Source: Adobe

LEVERAGING ARTIFICIAL INTELLIGENCE FOR CANADA'S ARMY:

Current Possibilities and Future Challenges

Major Geoffrey Priems, Canadian Army Land Warfare Centre, and Peter Gizewski, Defence Research and Development Canada – Centre for Operational Research and Analysis

Introduction

Interest in the military applications of artificial intelligence (AI) is growing worldwide. Indeed, much like a number of other advances in technology, AI is increasingly viewed as a potentially significant enabler of military effectiveness.

Not surprisingly, interest in the implications that AI holds for the Canadian Army (CA) and the possibilities that exist for its adoption are on the rise. Questions concerning how and to what extent AI may be employed to potentially benefit the realization of *Close Engagement: Land Power in an Age of Uncertainty*, the Canadian Army's capstone operating concept, and enhance the conduct of the Army's five operational functions, are particularly salient. So too are questions concerning the challenges that could confront the effective adoption of AI and the measures required to surmount them.

This article offers a preliminary examination of those questions. It derives from ongoing work on AI at the Canadian Army Land Warfare Centre[1] to examine and identify the implications that AI holds for the CA and the effective realization of the Army's capstone operating concept.

The article outlines the prospective benefits and challenges that AI poses in terms of adoption by militaries and the conduct of military operations. It then examines the potential impacts of AI on the realization of *Close Engagement*, identifying areas where the application of AI holds the prospect of enhancing the Army's operational effectiveness. The article concludes by outlining a number of key prerequisites and practices necessary to ensure that such efforts are pursued responsibly and effectively.

Artificial Intelligence

Definitions of AI are numerous and evolving.[2] As currently defined by the Department of National Defence however, AI is "the capability of a computer to perform such functions that are associated with human logic such as reasoning, learning and self-improvement."[3] While not universally accepted, such a formulation offers an institutionally familiar and sufficient basis for the discussion of AI within a CA context.

Potential Benefits

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.

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.[4] 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).[5] 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.[6]

The fact that such technologies are ever more ubiquitous, and increasingly available to friend and foe alike, further incentivizes the pursuit of AI-enabled military technologies. In the case of the former, growing interest in AI among allies highlights the need to have sufficient AI capabilities to ensure future allied interoperability and military effectiveness. As for the latter, evidence of sustained exploration and investment in military applications of AI on the part of adversaries (e.g. Russia, China) bolsters incentives to pursue such technologies to detect and defend against future prospects for ever more AI-enabled military threats.[7]

Limitations and Challenges to Adoption

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.

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.[8] For instance, with the addition of a few bits of graffiti, a stop sign can be read as a 45-mph speed limit sign.[9] Application to circumstances involving excessive uncertainty can in fact be especially dangerous.[10] 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.

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).[11]

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.[12] Data acquired may contain racial, gender and other biases stemming from data preparation and coding.[13] Furthermore, as algorithms become more complex, vulnerabilities to manipulation through the injection by adversaries of bad data in training datasets can grow.[14] To the extent that such challenges are present, trust in AI and its application in a military context is likely to suffer.

Those risks may be held in check through careful human supervision and robust testing. That said, truly effective oversight requires a familiarity with the details of the AI technology on the part of operators as well as significant systems integration and socialization that may be difficult to achieve. The challenge of effective oversight is compounded given the difficulties of understanding the technology itself. The processes involved in machine reasoning do not easily equate to those of humans,[15] nor is the logic that AI systems employ easy to comprehend. For commanders and system operators charged with and responsible for the use of capabilities—some of which can well determine life and death—placing faith in technologies whose decision-making processes are opaque at best can be a bridge too far.[16]

