

Artificial Intelligence use for Military Purposes

Artificial intelligence (AI) is changing the way wars are fought, as it is used by armies around the world. While its use is claimed to make military operations more efficient, it also raises concerns about the respect of IHL.

Acknowledgments

Case prepared by Clémence Duranleau-Hendrickx, Master student at Paris-Panthéon-Assas University, under the supervision of Louis Perez, doctoral student at Paris-Panthéon-Assas University and Professor Julia Grignon.

A. THE CANADIAN ARMY JOURNAL “LEVERAGING ARTIFICIAL INTELLIGENCE FOR CANADA’S ARMY: CURRENT POSSIBILITIES AND FUTURE CHALLENGES”

[Source: Geoffrey Priems & Peter Gizewski, “Leveraging artificial intelligence for Canada’s army: current possibilities and future challenges”, The Canadian army journal 19.2, 2021]

[...]

Potential benefits

[1] Incentives for the exploration, development and adoption of AI by military organizations are compelling. Given the capacity of high-speed computers (network speed and processing power) and AI algorithms to process and analyze massive quantities of data with a degree of speed and accuracy far beyond that of humans, claims that AI-enabled systems could potentially transform defence across the board are not surprising. By acting as a means of boosting the speed of analysis of humans and machines, AI holds the promise of enhancing data use, management and situational awareness capabilities. For militaries, the results could well translate into cost savings, improved control systems, faster decision-making, new operational concepts and greater freedom of action.

[2] Artificial intelligence-enabled information and decision support systems have the potential to facilitate better decision-making in “complex, time-critical battlefield environments,” allowing for a quicker identification of threats, faster and more precise targeting, and the creation of flexible options for commanders based on

changing conditions on the battlefield. Applications can range from command and control and intelligence, surveillance and reconnaissance to training and logistics. Moreover, as the backbone technology of robotic and autonomous systems, AI holds out prospects for innovations in weaponry by enabling the development of advanced autonomous systems with considerable military potential (e.g. robotic systems and drones). AI may even generate dramatic shifts in force structures and operational concepts, potentially reducing burdens on personnel and the costs of military hardware while at the same time increasing the efficiency and effectiveness of warfare itself.

Limitations and challenges to adoption

[3] Prerequisites for the effective introduction of AI are nonetheless considerable and may well impose limits on the capacity of military organizations to fully realize some of the possibilities that applications of AI offer. In addition, militaries may not be fully willing to pursue some of the possibilities inherent in AI technologies themselves.

[4] Indeed, current capability is confined to the performance of discrete functions and the learning of specific tasks (e.g. narrow AI). The brittleness of AI technology is concerning. Brittleness is reflected by any algorithm that cannot generalize or adapt to conditions outside a narrow set of assumptions. For instance, with the addition of a few bits of graffiti, a stop sign can be read as a 45-mph speed limit sign. Application to circumstances involving excessive uncertainty can in fact be especially dangerous. Take, for example, the erroneous selection and prosecution of a friendly target such as a friendly fighter or civilian vehicle. As such, limitations on the use of AI in military settings—and in military operations in particular—can be considerable. Faced with an environment in which incoming information may be unreliable, incomplete or even deliberately falsified by adversaries, willingness to trust in the solutions that such technologies may offer remains justifiably weak.

[5] Beyond that, and even in areas in which such technology is generally considered reliable, its development and application can be demanding. Requirements include ensuring that data is available in sufficient quantity for the development of the algorithms to be used for enabling military systems. They also include ensuring the quality of the algorithms themselves, a requirement that depends on the provision and effective preparation and coding of training data before AI is integrated into military systems, as well as ensuring the validity of incoming data from the real world, which includes edge cases (uncommon use cases). And they include ensuring that the AI developed and integrated in military systems is reliable (i.e. that it works in the manner in which it is intended).

[6] Each of those requirements can involve considerable challenges. The acquisition of large amounts of data for training may encounter organizational resistance to data-sharing based on political and legal constraints, thereby reducing the quality of algorithms to be trained and the reliability of those systems that use them. Data acquired may contain racial, gender and other biases stemming from data preparation and coding. Furthermore, as algorithms become more complex, vulnerabilities to manipulation through the injection by

adversaries of bad data in training datasets can grow. To the extent that such challenges are present, trust in AI and its application in a military context is likely to suffer.

[...]

Act

[...]

[7] Challenges also surround applications of AI to military systems for the delivery of lethal effects. Central to that question is the degree to which such systems may pose issues of reliability or violate existing Laws of Armed Conflict (LOAC). Questions concerning where to use AI in the Sense-Decide-Act loop will require careful consideration. While it is clear that it is appropriate to use AI as part of Sense, the decision to do so must be conducted by a human. Beyond that, a decision must be made if and when AI may be used within Act.

[8] In fact, current doubts regarding trust in the reliability of AI strongly suggest that, while the pursuit of fully autonomous and semi-autonomous lethal weapon systems areas should be investigated—particularly given the potential need to defend against such systems— their development and use must await the results of further experimentation and research. Any view to employment of such systems must be based on high confidence that they will perform as intended and on the understanding that such use would only occur within established ethical and legal parameters (e.g. the LOAC).

