

Canadian
Forces
College

Collège
des
Forces
Canadiennes



Major Serge Turcotte

**L'importance de l'intelligence artificielle dans
les communications tactiques et opérationnelles**

JCSP 47

Exercise Solo Flight

Disclaimer

Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission.

© Her Majesty the Queen in Right of Canada, as represented by the Minister of National Defence, 2022

PCEMI 47

Exercise Solo Flight

Avertissement

Les opinions exprimées n'engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite.

© Sa Majesté la Reine du Chef du Canada, représentée par le ministre de la Défense nationale, 2022

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES

JCSP 47 – PCEMI 47

2020 – 2022

Exercise Solo Flight – Exercice Solo Flight

Major Serge Turcotte

**L'importance de l'intelligence artificielle dans
les communications tactiques et opérationnelles**

“This paper was written by a student attending the Canadian Forces College in fulfilment of one of the requirements of the Course of Studies. The paper is a scholastic document, and thus contains facts and opinions, which the author alone considered appropriate and correct for the subject. It does not necessarily reflect the policy or the opinion of any agency, including the Government of Canada and the Canadian Department of National Defence. This paper may not be released, quoted or copied, except with the express permission of the Canadian Department of National Defence.”

“La présente étude a été rédigée par un stagiaire du Collège des Forces canadiennes pour satisfaire à l'une des exigences du cours. L'étude est un document qui se rapporte au cours et contient donc des faits et des opinions que seul l'auteur considère appropriés et convenables au sujet. Elle ne reflète pas nécessairement la politique ou l'opinion d'un organisme quelconque, y compris le gouvernement du Canada et le ministère de la Défense nationale du Canada. Il est défendu de diffuser, de citer ou de reproduire cette étude sans la permission expresse du ministère de la Défense nationale.”

L'IMPORTANCE DE L'INTELLIGENCE ARTIFICIELLE DANS LES COMMUNICATIONS TACTIQUES ET OPÉRATIONNELLES

“Artificial intelligence is the future, not only for Russia, but for all humankind. It comes with colossal opportunities, but also threats that are difficult to predict. Whoever becomes the leader in this sphere will become the ruler of the world.”
- Vladimir Putin, Sept 1st, 2017¹

INTRODUCTION

Comme le mentionne Christian Brose², l'avenir sera défini par l'intelligence artificielle, les systèmes autonomes et autres technologies émergentes qui révolutionnent les industries mondiales et sont maintenant en train de bouleverser les différents modèles de défense, dont le modèle américain. Les armées comme celle des États-Unis et le Canada doivent construire leur réseau de systèmes de combat qui permettra aux personnels de comprendre rapidement les menaces, de prendre des décisions et d'entreprendre des actions militaires.

L'intelligence artificielle (*Artificial Intelligence* / AI) est largement reconnue comme une capacité militaire vitale qui ne fera que gagner en importance à l'ère des opérations multi-domaines. Les besoins technologiques de l'AI et apprentissage machine (*Machine Learning*, ML) dans le contexte des communications opérationnelles et tactiques n'en font pas exception. La résilience et interopérabilité des systèmes de communication sont et seront encore plus critiques aux opérations. Par interopérabilité, on fait autant référence à la compatibilité des systèmes au sein d'une même armée et/ou élément de manœuvre qu'avec les systèmes de leurs alliées.

¹ Vincent, James. 2017. «Putin says the nation that leads in AI 'will be the ruler of the world'. » The Verge.

² Brose, Christian. 2020. The Kill Chain: Defending America in the Future of High-Tech Warfare. New York, NY: Hachette Books.

Ce mémoire argumentera que la communication est le terrain vital dans la guerre algorithmique et que la résilience de l'intelligence artificielle ainsi que l'apprentissage machine dans les systèmes de communications tactiques seront vitale dans les conflits à venir. Pour ce faire, quelques éléments clés seront d'abord définis suivis d'un portrait de la situation au niveau des réseaux de communication actuelle. Par la suite, les avantages de l'AI/ML seront mis de l'avant pour nous mener vers l'argumentaire du terrain vital de la guerre algorithmique et l'importance du caractère résilient de l'AI/ML. Avant de conclure, un bref aperçu des défis possible relié à la mise en œuvre sera partagé.