Source: Adobe

IMPLICATIONS FOR THE CANADIAN ARMY

Such realities indicate that adoption of AI on the part of the CA, while offering promise, must proceed with caution and be informed by a realistic sense of limits. Neither Canada nor the CA are immune from encountering the challenges described above. For instance, the closer that AI technology gets to the kill chain without appropriate human oversight, the greater the risk that catastrophic consequences could occur. Accordingly, care must be taken to study or adopt technology where it can aid human decision making. A "black box" AI that instructs a human on what to do would be unacceptable. An AI advisor must be able to explain its recommendations/conclusions so that a human can comprehend and has confidence in the recommendation proposed. The human decision-maker must be able to offer leadership a clear and comprehensible explanation of the AI-derived solution provided.[17]

Nevertheless, if pursued and applied carefully, much of what AI offers generally aligns well with CA requirements as detailed in *Close Engagement, Land Power in an Age of Uncertainty*. *Close Engagement* aims to address the challenges of an operational environment characterized by rapid change as well as by a wide range of complex humanitarian challenges and ever more technologically enabled adversaries capable of fielding a range of increasingly maneuverable lethal and non-lethal systems and elaborate countermeasures. Meeting such challenges rests heavily on the capacity to ensure access to the information and analysis needed for understanding and adjusting to changing conditions faster than adversaries. Such a goal requires versatile personnel, adaptable equipment, organization and processes, and "an ability to develop shared understanding."[18] As an advanced method of information processing, AI can offer an essential means of helping to address such needs by providing a capacity to process and analyze data from a widening array of sources faster and more accurately than is humanly possible. As such, AI can serve as an important decision-making aid, enabling the development of both the individual and shared understanding essential for determining potential courses of action, for prioritizing the acquisition, disposition and use of military assets, and for providing the data, information and actionable intelligence needed to conduct operations in a timely manner.

Beyond that, AI may even serve to bolster the security of the network upon which the Army relies. "High-capacity networks able to operate over long distances offers a significant advantage"[19] to the conduct of Army operations. In fact, a secure and robust network is central to ensuring the swift, secure distribution of the data and analysis needed for the effective conduct of Army operations.

Source: Department of National Defence

Data collection exercise for a Defence Research and Development Canada – Valcartier project known as Joint Algorithmic Warfighter Sensors. The project is part of a larger Canadian Army science and technology portfolio, Empowered Dispersed Operations in the Digital Age.

By offering the prospect of developing algorithms capable of guarding against network failure, electronic warfare and cyberattack, AI may serve to more fully ensure that the Army is capable of "reap(ing) the network's advantages,"[20] and thereby conduct operations in a more secure, coordinated and collaborative manner. Improvements in areas such as interoperability, force-generation, power projection and sustainment, and the conduct of dispersed operations, may all stand to benefit as a result.

Throughout, as AI technology is pushed to the tactical edge, there will be a need to ensure that enough electricity (energy) is available to support it. In addition to the network, work on advanced power management and battery technology will be essential.

ENHANCING OPERATIONAL FUNCTIONS: POTENTIAL OPPORTUNITIES

Examination of the implications of AI for each of the Army's five operational functions[21] provides fidelity both on the manner in which military applications of AI should be considered by Army decision-makers as well as on some of the possibilities it holds for supporting *Close Engagement* and Army operations.

COMMAND

Artificial intelligence has the potential to strengthen the command function of military operations by increasing human–machine collaboration in both the planning and execution of military operations. Indeed, the capacity of machines to process and make sense of vast amounts of information and to complete complex tasks and match or exceed human performance is increasingly evident.[22] As such, AI holds the promise of significantly lessening the cognitive burden on soldiers and significantly aiding decision-making.

