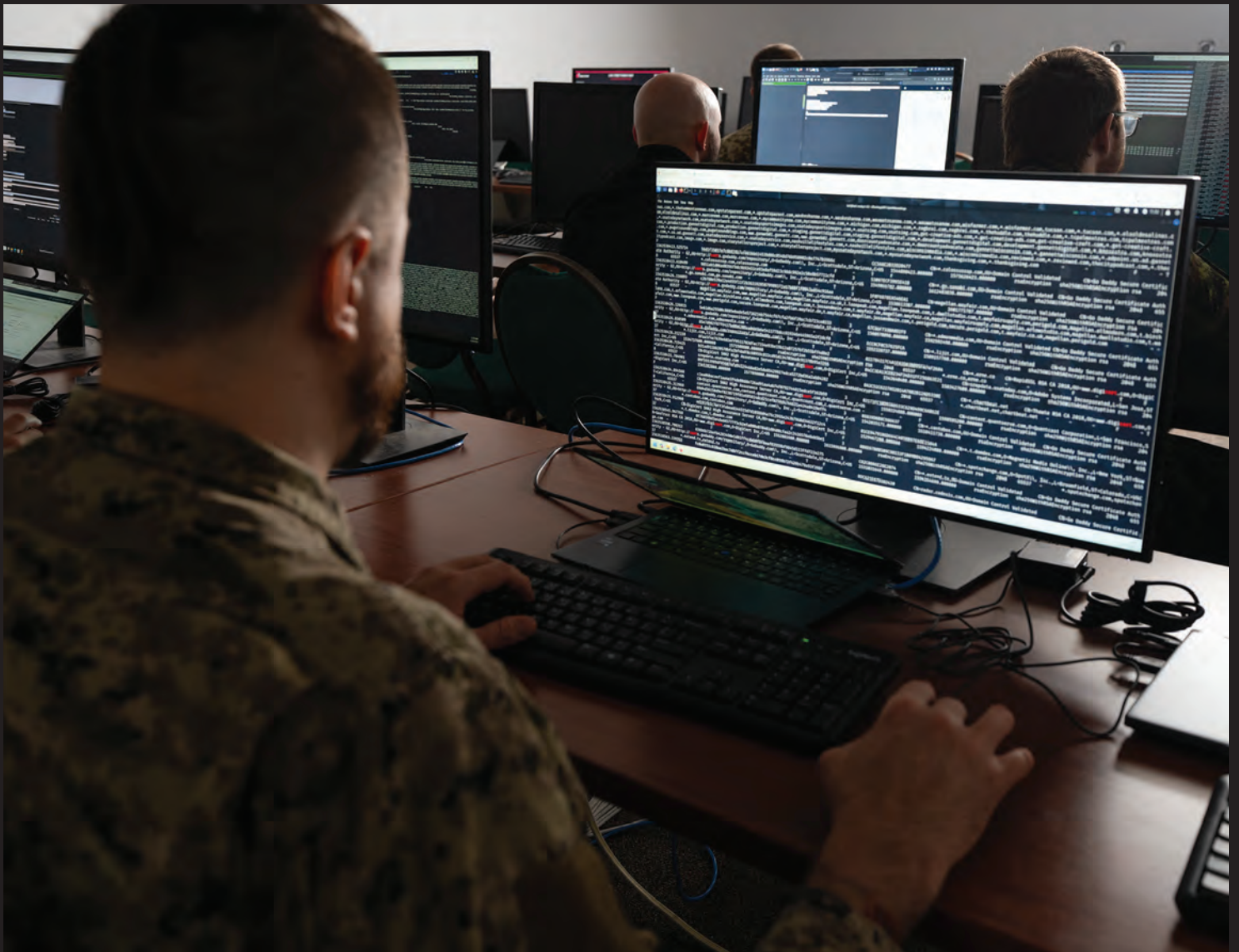


REVUE MILITAIRE CANADIENNE



Lignes directrices pour la présentation des manuscrits

La Revue militaire canadienne est la publication trimestrielle phare indépendante de la profession des armes au Canada. La Revue publie des articles professionnels et scientifiques, des commentaires, des articles d'opinion, des études critiques de livres, des comptes rendus de livres, ainsi que des lettres à l'éditeur.

Les manuscrits sur des sujets d'intérêt général pour la Défense canadienne et l'Équipe de la Défense sont également bien accueillis, notamment sur la profession des armes, la politique de sécurité et de défense, la stratégie, la doctrine, les opérations, la mise sur pied de la force, l'emploi de la force et la structure de la force, la technologie, l'acquisition de matériel, l'histoire militaire, le leadership, l'instruction et l'éthique militaire, la culture institutionnelle, le recrutement, la diversité, etc. La Revue s'intéresse plus particulièrement à des articles ouverts sur l'avenir qui présentent des idées ou des concepts originaux, de nouvelles approches aux problèmes actuels ou des interprétations novatrices.

Les militaires de tous les grades peuvent présenter des articles à la Revue. Le sous-ministre et le chef d'état-major de la Défense ont délégué au rédacteur en chef de la Revue militaire canadienne le pouvoir d'autoriser la publication des manuscrits lorsque le comité de rédaction en a fait la recommandation. Les membres des Forces armées canadiennes et les employés civils du ministère de la Défense nationale n'ont donc pas besoin d'obtenir la permission de leur supérieur pour soumettre un manuscrit à la Revue.

En retour, la Revue suit un processus d'examen par les pairs en double insu rigoureux qui fait appel à l'expertise des civils et des militaires en uniforme afin de vérifier la pertinence des soumissions. Les manuscrits sont évalués en fonction de leur originalité, de la qualité de l'argumentation ou de la discussion, de la pertinence et de l'actualité du sujet, ainsi que de la qualité du style d'écriture. Sauf entente contraire, la Revue militaire canadienne insiste sur le droit de première publication de toute communication donnée. Les soumissions ne doivent pas être examinées par toute autre publication pendant le processus d'examen réalisé par la Revue.

Lignes directrices pour la soumission :

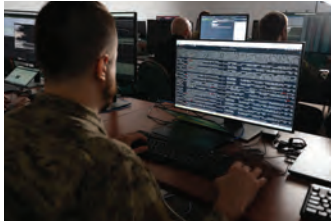
- Les auteurs doivent soumettre deux copies de leur manuscrit :
 - Première copie : Un manuscrit complet, avec un titre, le nom, la notice biographique et les coordonnées de l'auteur, un résumé, etc. Le manuscrit doit être nommé et soumis comme « Titre du manuscrit X-Nom de l'auteur-Anonymisé ».
 - Deuxième copie : Une version anonymisée dont le nom de l'auteur, les coordonnées et la notice biographique ont été retirés. Le manuscrit doit être nommé et soumis comme « Titre du manuscrit X-Anonymisé ».
- Les articles peuvent être rédigés dans l'une ou l'autre des langues officielles du Canada.
- En règle générale, les manuscrits ne doivent pas compter plus de 5 000 mots (mais ils peuvent être plus courts), notes comprises.
- Les manuscrits doivent être rédigés en format Word (.docx ou .doc) et soumis par courriel à l'adresse suivante : cmj.rmc@forces.gc.ca;
- Puisque la Revue est une publication bilingue, les manuscrits qui comportent des graphiques, des tableaux, des figures, des diagrammes ou des cartes doivent nous parvenir séparément dans un format inscriptible afin de les traduire dans l'une des langues officielles. Les formats acceptés sont Word (.docs or .doc), PowerPoint (.pptx or .ppt), Excel (.slx or .xlsx), Vector file (.ai, .eps, .pdf) ou tout autre format qui nous permet de modifier le texte. Toutes les photos qui illustrent l'article doivent nous être fournies en haute résolution (au moins 300 ppp) en format .jpg ou .tiff aux fins de qualité d'impression, et doivent être accompagnées d'une légende appropriée et de la source.
- Le style de rédaction des manuscrits doit répondre aux normes qui s'appliquent habituellement aux travaux universitaires, l'orthographe doit avoir été vérifiée à l'aide du Petit Robert ou de l'Oxford English Dictionary et les notes doivent se trouver à la fin du document plutôt qu'en bas de page.
- Les notes de fin de document doivent être intégrées et non jointes. Les renseignements bibliographiques doivent tous se trouver dans les notes de fin de document. Veuillez consulter les numéros récents de la Revue pour voir des exemples d'une présentation acceptable.
- L'emploi d'abréviations militaires devrait être limité au minimum; toutefois, lorsque leur emploi est inévitable, le terme doit être écrit au long la première fois qu'il apparaît dans le texte et être suivi de son abréviation, qui doit être placée entre parenthèses. Il faut aussi éviter d'employer le jargon militaire et des expressions familières : tous les manuscrits devraient être facilement compréhensibles par un lectorat public généralement bien informé.

Politique de rétraction

La Revue militaire canadienne s'engage à faire preuve d'intégrité dans ses publications. En consultation avec les comités de rédaction et de consultation, l'éditeur se réserve le droit de corriger le document en publiant une correction ou une rétraction subséquente. La rétraction repose sur les lignes directrices du Committee on Publication Ethics (COPE). Ainsi, un article peut faire l'objet d'une rétraction s'il comprend : des conclusions peu fiables (en raison d'une erreur majeure ou d'une falsification), du plagiat, une violation du droit d'auteur, des cas de publication redondante sans divulgation complète, le défaut de divulguer des intérêts concurrents ou conflictuels, des rapports étayés de recherches contraires à l'éthique ou, à la discrétion de l'éditeur, s'il s'avère que le contenu contrevient aux attentes éthiques, professionnelles, scientifiques et autres de la Revue.

NUMÉRO SPÉCIAL CONSACRÉ AU DOMAINE CYBERNÉTIQUE et à L'INTELLIGENCE ARTIFICIELLE

REVUE MILITAIRE CANADIENNE



Un instructeur principal de l'Unité de formation cyber préparant un exercice de simulation.

