificial Intelligence in the Security Policies of Major Powers

In recent years, applications of artificial intelligence have ceased to be merely supportive tools for security decision-making and have transformed into a fundamental pillar in the strategic planning architecture of major powers. It is used to enhance influence and achieve qualitative superiority in the fields of warfare, surveillance, and control. Recent trends in security policies indicate the integration of artificial intelligence into a number of sensitive domains, ranging from military targeting and intelligence data analysis, through autonomous drones, to cyber warfare and command and control systems.

4.1 Military Targeting and Intelligence Data Analysis

Precise targeting and objective identification have long been among the most challenging aspects of military operations. With the development of artificial intelligence, military targeting no longer relies solely on the human element for information collection and analysis. Instead, big data analysis is now conducted through algorithms that learn and evolve autonomously. This enables the identification of targets with extreme precision and in record time. Moreover, artificial intelligence has enhanced the ability of armed forces to integrate multiple intelligence sources within a single digital environment, relying on machine learning to determine high-priority targets and provide rapid recommendations based on accurate probabilistic analysis of the impact of military operations (Sultan & Jamy, 2024:12).

For example, the United States and Israel have developed complex systems that rely on artificial intelligence to analyze aerial imagery and monitor targets with extreme precision. In the recent Israeli aggression on Gaza (2023), Israel employed several AI-supported programs, such as the **Gospel Project**, a system that analyzes massive amounts of intelligence information to generate target lists in record time. The **Habon** system, used for target identification, processes vast quantities of intelligence data to determine targets quickly and automatically. In the military escalation against Iran (2025), Israel utilized automated imagery and intelligence data analysis systems through a program known as **"Fire Factory"**, which enables the real-time determination of operational priorities.

Reports from the Stockholm International Peace Research Institute (SIPRI) for 2024 indicate that the United States alone has conducted more than 1,200 AI-supported precision targeting operations over the past five years, with an average reduction of 35% in military decision-making time compared to previous decades. This illustrates how artificial intelligence has become a decisive factor in enhancing the effectiveness of military operations and reducing human errors. Meanwhile, the United States and China have developed AI programs capable of providing targeting recommendations based on the analysis of the adversary's past behavior, the geographical environment, and even weather conditions. It is notable that this development reduces decision-making time (Johnson, 2019:154).

4.2 Autonomous Decision-Making Unmanned Aerial Vehicles

Unmanned aerial vehicles (Drones) represent one of the most prominent manifestations of the deployment of artificial intelligence in modern warfare, given the advanced capabilities they provide in reconnaissance and precision strikes without exposing soldiers to the risks of direct confrontation. These systems have undergone a qualitative evolution, transitioning from mere surveillance tools into autonomous combat platforms capable of identifying targets, determining trajectories, assessing threats, and making real-time decisions without direct human intervention.

They are employed in carrying out precise assassinations and targeting individuals based on their behavioral patterns or communications, as well as in collecting intelligence information within complex urban environments.

In this context, official and international reports indicate that a number of countries, led by the United States, Israel, and China, are currently developing autonomous combat systems that rely on artificial intelligence and are capable of making field decisions based on continuous analysis of data received from sensors, thermal cameras and acoustic detection devices (Hoadley & Lucas, 2018:23). Reports by the U.S. Department of Defense, particularly within the framework of **Project Maven**, along with reports by the **Congressional Research Service (CRS)** on **Lethal Autonomous Weapon Systems**, have highlighted the growing expansion in the use of algorithms in targeting operations, battlefield analysis, and combat decision support. Human Rights Watch reports, notably *Losing Humanity: The Case Against Killer Robots*, also point to Israel's development of systems such as the loitering munitions **Harpy** and **Harop** which possess high levels of autonomy in target selection. In the same context, Chinese military documents issued by the **Academy of Military Sciences** discuss a shift toward what is known as **Intelligentized Warfare**, in which automated systems play an advanced role in command and control and in battlefield decision-making.