Given that the exercise of command is a fundamentally human endeavour, any AI application must be responsive to human control. Accordingly, system design must reflect human needs and requirements. User interfaces should be simple and/or intuitive in design to better ensure functionality. Moreover, given that AI technology has yet to reach the point where humans can rely unfailingly on algorithms, the provision of fail-safe mechanisms that allow operators to shut systems down should they perform in an unintended or incorrect manner, or to adjust systems when situations and/or orders so warrant, must be an essential component of design and development.[23]

Applications conforming to such parameters may be numerous. In the area of communications, AI technologies may prove useful for improving communication flow, offering means of distributing messages in a manner that is both more accurate and more timely than existing methods. Indeed, AI systems could be combined with procedural mechanisms (labelling) such as precedence—the communication differentiation scheme used by the now defunct Automated Data Defence Network—to prioritize messages based on content (i.e. Routine, Priority, Immediate, Flash and Flash Override). The result would be a practical and seemingly attainable means of allowing traffic to be throttled through the system with a level of speed, accuracy and skill, especially during combat operations.

Using AI in facilitating alliance communication may prove attractive as well. Notably, given security classifications and caveats, information sharing and trust can emerge as friction points within allied coalitions during the conduct of operations. Potential problems of this nature are best determined and resolved prior to operations (i.e. when time is not a factor). Otherwise, such discussion risks slowing the critical flow of information that can affect operational outcomes. While part of the solution involves improving both the type and nature of security markings contained on information, AI can serve as an efficient means of facilitating the quick and effective distribution of such information once processed. The result may well be an improved capacity to share more information with allies and joint, inter-agency, multinational and public partners.

Aspects of battlespace management may also profit from AI technologies. Here, possibilities might include the production of AI-generated courses of action (COA), as well as risk and options analysis of the COAs produced. Indeed, the AI-enabled gaming of options (using thousands of simulations) could lead to faster risk identification as well as to the identification of mitigation measures required to address them.

Beyond that, the commander's personal staff could be bolstered by using AI-enabled advisory support to legal and policy advisors.[24] For both, the body of scholarly work (legal articles, legislation, case law, and policies of foreign nations) that can be reviewed and flagged for human review by an algorithm is extremely fast and increasingly accurate. The implementation and use of such a process would provide a commander with timely and accurate information to make more complex and time-sensitive decisions.

SENSE

Artificial Intelligence may be particularly well suited for enhancing the operational function of Sense. AI systems have a relationship with data, which is derived from sensors (or inputs). It has been said that every soldier is a sensor. AI offers the promise of making each soldier, and every other sensor that is networked, available to many "clients" to complement human decision-making. The ability to network and share can be a significant force multiplier that could create synergies in operations that currently do not exist.

Potentially beneficial injects of AI in support of the Sense function are plentiful. Such technologies may be especially useful for performing imagery and signals analysis. As detailed and repetitive tasks, imagery and signals analysis consume an inordinate amount of human effort. Typically, these tasks require more people than currently practical to hire, with each person hired requiring high security clearance levels to enable data review (which gives rise to security risks and inordinate costs). Yet, if conducted by AI, not only would output be quick and accurate, but those personnel previously involved could be redirected to more profitable pursuits. Such a move would cue humans to focus more precisely on any anomalous data flagged by the AI system.

At some point, AI may also be highly useful for optimizing sensors for targeting. Here, while choices will need to be made in future to determine if direct kinetic effects will be permitted, or if there will be limitations or conditions set to govern kinetic or non-kinetic effects, the capacity of AI to support the process appears viable. AI could enhance the capacity of sensors to assist in determining targets (including targets of opportunity) and in notifying/cueing decision makers. Once targets of interest are established, AI could also assist in identifying those actions/options most appropriate for achieving the operational effects that decision-makers seek.

