

2023

Author
Stefan Venceljovski

The Potential and Risk of Artificial Intelligence in Conflict Areas and War Zones to Aid in Targeting and Eliminating Potential Enemy Combatants

ABOUT THE AUTHOR

Stefan Venceljovski is a Political Science and Canadian history student at the University of Waterloo, studying international relations and policy from the Cold War period to today. His primary focus of research and study is the broader implications of historical narratives and trends on the modern world and how the shaping of our narratives impacts how we preserve our outcomes today. While focusing primarily on his current studies, he also gives his professional time to The Waterloo Historical Review. This on-campus, student-run, peer-reviewed journal looks to give publishing experience and credits to the University of Waterloo students in history. He also gives his time to the University of Waterloo Historical Society, an organization dedicated to bringing scholarship and discussions to UW history students. AI is particularly interesting for him because it has an unprecedented impact on future study, inquiry and dissemination of information and news within history and the broader discipline of international relations.

Funding Acknowledgment

This Policy Brief was funded by the Mobilizing Insights in Defence and Security (MINDS) Targeted Engagement Grant program designed to facilitate collaboration and mobilize knowledge between the Department of National Defence, the Canadian Armed Forces, and academia and other experts on defence and security issues. Through its Targeted Engagement Grants, collaborative networks, scholarships, and expert briefings, MINDS works and collaborates with key partners to strengthen the foundation of evidence-based defence policy making. These partnerships drive innovation by encouraging new analyses of emerging global events, opportunities, and crises, while supporting a stronger defence and security dialogue with Canadians.

Executive Summary

The Canadian military needs to recognize the potential of Artificial Intelligence (AI) for warfare applications. AI can potentially improve the Canadian military's speed, accuracy, and effectiveness in modern-day war zones. However, using AI in these war zones and general military applications raises ethical, legal, and strategic concerns. This policy brief explores the benefits of AI in warfare and the ethical/legal risks of AI in warfare and provides recommendations for the Canadian military.

Background

AI technology in warfare involves using algorithms, machine learning, and automated processes to support decision-making, intelligence gathering and analysis, and automatic targeting of threats. AI technology can enhance the effectiveness of military operations in these areas by creating mechanisms for faster and more accurate decision-making, increasing situational awareness for human decision-makers, and reducing human error and risk to human life. However, ethical considerations and risks of cybersecurity threats make these advancements turbulent and require careful consideration.

Benefits:

More Accurate Decision Making and Improved Situational Awareness/Precision:

AI technology can analyze large amounts of data from various unique sources, such as sensors, satellites, the internet, and social media, to provide real-time information about the battlefield and conflict areas in condensed, palatable briefs. This information can help military commanders and decision-makers make more informed decisions and respond quickly to changing circumstances. AI technology can analyze data and identify targets more accurately, reducing the risk of collateral damage and civilian casualties. AI can also remove biases from target selection and better identify real-time targets using imaging software to remove further strain and the possibility of making errors in the target selection process. Finally, AI can be used to create real-time reports of conflict or disaster areas using the same data listed previously to aid in preparation for aid support and analysis of the extent of the damage.

Reduced Risk to Human Life

AI technology can remotely control drones, robots, and other autonomous systems, reducing the risk of human casualties in combat. This can also provide a strategic advantage by enabling the military to operate in hazardous environments that would be too dangerous for human soldiers. AI drones could effectively pilot through conflict areas to assess enemy combatants' combat effectiveness/readiness and resources, reducing the need for human intelligence agents to risk their lives and exposure to counter-intelligence operations. AI combatant drones and robots could also be used to accurately take out targets from long or short distances and eliminate the need for human life in war zones or conflict areas. Finally, AI systems are potentially better able to eliminate enemy combatants effectively and efficiently, reducing the need for human life to be present in conflict areas.

Risks and Potential Questions Raised

Ethics:

The use of AI in warfare raises ethical concerns about the responsibility and accountability for decisions made by autonomous systems. There is also a risk that AI technology could be used to develop indiscriminate weapons or violate international humanitarian law. Who decides that the AI has chosen the right target and executed the correct decision in eliminating the target? Moreover, what threshold does the AI need to reach to decide whether taking human life or engaging with «enemy» combatants is correct? How can data be fed without biases and potentially disastrous results? Is it moral to allow AI combatants to take human life while their handlers never enter the conflict zone or place any stake in the affected area? Questions like these are critical to establishing moral, responsible policy around AI uses in warfare. War is already ethically questionable, but removing the human aspect of it leaves more questions about the morality of warfare.