DÉFINITION

Qu'est-ce que la guerre algorithmique? C'est une guerre qui est menée par des systèmes autonomes alimentés par l'AI, qui peuvent contrôler les plateformes d'armes, les systèmes, et même les opérations et les tactiques dans un champ de bataille connecté³. C'est une guerre menée par des moyens artificiellement intelligents. Ces derniers sont ceux qui ne sont pas seulement intelligents dans la collecte et l'analyse de l'information, mais aussi dotée de capacité artificielle capable d'agir sur le renseignement d'une manière que les humains ne peuvent pas⁴. La guerre algorithmique ne peut être initiée que par des systèmes fonctionnels capables d'apprendre par eux-mêmes (ML) à partir de scénarios inconnus et imprévisibles. Elle convertit l'environnement complexe du champ de bataille en un aperçu utile (apprentissage en profondeur / *deep learning*) avec peu ou pas de manipulation humaine, de façon autonome, et ce, dans un environnement

³ Nair, Jayakrishnan N. 2020. «Algorithmic Warfare – World is Waiting.» *Indian Defence Review*.

⁴ Crosby, Courtney. 2020. «Operationalizing Artificial Intelligence for Algorithmic Warfare.» *Military Review*

opérationnel⁵. Le Pentagone américain définit un algorithme de guerre comme étant tout algorithme qui est exprimé en code informatique, qui s'effectue à travers un système construit, et qui est capable de fonctionner en relation avec un conflit armé.⁶

Qu'est-ce qu'un réseau de communication sans fil? Traditionnellement, il consistait en radios point-à-points transportant un message sonore d'un émetteur aux récepteurs dans un rayon donné. Ceci a évolué et inclus maintenant le transport de données multiples encore par la radio plus ou moins traditionnelle, mais qui a évolué, et également par une myriade d'autres technologies comme la communication satellite, le Wi-Fi, le LTE, l'optique (*lasercom*), etc., le tout de récepteurs à émetteurs autant statiques qu'en mouvement. Ces réseaux doivent être résilients, sécuritaires, stables et agiles.

Qu'est que l'AI/ML pour les réseaux de communication sans fil militaire? L'AI est un système intelligent créé par l'homme doté de compétences telles que l'apprentissage, le raisonnement et la résolution de problèmes. L'apprentissage automatique (ML) est inhérent à l'AI et le système apprend en permanence et évolue au cours des opérations, avec son expérience. Les machines intelligentes sont capables d'auto-apprentissage et de résultats optimisés en fonction de la situation tactique. Au niveau des communications tactiques et opérationnelles, l'AI/ML permet entre autres d'optimiser les réseaux en détectant et réagissant aux menaces, en créant une déception ou en confondant le brouillage ennemi. Ces réseaux dits cognitifs ont des capacités de

⁵ *Ibid*

⁶ Blum, Gabriella, Dustin Lewis, et Naz Modirzadeh. 2016. «Accountability for Algorithmic Autonomy in War.» *Lawfare*.

décisions permettant par exemple de réduire au besoin la puissance d'une radio pour en réduire la signature électromagnétique, faire le réacheminement automatique vers de meilleurs moyens pour optimiser le signal ou encore pour contourner une attaque cyber ou de guerre électronique, etc. Ces réactions et interventions doivent se produire en quelques secondes pour être efficaces; doivent s'exécuter plus rapidement que n'importe quel humain ne peut le faire. Ce ne sont que quelques exemples où l'AI/ML peut aider à fournir une supériorité technique dans les réseaux tactiques ⁷.