The data mining of social networks and open sources to determine relationships, plans and patterns of life and to confirm events, as well as the use of sentiment analysis to determine the specific or general feelings of a population on an issue based upon explicitly stated feelings or non-verbal behaviours, offer similarly promising avenues for AI application.[25] Other potential uses may include the development of immersive digital environments to help train soldiers, as well as AI-enabled translation applications to facilitate language understanding for operations abroad. The former may not only serve to enhance collective training but may also help lower the real-world costs of putting soldiers into the field. Meanwhile, AI-enabled language applications offer an accessible means for performing tasks such as real-time translation and the transcription of meetings. The results may not only include more accurate communication, but also the creation of better working relationships with local inhabitants (especially if combined with sentiment analysis). Eventually, soldier capability—a key element of *Close Engagement*—could also improve, given the cultural understanding, facial and name recognition, and the human intelligence information likely to be gained.[26]

ACT

Act integrates firepower, manoeuvre and offensive information operations to achieve desired effects. In terms of AI, such operations raise issues of human-machine teaming, trust, and the delivery of both lethal and non-lethal effects.

Human-machine teaming represents a cornerstone for AI development and operationalization, and maximizing the strengths of the human and machine, while minimizing the shortcomings of each, is central to its effectiveness. For example, the AI can spot an anomaly in a data set that would otherwise be unseen by a human and then pass it to a human, who can then decide what that anomaly may mean and the action to take. In many cases, such teaming may already meet this standard. Yet confidence in the capacity of such teaming to perform assigned tasks correctly in all potential circumstances still remains elusive.

Accordingly, building trust in the capacity of AI to perform correctly must represent a key area for further research and investigation. To that end, efforts could focus on the testing and eventual refinement of AI-enabled systems in "edge cases," i.e. in circumstances that pose particularly difficult or complex challenges (e.g. how an AI system might target a child soldier, or a non-combatant who may be providing intelligence to the enemy, or perfidy, i.e. false surrender under flag of truce). The insights gained could be used to further develop systems capable of optimizing soldier/operator trust.[27]

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.

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).

The active pursuit of AI-enabled non-kinetic effects may be more productive. Applications in the informational and cyber domains could yield benefits for shaping the operational environment.[28] Such applications may be used to prevent or slow the need for the application of kinetic effects. For instance, non-kinetic emails containing instructions for blocking communication, or that contain viruses that lead to a denial of service, may prove useful for preventing the transmission of information to a kinetic force (such as a soldier with a weapon, or the operation of a weapons system/platform). Investigation of smart virtual personal assistants (VPA)[29] such as Siri and Alexa may yield benefits as well. Systems such as those could support the Act function in areas such as navigation, communication, targeting, logistics and health systems. Applications may eventually be extended to include weapons systems (kinetic, or non-kinetic), with VPAs used to improve weapon accuracy and assess weapon impact on targets.

Finally, the exploration of AI technologies capable of enabling the use of swarming techniques is also worth pursuing.[30] The technique, which takes the form of multiple simultaneous (or near simultaneous) attacks to overwhelm a defender can be accomplished with technology such as AI-enabled robots/drones (in the tens, hundreds, or even thousands).[31] Growing interest in swarming techniques within both allied and adversarial defence establishments suggests that enabling technologies be investigated for adaptation to defensive (Shield) purposes at a minimum and, eventually, for purposes of offense.

SHIELD

AI applications appear well suited to supporting the Shield function. The prospect of unmanned robotic systems replacing humans in situations or acts likely to carry a high risk of serious injury or death accords well with the intolerance of Western nations for casualties.[32]

AI-enabled military systems could provide increased standoff detection of chemical, biological, and explosive threats, especially through sensors (integrated onto other platforms, or standalone). Smart adaptive clothing technology could be integrated into uniforms. And AI could also be used to help optimize personal protective equipment designs and configurations.[33]

Applications in the area of network protection may prove equally beneficial. Given *Close Engagement's* call for a mobile yet fully networked field headquarters, AI applications that allow for analysis of the electromagnetic environment (wired, optical, laser, wireless), security, and the optimization of means and methods of communication could offer greater functionality as well as security. Such efforts would help to reduce or mask electromagnetic signatures, thus lowering the prospect of headquarters being targeted during combat operations. Indeed, AI could help counter an enemy's ability to gain information from friendly transmissions by masking the quantity, nature, frequency and duration of communications.