Major Charles Paquin, Affaires publiques,
COMCYBERFAC



Crédits de photo p. 38



Crédits de photo p. 48

LE COIN DE L'ÉDITEUR

- 4 Avant-propos
Major-général Dave Yarker
- 5 Note du rédacteur invité
Matthew Kellett

COMMENTAIRES

- 8 Le Canada, puissance technologique responsable au XXI^e siècle
Christina Marcotte
- 12 Introduction aux notions de base sur la cybersécurité du gouvernement du Canada : un premier aperçu
Alexandra Green et Matthew Kellett
- 20 Le lien entre le renseignement d'origine électromagnétique et le cyberdomaine au sein des Forces armées canadiennes
Lieutenant-colonelle L. J. Rediger
- 25 Forger l'avenir : un écosystème intégré d'intelligence artificielle de défense au Canada
Lidia Korczynska
- 29 L'intelligence artificielle et la concurrence technologique entre la Chine et les États-Unis : Répercussions sur la défense canadienne et alliée
Jennifer Gearey et major Tyler Currie

LA MODERNISATION DES FORCES ARMÉES CANADIENNES

- 38 L'interopérabilité des alliés sous pression : l'IA, l'approvisionnement et l'avenir de la cohésion en matière de défense
Samuel Paquette et major Tyler Currie
- 48 Navigation au sextant et à l'astrocompas : une approche des FAC pour l'adoption de l'IA
Colonel Adam Moore et Matthew da Mota
- 57 L'authenticité comme arme : l'avantage des Forces armées canadiennes dans la guerre de l'information à l'ère de l'IA
Ali Manouchehri et major Tyler Currie

LA COMPOSANTE HUMAINE

- 66 La cybersécurité et la puissance aérienne : préserver l'intervention humaine
Kristen Csenkey et Alexis Rapin
- 73 Armes autonomes et cognition étendue
Major Andrew G. Holt

Revue militaire canadienne
CP 17000, succursale Forces
Kingston (Ontario)
CANADA, K7K 7B4
Courriel : cmj.rmc@forces.gc.ca



REVUE MILITAIRE CANADIENNE

www.Canada.ca/revue-militaire-canadienne

Directeur et Rédacteur en chef

Professeur Christian Leuprecht

Rédacteur invité de ce numéro spécial

Matthew Kellett, Ph.D.

Anciens rédacteurs en chef

Professeur

Michael A. Hennessy

Lieutenant-colonel (à la retraite)
John K. Martenson†

Lieutenant-colonel (à la retraite)
David L. Bashow

Directrice de la publication

Deesha Kodai

Rédactrice numérique en chef

Alex Green

Cheffe d'équipe, Engagement et partenariats

Katia Dalpé-Charron

Rédacteurs adjoints

Bruno Charbonneau, Ph.D.

Matthew Kellett, Ph.D.

Paul T. Mitchell, Ph.D.

Comité de lecture

Co-présidents

Irina Goldenberg, Ph.D. et
Peter Kasurak, Ph.D.

Membres

Major-général (à la retraite)
Craig Aitchison

Major (à la retraite) Michael Boire

James Boutilier, Ph.D.

H. Christian Breede, Ph.D.

Vanessa Brown, Ph.D.

Stéphanie Chouinard, Ph.D.

Lieutenant-colonel (à la retraite)
W.G. (Bill) Cummings

Karen D. Davis, Ph.D.

Barbara J. Falk, Ph.D.

Robert Fonberg

Major-général (mgén)
(à la retraite) David Fraser

Lieutenant-colonel
Andrew Godfrey, Ph.D.

Major-général (à la retraite)
Daniel Gosselin

Major Tanya Grodzinski, Ph.D.

Michael Hennessy, Ph.D.

Lieutenant-général (à la retraite)
Michael Hood

Colonel (à la retraite)
Bernd Horn, Ph.D.

Hamish Ion, Ph.D.

Rebecca Jensen, Ph.D.

Matthew Kellett, Ph.D.

Philippe Lagassé, Ph.D.

Lieutenant-colonel (à la retraite)
David Last, Ph.D.

Capitaine de corvette
Brent Lemon

Adam MacDonald, Ph.D.

Vice-amiral (vam)
Paul A. Maddison

Chris Madsen, Ph.D.

Craig Mantle, Ph.D.

Lieutenant-général (à la retraite)
Al Meinzinger

Paul T. Mitchell, Ph.D.

Mulry Mondélice, Ph.D.

Kerri-Lynn Nankivell, Ph.D.

Alan Okros, Ph.D.

Huw Osborne, Ph.D.

Gaëlle Rivard Piché, Ph.D.

Lieutenant-colonel (à la retraite)
Anne Reiffenstein

Michael A. Rostek, Ph.D.

Grazia (Grace) Scoppio, Ph.D.

Margaret BK Shepherd

André Simonyi, Ph.D.

Elinor Sloan, Ph.D.

Colonel Max Talbot MD, FRCS

Colonel (à la retraite)
Randall Wakelam, Ph.D.

Comité consultatif

Président

Major-général

Jeannot Boucher, Commandant,
Académie canadienne
de la défense (ACD)

Membres

Colonel Marty Cournoyer,
représentant du Chef
d'état-major de la Force
aérienne (CEMFA)

Jill Scott, Ph.D., Recteur
Collège militaire royal (CMR)

Capitaine de vaisseau

J. Jeffrey Hutchinson,
représentant du Chef d'état-
major de la Marine (CEMM)

Général de brigade Pascal
Godbout, Commandant, Collège
militaire royal du Canada (CMR)

Major Chris Young, représentant
du Chef d'état-major –
Stratégie armée

Lieutenant-colonel Eric J. Weaver,
Directeur, Centre de droit militaire
des Forces armées canadiennes
(CDMFC), Académie canadienne
de la défense (ACD)

Hanya Soliman, représentante
du Chef du renseignement de
la Défense (CRD)

NOTE AUX LECTEURS ET LECTRICES

La Revue militaire canadienne étant bilingue, lorsqu'une citation originale a été traduite, le sigle [TCO] après l'appel de note, qui signifie « traduction de la citation originale », indique que le lecteur trouvera le texte original de la citation dans la version de la Revue rédigée dans l'autre langue officielle du Canada. Afin de faciliter la lecture, le masculin sert de genre neutre pour désigner aussi bien les femmes que les hommes.

Objet : Action nécessaire - Confirmation de votre abonnement à la *Revue militaire canadienne*

Cher-ère abonné-e,

Afin de mettre à jour notre liste de diffusion, nous vous demandons de confirmer votre abonnement ainsi que la mise à jour de vos coordonnées. Pour recevoir une copie imprimée gratuite de la *Revue militaire canadienne*, **nous vous prions de mettre à jour vos préférences d'abonnement** à l'aide du code QR ou en cliquant l'hyperlien fourni ci-dessous. **Si vous ne remplissez pas le formulaire, votre abonnement cessera automatiquement à partir du 31 mars 2027.**

Pour confirmer votre abonnement, veuillez suivre ces étapes simples en choisissant l'une des deux options suivantes :

Accéder via le code QR

1

Connectez-vous au WiFi ou aux données.
Ouvrez l'application de l'appareil photo sur votre téléphone intelligent.
Orientez l'appareil photo vers le code QR.
Appuyez sur l'alerte qui s'affiche pour ouvrir l'hyperlien.



2

Accéder via l'hyperlien

Téléchargez l'hyperlien suivant: <https://forms.office.com/r/RqPPEHKHnS>.

Quelle que soit l'option que vous choisirez, cela vous dirigera vers notre formulaire Microsoft, où vous pourrez **1) confirmer votre abonnement, 2) indiquer votre nouvelle adresse postale s'il y a lieu; et 3) demander à recevoir notre infolettre.** Si vous avez des **questions ou des commentaires**, n'hésitez pas à communiquer avec l'équipe de la *Revue militaire canadienne* par courriel à l'adresse suivante : cmj.rmc@forces.gc.ca.

Sachez que votre engagement et votre fidélité nous tient à cœur. Nous serons ravis de continuer à vous fournir les dernières recherches, idées et analyses sur la profession des armes au Canada.

Veuillez agréer, madame, monsieur, nos salutations distinguées.

Professeur Christian Leuprecht, Ph.D.

Rédacteur en chef
Revue militaire canadienne

Avant-propos

MAJOR GÉNÉRAL DAVE YARKER

En 2024, le major-général (Mgén) Dave Yarker a été nommé premier commandant du nouveau Commandement des cyberopérations des Forces armées canadiennes (FAC). Avant cette nomination, il a occupé plusieurs fonctions au sein de la cybercommunauté des FAC, notamment des postes de commandement au niveau de l'unité et de la formation, ainsi que des fonctions de liaison auprès de l'United States Cyber Command et du Centre de la sécurité des télécommunications du Canada. Auparavant, il a servi au sein de la communauté des transmissions tactiques et dans le domaine des communications interarmées. Le Mgén Yarker est titulaire de diplômes de premier cycle en génie physique et en histoire; il détient également des maîtrises en génie physique ainsi qu'en études de la défense et en administration publique.

C'est pour moi un honneur et un privilège d'avoir l'occasion de rédiger la préface de ce numéro spécial de la *Revue militaire canadienne*, consacré aux enjeux liés au cyberspace et à l'intelligence artificielle. Avec la création récente du Commandement des cyberopérations des Forces armées canadiennes (FAC) et l'établissement officiel du Centre d'intelligence artificielle du ministère de la Défense nationale (MDN) et des FAC, notre institution militaire a franchi des étapes clés, en reconnaissant l'importance de ces deux domaines.

L'intelligence artificielle (IA) et les cyberopérations reposent toutes deux sur les technologies modernes et sur leur influence omniprésente dans la conduite de la guerre. Cette influence est à la fois profonde et étendue. Nous avons placé les technologies modernes au cœur de notre manière de faire la guerre, ce qui nous permet d'accroître la précision de l'emploi de la force sur les plans de l'intention, du lieu et du moment. Toutefois, ces technologies présentent des vulnérabilités intrinsèques. Elles ouvrent de nouvelles voies d'attaque et, par conséquent, de défense, ce qui explique que le cyberspace soit désormais considéré comme un domaine de la guerre. Pour sa part, l'IA modifie radicalement l'échelle et la vitesse de nombreuses technologies essentielles à la conduite des opérations militaires. Dans certains cas, elle accroît l'influence de la technologie sur notre réflexion; dans d'autres, elle élimine complètement la nécessité d'une intervention humaine. Il s'agit de sujets complexes auxquels tout professionnel sérieux devrait s'intéresser. La diversité même des articles réunis dans ce numéro spécial témoigne de la complexité de l'intégration de ces technologies essentielles à la profession des armes.