DISCUSSION

Réalité des systèmes de communication actuels

Peu importe l'armée, l'élément ou le contexte, les systèmes de communication actuels sont connus pour être une source de frustration des utilisateurs et des chaînes de commandement et trop souvent un, sinon le maillon faible lors d'opérations⁸. La communication est prise ici dans le contexte de communication tactique et opérationnelle, principalement sans fil au sein même d'un théâtre d'opérations, mais également avec des postes de commandements et autres parties prenantes à l'extérieur de la zone d'opération. La liste des problèmes en communication est longue et s'est alourdie au fil du temps. Par exemple : les demandes en capacité de bande passante (*bandwidth*) ne cessent d'augmenter avec les types de données à partager (cartes, images, vidéo, vidéoconférence, documents de plus en plus lourds, pilotage et conduite de véhicules, réalité augmentée, etc.), la limitation du débit (*throughput*), la faible puissance des

⁷ Harrison, Todd. 2021. «Battle Networks and the Future Force.» *Center for strategic & International studies*.

⁸ Mcelroy, Barry. 2017. «The network-centric approach: Solving the challenges of real-time battlefield communications.» *Military Embedded Systems*.

radios mobiles et donc leurs portées limitées, l'autonomie limitée de ces mêmes systèmes, l'incapacité de contourner les obstacles physique qui nécessite le relais de messages d'un signaleur à un autre augmentant les risques de distorsion du dit message, l'ajout de nouvelles technologies non compatible avec les précédentes ou encore avec celle d'autres systèmes provenant de différents fournisseurs.⁹

La bande passante facilite la capacité de communication et est devenue de plus en plus importante. Une bande passante élevée est critique aux capacités de communication, car elle prend en charge un plus grand volume de donnée avec un délai d'échange beaucoup plus court et fournit une plus grande stabilité de connexion.¹⁰ L'augmentation des besoins en bande passante ne fera qu'augmenter avec les nouvelles technologies connectées, les besoins en cryptage et sécurité ainsi que les portées à atteindre.

Les systèmes actuels sont trop souvent incompatibles entre eux, du moins sans l'ajout de technologie supplémentaire permettant de faire le pont entre deux (ou plus) technologies ce qui devient un potentiel point de défaillance supplémentaire dans le réseau. Défaillance autant d'un point de vue stabilité du réseau que de la sécurité de ce dernier étant un point d'entrée pour une éventuelle attaque. En plus d'un manque d'interopérabilité avec les alliées, elles manquent d'interopérabilité entre elles. Ce manque d'interopérabilité est entre autres causé par les

⁹ Thales. s.d. *Examining the Advantages of Networking Radios for Dismounted Combat*. Accès le Mai 15, 2022.

¹⁰ Leland, Joe, et Porche III Isaac. 2004. «Future Army Bandwidth Needs and Capabilities.» *Rand*.

différentes technologies¹¹ (formes d'onde (*waveforms*), protocole de données, etc.), les différents fabricants et leur propriété intellectuelle ainsi que leur niveau technologique.

La dernière décennie a vu l'émergence de nouvelles technologies sur le terrain dont les réseaux maillés (*mesh network*). Encore à ces balbutiements, ce type de réseau contrôlé à l'aide de logiciel et d'AI, combine des nœuds de réseau sans fil offrant la capacité d'acheminer instantanément des données via le meilleur chemin et la meilleure fréquence disponible. Ces nœuds consistent en n'importe quels moyens de communication disponibles et compatibles sur le réseau; que ce soient des radios montées sur véhicule (terrestre, drone, avion, etc.), montées sur mâts statiques, via les satellites, etc. Les chemins de transfert de données sont construits automatiquement et sont évalués en termes de qualité et de performances pour chaque paquet d'information envoyée et reçue. Il n'y a pas de nœud de contrôle central et donc pas de point de défaillance unique¹². Ce type de réseau est présentement utilisé principalement entre positions d'importances stratégiques et opérationnelles fixes comme les postes de commandement et les radars par exemple, ce qui limite beaucoup son potentiel. Les capacités de réseau actuelles et futures doivent se concentrer sur les capacités de transport qui permettent un transport multi-chemins automatique à grande vitesse et à haute capacité qui est transparent pour l'utilisateur.¹³

¹¹ Goure, Dan. 2020. «The Military Has An Intra-Service Communications Problem. SOCOM Might Have The Answer.» *The National Interest*.