A Canadian Armed Forces member works with the Telerob Explosive Ordnance Disposal and Observation Robot (tEODor) during the force integration training phase of Exercise ARDENT DEFENDER 18.

Source: Combat Camera

Source: Combat Camera

An Explosive Ordnance Disposal Technician operates a tEODor Remotely Operated Vehicle while his coworker uploads forensic images to their laptop during Exercise ARDENT DEFENDER.

Source: Combat Camera

A Remote Mobile Investigator inspects a vehicle containing a suspected simulated improvised explosive device during Exercise ARDENT DEFENDER.

Source: Combat Camera

Corporal Frederick Nadeau and Corporal Tyler Bell of 2nd Regiment Royal Canadian Horse Artillery perform maintenance on a Light Utility Vehicle.

To address security concerns, a robust AI-enabled red team could be formed to test the system and act upon any intrusions by authorized and unauthorized users that are detected.[34] The digital platform would offer a measure of control over communication, and its analysis would enhance understanding of what is happening within friendly systems. Anomalies detected, such as unusual access or information transfers (i.e. downloads) could then be flagged for immediate denial and followed up via human investigation.

Additional benefits may exist in the area of route security. Here, application of computer vision could assist in reducing the likelihood of being mined or booby-trapped without detection. Other systems such as autonomous route clearance or demining systems could be used as well. More specifically, such applications could form part of a larger system for overcoming battlefield obstacles through route planning.

Autonomous weapon systems for perimeter defence, ground-based air defence and similar anti-access/area-denial applications could also generate new capabilities, assuming that legal and policy enablers are in place. In this case, the term “autonomous” would be a version of supervised autonomous, which includes preparation of the system to delineate the area to be affected, the time that the area is to be affected, the nature of the targets to be engaged, and/or the type of systems that may be selected to engage a target, which could be a mix of kinetic and non-kinetic systems.

Finally, AI could be used in a variety of ways to reduce the likelihood of being targeted by integrated reconnaissance-strike systems through smaller or managed signatures in all spectra. Considerable research is needed into methods for reducing all signatures. Land forces should seek not only to be invisible or masked in electro-magnetic environments but also to be more opaque in all light spectra and quieter in operation.

SUSTAIN

Sustain encompasses most logistical functions and includes Health Services. Linkages with civilian advances in AI technology are clearer in the Sustain realm than in the case of other operational functions. As such, applications of AI may be especially conducive to the area of Sustain, as less work may be required to operationalize AI-enabled solutions.

Close Engagement suggests that “control of overall logistics capability must be centralized at formation level.”[35] The use of AI holds promise for enabling just such an approach, so long as all elements of the logistics chain remain connected with data.

Potential AI applications include support of predictive maintenance.[36] In order to make improvements in vehicle maintenance, consideration must be given to ensuring that information can be gleaned from the vehicle in an asynchronous but episodic manner (i.e. not always connected, but frequently connected). Accordingly, AI-enabled sensors could be installed to gather information such as vehicle diagnostic data, fuel consumption, mileage and tire wear, and track all work performed on a vehicle (this information is not currently collected in the CA fleet). The collection of such data fleet-wide would permit the conduct of data analytics for purposes of predictive vehicle maintenance. In addition, it could assist maintainers in deciding when optional maintenance could be performed under tactical conditions.

Smart supply chain management, as well as the development of advanced logistics, also represent attractive candidates for AI application.[37] Areas to be explored could include the use of drone and other technology for autonomous delivery and return of logistics. Moreover, risks to soldiers could be reduced through use of autonomous convoy and resupply. Leader/follower and wingman concepts could be investigated in support of the effort.

Beyond that, AI could support medical and casualty evacuation using smart systems to enable recovery of personnel. Expertise can be shared (virtually) closer to patients for local treatment by non-experts and AI can also assist in providing personalized medical treatment plans and robotic surgery.[38] Accordingly, the CA should advocate for AI within the Surgeon General's line of authority.