It appears to me that this technological development fundamentally reshapes the principle of "responsibility in killing," as it becomes difficult to identify the party legally and ethically accountable for combat errors when the decision arises from a self-learning algorithm rather than a direct human actor. This argument is supported by specialized studies in AI safety, including the study by **Amodei et al. (2016)** entitled *Concrete Problems in AI Safety*, which emphasizes that intelligent systems may behave unpredictably when deployed in environments different from those in which they were trained. The study by **Goodfellow et al. (2015)** on *Adversarial Examples* also concluded that minor changes in context or data can lead to incorrect and unexpected decisions (Sajduk, 2019:91).

These concerns are further reinforced by United Nations reports, including the **UN Expert Panel report on Libya (2021)**, which indicated the use of an autonomous Kargu-2 drone that reportedly carried out an attack without direct human intervention highlighting the practical risks of unpredictable behavior of autonomous combat systems in complex conflict environments.

4.3 AI-Supported Cyber Warfare

Cyber warfare has become one of the most prominent arenas of strategic conflict in the digital age, and its effectiveness has increased unprecedentedly with the employment of artificial intelligence technologies. While traditional cyberattacks relied on software and manual intrusions, they are now driven by algorithms capable of self-learning, analyzing the enemy's digital infrastructure, and automatically and rapidly identifying security vulnerabilities. Artificial intelligence is employed not only in detecting cyberattacks but also in conducting proactive attacks based on the analysis of digital data and the identification of threat sources.

These technologies also enable the simulation of intrusion scenarios before execution, granting the defensive or offensive system the ability to predict and plan with high accuracy. More dangerously, when these attacks are executed by autonomous systems, they may surpass human comprehension and cause widespread damage without the possibility of timely containment.

A study conducted in 2018, entitled *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*, and supported by international universities and research institutions

including **Oxford** and **OpenAI**, indicates that artificial intelligence can be used to develop self-adaptive cyberattacks capable of modifying their behavior instantaneously based on the target environment. The study explains that these systems may rely on machine learning to analyze cyber defense patterns, test vulnerabilities, and then automatically alter intrusion methods to bypass firewalls and conventional encryption systems. This represents a shift from pre-programmed attacks to "self-learning" attacks that are difficult to predict or contain using traditional means (Meleouni & Efthymiou, 2024:7).

Reports issued by the **RAND Corporation** indicate that AI-supported cyber warfare represents one of the most prominent threats that major powers will face over the next decade, particularly with the expanding use of **Industrial Control Systems (ICS)** and the **Internet of Things (IoT)**, especially in critical infrastructures such as electricity water, and transportation networks. This expansion, despite providing efficiency and real-time connectivity, makes these systems more vulnerable to cyberattacks, as they create new entry points that could be exploited to compromise national security and threaten state stability (Russell et al., 2024:11).

4.4 Strategic Decision-Making Systems

Arguably, the most critical aspect of artificial intelligence in security policies is its integration into strategic decision-making systems within operations rooms and high-level decision-making echelons. Algorithms are not only used for tracking targets but are also employed in generating response scenarios, analyzing adversaries' intentions and assessing the probabilities of escalation in crises. Recent developments indicate that intelligent systems are now used to construct probabilistic projections regarding the outbreak of wars or how an adversary might respond to a specific strike. In some countries, these models are presented directly to top decision-making circles, reshaping the communication mechanisms between political leadership and the military establishment (Kanellopoulos, 2024:18).

I tend to consider that the integration of these systems places decision-makers before a dual dilemma: how can a decision be built based on a recommendation whose logic is not understood, and who bears the consequences in case of an error? A report published by the **Carnegie Corporation** in 2024, entitled *How AI Might Affect Decisionmaking in a National Security Crisis*, indicated that one of the major threats is the "unintelligible decision," issued by a complex algorithm not even understood by its developers (Chivvis & Kavanagh, 2024:9).

It becomes clear from reviewing the applications of artificial intelligence in the security policies of major powers that this technology has transformed into a fundamental pillar of modern national security. Instead of remaining a supportive technical tool, artificial intelligence has become a key actor in shaping decisions directing attacks, and identifying the enemy and appropriate response strategies. This transformation ushers international security into a new phase characterized by complexity and acceleration, posing a central question to the international community: how can we balance the efficiency of artificial intelligence with the risks of losing control, in the absence of clear regulatory and ethical standards governing its use?