Cela dit, il est impressionnant de constater le talent avec lequel leurs auteurs s'attaquent à ces défis. Pour ce qui est du cyberspace, ce numéro spécial nous mène des fondements théoriques des politiques et des affaires étrangères, présentés dans l'article de Christina Marcotte, jusqu'aux bases conceptuelles exposées par Alex Green et Matthew Kellett, en passant par les rappels pratiques formulés par un praticien du domaine. C'est un réel plaisir de voir ces idées exprimées dans des textes de réflexion professionnelle. En ce qui concerne l'IA, les

articles de ce numéro spécial mettent en évidence l'influence grandissante du Centre d'intelligence artificielle du MDN/FAC. Ils couvrent un large éventail de sujets et proposent des conseils pratiques sur la mise en œuvre de cette technologie essentielle. Le numéro spécial propose également un point de vue externe qui rejoint, de façon indépendante, cette vision et les risques qui y sont associés.

Les sujets abordés dans ce numéro spécial sont d'une grande actualité et occupent le devant de la scène. Au moment où j'écris cet avant-propos, il me suffit de repenser à ce matin pour trouver des exemples opérationnels précis et des manchettes récentes portant sur l'IA ou la cybersécurité qui ont une incidence directe sur la sécurité nationale et la conduite de la guerre. J'aurais certes pu écrire cette phrase à presque n'importe quel moment au cours des dernières années, mais les développements récents en ont accentué et accéléré la pertinence. Nous avons même vu converger l'IA et le cyberspace, avec des modèles comme Mythos, capables d'automatiser la découverte de vulnérabilités dans les logiciels et de transformer profondément le cyberdomaine.

C'est précisément pour cette raison qu'il importe d'examiner avec sérieux les réflexions présentées dans ce numéro spécial. Nous vivons une période marquée par des transformations majeures des capacités militaires, découlant des avancées technologiques, et nous assistons à une évolution remarquablement rapide du caractère de la guerre, alors même que le conflit en Ukraine continue de démontrer que la guerre demeure avant tout un affrontement violent de volontés. Cette violence met en évidence une réalité fondamentale : la question n'est plus de savoir si l'IA et les cyberopérations transformeront la manière occidentale de faire la guerre, mais si nous saurons nous adapter aux transformations qu'elles ont déjà engendrées. Ce numéro spécial rassemble des points de vue variés et particulièrement opportuns qui contribueront à approfondir notre compréhension de ces enjeux.

Bonne lecture.



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.



L'officier de pont à bord du NCSM MARGARET BROOKE, travaille sur la passerelle alors que le navire se dirige vers la station de recherche Rothera sur l'île Adelaïde, en Antarctique, au cours de l'opération PROJECTION 25-01, le 15 mars 2025.

Caporal Connor Bennett, Forces armées canadiennes

Le Canada, puissance technologique responsable au XXI^e siècle

CHRISTINA MARCOTTE

Christina Marcotte est directrice adjointe au Secteur de la sécurité internationale et des affaires politiques d'Affaires mondiales Canada. Elle consacre beaucoup trop de temps à la lecture d'ouvrages d'histoire et demeure convaincue que Vespasien est l'empereur romain le plus sous-estimé. Les opinions exprimées dans le présent commentaire n'engagent qu'elle.

À mesure que le Canada progresse dans le XXI^e siècle, je repense aux paroles de Lord Palmerston, premier ministre britannique du XIX^e siècle : « Nous n'avons pas d'alliés éternels, et nous n'avons pas d'ennemis perpétuels. Nos intérêts sont éternels et perpétuels, et c'est notre devoir de les suivre. »¹

Le présent commentaire décrit les mesures prises par le gouvernement du Canada pour protéger et promouvoir les intérêts du pays en matière de sécurité à l'ère de la puissance technologique. Il porte principalement sur le cyberspace et les cyberoutils, y compris l'intelligence artificielle (IA). Aux fins du présent

commentaire, je ne tiendrai pas compte des avantages potentiellement transformateurs de l'IA et des autres technologies pour les processus opérationnels. Je m'intéresserai plutôt à l'adoption des technologies par l'État ainsi qu'à la gouvernance de leur utilisation, selon une approche responsable dans les deux cas. Dans ce

contexte, la responsabilité signifie que les mesures prises renforcent la coopération internationale, dont le Canada tire profit, et qu'elles respectent les principes démocratiques. En agissant ainsi, le Canada consolide les mécanismes de gouvernance qui ont permis au pays et à sa population de prospérer.

Premièrement, pour assurer la sécurité au XXI^e siècle, l'État doit s'adapter à l'évolution des technologies, sans quoi la population canadienne risque d'être exposée à des menaces pesant sur ses renseignements personnels et financiers, et le Canada se retrouverait désavantagé face aux menaces provenant d'États adverses et d'acteurs non étatiques. Les forces armées étrangères, les services d'espionnage, les organisations criminelles, les cyber-militants et d'autres acteurs malveillants mènent leurs activités dans le cyberspace.

Compte tenu du grand nombre de menaces auxquelles la population est confrontée dans le cyberspace, le Canada manquerait à ses obligations, découlant du contrat social, s'il ne développait pas et n'utilisait pas les outils nécessaires pour les contrer. Ce contrat social prévoit notamment que le gouvernement utilise les ressources financières fournies par les citoyens afin d'assurer leur protection. La capacité d'agir dans le cyberspace pour perturber les activités des cyberacteurs malveillants, les affaiblir et neutraliser les infrastructures cybernétiques qu'ils utilisent, y compris les organisations criminelles, fait partie intégrante de cette protection.²

Deuxièmement, en ce qui concerne la gouvernance, celle-ci est liée à l'ordre international qui est fondé sur des règles. Cet ordre international s'est développé depuis la Seconde Guerre mondiale et repose sur le multilatéralisme ainsi que sur ses institutions, notamment l'Organisation des Nations Unies (ONU), le droit international, les traités et les normes.

La prospérité économique du Canada découle en grande partie du fait que l'ordre international fondé sur des règles offre un cadre stable et prévisible pour le commerce mondial et les relations économiques internationales. Parallèlement, il contribue à la sécurité du Canada, en fournissant un cadre stable de coopération face aux défis internationaux ainsi qu'un mécanisme permettant d'élaborer des règles de conduite et des normes de comportement reconnues par tous. En tant que l'un des 193 États membres de l'ONU et puissance moyenne dans un monde qui compte un nombre croissant de puissances moyennes aux côtés de plusieurs superpuissances, le Canada ne peut pas façonner le monde à son image. Il est donc dans son intérêt de travailler avec des pays aux vues similaires. L'ordre international fondé sur des règles offre un cadre de coopération connu et fiable. Il n'est pas parfait, mais les principes d'égalité et de prévisibilité sur lesquels il repose servent beaucoup mieux les intérêts du Canada qu'un système où seule la force détermine l'issue des rapports entre les États.

Dans cet ordre international, la responsabilité constitue un pilier fondamental des principes et des processus du Canada. Cette responsabilité comporte deux dimensions : celle d'agir et celle de le faire de façon responsable. D'abord, les États qui disposent des

moyens d'action devraient le faire. Un État responsable intervient lorsqu'il en a la capacité. Il conteste l'espace dans lequel évoluent les acteurs malveillants. Laisser cet espace sans opposition expose inutilement les citoyens à des risques. Cette responsabilité vaut autant envers la population canadienne qu'envers les citoyens des États qui ne disposent ni des ressources ni des moyens permettant de prendre les mêmes mesures que le Canada.

Ces interventions doivent également être menées de manière responsable. Le Canada doit utiliser ces outils dans le respect de l'ordre international et de ses règles. Plus précisément, il doit agir conformément au *Cadre des Nations Unies pour le comportement responsable des États dans le cyberspace* auquel il a publiquement souscrit.³ Ce cadre reconnaît notamment que le droit international s'applique au cyberspace, prévoit la mise en œuvre des normes convenues, en particulier les onze normes des Nations Unies, l'application de mesures de confiance liées au cyberspace et le renforcement des capacités des États en développement.⁴

L'utilisation responsable de ces outils soutient et renforce l'ordre international fondé sur des règles, le système même qui a contribué à la prospérité du Canada. Cet enjeu revêt une importance particulière à un moment où cet ordre est confronté à des défis considérables. Certains États cherchent activement à remodeler l'ordre international afin de servir leurs propres intérêts, sans égard aux conséquences pour les autres États, ou encore à tirer parti des faiblesses de pays moins puissants dans un système où la loi du plus fort prévaut.

En tant que démocratie, le comportement responsable du Canada comprend également la reddition de comptes et la transparence. La reddition de comptes signifie que le Canada respecte les obligations qui lui incombent en vertu du droit international et du droit interne applicables, les engagements qu'il a pris relativement aux normes volontaires et aux autres engagements publics, ainsi que les mécanismes de gouvernance qui lui sont propres, notamment la chaîne de commandement militaire. La transparence signifie que le Canada informe le public de ses capacités et de la manière dont il les utilise, sans divulguer les détails opérationnels, et qu'il se soumet aux mécanismes de surveillance appropriés. Ces deux principes sont essentiels pour prévenir les abus de pouvoir et maintenir la confiance de la population envers son gouvernement.