¹² McElroy, 2017

¹³ Walker, Amy, et Claire Heining. 2022. «Army National Guard signal conference highlights data, data transport modernization.» *U.S. Army*.

“Our networks are a core piece of our warfighting architecture. Our networks are weapons, and, so, we have to treat them like weapons. We have to, we have to plan to protect them, make them resilient because everything that we're going to do in an artificial intelligence or data-driven way will depend on the security of those networks.”
 - Marine Corps Lt. Gen. Michael S. Groen, Oct 8th, 2021 ¹⁴

Les avantages de l’AI/ML dans le domaine militaire.

D’entrée de jeu, l’intelligence artificielle et l'apprentissage automatique (AI/ML) offrent plusieurs avantages au-delà des réseaux de communication. Elle permet entre autres la mise en place de système autonome œuvrant dans tous les domaines et supportant à différents niveaux les cinq fonctions opérationnelles (Action, Détection, Protection, Maintien en puissance et Commandement).

En ce moment, l’AI/ML dans le domaine militaire est utilisé dans plusieurs technologies à des degrés variant de la simple classification de données à de la surveillance avec analyse d’image et vidéo et aide à la décision. Les systèmes dits autonomes en sont encore à leur début, principalement avec de l’aide à la navigation / pilotage pour certains véhicules comme les drones, satellites, etc. L’AI est très présente dans le domaine cyber et les opérations d’informations et ouvre la porte à un plus grand spectre d’actions possible au niveau des opérations en zone grise ainsi que la détection et contre-manœuvre dans cette même zone.

L’avancement de l’AI/ML offrira de plus en plus de techniques prometteuses et révolutionnaire afin d’améliorer la façon d’exploiter les systèmes en réseau et satisfaire les

¹⁴ Vergun, David. 2021. «General Says Artificial Intelligence Will Play Important Role in Network Defense.» *DoD News*.

besoins d'information des utilisateurs.¹⁵ En agissant comme un moyen d'accélérer la vitesse d'analyse des humains et des machines, l'AI permet d'améliorer les capacités d'utilisation, de gestion et de connaissance de la situation des données. De plus, l'AI permet de rehausser le niveau d'entraînement des troupes en offrant différentes options comme la réalité virtuelle et augmentée pour ne nommer que ceux-ci.

Pour les militaires, ceci pourrait entraîner des économies de coûts, des systèmes de contrôle améliorés, une prise de décision plus rapide, de nouveaux concepts opérationnels et une plus grande liberté d'action¹⁶.

Au niveau des réseaux de communication, cruciaux au bon fonctionnement des cinq fonctions opérationnelles, l'utilisation de l'AI sur le champ de bataille offre plusieurs avantages. Premièrement, l'AI permet une réduction des risques en offrant une protection accrue contre les menaces au réseau. Cette protection est démontrée par une capacité accrue de détection et de défense contre des menaces de types cyber et/ou de guerre électronique. Celles-ci ne seraient pas détectées aussi rapidement par un opérateur humain¹⁷ et ce délai rendrait inutile toute action tardive. Cette capacité de rapidité d'action permet entre autres une protection des données, une plus grande stabilité du réseau et donc un meilleur commandement et contrôle et support aux unités déployées. De plus, l'AI réduit le risque d'erreur humaine, offre une disponibilité 24/7 et une prise de décision rapide. Au niveau du maintien en puissance, l'AI permet une meilleure

¹⁵ U.S. Army CCDC Army Research Laboratory Public Affairs. 2020. «Machine learning algorithms promise better situational awareness.» *U.S. Army*.

¹⁶ Priems, Geoffrey, et Peter Gizewski. 2022. «Leveraging Artificial Intelligence for Canada's Army: Current Possibilities and Future Challenges.» *The Canadian Army Journal* 19.2 40-51

¹⁷ Vergun, 2021

agilité en offrant une meilleure visibilité sur la situation logistique, en produisant des prédictions en temps réel sur les besoins¹⁸, en surveillant et planifiant les activités de maintenance de véhicules ou autres. De plus, en cas d'évacuation médicale, l'AI pourrait supporter et optimiser l'évacuation et mieux supporter les équipes dans les traitements du patient par du personnel pas nécessairement expert en la matière¹⁹. Tout ceci n'est pas possible sans le support d'un réseau de communication stable et sécuritaire.