5. Ethical and Legal Challenges of Artificial Intelligence Applications in the Security Field

The most prominent challenge posed by artificial intelligence in the security domain lies in its ethical and legal dimensions. It is not merely a matter of the efficiency of intelligent systems, but also extends to the capacity of states and the international community to regulate their use within a binding legal framework and to prevent their slide toward inhumane decisions.

5.1 Legal Responsibility for Combat Actions

One of the most prominent legal issues related to artificial intelligence in warfare is the difficulty of determining responsibility in the event of serious violations. When autonomous combat systems are used to make decisions regarding killing or targeting—essentially transferring the authority to kill from humans to machines—questions arise about who bears the consequences of these actions: is it the state, the designers, the military commanders, the system itself, or the manufacturing company?

The absence of a direct human actor in making combat decisions creates a legal vacuum in determining responsibility, rendering the justice system incapable of addressing the nature of the new actor on the battlefield. This situation undermines the principle of accountability in international humanitarian law. Indeed, this dilemma threatens to widen the gap between international humanitarian law and rapidly advancing technological developments (Meleouni & Efthymiou, 2024:9). It is observed that some states are attempting to establish internal regulatory frameworks, yet the absence of a comprehensive international agreement renders these frameworks of limited effectiveness. Multiple studies have emphasized that determining responsibility becomes increasingly difficult as the "autonomy" of the combat system in decision-making grows (Sajduk, 2019:93).

5.2 Algorithmic Bias

If these systems rely on training data provided by humans, which contain elements of discrimination, whether overt or hidden, the algorithms may reproduce cultural or racial biases present in this data or during its analysis. The risk here is not limited to technical errors if a mistake occurs, but extends to the potential for making security or combat decisions based on flawed data, thereby exposing individual rights and principles of justice to real dangers.

Recent studies, such as the research by Joy Buolamwini and Timnit Gebru at MIT and Stanford University (2018), revealed that commercial facial recognition algorithms exhibited significantly higher error rates in identifying dark-skinned women compared to light-skinned men. In this study, error rates reached approximately 34.7% in classification, compared to less than 1% for light-skinned individuals. Moreover, some AI-based visual recognition systems have shown high error rates when dealing with specific racial groups, which could lead to disastrous incorrect decisions in sensitive security contexts (Srivastava & Bullock, 2024:6).

Hence, errors resulting from bias do not merely reflect a technical flaw, but constitute a genuine human and ethical risk. It is therefore insufficient to simply state that "the algorithm erred"; rather, accountability must extend to those who designed it, those who deployed it, and those who ignored its discriminatory effects. Correcting this bias requires re-evaluating the methodologies for building intelligent security systems starting from the design phase, through integrity testing, and up to ensuring transparency and accountability.

5.3 Algorithmic Integrity and Transparency

The use of artificial intelligence in security contexts raises a central issue concerning the integrity and transparency of algorithms. AI often operates according to complex algorithms that cannot be fully understood by ordinary users, and sometimes not even by programmers and developers themselves. From this perspective, it can be argued that no system used in decisions

affecting life and death should operate as a "black box." Many AI applications in the security domain lack transparency, either due to technical complexity or for reasons of security confidentiality. This undermines public and institutional trust in the fairness of AI-based security systems (Chivvis & Kavanagh, 2024:10).

It is observed that the lack of transparency hinders the possibility of legal review and accountability. It becomes difficult to verify the legitimacy of an offensive decision made by an algorithm that is not even fully understood by its developers. International research reports have suggested the adoption of so-called **Auditable Transparency** as a potential solution (Zaidan & Ibrahim, 2024:14).

5.4 Fear of Losing Control

Perhaps the most pressing concern today regarding the use of artificial intelligence technologies, especially in the security domain, is the possibility of losing control over them by their developers or operators. The worry lies in the ability of self-learning algorithms to generate unexpected or non-adaptive behavior at critical moments, which could lead to uncontrolled escalation or catastrophic decisions beyond the operators' intent.

