



THE IMPACT OF ARTIFICIAL INTELLIGENCE ON SECURITY AND DEFENCE: A STRATEGIC NECESSITY OR AN UNDERESTIMATED RISK?

Major General Adrian BRÎNZĂ

Deputy Chief of Defence Staff for Planning



The world is entering a new era of conflict, where technology and data are becoming weapons just as important as conventional ammunition. Artificial Intelligence (AI) is no longer just a concept of the future, but a concrete reality of the Fourth Industrial Revolution and a key factor that can determine the structure of power, both regionally and globally, as well as a tool already used in modern warfare. The United States of America, China, Russia, and other world powers are allocating enormous resources to develop autonomous systems capable of analysing data, identifying threats, and even deciding the course of military operations.

In practice, the rapid evolution of AI is redefining defence structures, tactics, and military strategies on a global level. Technology is becoming a decisive factor in the response capacity of states, influencing both operational efficiency and national security. Romania, as a NATO member and a state located in a geopolitically sensitive area, must understand that AI is no longer just an option, but a strategic necessity. However, the integration of this technology brings multiple challenges: Who controls military AI? How secure are autonomous systems? Are we prepared to defend ourselves against cyberattacks targeting AI-based infrastructures?

Artificial Intelligence – Exponential Impact and Emerging Trends in the Field of Defence

AI-augmented weapon systems are already being employed in missions involving reconnaissance, surveillance, logistics, and combat operations, executing complex tasks while reducing human risk. The transformational impact of AI in defence is no longer a matter of debate – it is an inevitability. The critical question is how to move beyond theoretical potential toward achieving exponential gains in capability development and military readiness. The role of artificial intelligence in modern warfare extends far beyond traditional notions of speed and efficiency. Its strategic value lies in the ability to convert



data into actionable intelligence, thereby enhancing decision-making speed, operational accuracy, and ultimately, mission success.

Currently, three key AI-driven trends are reshaping the defence landscape. Firstly, AI integration into command and control (C2) architectures enables faster and more informed decision-making in critical situations. The era in which military leaders were required to manually sift through overwhelming amounts of data is rapidly fading. AI algorithms can analyse vast data streams in real time, identifying patterns and potential threats with remarkable speed. This capability provides military leadership with timely and actionable insights, significantly reducing the time between decision and execution – a decisive advantage in contemporary warfare.

Secondly, AI is redefining operational readiness by enabling predictive maintenance, efficient logistics, as well as advanced military simulations and training. AI systems can assess the condition of military equipment and anticipate potential failures, thus optimizing maintenance schedules and minimizing the downtime of combat units. Through AI-driven predictive maintenance and decision-making optimization across the logistics chain, armed forces can ensure sustained mission readiness by reducing preparation time and avoiding unnecessary resource expenditure. Moreover, advanced algorithms can be used to generate realistic combat scenarios, significantly enhancing the quality of soldier training and preparedness for a wide range of operational situations. These capabilities allow military organizations to adopt a proactive approach to maintenance while ensuring operational flexibility and responsiveness to evolving mission demands.

Thirdly, artificial intelligence has fundamentally transformed the nature of military tactics. Modern confrontations increasingly take place within the cyber domain, where AI plays a critical role in monitoring, preventing, and responding to cyberattacks. Armed forces that integrate AI into their defence strategies are better equipped to anticipate and neutralize threats, thereby protecting critical infrastructure more effectively. Furthermore, AI facilitates the development and deployment of autonomous systems, such as unmanned ground vehicles and combat drones. These platforms are capable of executing military operations without direct human intervention, significantly altering battlefield

dynamics. AI-augmented autonomous systems offer new opportunities for minimizing operational risks while enhancing mission efficiency. AI is already enhancing the capabilities of unmanned vehicles – whether aerial, terrestrial, or maritime – enabling them to operate in complex environments, provide real-time intelligence, and carry out sophisticated missions including surveillance, reconnaissance, and even strategic strikes against enemy targets. All of this can be achieved while keeping personnel out of harm's way, thus contributing to force protection and operational sustainability.

Looking ahead, the role of quantum computing in enhancing encryption and operational precision is expected to further strengthen AI-driven defence systems. Additionally, artificial intelligence enables what can be described as an “amplification of operational capacity” – allowing armed forces to achieve more with the same set of resources. This capability is critical in an era characterized by high-intensity conflicts, escalating threats, and constrained defence budgets, where efficiency and adaptability are of paramount importance. AI-based command centres, for instance, are already improving the agility and effectiveness of military coalitions around the world.

Risks and Challenges of Artificial Intelligence in Defence Sector

Artificial intelligence is having a profound impact on modern warfare, fundamentally transforming how armed conflicts are conducted and reshaping military tactics. While AI offers significant opportunities for enhancing operational efficiency and strengthening defence capabilities, it also presents critical ethical and strategic challenges that demand careful consideration. Moreover, AI has the potential to exacerbate international tensions, as states compete to develop increasingly advanced military technologies. This emerging technological arms race may contribute to global instability, while the use of AI in the military risks undermining existing international norms governing armed conflict.