L'AI est vitale pour l'amélioration du transport de données longue distance, la gestion de ces données et du trafic en améliorant le processus d'acheminement des bonnes données aux bonnes personnes au bon moment pour prendre les bonnes décisions. Les réseaux à grande capacité capables de fonctionner sur de longues distances offrent un avantage significatif à la conduite des opérations.

Bien qu'à ce jour, différentes capacités de l'AI/ML soient utilisées, le potentiel d'exploitation et d'optimisation est encore très grand.

Le terrain vital

Ce mémoire propose que le réseau de communication, opérationnel et tactique, est le terrain vital de la guerre algorithmique. Le terrain vital se définit comme un terrain d'une importance telle que sa rétention ou son contrôle s'avère nécessaire au succès de la mission en

¹⁸ Polowczyk, John, Robert Lytle, et Frank Fletcher. 2022. «Four actions to modernize military logistics and supply chain security.» *EY Parthenon*.

¹⁹ Priems et Gizewski, 2022

contraste à la position clé qui est pour sa part, un lieu ou zone dont la capture ou la rétention donne un avantage marqué à l'adversaire²⁰. Comme mentionné plus haut, la guerre algorithmique est une guerre menée par des systèmes autonomes alimentés par l'AI, qui peuvent contrôler les plateformes d'armes, les systèmes, et même les opérations et les tactiques dans un champ de bataille connecté. Tous ces systèmes dits autonomes et alimentés par l'AI ne sont pas indépendants pour autant et ont un besoin de connexion à diverses ressources comme les satellites pour le positionnement GPS ou l'échange de données, l'accès à des capacités d'analyse de données externe, des besoins d'autorisations humaines pour entreprendre certaines actions, des besoins de communication machine-à-machine, etc. Ceci n'est pas possible sans réseaux de communication.

Les aptitudes supplémentaires qu'apporte l'AI aux réseaux de communication viennent augmenter leurs résilience, sécurité, stabilité et agilité. Tel qu'apporté par le LtGen Groen, les réseaux sont un élément central de l'architecture de combat; les protéger et les rendre résilients est ce que les armées doivent faire, car toutes nos actions futures seront basées sur la sécurité de ces réseaux.

D'autres éléments de la guerre algorithmique sont également très importants et indispensables à ce type de guerre tel que la puissance de traitement informatique (*computer-processing power*), le big-data, l'infonuagique, les supports physiques, etc.²¹. Mais reste que

²⁰ Canada. Défense nationale. 2008. Opération terrestre. Kingston, Ontario: Bureau d'édition de l'Armée de terre, p.7-52

²¹ Layton, Peter. 2018. «Algorithmic Warfare: Applying Artificial Intelligence to Warfighting.» *Air Power Development Centre*.

toutes ces technologies et capacités ne sont pas utiles si le réseau de communication qui permet les interactions entre ces technologies est déficient ou inexistant.

Les changements et percées technologiques changent la façon dont les guerres seront appelées à être menées et les réseaux de communication dans ce contexte seront indispensables. Ceci justifie le qualificatif de terrain vital au réseau de communication dans le contexte de guerre algorithmique.

La résilience des systèmes

La résilience de l'intelligence artificielle ainsi que l'apprentissage machine dans les systèmes de communications tactiques sera vitale dans les conflits à venir. Elle sera vitale, car sans réseaux de communications fonctionnels, l'armée du futur n'est plus. Selon le Larousse, la résilience informatique est la capacité d'un système à continuer de fonctionner, même en cas de panne²². Elle est également définie comme la capacité d'un système à se rétablir après une perturbation extérieure. C'est exactement ce que l'on recherche de nos systèmes et réseaux de communication. Un réseau résilient sera stable pour les utilisateurs et sera en mesure de se défendre d'une façon ou d'une autre aux différentes attaques et perturbations.