It is evident that these concerns are no longer merely hypothetical scenarios, but are seriously addressed in U.S. national security reports and those of several other countries. A report by the Brookings Institution noted that the risk lies not only in the loss of technical control, but also in the increasing "psychological dependence" of decision-makers on the AI system's outputs. From this, we deduce that the challenge is not only to improve AI capabilities, but also to regulate them within clear limits and to establish emergency stop mechanisms (**Kill Switches**) that prevent automatic escalation or catastrophic decisions resulting from a misinterpretation of context (Meserole, 2018: 3).

Despite the strategic gains of using artificial intelligence in the security domain, this raises numerous complex legal and ethical issues: who bears responsibility? Who regulates algorithmic bias? Who holds the authority to oversee these systems? And how should we act if control over the system is lost?

From this, it becomes evident that the future of security policies is not measured solely by the level of technological advancement, but by states' ability to build a comprehensive framework of values, accountability, and good governance for these technologies.

CONCLUSION

In light of the above, it is clear that artificial intelligence is no longer merely a neutral technical tool employed to enhance security efficiency, but has become a strategic actor reshaping the concepts of national security and international relations. With its growing use in monitoring, analysis, attack, and defense, the state's perception of threats has changed, and the arenas of conflict have extended to include the digital and algorithmic domains. The deployment of AI in decision-making during critical moments may also reduce the time gap between action and reaction, increasing the likelihood of uncontrolled escalation. As reliance on autonomous systems grows complex legal and ethical challenges arise, related to responsibility, transparency, and sovereignty.

Accordingly, it appears that concepts such as national security, sovereignty, and deterrence have undergone profound transformations, necessitating that states reconsider their defensive and preventive strategies. What is particularly concerning is the technological acceleration that outpaces the capacity of ethical and legal frameworks to regulate it, creating an environment fraught with risks whose outcomes are difficult to predict or control.

Thus, the real challenge lies not only in developing more advanced technologies but in re-examining the philosophical and ethical foundations upon which the very concept of national security is based. In my view, the question of "who holds power?" is no longer sufficient to understand the balances of the international system; rather, it has become contingent upon who controls the algorithm.

Results

1. AI's Transformation from a Tool of Power to a Determinant of Power Itself

The study shows that artificial intelligence is no longer merely a means of enhancing military capabilities; it has become an element that redefines the nature of power in international relations. Superiority is no longer linked solely to material capabilities, but also to possessing algorithms capable of learning, adapting, and making decisions in real time.

2.Weakening Human Centrality in the Security Loop without Officially Eliminating It

The study finds that the increasing reliance on intelligent systems does not explicitly exclude the human actor, but gradually diminishes their crucial role, transforming them into a formal supervisor of decisions generated by algorithms. This creates a gap between legal responsibility and actual decision-making authority.

3.Transforming Uncertainty from a Strategic Factor to a Technical Feature of the International System

The results indicate that AI does not necessarily reduce uncertainty in international behavior, but reproduces it in a new form. Ambiguity arises from the behavior of the algorithms themselves, not only from the intentions of states, which increases the complexity of crisis management and the risk of strategic miscalculation.

4.Reproducing Power Imbalances Rather Than Correcting Them

Contrary to the discourse suggesting that AI equalizes states in the distribution of power the study demonstrates that it effectively deepens the gap between states by consolidating the advantage of those possessing data, digital infrastructure, and the capacity to translate innovation into effective security policies.

5.Incorporating AI into Security Decision-Making Reduces Political Responsibility and Creates an Unprecedented Ethical–Legal Vacuum

The study reveals that the increasing reliance on intelligent systems for monitoring, assessment, and targeting transfers decision-making from the human actor to algorithmic logic that is not fully accountable. This shift does not only create a technical problem but generates a vacuum of responsibility: who is held accountable when the decision results from self-learning algorithms? The state? The programmer? The military commander?

This vacuum reshapes the rules of deterrence, as the ambiguity of responsibility undermines the logic of accountability and lowers the political cost of using force thereby increasing the likelihood of sliding into uncontrolled conflicts, particularly in cyber and hybrid environments.