CONCLUSION: THE WAY AHEAD

Clearly, application of AI offers numerous possibilities for enhancing Army capabilities in a range of areas. Potentially beneficial applications are evident in the case of all five of the Army's operational functions. If effectively pursued, the results could serve to make the conduct of *Close Engagement* more efficient, effective and secure in the process. Indeed, the development of AI technology promises to aid the speed of decision making, enable the achievement of desired effects through a more effective use of lethal or non-lethal actions, reduce risks to the force, and reduce the cognitive burden from the individual soldier to the formation commander, and it also holds the promise of aiding defence against many offensive AI technologies/techniques.

Achieving such results will require ingenuity, resources and allocative skill. Sustained investment in the materiel and human resources required for pushing AI forward will be essential.[39] So too will organizations capable of adopting and integrating technologies from the non-defence commercial sector to ensure innovation as well as effectively procuring the technologies and systems required.[40]

To those ends, the CA must work with others in a collaborative environment to share ideas and knowledge and, later, to share data/information during the employment of AI systems. Development of a viable data strategy capable of ensuring the effective marking, processing and sharing of data both domestically (i.e. with other government departments and agencies) and abroad (with allies and partners) will be particularly important.[41] Moreover, given the speed with which developments in AI can take place, technology horizon scanning should be conducted on a regular basis with an emphasis on AI.

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).

Addressing such requirements will be challenging. Indeed, it will require considerable engagement and cooperation as well as the clear and continual articulation of Army needs and requirements, both within and beyond the military.[42] That said, given the growing significance of AI to defence and security, pursuit of such efforts are essential. Not only is the promise that AI holds for military organizations, including the CA, clear, but the potential threats that may arise given its pursuit by our adversaries cannot be ignored.

ABOUT THE AUTHORS

Major Geoff Priems is a full-time Reservist who works in the Concepts Section of the Canadian Army Land Warfare Centre (CALWC). He serves as the desk officer for Artificial Intelligence, the Crisis in Baltika project, Robotics and Autonomous Systems. This article stems from his soon to be published paper, "Toward a Canadian Army Artificial Intelligence Concept: Some Initial Food for Thought."

Peter Gizewski is a Senior Defence Scientist for the Defence Research and Development Canada Centre for Operational Research and Analysis (DRDC – CORA) and a member of the Land Operational Research and Analysis Team. Mr. Gizewski provides support to CALWC's ongoing work toward the development of an AI concept for the CA.

ENDNOTES

1. See Canadian Army Land Warfare Centre, "Toward an Army Artificial Intelligence Concept: Some Initial Food for Thought" (Kingston: unpublished manuscript, December 2020).

2. Indeed, ongoing progress in the development of AI technology has served to ensure that definitive definitions of AI are elusive. As Evan Stubbs, Chief Analytics Officer of SAS Australia, has noted "…the definition [of AI] is a set of moving goal posts…."

See Asha Barbaschow, “Artificial Intelligence,” at https://www.zdnet.com/article/ai-tends-to-lose-its-definition-once-it-becomes-commonplace-sas/ 31 May 2016, (accessed on 30 October 2019).

3. Canada, Artificial Intelligence (Online: Defence Terminology Bank Record 1596 (01/04/2005); accessed 2 July 2020 (Usage Canada).

4. According to Matej Tonin, AI holds the potential to:

   - vastly improve the reaction times of defensive systems against fast-acting weapon systems, such as hypersonic missiles, cyber-attacks, or directed-energy weapons;

   - deliver actionable information faster to decision makers, which could potentially deliver a decisive edge on adversaries;

   - quickly discover cyber intrusions by detecting evasive malicious codes or by scanning for suspicious patterns of behaviour rather than for specific code; and,

   - help identify attempts to manipulate citizens through disinformation campaigns.