La complexité des réseaux de communication est telle que les opérateurs traditionnels ne sont et ne seront pas en mesure d'en assurer une opérationnalité complète sans un support non seulement en traitement et analyse de données, mais également en support et automatisation

²² Larousse. s.d. *Résilience*. Accès le Mai 15, 2022.

décisionnels. Cette ressource additionnelle en support des opérateurs est et sera fournie par des algorithmes évolutifs que sont l'AI/ML. La capacité des algorithmes renforcer par de l'apprentissage automatique augmente tous les aspects reliés à la fonctionnalité et sécurité des réseaux de communication actuels et du futur.

Les défis possibles dans la mise en œuvre

Avant de conclure, il est important de souligner brièvement quelques défis dans la mise en œuvre de réseaux de communication munis d'AI/ML jumelant résilience, sécurité, stabilité, agilité et interopérabilité. Ceci pourrait être résumé ainsi. Premièrement, la synchronisation des besoins au sein d'une même armée, entre les différents éléments et composantes, puis avec les différents alliés afin d'assurer une certaine interopérabilité. Par la suite, il y a les délais énormes et manques d'agilité du processus d'acquisition de la plupart des forces armées en opposition aux avancements relativement rapides et diversifiés des technologies autant de communication que d'AI/ML. Finalement et faisant suite au point précédent, le manque d'agilité marquée de plusieurs forces armées quant aux réponses et capacité d'adaptation lors d'opération pour faire face aux menaces de toutes sortes tel que rapporté récemment par le DoD suite à une action de SpaceX en réponse à une attaque russe en Ukraine: « *In the way that Starlink was able to upgrade when a threat showed up, we need to be able to have that agility* »²³.

Un dernier défi serait la confiance des utilisateurs à tous les niveaux des systèmes d'intelligence artificielle, dont les réseaux de communication. La complexité des systèmes

²³ Duffy, Kate. 2022. «A top Pentagon official said SpaceX Starlink rapidly fought off a Russian jamming attack in Ukraine.» *Business Insider*.

autonomes signifie inévitablement qu'une compréhension complète de ces systèmes est impossible des utilisateurs. Cet écart dans la compréhension doit être comblé par la confiance dans les systèmes. Cette confiance, ou manque de, peut mener à des erreurs de mauvaise utilisation, de rejet ou d'abus de système²⁴. Le bon niveau de confiance minimisant les risques d'erreurs sera obtenu principalement par l'éducation et l'expérience des opérateurs et ceux qui dépendent de ces systèmes.

On ne peut passer sous silence les considérations éthiques qui sont également présentes dans le domaine des communications habilitées en grande partie par l'AI. Par exemple, la réponse automatique à une attaque sur le réseau pourrait être de brouiller, perturber, voir détruire le réseau attaquant qui pourrait être également utilisé par des organisations non gouvernementales d'aide humanitaire ou autres. Les conséquences pourraient être considérables et le tout devra être bien géré et anticipé. Les efforts visant à développer et à utiliser les systèmes de communication et autres, activés par l'AI, doivent respecter les normes éthiques en vigueur ainsi que les normes et lois internationales régissant les conflits armés²⁵.

CONCLUSION

Ce mémoire a démontré que la communication est le terrain vital dans la guerre algorithmique et que la résilience de l'intelligence artificielle ainsi que l'apprentissage machine

²⁴ Davis, Steven Edward. 2019. «Individual Differences in Operators' Trust in Autonomous Systems: A Review of the Literature.» *Defence Science and Technology Group (DST)*.

²⁵ Priems et Gizewski, 2022

(AI/ML) dans les systèmes de communications tactiques seront vitale dans les conflits présents et à venir.

Le développement de l'AI au sein des Forces armées canadiennes exigera de l'ingéniosité, des ressources et des compétences spécifiques plus ou moins disponibles au sein de l'organisation. Une diversification dans le recrutement et/ou dans l'emploi de personnel civil expert en la matière devra être davantage explorée ainsi que de continuer les efforts de formation des utilisateurs. Un investissement majeur et soutenu dans le matériel et les ressources humaines sera essentiel.