Commençons par la question de la responsabilité. La technologie est utilisée comme un outil du pouvoir étatique, y compris l'IA, que ce soit à des fins d'espionnage ou d'armement ou pour d'autres usages encore imprévisibles. Toutefois, la technologie et l'IA ne peuvent être dissociées des infrastructures qui les soutiennent. Lorsque j'écris que « l'IA sera utilisée comme un outil du pouvoir étatique », cela signifie également que « l'IA sera utilisée dans le cyberspace et en tant que cyberoutil du pouvoir étatique ». Le cyberspace constitue à la fois un domaine et un outil. À l'instar des domaines terrestre, maritime, aérien et spatial, le cyberspace est un domaine d'activités civiles et militaires, un espace doté de dimensions dans lequel se déroulent des opérations. C'est

« Le Canada dispose déjà de règles et de normes claires concernant le cyberspace et l'utilisation des cyberoutils, notamment le cadre des Nations Unies pour le comportement responsable des États. »

d'ailleurs dans le cadre international basé sur des règles que les États ont établi les principes qui régissent le cyberspace. Le Canada dispose déjà de règles et de normes claires concernant le cyberspace et l'utilisation des cyberoutils, notamment le cadre des Nations Unies pour le comportement responsable des États mentionné précédemment. De plus, à mesure que l'IA est intégrée aux systèmes d'armes, leur emploi continue d'être régi par les règles d'engagement et le droit applicable.

L'IA représente également bien davantage qu'une simple évolution du cyberspace, et il demeure difficile d'anticiper l'ensemble de ses applications possibles. Les États en sont conscients et travaillent actuellement, selon les normes sur lequel repose l'ordre international, à l'élaboration de règles encadrant l'utilisation de l'IA comme outil du pouvoir étatique. Dans le domaine militaire, plusieurs initiatives plurilatérales portent expressément sur l'IA et son utilisation. Parmi celles-ci figure la *Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy*,⁵ lancée en 2023 sous la direction des États-Unis à l'occasion du Sommet sur l'intelligence artificielle responsable dans le domaine militaire (REAIM), organisé par les Pays-Bas. Par ailleurs, la version révisée en 2024 de la *Stratégie OTAN pour l'intelligence artificielle* comprend un objectif consacré au comportement responsable, précisant de « jeter les bases qui permettront à l'OTAN et aux alliés de montrer l'exemple et de piloter le développement et l'utilisation responsables de l'IA pour les besoins de la défense et de la sécurité des alliés ».⁶ Sur le plan multilatéral, il convient également de mentionner la résolution 79/239 de l'Assemblée générale des Nations Unies sur l'intelligence artificielle dans le domaine militaire.⁷

À l'échelle nationale, le gouvernement du Canada doit rendre compte de ses actes à ses citoyens. Les mesures qu'il a prises au cours des dernières années témoignent également de sa crédibilité comme acteur responsable et de son engagement à respecter les obligations qu'il a envers la population canadienne en matière de sécurité. Ces mesures comprennent notamment la publication de la *Stratégie nationale de cybersécurité* en 2018 et en 2024,⁸

en 2018 la création du Centre canadien pour la cybersécurité et l'établissement du Centre national de coordination en cybercriminalité de la Gendarmerie royale du Canada (GRC), la place importante accordée aux technologies dans les politiques de défense *Protection, Sécurité, Engagement* (2017)⁹ et *Notre Nord, fort et libre* (2024),¹⁰ ainsi que la mise à jour en 2019 de la *Loi sur le Centre de la sécurité des télécommunications*.¹¹

Moins visible pour le public, mais tout aussi importante, la création, en 2018, d'une unité au sein d'Affaires mondiales Canada chargée des politiques internationales en matière de cybersécurité, dont le mandat englobe maintenant également la gouvernance de l'IA, mérite aussi d'être soulignée. Cette unité possède l'expertise nécessaire pour représenter le Canada et défendre les intérêts du pays en matière de sécurité aux Nations Unies et dans d'autres forums multilatéraux. Elle coordonne également la contribution du Canada à des initiatives internationales, notamment le Processus de Pall Mall,¹² dirigé par le Royaume-Uni et la France afin de lutter contre la prolifération des outils de cyberintrusion. En parallèle, la Direction générale du droit international d'Affaires mondiales Canada compte des juristes, spécialisés dans le cyberspace. Cette direction a contribué de façon importante à l'ordre international fondé sur des règles et à la transparence du gouvernement du Canada, en élaborant et en publiant la position officielle du Canada sur l'application du droit international dans le cyberspace.¹³

Parmi les autres mesures, favorisant la transparence, figure l'initiative 88 de la politique de défense *Protection, Sécurité, Engagement* (2017), qui prévoit expressément ce qui suit : « nous nous doterons de la capacité de mener des cyberopérations actives axées sur les menaces externes au Canada dans le contexte de missions militaires autorisées par le gouvernement. L'emploi de cette capacité [...] sera assujéti à la même rigueur que d'autres formes de recours à la force militaire. Les cyberopérations seront assujetties à toutes les lois nationales et internationales applicables ainsi qu'aux garde-fous éprouvés comme les règles d'engagement et les évaluations de ciblage et de dommages collatéraux. »¹⁴ Que ces cyberoutils soient ou non renforcés par l'IA, ils demeureront assujettis aux mécanismes de reddition de comptes. En informant publiquement la population de la capacité des forces armées à mener des cyberopérations actives, également appelées cyberopérations offensives, ainsi que du cadre qui en régit l'emploi, le Canada contribue à renforcer l'ordre international.

La *Loi sur le Centre de la sécurité des télécommunications* traite également publiquement des cyberopérations actives du Canada. L'article 30 de cette loi prévoit que les ministres de la Défense nationale et des Affaires étrangères autorisent les cyberopérations actives. Les articles suivants précisent les types d'activités autorisées et interdites ainsi que les procédures applicables à leur autorisation.¹⁵

Par ailleurs, tant du point de vue des principes démocratiques que de la transparence, l'Office de surveillance des activités en

matière de sécurité nationale et de renseignement (OSSNR) et le Comité des parlementaires sur la sécurité nationale et le renseignement (CPSNR) jouent un rôle essentiel. Le mandat de l'OSSNR comprend l'examen et l'enquête sur les activités du gouvernement du Canada en matière de sécurité nationale et de renseignement afin de vérifier qu'elles sont légales, raisonnables et nécessaires.¹⁶ De façon plus générale, le CPSNR examine le cadre législatif, réglementaire, stratégique, administratif et financier applicable à la sécurité nationale et au renseignement, ainsi que toute activité menée par un ministère en lien avec ces domaines.¹⁷ L'OSSNR et le CPSNR doivent chacun présenter un rapport annuel au premier ministre, qui dépose ensuite les rapports du Comité devant les deux chambres du Parlement.

Enfin, le fait d'agir comme une puissance technologique responsable renforce également la crédibilité du Canada lorsqu'il approfondit sa coopération avec ses partenaires et ses alliés. L'ampleur et la diversité des menaces font en sorte que le Canada ne peut assurer seul sa sécurité, d'où l'importance essentielle de ces partenariats. Ils permettent de mieux comprendre les menaces, d'élaborer les moyens les plus efficaces pour les atténuer et les gérer, puis de les contrer. Travailler ensemble exige de la confiance; travailler efficacement ensemble en exige davantage

encore. La cohérence entre les actions du Canada et les principes qu'il défend contribue à établir sa réputation de partenaire digne de confiance. Cela vaut autant pour des partenariats de longue date, comme l'OTAN, que pour ceux établis et approfondis dans le cadre de la *Stratégie du Canada pour l'Indo-Pacifique*.

En se tournant vers l'avenir et en répondant à ses besoins de sécurité dans les années à venir, le Canada continuera d'agir comme un acteur étatique responsable dans le cyberspace, y compris à mesure que de nouvelles technologies feront leur apparition. Cela concerne notamment la manière dont le Canada utilisera l'IA et toute autre technologie comme outil du pouvoir étatique. Les progrès technologiques et les changements qui les accompagnent ne modifieront ni le contrat social qui unit la population canadienne à son gouvernement ni l'engagement constant de celui-ci à protéger ses citoyens. Les mesures déjà prises par le gouvernement du Canada témoignent de cet engagement. En continuant d'agir comme un acteur étatique responsable, le Canada réaffirme son attachement aux mécanismes de gouvernance, tant sur le plan international qu'à l'échelle nationale, qui ont permis à la population canadienne de prospérer.