   See Matej Tonin, “Artificial Intelligence: Implications for NATO’s Armed Forces,” Report No. 149, Science and Technology Committee (STC), Subcommittee on Technology, Trends and Security (STCC), 13 October 2019, pp. 3–4.

5. Ibid. p. 3.

6. Ibid. p. 4.

7. Ongoing Chinese and Russian investments in autonomous systems have fueled an increasing unease about a potential new revolution in military affairs and a subsequent AI arms race. Given that reality, and notwithstanding the possibility that adversarial applications of artificial intelligence are speculative and may at times be based on worst-case analysis, the need to be vigilant and explore as well as adopt and integrate AI where possible to improve capability would be both responsible and sensible. See Mary Cummings, “The AI that Wasn’t There: Global Order and the (Mis)Perception of Powerful AI,” and Michael C. Horowitz, Lauren Kahn and Christian Ruhl, “Introduction: Artificial Intelligence and International Security,” both in Policy Roundtable: Artificial Intelligence and International Security, *Texas National Security Review*, June 2020, pp. 8–9, and p. 3 respectively. Available online at https://tnsr.org/roundtable/policy-roundtable-artificial-intelligence-and-international-security/ (accessed on 26 June 2020).

8. M.L. Cummings, “The Surprising Brittleness of AI,” https://www.womencorporatedirectors.org/WCD/News/JAN-Feb2020/Reality%20Light.pdf.

9. Ibid.

10. Michael Horowitz, Lauren Kahn and Christian Ruhl, “Introduction: Artificial Intelligence and International Security,” p. 2.

11. On these points, see Michael C. Horowitz, Lauren Kahn and Christian Ruhl, “Introduction: Artificial Intelligence and International Security,” both in Policy Roundtable: Artificial Intelligence and International Security, *Texas National Security Review*, June 2020, p. 3.

12. Ibid.

13. Ibid.

14. Ibid.

15. Peter Gizewski, “Building Trust in Artificial Intelligence-Enabled Capabilities: Problems and Prospects,” DRDC-RDDC-2020-L164 (Ottawa: Defence Research and Development Canada, September 2020), p. 5.

16. Ibid.,

17. For example, an AI system can identify a target and flag it for review by a human technician, who then verifies the observed target. From that point, the image is shared with the decision, maker, who then reviews the evidence (e.g. a photo) and confirms the target (individual, location or equipment) in question. The operational environment is considered by the decision-maker, and the type of target engagement is selected by the decision-maker to prosecute the target. Finally, the executive decision is made to engage (or prosecute) the target.

18. Canadian Army Land Warfare Centre, *Close Engagement: Land Power in an Age of Uncertainty* (Kingston: Army Publishing Office, 2019), pp. 15–16.

19. Ibid., p. 38.

20. Ibid.

21. The operational functions provide a means of understanding key aspects of the operational environment. Such categorization constitutes a “bucketing” or sorting system and, as such, is imperfect. In a similar way, AI is a cross-cutting discipline that has the potential to affect almost every aspect of the military. Consequently, the categorization of AI applications discussed in this section cannot be definitive. In fact, in some cases, applications discussed in the context of one particular operational function may arguably have equal if not more relevance for another. That said, such categorization is suggestive of the various possibilities that AI offers in each of these areas.

[22] As Matej Tonin notes, “AI’s ability to sift through today’s data-rich environment and communicate findings in a compelling manner…will become ever-more important. While human resources currently allow for the processing of, at best, 20% of the information produced today, this percentage could go down to a mere 2%.” See Matej Tonin, “Artificial Intelligence: Implications for NATO’s Armed Forces,” Report No. 149, Science and Technology Committee (STC), Subcommittee on Technology, Trends and Security (STCC), 13 October 2019, p. 3.