De plus, une certaine tolérance au risque devra être cultivée pour faire face aux défis du système d'approvisionnement difficilement compatible avec le cycle de développement et d'évolution de cette technologie ainsi que les nombreux échecs menants à un produit adéquat. Un effet de levier devra être utilisé lorsque possible par les organisations capables d'adopter et d'intégrer des technologies du secteur commercial pour garantir l'innovation ainsi que pour se procurer efficacement les technologies et les systèmes nécessaires²⁶. Un partenariat avec le privé serait à considérer ainsi qu'une veille technologique afin de rester à l'affut des plus récents développements dans le domaine ainsi que chez nos alliés pour maximiser l'interopérabilité de nos systèmes.

²⁶ Priems et Gizewski, 2022

Malgré que la politique de défense du Canada²⁷ ne mentionne par l'intelligence artificielle directement, elle fait tout de même référence à des technologies utilisant des technologies d'AI/ML. De plus, un effort semble être mis sur l'amélioration des communications via des investissements qui passeront inévitablement par l'AI. Depuis la publication de la politique, le Canada a publié au moins deux stratégies^{28&29} afin de coordonner certains efforts en ce sens. Le Canada ne peut pas passer à côté des évolutions technologiques incluant entre autres l'AI et ce autant dans les communications tactiques et opérationnelles que dans les autres évolutions technologiques. Le Canada se doit d'être capable d'opérer avec ses alliés et capable de faire face à des adversaires munis de capacités modernes. L'Armée canadienne doit continuer d'évoluer et améliorer son agilité afin de répondre aux exigences et être prête à opérer dans l'environnement opérationnel de demain.

²⁷ Canada. 2017. «Strong, Secure, Engaged: Canada's Defence.» Department of National Defence, Ottawa.

²⁸ Canadian Army Land Warfare Centre. 2019. «Close Engagement – Land Power in an Age of Uncertainty – Evolving Adaptive Dispersed Operations. »

²⁹ HQ, Canadian Army. 2020. *Advancing with Purpose: The Canadian Army Modernization Strategy, 4th ed.*

BIBLIOGRAPHIE

- Blum, Gabriella , Dustin Lewis, et Naz Modirzadeh. 2016. «Accountability for Algorithmic Autonomy in War.» *Lawfare*. <https://www.lawfareblog.com/accountability-algorithmic-autonomy-war>.
- Brose, Christian. 2020. *The Kill Chain: Defending America in the Future of High-Tech Warfare*. New York, NY: Hachette Books.
- Canada. 2017. «Strong, Secure, Engaged: Canada's Defence.» Department of National Defence, Ottawa. <https://www.canada.ca/en/departement-national-defence/corporate/reports-publications/canada-defence-policy.html>.
- Canada. Défense nationale. 2008. *Opération terrestre*. Kingston, Ontario: Bureau d'édition de l'Armée de terre.
- Canadian Army Land Warfare Centre. 2019. «Close Engagement – Land Power in an Age of Uncertainty – Evolving Adaptive Dispersed Operations.» Kingston. http://www.army-armee.forces.gc.ca/assets/ARMY_Internet/docs/en/close-engagement.pdf.
- Crosby, Courtney. 2020. «Operationalizing Artificial Intelligence for Algorithmic Warfare.» *Military Review*. <https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/JA-20/Crosby-Operationalizing-AI-1.pdf>.
- Davis, Steven Edward. 2019. «Individual Differences in Operators' Trust in Autonomous Systems: A Review of the Literature.» *Defence Science and Technology Group (DST)*. https://www.researchgate.net/publication/332439462_Individual_Differences_in_Operators%27_Trust_in_Autonomous_Systems_A_Review_of_the_Literature.
- Duffy, Kate. 2022. «A top Pentagon official said SpaceX Starlink rapidly fought off a Russian jamming attack in Ukraine.» *Business Insider*. <https://www.businessinsider.com/spacex-starlink-pentagon-russian-jamming-attack-elon-musk-dave-tremper-2022-4>.
- Goure, Dan. 2020. «The Military Has An Intra-Service Communications Problem. SOCOM Might Have The Answer.» *The National Interest*. <https://nationalinterest.org/blog/buzz/military-has-intra-service-communications-problem-socom-might-have-answer-135467>.
- Harrison, Todd. 2021. «Battle Networks and the Future Force.» *Center for strategic & International studies*. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210805_Harrison_BattleNetworks_PartOne.pdf?JZYHYCAk5zZnL4a5C38ZbIZ70f..bDeL.
- HQ, Canadian Army. 2020. *Advancing with Purpose: The Canadian Army Modernization Strategy, 4th ed.* Canadian Army. <https://www.canada.ca/content/dam/army->