Notes

- 1 Le vicomte Palmerston, « Treaty of Adrianople—Charges Against Viscount Palmerston », *House of Commons Debates*, 1^{er} mars 1848, Hansard, vol. 97, col. 122. Source originale : <https://api.parliament.uk/historic-hansard/commons/1848/mar/01/treaty-of-adrianople-charges-against>
- 2 Jacques J. M. Shore, « An Obligation to Act: Holding Government Accountable for Critical Infrastructure Cyber Security », *International Journal of Intelligence and Counterintelligence* 28, no 2 (2015) : 238. Source originale : <https://doi.org/10.1080/08850607.2014.96235>
- 3 Affaires mondiales Canada, « Politique internationale en matière de cybersécurité », consulté le 11 août 2026. Source originale : https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_scurite/cyber_policy-politique_cyberspace.aspx?lang=eng, citant Assemblée générale des Nations Unies, source originale : *Progrès de l'informatique et des télécommunications et sécurité internationale*, A/RES/70/237 (23 décembre 2015).
- 4 Assemblée générale des Nations Unies, Groupe d'experts gouvernementaux, A/RES/70/237.
- 5 Département d'État des États-Unis, Bureau du contrôle des armements, de la dissuasion et de la stabilité, *Déclaration politique sur l'utilisation militaire responsable de l'intelligence artificielle et de l'autonomie*, 9 novembre 2023, source originale : <https://www.state.gov/political-declaration-on-responsible-military-use-of-artificial-intelligence-and-autonomy-2/>
- 6 *Résumé de la stratégie révisée de l'OTAN en matière d'intelligence artificielle* (IA), 5, 1.1, 10 juillet 2024. Source originale : <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/07/10/summary-of-natos-revised-artificial-intelligence-ai-strategy>
- 7 Assemblée générale des Nations Unies, *L'intelligence artificielle dans le domaine militaire et ses incidences sur la paix et la sécurité internationales*, A/RES/79/239 (24 décembre 2024).
- 8 Sécurité publique Canada, *Stratégie nationale de cybersécurité : Vision du Canada pour la sécurité et la prospérité dans l'ère numérique* (gouvernement du Canada, juin 2018). Source originale : <https://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/ntnl-cbr-scr-tstrtg/ntnl-cbr-scr-tstrtg-en.pdf>; Sécurité publique Canada, *Stratégie nationale de cybersécurité : Sécuriser l'avenir numérique du Canada* (gouvernement du Canada, 2025), source originale : <https://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/ntnl-cbr-scr-tstrtg-2025/ntnl-cbr-scr-tstrtg-2025-en.pdf>
- 9 Ministère de la Défense nationale, *Protection, Sécurité, Engagement : La politique de défense du Canada* (gouvernement du Canada, juin 2017). Source originale : <https://www.canada.ca/en/departement-national-defence/corporate/reports-publications/canada-defence-policy.html>
- 10 Ministère de la Défense nationale, *Notre Nord, fort et libre : Une vision renouvelée pour la défense du Canada* (gouvernement du Canada, avril 2024). Source originale : <https://www.canada.ca/en/departement-national-defence/corporate/reports-publications/north-strong-free-2024.html>
- 11 *Loi sur le Centre de la sécurité des télécommunications*, LC 2019, ch. 13, art. 76. Source originale : <https://laws-lois.justice.gc.ca/eng/acts/C-35.3/page-1.html>
- 12 Royaume-Uni, Foreign, Commonwealth & Development Office, *Code de pratique du Processus de Pall Mall à l'intention des États* (gouvernement du Royaume-Uni, 4 avril 2025). Source originale : <https://www.gov.uk/government/publications/the-pall-mall-process-code-of-practice-for-states>
- 13 *Le droit international applicable dans le cyberspace*. Source originale : https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_scurite/cyberspace_law-cyberespace_droit.aspx?lang=eng
- 14 Ministère de la Défense nationale, *Protection, Sécurité, Engagement*, p. 73.
- 15 *Loi sur le Centre de la sécurité des télécommunications*, art. 30.
- 16 *Loi sur l'Office de surveillance des activités en matière de sécurité nationale et de renseignement*, LC 2019. Source originale : <https://laws-lois.justice.gc.ca/eng/acts/N-16.62/page-1.html>
- 17 *Loi sur le Comité des parlementaires sur la sécurité nationale et le renseignement*. Source originale : <https://laws-lois.justice.gc.ca/eng/acts/N-16.61/page-1.html>

Introduction aux notions de base sur la cybersécurité du gouvernement du Canada : un premier aperçu

ALEXANDRA GREEN ET MATTHEW KELLETT

Alex Green a été la toute première officière responsable de l'Équipe de cybergdéfense de la Flotte dans les Forces maritimes du Pacifique [FMAR (P)], de 2018 à 2020. Elle prépare actuellement un doctorat en études de la guerre au Collège militaire royal du Canada, où elle se spécialise en cyberterrorisme. En 2024, elle a reçu le prix Franklin-Pinch pour ses recherches sur la mise au point d'applications personnalisées à des fins terroristes.

Matthew Kellett, Ph.D. est conseiller spécial au Commandement des cyberopérations des Forces armées canadiennes. Il a déjà été programmeur de logiciels dans le secteur commercial et scientifique de la défense. Il est titulaire d'un doctorat en informatique théorique, plus précisément sur la conception et l'analyse d'algorithmes répartis. Il aime les échecs, la course à pied et le curling, et il a déjà été président du Ottawa Curling Club.

Les Forces armées canadiennes (FAC) et le ministère de la Défense nationale (MDN) s'empresent de répondre à la demande en matière de capacités de cybersécurité. Les FAC ont créé le groupe professionnel des opérateurs de cyberopérations en 2017,¹ et l'École d'électronique et des communications des Forces canadiennes (EEFCF) a annoncé la première promotion de diplômés en 2021.² Trois ans plus tard, en septembre 2024, les FAC ont officiellement établi le Commandement des cyberopérations des Forces armées canadiennes (COMCYBERFAC). Ce commandement est la seule autorité reconnue du MDN et des FAC pour les cyberopérations, qui englobent le renseignement électromagnétique et la guerre électronique interarmées. La création du COMCYBERFAC est importante, car elle permet de regrouper en une seule chaîne de commandement unifiée et transparente plusieurs efforts pandomaines, visant à tirer parti des capacités de cyberopérations, créant ainsi un « guichet unique » pour l'expertise en cyberopérations.

Au cours des sept années qui ont mené à la mise sur pied du Commandement des cyberopérations, les FAC ont créé un nouveau groupe professionnel et diplômé leur première cohorte d'opérateurs de cyberopérations. Les FAC investissent dans les capacités de cyberopérations. La dotation représentait autrefois un défi, mais le nombre d'opérateurs qualifiés est en croissance. Malgré cette croissance, un rapport de 2020 du directeur général – Évaluation, intitulé *Évaluation des cyberforces*, a conclu que les « cyberforces comptent un nombre suffisant de postes; toutefois, la dotation de ces postes pose problème », et a fait état de difficultés liées à l'embauche et au maintien en poste de civils, ainsi qu'à l'arrimage des besoins en matière de capacités de cyberopérations avec l'approche conventionnelle du perfectionnement professionnel militaire. Le rapport faisait état plus particulièrement de la frustration liée aux situations de « cyberpersonnel qui compte le plus d'expérience, et qui travaille pour du personnel qui possède peu d'expérience du cyberdomaine ». La création du Commandement devrait grandement contribuer à résoudre ces problèmes.

La situation s'améliore à mesure que le groupe professionnel de cyberopérateur arrive à maturité et que l'Unité d'instruction sur le cyberspace forme des opérateurs. Même si cette capacité se développe rapidement, les connaissances de base en cybersécurité dans le reste du MDN et des FAC n'ont pas suivi le même rythme. Les membres de l'Équipe de la Défense sont souvent affectés à des postes nécessitant des connaissances en cyberopérations sans avoir de solides antécédents en la matière. Bon nombre de ces militaires ne sont pas nés à l'ère du numérique. Cela se comprend, puisque l'âge moyen des militaires des FAC est de 36 ans³ et que le *World Wide Web* est accessible au grand public depuis 30 ans; l'effectif moyen des FAC n'est donc pas né dans un monde où l'Internet était déjà présent. La plupart des personnes en poste à la haute direction des FAC ont plus de 30 ans; il est donc raisonnable de supposer que beaucoup de personnes ne sont pas nées dans un univers entièrement connecté à l'Internet et médiatisé par celui-ci. Elles représentent une génération de militaires des FAC qui doivent composer avec le cyberdomaine dans leurs tâches militaires, mais pour qui l'Internet a d'abord été une

idée nouvelle apparue au début de leur carrière. À mesure que les FAC élargissent et priorisent les cyberopérations et les cybercapacités, de nombreux militaires doivent rapidement s'approprier et comprendre la terminologie du domaine.

Il va de soi qu'un grand nombre de membres de la communauté de défense canadienne connaissent bien les aspects techniques et non techniques de la cybersécurité. Ces personnes peuvent juger le présent article utile comme aide-mémoire. Cet article vise surtout à servir de texte d'initiation pour établir un niveau de connaissances de base chez les militaires et les civils qui viennent tout juste d'être affectés à un poste, où ils doivent se familiariser avec ces concepts.

En plus de présenter certaines notions de base dans un cadre militaire, le présent article traite des fausses idées courantes auxquelles ces nouveaux membres de l'équipe peuvent être confrontés. D'abord, nous présentons certains termes fréquemment utilisés. Même si les employés du gouvernement du Canada peuvent avoir accès aux notes de doctrine interarmées, à la Banque de terminologie de la Défense et à Termium, nous croyons que le fait de regrouper les notions dans un même article, avec des exemples, aidera les nouveaux membres à s'adapter plus rapidement. Nous présentons des termes tels que *cyberespace*, *cyberenvironnement*, *nuage*, *cyberdomaine* et l'emploi de « *cyber* » comme adjectif. Nous expliquons ensuite que le cyberespace est souvent considéré comme un bloc monolithique et nous exposons les nuances entre les différents types de technologies qui se rattachent au cyberespace. Compte tenu de ces nuances, nous établissons une distinction entre le cyberespace et l'environnement de l'information. Les deux sont souvent confondus, car les équipes de cyberopérations doivent souvent soutenir des effets d'information. Nous expliquons également la populaire analogie du château et la façon dont elle peut servir à comprendre la différence entre les cyberopérations et les opérations de réseau. L'article se termine par deux autres distinctions importantes : la première entre cybersécurité et cyberdéfense, et la seconde entre cyberévénement, cyberincident et cyberattaque. Après avoir lu le présent article, les lecteurs devraient posséder une base solide pour approfondir les concepts et participer à des discussions plus poussées.

Définitions et termes courants

D'abord, nous expliquons des termes courants avant d'aborder les différences nuancées entre les concepts. Tout membre de la communauté de la défense sait que les FAC et le MDN peuvent être perçus comme un véritable alphabet de sigles et de termes déroutants. Il est donc pertinent de traiter d'emblée certains termes normalisés que les lecteurs pourraient trouver dans leur travail. Pour les FAC et le MDN, l'*environnement des cyberopérations*, le *cyberenvironnement* ou, en abrégé, le *cyberespace*, est un environnement physique, tout comme la mer, la terre, l'air et l'espace. Une infrastructure matérielle sous-tend le monde virtuel et en est

indissociable. Chaque équipement avec lequel un utilisateur interagit est relié à un autre équipement matériel situé ailleurs, soit par des fils et des câbles de fibre optique, soit par des photons qui circulent dans l'air et l'espace. Le nuage n'est pas réellement un nuage; il s'agit généralement d'un immense entrepôt rempli d'équipements de réseautage et de serveurs informatiques qui exécutent des logiciels chargés de veiller à ce que les données continuent d'exister même après la défaillance inévitable du matériel sur lequel elles sont stockées. Ainsi, plutôt que d'être entreposées sur votre appareil physique, ces données sont sauvegardées sur un serveur ou un groupe de serveurs et sont accessibles par l'Internet ou par un autre grand réseau. C'est de là que vient notre premier mot à la mode, soit le terme *nuage*. Les ingénieurs de réseaux, informaticiens et autres spécialistes qui tracent des diagrammes de réseaux utilisent traditionnellement un symbole en forme de nuage comme substitut pour représenter l'infrastructure sous-jacente complexe qui échappe au contrôle de l'organisation. Lorsque des compagnies comme Amazon et Google ont commencé à offrir des ressources informatiques à distance, le *nuage* a été présenté comme un nouveau type de prestation de services, les entreprises interagissant avec ces services sans exercer de contrôle direct sur l'infrastructure.