Recommendations

1.Establish "Intermediate Institutions" to Monitor Multinational Security Algorithms

Create independent international bodies to review and evaluate algorithms used in military and intelligence systems, with the capacity to understand "uninterpretable decisions" before their deployment or use in operations. This adds a proactive dimension to governance, rather than merely setting general rules.

2.Design "Ethical Warning Systems" within Military AI

Integrate AI layers that automatically monitor the decisions of other systems and issue alerts when a decision risks violating ethical standards or international law.

3.Adopt a "Complex Virtual Battle Simulation Model" to Assess Algorithmic Dependence on National Security

Develop virtual environments that represent realistic and unfamiliar scenarios to test autonomous systems before their real-world deployment. This reduces unforeseen risks arising from self-learning in environments not included in training data.

4.Establish an Open International Database for Advanced Cyber Threats

Create a collaborative platform that gathers information on self-learning cyberattacks and methods for bypassing firewalls and encryption, aiming to improve joint defense capabilities and reduce the power gap between states.

5.Integrate Political and Strategic Variables in Algorithm Design

When programming military AI systems, do not rely solely on field or technical data include diplomatic and strategic criteria to assess the impact of decisions on international relations, making the algorithm itself part of crisis management rather than just an execution tool.

6.Launch "Digital Exchange Training Programs" for Technologically Less Capable States

To reduce the gap between states, implement programs for exchanging data, expertise and AI simulation models, enabling developing countries to participate in the AI race without compromising international security.

6. Bibliography List

1. Allen, G. C., & Chan, T. (2018). *Artificial intelligence and national security*. Center for a New American Security.
2. Chivvis, C. S., & Kavanagh, J. K. (2024). *How AI might affect decision making in a national security crisis*. Carnegie Endowment for International Peace. https://carnegieendowment.org
3. Hanson, R., Grissom, A. R., & Moton, C. A. (2024). *The future of Indo-Pacific information warfare: Challenges from AI*. RAND Corporation.
4. Hoadley, D. S., & Lucas, N. J. (2018). *Artificial intelligence and national security*. Congressional Research Service. https://www.crsreports.congress.gov
5. Ishkhanyan, A. (2025). The sovereignty-internationalism paradox in AI governance: Digital federalism and global algorithmic control. *Discover Artificial Intelligence*, *5*(123),1-14. https://doi.org/10.1007/s44163-025-00374-x
6. Johnson, J. (2019). Artificial intelligence & future warfare: Implications for international security. *Journal of Defense & Security Analysis*, *35*(2), 147–169. https://doi.org/10.1080/14751798.2019.1600800

7. Kanellopoulos, A. N. (2024). Counterintelligence, artificial intelligence and national security: Synergy and challenges. *Journal of Politics and Ethics in New Technologies and AI*, *3*(1),1-18, https://doi.org/10.12681/jpentai.35617
8. Meleouni, C., & Efthymiou, I. P. (2024). The use of artificial intelligence (AI) in national security: Defining international standards and guidelines.
9. *Journal of Politics and Ethics in New Technologies and AI*, *3*(1), 1-11. https://doi.org/10.12681/jpentai.37847
10. Meserole, C. (2018). *Artificial intelligence and the security dilemma*. Brookings Institution. https://www.brookings.edu/articles/artificial-intelligence-and-the-security-dilemma
11. Sajduk, B. (2019). Theoretical premises of the impact of artificial intelligence on international relations and security. *Copernicus Journal of Political Studies*, (2),157-180. https://doi.org/10.12775/CJPS.2019.017
12. Srivastava, S., & Bullock, J. (2024). *AI, global governance, and digital sovereignty*. arXiv. https://arxiv.org/abs/2402.00501
13. Sultan, A., & Jamy, S. H. (2024). Artificial intelligence revolution: Contemporary trends and implications for the future of warfare. *Journal of Security & Strategic Analyses*, *8*(1), 1-18.
14. Zidane, I., & Ibrahim, I. A. (2024). Governance of artificial intelligence in a complex and rapidly changing regulatory environment. *Humanities and Social Sciences Communications*, *11*(1),1-18, https://doi.org/10.1057/s41599-024-03560-x