[...]

Conclusion: the way ahead

[...]

[9] Beyond that, considerable effort must be made to ensure trust in the development and use of AI-enabled military systems. Accordingly, rigorous experimentation and testing practices and more intuitive man-machine integration will be needed to ensure that the strengths of each are emphasized. While some tolerance for failure must be allowed in the process of developing and integrating AI into military systems, criteria for success must be clear so as to allow for learning if and when failure occurs. Throughout, care must be taken to ensure that efforts aimed at the development and use of all AI-enabled systems are informed by the need to fully adhere to prevailing ethical standards within the Canadian military as well as international norms and laws governing armed conflict (i.e. LOAC).

[...]

B. GOVERNING AI FOR HUMANITY: FINAL REPORT OF THE HIGH-LEVEL ADVISORY BODY ON ARTIFICIAL INTELLIGENCE

[Source: United Nations's High-level Advisory Body on Artificial Intelligence, Governing AI for Humanity: Final Report, September 2024, available at: <https://www.un.org/en/ai-advisory-body/about>]

[...]

[1] Among the challenges of AI use in the military domain are new arms races, the lowering of the threshold of conflict, the blurring of lines between war and peace, proliferation to non-State actors and derogation from long established principles of international humanitarian law, such as military necessity, distinction, proportionality and limitation of unnecessary suffering. On legal and moral grounds, kill decisions should not be automated through AI. States should commit to refraining from deploying and using military applications of AI in armed conflict in ways that are not in full compliance with international law, including international humanitarian law and human rights law.

[2] Presently, 120 Member States support a new treaty on autonomous weapons, and both the Secretary-General and the President of the International Committee of the Red Cross have called for such treaty negotiations to be completed by 2026. The Advisory Body urges Member States to follow up on this call.

[3] The Advisory Body considers it essential to identify clear red lines delineating unlawful use cases, including relying on AI to select and engage targets autonomously. Building on existing commitments on weapons reviews in international humanitarian law, States should require weapons manufacturers through contractual obligations and other means to conduct legal and technical reviews to prevent unethical design and development of military applications of AI. States should also develop legal and technical reviews of the use of AI, as well as of weapons and means of warfare and sharing related best practices.

[4] Furthermore, States should develop common understandings relating to testing, evaluation, verification and validation mechanisms for AI in the security and military domain. They should cooperate to build capacity and share knowledge by exchanging good practices and promoting responsible life cycle management of AI applications in the security and military domain. To prevent acquisition of powerful and potentially autonomous AI systems by dangerous non-State actors, such as criminal or terrorist groups, States should set up appropriate controls and processes throughout the life cycle of AI systems, including managing end-of-life cycle processes (i.e. decommissioning) of military AI applications.

[...]

C. UNITED STATES BUREAU OF ARMS CONTROL, DETERRENCE, AND STABILITY, "POLITICAL DECLARATION ON RESPONSIBLE MILITARY USE OF ARTIFICIAL INTELLIGENCE AND AUTONOMY"

[Source: Bureau of Arms Control, Deterrence, and Stability, “Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy”, United States department of State, November 9, 2023, available at: <https://www.state.gov/political-declaration-on-responsible-military-use-of-artificial-intelligence-and-autonomy-2/>]

An increasing number of States are developing military AI capabilities, which may include using AI to enable autonomous functions and systems. Military use of AI can and should be ethical, responsible, and enhance international security. Military use of AI must be in compliance with applicable international law. In particular, use of AI in armed conflict must be in accord with States’ obligations under international humanitarian law, including its fundamental principles. Military use of AI capabilities needs to be accountable, including through such use during military operations within a responsible human chain of command and control. A principled approach to the military use of AI should include careful consideration of risks and benefits, and it should also minimize unintended bias and accidents. States should take appropriate measures to ensure the responsible development, deployment, and use of their military AI capabilities, including those enabling autonomous functions and systems. These measures should be implemented at relevant stages throughout the life cycle of military AI capabilities.

[...]

D. UNITED NATIONS GENERAL ASSEMBLY, RESOLUTION ON ARTIFICIAL INTELLIGENCE IN THE MILITARY DOMAIN AND ITS IMPLICATIONS FOR INTERNATIONAL PEACE AND SECURITY

[Source: United Nations General Assembly, “Artificial intelligence in the military domain and its implications for international peace and security”, A/C.1/79/L.43, 16 October 2024, available at: <https://docs.un.org/en/A/C.1/79/L.43>]

The General Assembly,

Affirming that international law, including the Charter of the United Nations, international humanitarian law and international human rights law, applies to matters governed by it that occur throughout the life cycle of artificial intelligence capabilities as well as the systems they enable in the military domain,

Stressing the importance of ensuring responsible application of artificial intelligence in the military domain, which, for the purpose of this resolution, includes human-centric, accountable, safe, secure and trustworthy artificial intelligence used in compliance with international law,