[23] Efforts aimed at rendering the logic of AI more comprehensible to human operators should be pursued in tandem with such efforts. Indeed, the investigation of measures aimed at ensuring that the outputs of AI and the manner in which they are arrived at are easily understood will be a key component in facilitating greater trust and confidence in the adoption and use of AI in command. For a useful overview of potential measures aimed at generating such trust, see Marlon W. Brown, “Developing Readiness to Trust Artificial Intelligence within Warfighting Teams,” *Military Review*, (January–February 2020), pp. 36–44. Available online at https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/January-February-2020/Brown-AI-ready/ (accessed on 7 July 2020).

[24] Ibid.

[25] Ibid.

[26] Canadian Army Land Warfare Centre, *Close Engagement: Land Power in an Age of Uncertainty* (Kingston: Army Publishing Office, 2019), p. 33.

[27] To this end, a series of common cases could be drawn up, as well as a list of the most complex cases (i.e., edge cases) for testing purposes. Studies should be undertaken to understand attitudes towards AI algorithms, and the trust that the soldier and commanders place in them, and how this trust is achieved for optimal employment of a system.

[28] Alain Auger, *Artificial Intelligence (AI)-enabled Applications for the Canadian Army*, DRDC-RDDC-2019-L080 (Valcartier: Defence Research and Development Canada, April 2019), p. 4.

[29] Ibid.

[30] Ibid.

[31] BBC News, “Shanghai New Year drone display was pre-recorded,” BBC News online https://www.bbc.com/news/world-asia-china-50979557, 3 January 2020 (accessed on 2 July 2020).

[32] Erin A. McDaniel, “Robot Wars: Legal and Ethical Dilemmas of Using Unmanned Robotic Systems in 21st Century Warfare and Beyond” (Fort Leavenworth, Kansas: US Army Command and General Staff College, 2008), p. 4.

[33] Alain Auger, *Artificial Intelligence (AI)-enabled Applications for the Canadian Army*, DRDC-RDDC-2019-L080 (Valcartier: Defence Research and Development Canada, April 2019), p. 4.

[34] On this point, see Alain Auger, *Artificial Intelligence (AI)-enabled Applications for the Canadian Army*, DRDC-RDDC-2019-L080 (Valcartier: Defence Research and Development Canada, April 2019), p. 3.

[35] Canadian Army Land Warfare Centre, *Close Engagement: Land Power in an Age of Uncertainty* (Kingston: Army Publishing Office, 2019), p. 46.

[36] Alain Auger, *Artificial Intelligence (AI)-enabled Applications for the Canadian Army*, DRDC-RDDC-2019-L080 (Valcartier: Defence Research and Development Canada, April 2019), p. 4.

[37] Ibid.

[38] Ibid.

[39] AI is not a field that is static. It is growing and evolving rapidly, and a lack of investment can result in being left behind. Hiring qualified personnel at the outset, investing in education, and planning for the employment of AI will require long-term thought and planning. Investment in technology will involve building the infrastructure that supports AI research and development, testing and deployment. That will be costly, as systems are routinely and frequently upgraded (on the order of every six months).

[40] Given the rapidly evolving nature of AI technology, its development and integration for the purpose of enhancing military capability promises to pose significant challenges for procurement. AI technology evolves at a pace of days/weeks/months as opposed to military procurement, which normally occurs within Horizons 2 or 3 (5–15+ years). Moreover, at present, the procurement system is most comfortable with known products that help ensure that the government gets value for the investment. Risky endeavours that may fail are not well tolerated. AI research is often slow and beset with failure, which represents opportunity for learning and growth.

[41] Data issues involve the life cycle of data, which should be addressed through consultation with the Assistant Deputy Minister (Data, Innovation and Analytics) (i.e. ADM [DIA]) and the Assistant Deputy Minister (Information Management, (i.e. ADM [IM]).

[42] The CA does not own all the issues related to AI technology. Consequently it must work with partners and must be able to compromise in order to make gains.