armee/migration/assets/army_internet/docs/en/national/2021-01-canadian-army-modernization-en.pdf.

Larousse. s.d. *Résilience*. Accès le Mai 15, 2022.

<https://www.larousse.fr/dictionnaires/francais/r%C3%A9silience/68616>.

Layton, Peter. 2018. «Algorithmic Warfare: Applying Artificial Intelligence to Warfighting.» *Air Power Development Centre*. <https://airpower.airforce.gov.au/sites/default/files/2021-03/AP33-Algorithmic-Warfare-Applying-Artificial-Intelligence-to-Warfighting.pdf>.

Leland, Joe, et Porche III Isaac. 2004. «Future Army Bandwidth Needs and Capabilities.» *Rand*. https://www.rand.org/content/dam/rand/pubs/monographs/2004/RAND_MG156.pdf.

Mcelroy, Barry. 2017. «The network-centric approach: Solving the challenges of real-time battlefield communications.» *Military Embedded Systems*. <https://militaryembedded.com/comms/communications/the-network-centric-approach-solving-the-challenges-of-real-time-battlefield-communications>.

Nair, Jayakrishnan N. 2020. «Algorithmic Warfare – World is Waiting.» *Indian Defence Review*. <http://www.indiandefencereview.com/news/algorithmic-warfare-world-is-waiting/>.

Polowczyk, John, Robert Lytle, et Frank Fitcher. 2022. «Four actions to modernize military logistics and supply chain security.» *EY Parthenon*. https://www.ey.com/en_us/strategy/four-actions-to-modernize-military-logistics-and-supply-chain-security.

Priems, Geoffrey, et Peter Gizewski. 2022. «Leveraging Artificial Intelligence for Canada's Army: Current Possibilities and Future Challenges.» *The Canadian Army Journal* 19.2 40-51. <https://www.canada.ca/content/dam/dnd-mdn/army/lineofsight/files/articlefiles/en/leveraging-artificial-intelligence-for-canadas-army.pdf>.

Thales. s.d. *Examining the Advantages of Networking Radios for Dismounted Combat*. Accès le Mai 15, 2022. <https://www.thalesgroup.com/en/global/presence/europe/united-kingdom/defence/land-systems/soldier-systems/squadnet/examining>.

U.S. Army CCDC Army Research Laboratory Public Affairs. 2020. «Machine learning algorithms promise better situational awareness.» *U.S. Army*. https://www.army.mil/article/236647/machine_learning_algorithms_promise_better_situational_awareness.

Vergun, David. 2021. «General Says Artificial Intelligence Will Play Important Role in Network Defense.» *DoD News*. <https://www.defense.gov/News/News->

Stories/Article/Article/2805760/general-says-artificial-intelligence-will-play-important-role-in-network-defense/.

Vincent, James. 2017. «Putin says the nation that leads in AI ‘will be the ruler of the world’.» *The Verge*. <https://www.theverge.com/2017/9/4/16251226/russia-ai-putin-rule-the-world>.

Walker, Amy, et Claire Heininger. 2022. «Army National Guard signal conference highlights data, data transport modernization.» *U.S. Army*.
https://www.army.mil/article/256959/army_national_guard_signal_conference_highlights_data_data_transport_modernization.