Bearing in mind that this resolution focuses on the whole life cycle of artificial intelligence capabilities applied in the military domain, including the stages of pre design, design, development, evaluation, testing, deployment, use, sale, procurement, operation and decommissioning, and that this resolution does not cover

artificial intelligence in the civilian domain,

Mindful that States have started to increasingly integrate artificial intelligence into a broad array of applications in the military domain, including into weapons, weapon systems, and other means and methods of warfare, as well as systems that support military operations,

Cognizant of potential implications for international peace and security, in particular in the fields of arms control, disarmament and non-proliferation, resulting from developments related to the application of artificial intelligence in the military domain,

Recognizing the need to enhance a shared understanding of potential effects of artificial intelligence in the military domain to harness the benefits while minimizing the risks of its use, and the need to further assess them,

Mindful of the potential opportunities and benefits of artificial intelligence in the military domain, such as in the areas of compliance with international humanitarian law, including protection of civilians and civilian objects in armed conflict,

Mindful also of the challenges and concerns that the application of artificial intelligence in the military domain raises from humanitarian, legal, security, technological and ethical perspectives, as well as the possible impact of such applications on international security and stability, including the risk of an arms race, miscalculation, lowering the threshold for conflict and escalation of conflict, proliferation to non-State actors, and also noting the possible consequences with regard to, inter alia, gender, racial, age or social aspects that could potentially be caused by bias in datasets or other algorithmic biases of artificial intelligence,

Mindful further of the need for States to implement appropriate safeguards, including measures that relate to human judgment and control over the use of force, in order to ensure responsible application of artificial intelligence in the military domain consistent with their respective obligations under applicable international law,

[...]

1. *Affirms* that international law, including the Charter of the United Nations, international humanitarian law and international human rights law, applies to matters governed by it that occur throughout all stages of the life cycle of artificial intelligence, including systems enabled by artificial intelligence, in the military domain;

2. *Encourages* States to pursue national, regional, subregional and global efforts to address the opportunities and challenges, including from humanitarian, legal, security, technological and ethical perspectives, related to the application of artificial intelligence in the military domain;

3. *Also encourages* States to continue assessing implications of the application of artificial intelligence in the military domain for international peace and security, including through a multilateral dialogue in relevant international forums;

[...]

DISCUSSION

I. General questions

1. (*Document A, paras 1 & 2; Document D*)

- a. How is Artificial Intelligence (AI) used for military purposes? How widespread is this use? What are the benefits of using it? Could AI improve the compliance of military operations with IHL? If so, to what extent?
- b. Does IHL authorize or prohibit the use of AI for military purposes? Does it impose any limits on such use?

2. (*Document A, paras. 4-6*)

- a. What are the different limitations that AI systems can face in military applications, particularly in combat situations?
- b. In what ways could these limitations result in violations of IHL?

3. (*Document B, para. 1; Document D*)

- a. How does the use of AI for military purposes challenge the rules governing the conduct of hostilities under IHL? How do the cardinal rules on the conduct of hostilities apply to the use of AI in military operations? (P I, Art. 48, 51, 52, 57, 58; P II, Art. 13; CIHL, Rules 1, 7, 11, 14, 15)
- b. How does the rule on precautionary measures in attack apply to military AI systems? (P I, Art. 57; CIHL, Rule 15)
- c. What are the risks of potential bias in AI military systems? How could compliance with IHL be affected by such bias?

4. Under International Criminal Law, how can responsibility be attributed if it is a military AI system that conducts operations? Does the principle of command responsibility apply to military personnel supervising the system? (Rome Statute, Art. 28)

II. Autonomous weapons under IHL

5. (*Document A, para. 8; Document B, para. 2; Document C*)

- a. How does the rule of distinction apply to AI-driven autonomous weapons? (P I, art. 48, 51, 52; P II, art. 13; CIHL, Rule 1)
- b. How does the obligation to review new weapons to ensure their compliance with IHL applies to AI-driven autonomous weapons? (P I, Art. 36)

III. The role of the international community

6. (Document B, para. 4; Document D)

- a. What is the role of States in ensuring that military AI complies with IHL? How can States ensure to respect their obligations under IHL, while still leveraging and benefiting from AI's efficiency and speed? (GC I-IV, art. 1)
- b. What measures or mechanisms should States adopt to ensure that AI military systems comply with IHL? Is human control and supervision necessary to ensure respect of IHL?

7. (Document B, para. 2; Document C; Document D)

- a. Is IHL sufficient to regulate the use of military AI? Do you think that military AI should be the subject of a new legally binding instrument?
- b. Do you think the international community could reach a consensus on what constitutes an ethical and responsible use of military AI, and is therefore allowed under IHL? What factors may hinder such a consensus? Are you aware of any international initiatives moving in this direction?
- c. Do you think a political declaration such as the one issued by the United States Bureau of arms control, deterrence and stability is important for respecting and ensuring respect of IHL? Should more initiatives of this kind be encouraged? Would they be sufficient? (GC I-IV, art. 1)
- d. Should the use of military AI be encouraged or discouraged? Should the proliferation of AI-driven military systems, including autonomous weapons, to armed groups be prevented?