Ensuite, le *cyberdomaine* correspond au cyberespace, ainsi qu'à tout ce qui l'entoure et le soutient, notamment les personnes, les processus et les infrastructures. Le gouvernement du Canada utilise ce terme pour désigner « toute l'infrastructure, toutes les entités, tous les utilisateurs et toutes les activités liées au cyberespace ou qui ont une incidence sur celui-ci ».⁴ Le cyberdomaine peut englober la vérification de l'identité d'un nouvel employé avant qu'on lui attribue des preuves d'identité pour accéder au réseau ministériel, la sécurité des locaux abritant les serveurs et l'équipement de réseautage, et même les personnes qui administrent le réseau; autant d'éléments essentiels au maintien du cyberespace, mais qui ne relèvent pas à proprement parler du cyberespace. Le Canada, l'OTAN et de nombreux alliés ont reconnu le cyberdomaine comme un domaine de guerre, au même titre que les domaines maritime, terrestre, aérien et spatial. Cette reconnaissance signifie que les FAC doivent être prêtes à mener des cyberopérations dans le cyberenvironnement (c'est-à-dire le cyberespace) et être capables de défendre leur part du cyberdomaine.⁵

Le terme *cyber* n'est donc qu'un adjectif, indiquant que l'élément qu'il qualifie est lié au cyberdomaine ou au cyberespace. Pensez, par exemple, à son emploi dans la cybersécurité, les cyberopérations et les cyberincidents. Le mot *cyber* est d'ailleurs utilisé à outrance. Dans un contexte militaire, les lecteurs entendront peut-être le terme *cyberplanification* beaucoup trop souvent. La *cyberplanification* n'est rien d'autre qu'une planification militaire appliquée au cyberdomaine; elle n'a rien de particulièrement *cyber* et devrait simplement être appelée par son nom, soit la planification. Par ailleurs, le terme *cyber* ne devrait pas être utilisé comme un nom ni comme un verbe, même si c'est souvent le cas

dans la langue courante. Ainsi, on ne devrait jamais écrire : « Ils devraient utiliser le cyber pour cela » ou « Nous devrions cyber ceci ». Dans la prochaine section, nous décomposerons le vaste concept de *cyberespace*, puis nous en établirons la distinction par rapport à l'environnement de l'information.

Décomposer le cyberespace : notions de TO, TP et IdO

Même s'il est courant de regrouper tous les éléments sous le terme de *technologie de l'information (TI)*, les FAC et le MDN doivent être plus précis au sujet des composantes du cyberespace s'ils veulent les gérer correctement. Au sein des FAC et du MDN, nous disons TI pour désigner l'infrastructure classique de bureautique et de réseautage, pour faire la distinction avec la technologie opérationnelle, qui sert à faire fonctionner les systèmes physiques, comme les pompes et les appareils de chauffage, et de la technologie de plateforme, qui correspond à la technologie opérationnelle, installée sur des plateformes militaires, comme les navires, les systèmes de commande des moteurs et les systèmes de guidage des missiles. Nous pouvons diviser le cyberespace en sous-catégories : technologie de l'information (TI), technologie opérationnelle (TO) et technologie de plateforme (TP). Il vaut également la peine de préciser où se situent les appareils de l'Internet des objets (IdO) dans ces différentes catégories. Si vous êtes nouveau dans le domaine, vous entendrez probablement ces termes employés pour désigner des biens du gouvernement. Nous avons simplifié les définitions ci-dessous pour rendre ces concepts plus accessibles.

Technologie opérationnelle (TO)

La technologie opérationnelle concerne l'ensemble des systèmes industriels cyberphysiques. Elle comprend les systèmes de contrôle industriel et les systèmes de contrôle et d'acquisition de données. À la maison, le thermostat qui commande votre fournaise est un exemple de TO. La TO assure l'interface entre le cyberespace et les systèmes physiques, comme les vannes, les registres et les ventilateurs, que l'on retrouve dans tout, des systèmes de chauffage, de ventilation et de climatisation jusqu'aux oléoducs servant au transport du carburant. Même s'il est souvent possible de mettre à jour le code informatique de ces systèmes, cela ne se produit généralement qu'à l'occasion de révisions majeures ou, dans le pire des cas, lors de leur remplacement. Parfois, il est difficile de mettre ces systèmes à jour, car ils soutiennent des systèmes essentiels. On ne voudrait certainement pas arrêter une usine de traitement de l'eau ou désactiver régulièrement les systèmes de sûreté d'une centrale nucléaire pour mettre à jour leurs logiciels.

Dans certains cas, les mises à jour sont difficiles, voire impossibles, parce que l'équipement est inaccessible. Par exemple, il peut être nécessaire de vider des sections de l'usine de

traitement de l'eau pour accéder à certains équipements, ou un organe de commande essentiel peut se trouver dans une zone radioactive d'une centrale nucléaire. Même si les systèmes de TO relient le cyberespace aux systèmes physiques, la bonne pratique consiste à les isoler sur leurs propres réseaux et à ne pas, par exemple, les brancher directement à l'Internet.

Technologie de plateforme (TP)

La technologie de plateforme désigne la technologie opérationnelle utilisée sur les plateformes militaires. Elle comprend le matériel et les logiciels qui se trouvent à bord des navires, des avions, des véhicules et des systèmes d'armes. Comme pour votre voiture, les microprocesseurs et les fils servant à contrôler les fonctions d'un véhicule blindé sont tous des exemples de TP. La TP comprend souvent des processeurs ou des microprocesseurs spécialisés qui commandent les fonctions de la plateforme, comme un système de guidage de missile. Il est souvent presque impossible de remplacer ces microprocesseurs; toute vulnérabilité qu'elles présentent subsiste donc pendant toute la durée de vie de l'équipement.

Puisqu'il est difficile de mettre à jour ou de remplacer la TO et la TP, nous devons assurer leur sécurité et veiller à ce que les mises à jour n'introduisent pas de vulnérabilités. Cette protection s'inscrit dans un effort plus vaste appelé *cyberassurance de la mission (CAM)* que le gouvernement du Canada définit comme « processus consistant à protéger ou à assurer la résilience des ressources et des capacités essentielles à la mission, contre les cybermenaces ou cyberactions, dans tout environnement d'opérations ou toute condition opérationnelle ». ⁶ En termes simples, la CAM est la capacité de mener des cyberopérations militaires au moyen de capacités militaires qui reposent sur le cyberespace, lequel peut être contesté. Dans un contexte naval, par exemple, un navire devrait encore être en mesure d'utiliser ses réseaux et ses capacités techniques pour combattre, flotter ou se déplacer dans un cyberenvironnement contesté. La CAM peut aussi consister à assurer la sécurité de ces systèmes et de leurs chaînes d'approvisionnement, tant au cours de leur mise au point qu'une fois qu'ils sont déployés. Puisque les chaînes d'approvisionnement technologiques sont souvent de nature mondiale, il existe toujours un risque que les systèmes, les logiciels et les capacités techniques que les FAC acquièrent soient éventuellement exploités. Les commandants qui adhèrent aux principes de la CAM doivent prévoir des plans de rechange pour continuer à exécuter la mission, peu importe la cybermenace.

Internet des objets (IdO)

Les appareils de l'Internet des objets deviennent moins coûteux, plus pratiques et faciles à adapter, si bien qu'il ne soit pas surprenant qu'ils finissent par fournir certaines capacités essentielles dans le cadre d'une opération militaire. L'Internet des objets

comprend des éléments de TI et de TO de qualité grand public et d'entrée de gamme. Parmi les exemples d'IdO, mentionnons les ampoules intelligentes, les verrous intelligents et les appareils électroménagers intelligents, ainsi que les thermostats connectés, caméras, sonnettes et moniteurs pour bébé connectés à l'Internet. Ils offrent souvent des capacités utiles, comme la surveillance de votre propriété au moyen d'une caméra ou la commande automatique de lait par votre réfrigérateur lorsque vos réserves sont faibles. Les appareils de l'IdO sont souvent peu coûteux, dotés de processeurs à faible puissance et munis de mesures de sécurité minimales ou inexistantes, et ils peuvent être difficiles, voire impossibles à mettre à jour.

À mesure que les FAC sont confrontées à un environnement de menaces plus complexe et qu'elles doivent composer avec des processus d'approvisionnement difficiles, les appareils de l'IdO, qui étaient auparavant nouveaux et difficiles à intégrer, offrent maintenant des solutions simples. Cependant, ces appareils posent un *problème de complexité à faible coût*.⁷ Dans le passé, si les FAC voulaient acquérir une machine ou un dispositif spécialisé et complexe, elles devaient trouver un fournisseur spécialisé. Ce dispositif coûtait très cher, compte tenu des efforts et des ressources nécessaires à sa conception. Or, la situation est différente avec les appareils de l'IdO. Aujourd'hui, il est souvent moins coûteux de prendre un dispositif complexe et de le *faire passer* pour un dispositif simple que de fabriquer réellement un dispositif simple. Par défaut, en raison des économies d'échelle (il est moins coûteux de fabriquer des millions d'exemplaires d'un même produit que d'en fabriquer quelques exemplaires sur mesure), les fournisseurs sont encouragés à doter les appareils de l'IdO de toutes les fonctions possibles : Wi-Fi, stockage en nuage, apprentissage automatique, logiciels complexes, Bluetooth et microphones. Si une organisation (comme les FAC) veut utiliser ce dispositif pour une capacité opérationnelle sans la connectivité Wi-Fi, il est souvent plus simple et moins coûteux de désactiver cette fonction que de fabriquer une version sur mesure qui en est dépourvue. Néanmoins, cette fonction résiduelle demeure une vulnérabilité et, comme les appareils de l'IdO sont tristement célèbres pour la rareté des mises à jour de leur micrologiciel, cette vulnérabilité peut demeurer non corrigée et sujette à l'exploitation.