1. Cyber Warfare and AI Vulnerabilities

Modern conflict is no longer confined to physical confrontations on the battlefield. As previously mentioned, cyber warfare has become



an essential component of contemporary military engagements. Artificial intelligence plays a significant role in detecting and preventing cyberattacks, thereby safeguarding a state's critical infrastructure. However, AI can also be exploited by malicious actors to bypass security systems, creating new and highly sophisticated threats. The ability to automate cyberattacks through AI empowers both state and non-state actors to conduct sabotage and espionage operations with increased efficiency. Such capabilities have the potential to destabilize state structures, inflict severe economic and social damage, and do so without the need for direct armed confrontation. Cyberattacks targeting AI-based military systems represent one of the most serious threats in today's defence landscape. A vulnerable AI infrastructure can be exploited by adversaries to:

- **manipulate data inputs** – adversaries may inject false or misleading information into AI networks, distorting the situational awareness and decision-making processes of military forces;
- **seize control of autonomous systems** – sophisticated hackers can potentially take over drones or automated defence systems, effectively turning them into weapons against their own operators;
- **disrupt critical communications** – if AI is integrated into command-and-control networks, a successful cyberattack could paralyze the decision-making and operational response capabilities of an entire military force.

2. Loss of Human Control over Military Decision-Making

The growing impact of artificial intelligence on armed conflict raises major ethical and legal challenges that require serious international deliberation. One significant concern is the potential desensitization of soldiers and political-military leaders to the use of violence, as direct human involvement in operational decisions diminishes. At present, decisions to initiate attacks remain under human authority; however, in the near future, advanced algorithms may be capable of making such decisions autonomously. This development raises several critical questions, including:

- Who is responsible if an AI algorithm makes an error and causes the death of innocent civilians?

- How can we ensure that AI systems comply with the principles of international humanitarian law?
- Is it ethical to allow machines to make lethal decisions without human intervention?

In light of these concerns, there is a clear need for comprehensive international regulation governing the use of AI in armed conflict. Such regulation must ensure that AI is employed in ways that uphold human rights and adhere to established norms of international law. Many experts advocate for maintaining human oversight – keeping humans “in the loop” – with respect to all critical decisions involving the military use of AI.

3. Economic and Social Implications

One of the most evident ways in which artificial intelligence can influence the global balance of power is through its impact on national and international economies. Countries that successfully integrate AI into their economic systems can gain a substantial competitive advantage. For instance, nations such as the United States of America and China are investing heavily in AI research and development – not only to enhance economic efficiency but also to reinforce their geopolitical influence. These innovations allow them to position themselves as global leaders in key sectors such as healthcare, transportation, and manufacturing. This leadership, in turn, grants them greater control over essential resources, markets, and emerging technologies. Furthermore, AI facilitates the development of personalized and adaptive solutions tailored to the specific needs of national economies, which may widen the gap between technologically advanced nations and those unable to adapt to these emerging trends.

The AI impact extends beyond economic and military domains; it also carries profound social implications. The widespread adoption of AI-powered social media platforms has the potential to shape public opinion and influence political behaviour. Both state and non-state actors can more easily manipulate information and sway electoral outcomes by leveraging algorithms that target citizens based on their preferences and behavioural patterns. Moreover, AI may contribute to the deepening of existing social and economic tensions, as power disparities are exacerbated by unequal access to advanced technologies.





Countries that fail to develop AI capabilities or invest in digital specialization risk falling behind, which could lead to heightened social and political instability.

The majority of innovations in the field of artificial intelligence are being developed by private companies based in technologically advanced countries such as the United States of America, China, and others. In order to remain relevant in the new global reality shaped by AI, smaller powers are compelled to invest in national-level AI research and development centres. Additionally, these nations must foster collaboration between the public sector, private industry, and academic institutions to support the development of indigenous technologies. Equally important is the need to advocate for the adoption of common standards that ensure interoperability with allied forces, while safeguarding data security and national interests.

To fully harness the AI advantages, Romania must adopt a clear and well-directed national strategy. Key measures that could be considered include:

1. Developing a robust digital infrastructure in the defence sector by implementing secure networks that enable the safe operation of AI systems without the risk of cyberattacks.
2. Establishing a national ecosystem for research and innovation in military AI, supported by sustained investment in specialized laboratories and the attraction of technological talent.
3. Adopting clear policies for the use of AI in combat, including strict regulations to ensure that AI systems are not deployed without human oversight and are fully compliant with international legal standards.
4. Training military personnel in AI operations by updating the Romanian Armed Forces' educational and training programmes to reflect the requirements of emerging digital technologies.

Conclusion: A One-Way Path Having a Purposeful Direction!

Artificial intelligence holds the potential to profoundly reshape the global and regional balance of power. With far-reaching economic, military, and social implications, AI is not merely a technological

tool but a transformative force that introduces complex ethical, strategic, and operational challenges, thus requiring a carefully balanced and forward-looking approach. It is therefore essential for nations to recognize both the opportunities and the risks of a world increasingly shaped by AI. These changes may redefine international alliances, exacerbate uneven economic development, and generate new geopolitical tensions. Ultimately, the way in which the international community manages the rapid evolution of these technologies will determine the future trajectory of global stability and international relations.

The integration of AI into the fields of security and defence presents unique challenges. AI systems used for sovereign tasks – particularly in defence – are fundamentally different from the data-intensive models typically employed in consumer-oriented AI applications. This distinction underscores the need to develop a hybrid form of AI specifically tailored for security and defence contexts. Such an approach would combine two methodologies: one based on machine learning and statistical processing of large or moderate volumes of data, and another based on rule-based logic, often referred to as symbolic AI, which operates on predefined rules and logical frameworks.

Artificial intelligence will play a central role in the future of warfare, whether we are prepared for it or not. Romania cannot afford to fall behind, but it must adopt a strategic approach that combines innovation with strict security and ethical safeguards. If we aspire to build a modern, efficient, and geopolitically aware military force, the time to invest in AI and prepare for future challenges is now. Moreover, we must adapt our defence doctrine and allocate resources to remain competitive in an increasingly complex geopolitical landscape. The technological race waits for no one, and states that fail to keep pace risk becoming increasingly vulnerable. Romania must be ready!

