



Un membre d'équipage du NCSM MARGARET BROOKE prend une photo de la statue du Christ Rédempteur lors de l'arrivée du navire à Rio de Janeiro, au Brésil, au cours de l'opération PROJECTION 25-01, le 1^{er} février 2025.

Caporal Connor Bennett, Forces armées canadiennes

Note du rédacteur invité

MATTHEW KELLETT

Matthew Kellett, Ph.D., est conseiller spécial au Commandement des cyberopérations des Forces armées canadiennes et rédacteur invité pour ce numéro spécial sur les cyberopérations auprès de la Revue militaire canadienne. Il a commencé sa carrière comme programmeur de logiciels commerciaux. Il a travaillé comme soutien scientifique, puis comme scientifique de la défense pendant 15 ans à Recherche et développement pour la défense Canada (RDDC), menant des recherches en cybersécurité. Depuis 2017, il conseille les commandants des cyberopérations des Forces armées canadiennes (FAC) sur l'opérationnalisation du cyberdomaine, avec un accent mis ces dernières années sur les concepts, la doctrine et la terminologie. Il détient deux baccalauréats, un en informatique et l'autre en littérature anglaise ainsi qu'un doctorat en informatique théorique, tous obtenus à l'Université d'Ottawa.

Bienvenue dans ce numéro spécial de la *Revue militaire canadienne* dédiée à la cyberintelligence et à l'intelligence artificielle (IA). Le cyberspace se trouve partout dans nos vies. Du défilement anxigène sur nos téléphones aux innombrables courriels au travail, cela semble être la chose la plus familière au monde. En même temps, on entend parler d'entreprises compromises et d'infrastructures critiques attaquées. Il peut être difficile de comprendre comment ces deux mondes sont liés.

En vérité la partie du cyberspace avec laquelle nous interagissons—les interfaces de nos iPhone et ordinateurs Windows—est une fine couche recouvrant une vaste infrastructure, et cette fine couche donne l'impression que tout fonctionne de façon

transparente, comme par magie. Il n'y a pas de magie. Il y a tout simplement un système complexe qui exige un ensemble de compétences techniques approfondies pour être compris.

L'Organisation du Traité de l'Atlantique Nord (OTAN), le Canada et plusieurs de ses alliés reconnaissent le cyberspace comme un domaine de la guerre. En pratique, cette désignation reconnaît que le fait de ne pas déployer une capacité militaire spécialisée dans le cyberspace pourrait nous faire perdre notre capacité à opérer dans tous les autres domaines : mer, terre, air et espace. C'est pour cette raison que le Commandement des cyberopérations des Forces armées canadiennes (COMCYBERFAC) a été créé le 26 septembre 2024 en tant que commandement à deux étoiles dirigé par le major-général Dave Yarker, relevant directement du chef d'état-major de la défense.

Le COMCYBERFAC a pour mandat des Forces armées canadiennes de mener des opérations cybernétiques, de renseignement électromagnétique et de guerre électronique interarmées. Ces domaines partagent des compétences similaires et, dans certains cas, se renforcent mutuellement. Ces capacités existaient déjà et étaient opérationnellement efficaces avant que le commandement ne soit mis en place. La création du commandement a simplifié la structure hiérarchique militaire et facilité l'intégration de ces capacités dans les opérations militaires.

Dans ce numéro spécial, nous examinons le cyberspace sous plusieurs angles différents. Nous commençons par la place qu'occupe le Canada dans le monde avec nos attentes sur la façon dont les États devraient agir dans cet espace. Le commentaire : « Le Canada comme puissance technologique responsable au XXI^e siècle » de Christina Marcotte examine les actions du gouvernement du Canada dans ce domaine, y compris la façon dont il s'adapte aux nouvelles technologies comme l'intelligence artificielle, gouverne ses actions et relie cette gouvernance au système international fondé sur des règles.