Ces caractéristiques font des appareils de l'IdO une cible idéale pour l'exploitation par des acteurs malveillants. Par exemple, le botnet Mirai a été observé pour la première fois en août 2016. Il a tiré parti de centaines de milliers d'appareils de l'IdO mal sécurisés, comme les moniteurs pour bébé et les caméras connectées à l'Internet, pour créer un réseau capable de submerger des cibles de paquets réseau dans le cadre d'attaques par déni de service distribué.⁸ Même si sa cible initiale était *Minecraft*, il a servi à de nombreuses autres attaques et son code source a fini par être publié dans un dépôt de code libre.⁹ Malgré les problèmes que ces appareils posent sur le plan de la sécurité, leur utilisation augmente en raison de leur commodité. Il ne serait pas surprenant qu'ils viennent un jour à fournir certaines

capacités essentielles dans le cadre d'une opération militaire. Si tel est le cas, nous devons être conscients des risques en cause, tout comme nous devrions l'être des risques liés à leur utilisation dans nos foyers.

Différence entre le cyberspace et l'environnement de l'information

Les lecteurs qui découvrent ce domaine pourraient employer indifféremment les termes *environnement de l'information* et *cyberspace*. Mais qu'est-ce que l'environnement de l'information? Le gouvernement du Canada le définit ainsi : « environnement comprenant l'information elle-même et les personnes, les organisations et les systèmes qui reçoivent, traitent et transmettent l'information, ainsi que les espaces cognitif, virtuel et physique dans lesquels cela se déroule ».¹⁰ Cependant, ce n'est pas la seule définition. Il en existe plusieurs autres, et la définition canadienne n'est pas universelle. Par exemple, selon le *Tallinn Manual*, une vaste étude universitaire (non contraignante) sur l'applicabilité du droit international à la cyberguerre et aux cyberopérations, l'environnement de l'information est « l'ensemble des personnes, des organisations et des systèmes qui recueillent, traitent et diffusent l'information, ou qui agissent sur cette base ».¹¹ Les deux définitions diffèrent, car la définition du *Tallinn Manual* met l'accent uniquement sur les acteurs et les systèmes, tandis que la définition du gouvernement du Canada englobe les acteurs, les systèmes et l'environnement dans lequel ils interagissent. À cet égard, la définition du gouvernement du Canada mentionne explicitement l'information comme partie intégrante du système, alors que la définition du *Tallinn Manual* ne mentionne pas l'information comme un objet en soi. Par ailleurs, même si la définition du gouvernement du Canada décrit explicitement l'environnement de l'information comme un environnement et insiste sur ce contexte, elle n'aborde pas le concept plus large d'*environnement*.

À la différence des environnements maritime, terrestre, aérien, spatial et cyberspatial, l'environnement de l'information n'est pas un environnement physique, même s'il interagit avec l'environnement physique à titre de support. Par exemple, si des troupes du pays A sont déployées dans un pays allié B pour dissuader une agression du pays C, et que le pays C ne souhaite pas encore recourir à une action militaire conventionnelle contre le pays B, il peut tirer parti de l'environnement de l'information. Le pays C pourrait créer des comptes sur les médias sociaux et des robots conversationnels pour diffuser de la désinformation sur les activités du pays A dans le pays B, en avançant que les troupes du pays A terrorisent la population locale, laissent des déchets un peu partout et commettent des crimes. Dans cet exemple, tous les commentaires laissés par les robots sur les médias sociaux sont des éléments de l'environnement de l'information. Le pays C utilise du matériel pour faire fonctionner ces robots (serveurs accueillant les réseaux de robots, stockage des données des utilisateurs, fichiers journaux et alimentation

permettant l'intégration aux applications de médias sociaux), et ce matériel fait partie du cyberspace. Une partie de ce contenu diffusé sur les médias sociaux peut se retrouver dans un journal, où ces allégations seront imprimées sur un support physique. Les citoyens du pays B consulteront ces messages au moyen d'appareils physiques, en passant par l'Internet. Ces appareils font eux aussi partie du cyberspace. Si les citoyens du pays B croient ces allégations et modifient leur opinion quant à l'accueil des troupes du pays A, l'environnement de l'information s'en trouve modifié.

Cet exemple illustre également la différence entre les opérations d'information et les cyberopérations, qui se distinguent par leurs objectifs et leur nature. Les opérations d'information portent principalement sur l'environnement de l'information et visent à modifier la façon dont la cible perçoit l'information. Les opérations d'information sont des « activités d'informations coordonnées dans ou par le biais de l'environnement d'information visant à produire des effets désirés sur la volonté, la compréhension et la capacité de personnes ».¹² Cette définition comporte quelques éléments essentiels : les actions ou opérations doivent être délibérées et synchronisées, viser à atteindre des résultats ou des effets précis, et cibler principalement des personnes. Supposons que Bob envoie un courriel à Alice pour lui présenter les points saillants de son projet, en vue de lui demander plus tard du financement. Ce courriel constitue une opération d'information, car Bob modifie positivement la perception qu'elle a du projet.

Alors que les opérations d'information visent à modifier la perception ou le comportement du sujet, les cyberopérations servent à modifier le support que constitue le cyberspace, en permettant des activités qui seraient normalement interdites, intentionnellement ou non, ou en empêchant des activités qui seraient normalement permises, intentionnellement ou non. Le cyberspace est au cœur des cyberopérations. Il est impossible de mener une cyberopération sans l'infrastructure du cyberspace. Les définitions usuelles mettent en évidence ce lien. Par exemple, le gouvernement du Canada définit une opération dans le cyberspace comme un « ensemble d'actions menées dans ou via le cyberspace dans le but de préserver la liberté de ses propres forces ou des forces amies dans le cyberspace ou de créer des effets permettant d'atteindre les objectifs militaires ».¹³ En termes plus simples, le *Tallinn Manual* décrit une cyberopération comme « l'emploi de cybercapacités ayant pour objectif principal d'atteindre des objectifs dans le cyberspace ou au moyen du cyberspace ».¹⁴ Quand on entend parler de *cyberopérations*, on pense souvent à des opérations spectaculaires du niveau de Stuxnet. Cependant, une cyberopération peut être aussi simple que l'application d'un correctif pour contrer délibérément un virus connu et, en définitive, modifier le cyberspace afin d'améliorer la santé du réseau.

Pourquoi les cyberopérations et les opérations d'information sont-elles souvent confondues, et comment sont-elles liées? D'abord, dans les deux cas, il s'agit de produire des effets, qu'ils portent sur la psyché humaine (opérations d'information) ou

sur des systèmes techniques (cyberopérations), et ces effets peuvent parfois se recouper. Certains peuvent présumer que les opérations d'information sont des cyberopérations, parce que des cyberopérations peuvent être menées en même temps que des opérations d'information. Comme nous l'avons mentionné, le cyberspace est un support que les gens utilisent pour accéder à l'environnement de l'information (par exemple, en se servant d'un ordinateur pour effectuer des recherches). Nous confondons souvent les câbles, les serveurs et les routeurs (les éléments matériels du cyberspace) avec l'environnement de l'information, parce que nous pouvons les utiliser pour communiquer de l'information. Ces deux concepts prêtent aussi à confusion parce qu'à une certaine époque, les opérations d'information et les cyberopérations étaient regroupées dans une seule et même catégorie. Enfin, la confusion est entretenue par le fait que les équipes désignées pour les cyberopérations se voient habituellement confier la tâche d'influer sur l'environnement de l'information : une cyberopération peut avoir des effets liés à l'information, et les opérations d'information peuvent tirer parti du cyberspace. Par exemple, si Alice hésite encore à financer le projet de Bob, celui-ci pourrait engager Ève pour lui envoyer un enregistreur de frappes (application cachée qui enregistre les touches du clavier et parfois l'écran) afin d'infecter l'ordinateur d'Alice et de recueillir des renseignements susceptibles de servir au chantage. Bob pourrait ensuite utiliser ces renseignements pour influencer sur la décision d'Alice. Il est toutefois possible de mener cette opération d'information entièrement en dehors du cyberspace. Par exemple, Bob pourrait agraffer sur le campus des affiches contenant de la désinformation au sujet des recherches d'Alice afin de susciter un climat défavorable.

Il existe donc des moyens d'influer sur le comportement ou les décisions d'un public cible sans recourir au cyberspace. Nous avons utilisé un exemple fictif pour illustrer la différence entre les opérations d'information et les cyberopérations, et la section suivante porte sur la métaphore bien connue du château, qui fait ressortir les distinctions entre les cyberopérations et les opérations de réseau. L'article distingue ensuite la cyberdéfense de la cybersécurité.