Cybersecurity:

AI systems are vulnerable to cyberattacks. There is always a risk that with constantly evolving technologies and cyber strategies, AI systems would be at risk of being taken over by foreign or independent actors looking to use the systems against their makers or their own «targets.» The potential for manipulation of data and the risk of that data being stolen is also very high. This data, mined from intelligence, can be extremely sensitive and contain state secrets concerning satellite placement and use, data on individuals deemed targets and information on the nation's intelligence apparatus. Given that all this data needs to be fed into the AI to make it effective, if not monitored closely, actors may be able to manipulate the outputs of the AI to eliminate incorrect targets or civilians or steal that data for their benefit.

Shortcomings Yet to be Addressed:

AI systems are currently very poor at understanding the context of inputted data. Recognition algorithms struggle to understand the data they are fed; they learn textures and gradients of the image's pixels, for example, and use that to match patterns in other images. AIs often incorrectly identify portions of the picture when given similar or identical scenes. When feeding AI large amounts of enemy combatant data, this becomes an issue, which can result in misidentifying targets and executing commands/prerogatives in incorrect areas or misclassifying images as enemy targets, misleading decision-makers. AI systems at present also cannot explain their reasoning and decision-making process. They are fed data and spit out results; the makers can then interpret this, but the decision-making process of the AI is still left unknown. This is important when we attempt to answer questions about liability and responsibility in cases where AI makes mistakes. If we can not correctly ascertain why an AI made the decision it did and using what data, we can not fully keep systems accountable.

Policy Recommendations

The following policy recommendations could be offered to the Canadian military regarding the use of AI in warfare:

1. Develop Clear and Universal Ethical Guidelines:

The Canadian military should develop clear ethical guidelines that outline the acceptable uses of AI in warfare, including developing and using autonomous weapons systems against enemy combatants. These guidelines should ensure that AI technology is consistent with international humanitarian law and human rights standards. Regularly reviewing and updating the guidelines is necessary to keep up with technological advancements and the evolving discourse surrounding AI. Educating and promoting ethical guidelines among individuals involved in developing and monitoring AI systems is essential to ensure that personnel and AI effectively adhere to and incorporate them. It is imperative to disseminate these guidelines internationally for global collaboration in the ethical use of AI. This ensures that all nations unite to promote and uphold ethical AI practices.

2. Invest in Cybersecurity:

The Canadian military should invest in cybersecurity measures to protect AI systems from cyberattacks. This includes ensuring that AI systems are secure and resilient against cyber threats and training personnel on cybersecurity best practices. The military should also establish procedures for responding to cybersecurity incidents involving AI systems.

3. Conduct Regular Risk Assessments:

The Canadian military should conduct regular risk assessments to evaluate the potential risks and benefits of using AI in warfare. This includes assessing the risks associated with using autonomous weapons systems and other AI technologies and the potential strategic implications of AI in warfare.

4. Participate in International Efforts to Regulate AI and in Cross-disciplinary Conversation:

The Canadian military and the Canadian government should participate in international bodies and treaties that are looking to regulate the use of AI in warfare and for military benefits. It should also facilitate policymakers and AI researchers to learn from each other to create a more well-rounded and informed base for development where both the creators and implementers are well-informed and knowledgeable. By actively pursuing these treaties and spearheading the conversation internationally while keeping critical players in the decision-making process informed and educated, Canada will be able to develop a better sense of the direction that other nations and allies are taking regarding AI and will be able to position itself as a leader in technology.

Conclusion

By implementing these policy recommendations, the Canadian military can ensure that the use of AI in warfare is consistent with ethical principles, respects international law and human rights standards, and minimizes the potential risks associated with AI technology. Continuing research into AI as a tool for warfare is needed. This looks like a general discussion around its ethics and uses as a tool to eliminate combatants. This conversation needs to be internally within the military and externally with consultation from experts in the AI and ethics fields. This way, the decided policy will be unbiased and well-rounded. Overall, it is an essential consideration for the Canadian military if it seeks to be a modern, combat-ready and influential force in the near future.