Comme mentionné plus haut, la plupart des gens pensent aux téléphones et aux ordinateurs lorsqu'il est question du cyberspace, ce que nous appellerions collectivement les technologies de l'information (TI), mais le cyberspace peut être bien plus que cela. Dans leur article « Introduction aux notions de base sur la cybersécurité du gouvernement du Canada : un premier aperçu », Alexandra Green et Matthew Kellett essayent de tracer un portrait plus complet du cyberspace en termes simples. Entre autres, ils parlent des domaines du cyberspace auxquels les utilisateurs pensent rarement, comme les systèmes de contrôle industriels, les plateformes militaires et les ampoules intelligentes. Ils discutent de la différence entre la cybersécurité et la cyberdéfense; et ils évoquent la raison pour laquelle on entend rarement le terme cyberattaque dans des contextes officiels.

Enfin, pour la partie de ce numéro consacré aux cyberopérations, je voulais souligner l'importance du renseignement électromagnétique pour les cyberopérations militaires. À cet égard, le commentaire : « Le lien entre le renseignement d'origine électromagnétique et le cyberspace au sein des Forces armées canadiennes » du lieutenant-colonel Leslie Rediger montre comment ces deux disciplines, bien que distinctes, partagent des caractéristiques similaires et se renforcent mutuellement,

ce qui explique pourquoi elles ont été regroupées au sein du COMCYBERFAC.

L'intelligence artificielle est une promesse et un mot à la mode depuis des décennies. Les récentes avancées en matière d'intelligence artificielle générative, en commençant par le lancement de ChatGPT en 2022, ont changé cette discussion. Alors que de nombreuses avancées technologiques, par exemple la 5G, ont été présentées comme la prochaine révolution industrielle pour offrir des améliorations apparemment modérées et incrémentales, l'intelligence artificielle a toutes les apparences et l'élan d'être révolutionnaire. Que vous soyez sceptique au sujet de l'intelligence artificielle ou en fassiez l'apologie (pour ma part, je suis resté du côté sceptique de ce fossé), il est indéniable que l'intelligence artificielle représente un ensemble de technologies émergentes qu'on ne peut ignorer. Nous devons y faire face et en envisager les répercussions, sans quoi nous pourrions nous retrouver, en tant qu'État, dans une situation désavantageuse sur le plan technologique.

Le ministère de la Défense nationale (MDN) et les FAC ont reconnu cette menace et, en mai 2024, ont publié la *Stratégie d'intelligence artificielle*. La Stratégie est importante, car puisqu'elle s'applique tant au MDN qu'aux FAC, elle doit répondre à la fois aux exigences ministérielles/organisationnelles et militaires/opérationnelles, ce qui n'est pas une tâche facile. La Stratégie met fortement l'accent sur l'utilisation responsable de l'intelligence artificielle.

Un des éléments majeurs de la Stratégie a été la création du Centre d'IA de la Défense. Dans l'article « Forger l'avenir : un écosystème intégré d'IA de défense au Canada » de Lydia Korczynska, nous avons un aperçu de la Stratégie et de sa mise en œuvre au MDN par le directeur du Centre d'IA de la Défense. La Stratégie fixe un objectif ambitieux : que le MDN et les FAC puissent adopter l'intelligence artificielle de manière intégrée d'ici 2030, et le Centre d'IA de la Défense est chargé de concrétiser cette ambition.



Les participants à un cours sur les systèmes de défense contre les aéronefs sans pilote à bord visitent un véhicule de défense aérienne SA-8, en Pologne, le 11 décembre 2024.

Technicien en imagerie des Forces armées canadiennes

Les deux articles suivants proviennent du Centre d'IA de la Défense. L'article « L'intelligence artificielle et la concurrence technologique entre la Chine et les États-Unis : répercussions sur la défense canadienne et alliée » de Jennifer Gearey et du major Tyler Currie utilise le prisme de la concurrence technologique entre la Chine et les États-Unis pour discuter de la façon dont l'intelligence artificielle transforme le paysage de la défense. Il souligne la nécessité pour le Canada d'agir de manière décisive dans quatre domaines clés : les données, la capacité de calcul, les organisations et les talents.

L'article « L'interopérabilité des alliées sous pression : l'IA, l'approvisionnement et l'avenir de la cohésion en matière de défense » de Samuel Paquette et du major Tyler Currie examine l'interopérabilité avec nos alliés, en particulier l'OTAN, et les défis auxquels nous faisons face. Il évalue les obstacles critiques : chaînes d'approvisionnement volatiles, systèmes d'approvisionnement lents et modèles de gouvernance divergents.

Par la suite, l'article « Navigation au sextant et à l'astrocompas : une approche des FAC pour l'adoption de l'IA » du colonel Adam Moore et de Matthew da Mota est notable, car ne provenant pas du Centre d'IA de la Défense, il soulève indépendamment plusieurs des mêmes préoccupations. Il examine la capacité de l'intelligence artificielle à perturber les processus décisionnels militaires et ce que cela signifie pour la manière dont l'IA est mise en œuvre et utilisée dans un contexte militaire. Autrement dit, un commandant ne peut pas simplement blâmer l'IA si quelque chose tourne à la catastrophe. Cette réalité signifie que l'IA sera nécessairement utilisée différemment en défense par rapport à d'autres domaines.

Le dernier article provient aussi du Centre d'IA de la Défense. Il porte sur « L'authenticité comme arme : l'avantage des Forces armées canadiennes dans la guerre de l'information à l'ère de l'IA. » Dans leur article, Ali Manouchehri et le major Tyler Currie s'intéresse spécifiquement à la désinformation habilitée par l'intelligence artificielle qui est probablement le problème le plus connu publiquement et le plus difficile à résoudre concernant l'utilisation malveillante de l'IA. L'article propose des approches pour contrer cette désinformation. Fait intéressant : les solutions ne sont pas uniquement technologiques.

Si je peux vous laisser avec une dernière réflexion avant que vous ne plongiez dans les commentaires et les articles de ce numéro spécial, c'est que dans ce domaine les gens sont plus importants que la technologie. Les gens sont un multiplicateur de force dans le cyberdomaine, d'une manière qui est inédite dans d'autres domaines. Un opérateur ou un spécialiste peut être beaucoup plus efficace que des personnes formées simplement pour utiliser un outil. Bien que la technologie puisse faciliter leur travail ou leur permettre de faire des choses plus avancées, la technologie seule ne suffit pas pour permettre à ces utilisateurs de fonctionner efficacement dans le cyberdomaine. L'IA peut modifier le rythme et le type de problèmes posés par le domaine, mais il est peu probable qu'elle supplante les gens comme force

« Les gens sont un multiplicateur de force dans le cyberdomaine, d'une manière qui est inédite dans d'autres domaines. »

majeure dans le domaine pour des raisons purement pratiques : les choses qui nous tiennent le plus à cœur dans le domaine, comme un adversaire d'un État compromettant un réseau informatique, sont extrêmement rares comparées à la totalité des données disponibles. C'est l'expertise de nos collaborateurs et leur intuition aiguisée qui nous donnent l'avantage. L'IA pourrait ultimement changer cette équation, mais il est peu probable que ce soit le cas bientôt.

Je tiens à remercier tous les auteurs et autrices ainsi que les responsables des évaluations par les pairs qui ont rendu possible ce numéro spécial. Je suis redevable au Centre d'IA de la Défense pour son soutien et ses contributions significatives. Je remercie le COMCYBERFAC pour son soutien dans mon rôle de rédacteur invité. Je remercie également les membres du commandement qui ont travaillé sur des commentaires et des articles qui n'ont finalement pas été retenus, principalement en raison d'exigences opérationnelles contradictoires. J'espère vous présenter certains de ces articles dans les prochains numéros de cette revue. Un grand merci à l'équipe éditoriale de la *Revue militaire canadienne* pour avoir géré ce numéro spécial avec autant de professionnalisme. Enfin, je tiens à remercier Alexandra Green qui m'a guidée avec son expertise à chaque étape du processus.

Les articles sollicités pour ce numéro ont été rédigés en 2025 et leurs versions finales ont été soumises en mars 2026. Le délai nécessairement long entre la rédaction, la soumission finale et la publication peut avoir une incidence sur l'actualité et la pertinence des informations présentées, en particulier pour des sujets en constante évolution comme l'intelligence artificielle.