La métaphore du château : cyberopérations et opérations de réseau

Les débutants peuvent rencontrer la métaphore de la forteresse ou du château en tant qu'explication simplifiée de la façon dont un réseau ou un ordinateur est protégé. Dans cette métaphore, un défenseur peut protéger un bien derrière des couches de défense, comme les dirigeants de l'époque médiévale qui fortifiaient une structure au moyen d'un fossé et de murs d'enceinte épais, parfois arrondis pour empêcher l'ennemi de les escalader, et de murs intérieurs servant à diviser le château en différentes zones d'accès (basse cour, haute cour, donjon). Même si les couches de défense réduisent le risque d'intrusion, il demeure toujours

possible qu'une force ennemie tente de briser ces défenses. De même, le fait de creuser un fossé et d'ériger des murs d'enceinte ne signifie pas que le travail est terminé. Les défenseurs doivent évoluer au même rythme que leurs adversaires. Si les murs offrent une bonne protection contre les flèches et les frondes, rien ne garantit que ces murs et ce fossé résisteront suffisamment bien aux catapultes. Par ailleurs, le défenseur doit assurer l'entretien continu de ces défenses. Les murs doivent être réparés lorsqu'ils sont endommagés et surveillés pour repérer les ennemis et toute personne qui tenterait de les escalader.¹⁵

Les parallèles avec un réseau sont évidents. Les murs du château sont souvent assimilés à un pare-feu, qui laisse entrer certains éléments, mais pas d'autres, et qui assure un périmètre défensif. Les murs intérieurs du château ressemblent aussi au cloisonnement des réseaux, qui permet de segmenter les différentes parties du réseau en fonction des niveaux d'accès privilégiés. Ainsi, si un assaillant franchit les murs du château, il se peut qu'il soit incapable d'accéder à la basse-cour ou au donjon. L'exigence d'un mot de passe pourrait s'apparenter au levage de la herse. À l'instar d'un château, les défenses du réseau doivent être constamment mises à jour au fur et à mesure que les ennemis évoluent : les défenseurs du réseau doivent appliquer des correctifs, mettre à jour les listes de signatures de logiciels malveillants et ajuster la configuration de leurs listes de permissions et d'interdictions. Ce processus est sans fin.

La défense peut aussi devenir encore plus active. Si vous envoyez vos troupes au-delà des murs pour repérer la catapulte et la détruire, nous appellerons ces actions des *cyberopérations défensives—mesures d'intervention*, ce qui correspond simplement à une forme d'autodéfense dans le cyberdomaine afin d'assurer la *liberté d'action*.¹⁶ Si vous prenez pour cible les troupes adverses et détruisez leur château, ou si vous capturez leur drapeau et hissez le vôtre, dans le monde du cyberspace, nous parlerions alors de *cyberopérations offensives*, puisqu'il s'agit d'une opération visant à « projeter une puissance dans le cyberspace ou au moyen de celui-ci pour produire des effets à l'appui d'objectifs militaires ». ¹⁷ Dans un contexte de cybersécurité, cela pourrait consister, par exemple, à surcharger l'infrastructure de l'adversaire de trafic pour perturber sa capacité à mener des campagnes de désinformation.

La métaphore du château peut aussi servir à préciser les différences entre les cyberopérations et les opérations de réseau. Nous avons déjà abordé les cyberopérations, mais les opérations de réseau s'entendent des « activités entreprises pour approvisionner, sécuriser, configurer, exploiter, étendre, maintenir et soutenir un réseau ». ¹⁸ Dans le cadre de cette métaphore, il s'agit des activités générales nécessaires au maintien du château : veiller à l'entretien des murs d'enceinte, s'assurer que les ressources, comme la nourriture, l'eau et les armes sont disponibles, que les portes fonctionnent pour permettre les entrées et les sorties, et que des gardes sont présents pour surveiller les murs et l'entrée. Ces fonctions sont analogues à des éléments des opérations de

réseau : pare-feu, listes de contrôle d'accès, disponibilité de la bande passante et présence d'administrateurs réseau pour régler les problèmes. Si les murs du château tombent en ruine, il peut être difficile de savoir si cela est dû à l'action d'un assaillant ou au mauvais entretien des murs. Il en va de même pour les opérations de réseau. Si certains appareils ne sont plus connectés au réseau, cela peut être attribuable à un acteur malveillant qui les a pris pour cible ou au fait que le Centre d'opérations des réseaux n'a pas mis à jour le micrologiciel et qu'un correctif récent a provoqué la déconnexion de ces appareils. Si un réseau est mal entretenu, comme un château, il devient difficile de savoir rapidement si un problème est banal ou malveillant.

Cependant, la métaphore du château comporte des limites générales. Premièrement, elle établit une dangereuse dichotomie entre l'intérieur et l'extérieur. ¹⁹ Tous les réseaux ne sont pas aussi tranchés. Par exemple, de nombreux réseaux comportent des zones démilitarisées, où sont hébergés des biens accessibles à partir de l'Internet, mais qui ne peuvent pas communiquer directement avec les bases de données internes. La zone démilitarisée constitue donc un type de zone intermédiaire qui est protégée par le pare-feu, mais qui n'est pas entièrement interne. Deuxièmement, la métaphore du château suggère que toutes les menaces proviennent de l'extérieur. Tandis que les châteaux ne privilégiaient généralement pas les défenses internes, les réseaux modernes appliquent souvent un contrôle d'accès fondé sur les rôles pour limiter les privilèges, même une fois à l'intérieur du réseau. Toutefois, même avec ces contrôles, les menaces internes (Ortis, Snowden, Reality Winner, Manning, etc.) prouvent que toutes les menaces ne viennent pas de l'extérieur.²⁰

Cybersécurité et cyberdéfense : principales différences

Si vous travaillez depuis peu en cybersécurité au ministère de la Défense nationale, vous aurez peut-être remarqué que l'on emploie parfois indifféremment les termes cybersécurité et cyberdéfense, même s'il s'agit de notions tout à fait distinctes au sein du MDN. Dans l'appareil gouvernemental en général, le terme cybersécurité sert à décrire les processus visant à sécuriser la composante TI du cyberspace. Toutefois, au MDN, on distingue la cybersécurité de la cyberdéfense. Contrairement aux autres ministères, le MDN dispose de technologies de plateforme et doit protéger ces technologies contre l'ennemi dans des contextes opérationnels. La cybersécurité constitue la base nécessaire à toutes les activités de cyberdéfense, ce qui pourrait expliquer en partie pourquoi ces deux termes sont souvent confondus. La cybersécurité englobe les activités qui visent à assurer la santé et le stockage sécuritaire des biens, indépendamment de la présence d'un acteur hostile. La confidentialité, l'intégrité et la disponibilité sont au cœur de ces préoccupations. La confidentialité garantit que l'information demeure privée et accessible uniquement aux personnes autorisées à la consulter; l'intégrité

assure que l'information reste exacte et inchangée; et la disponibilité signifie que les utilisateurs peuvent accéder à l'information dont ils ont besoin, au moment voulu, sans retard ni difficulté.²¹

En pratique, la cybersécurité peut, par exemple, consister à exiger que les utilisateurs emploient des mots de passe pour accéder aux biens ou aux systèmes, à appliquer un contrôle d'accès fondé sur les rôles pour gérer l'accès et les privilèges (confidentialité), à utiliser des sommes de contrôle pour vérifier que le logiciel offert en téléchargement est bien la bonne version (intégrité), à exiger des signatures numériques (intégrité), à prévoir un plan de reprise après sinistre en cas de catastrophe naturelle ou d'urgence (disponibilité) ou à surveiller le rendement du système (disponibilité).

Alors, en quoi la cybersécurité diffère-t-elle de la cyberdéfense? Certes, les pratiques de cybersécurité peuvent contribuer à dissuader un acteur de menace d'accéder aux données, de les modifier ou d'en refuser l'accès. Cependant, la cyberdéfense s'en distingue, car, contrairement à la cybersécurité, elle suppose la présence d'un acteur hostile dans le cyberspace et comporte des efforts visant à détecter, à prévenir et à contrer les menaces dirigées contre le réseau. Une cybermenace ou un acteur de menace est au cœur de cette définition, alors que cette notion est absente de la définition de la cybersécurité.

Même si aucune analogie n'est parfaite (comme l'a montré la métaphore du château plus haut), la différence entre les deux concepts se prête bien à une analogie sur le hockey. La cybersécurité ressemble beaucoup au filet en dehors d'un match de hockey. Plus le cadre du filet est petit, plus il est difficile pour des éléments indésirables (y compris la rondelle) de pénétrer dans la zone de but. Il se peut que le filet reste sur la glace pendant les séances de patinage libre et que de jeunes enfants s'y aventurent par mégarde. On espère alors que le personnel d'entretien de la patinoire sera présent pour s'assurer que le filet demeure intact et qu'il reste en dehors de la zone accessible. Si un patineur trop enthousiaste fonce accidentellement dans le but et déchire le filet, le personnel d'entretien réparera la déchirure pour que le filet puisse remplir sa fonction. Ce même personnel pourra remplacer le cadre s'il se corrode, afin d'en préserver l'intégrité de la structure. Le personnel pourra ensuite retirer le filet de la glace pendant le patinage libre pour qu'il soit disponible pour les parties. Toutes ces pratiques se rapprochent de l'entretien courant en cybersécurité : veiller à ce que le trafic indésirable soit tenu à l'écart du réseau et, si le réseau est endommagé par inadvertance, le réparer et éventuellement l'isoler d'autres incidents susceptibles d'avoir une incidence sur sa disponibilité; il s'agit là de pratiques normales.

À l'inverse, la cyberdéfense s'apparente à un match de hockey. Le filet peut être considéré comme la composante de cybersécurité. Plus la cybersécurité est robuste, plus le « filet » est petit (et plus la surface d'attaque est réduite). Le filet peut être fait d'un meilleur matériau, équipé d'un système d'ouverture automatisé, remplacé et remis à neuf à chaque changement, etc. Tous ces

ajustements rendent plus difficile la réussite de l'équipe adverse. De la même façon, ils évoquent les pratiques de cybersécurité, où les propriétaires de réseaux peuvent ajuster les règles des pare-feu et appliquer régulièrement des correctifs pour réduire la surface d'attaque de leur réseau. Néanmoins, comme au hockey, peu importe la qualité de conception de votre filet (ou de vos pratiques de cybersécurité), si vous n'avez pas de gardien de but, l'adversaire pourra marquer des points facilement. La cyberdéfense revient à ajouter un gardien devant le filet. L'équipe locale place un gardien dans le but pour empêcher la rondelle d'y entrer. Plus l'équipement du gardien est imposant et plus ses réflexes sont rapides, plus il est difficile pour l'autre équipe de marquer. L'entraîneur peut aussi informer le gardien et les joueurs en défense sur les attaquants de l'autre équipe et sur les stratégies ou les jeux qu'ils privilégient. L'équipe locale peut ensuite utiliser ces renseignements pour empêcher l'autre équipe de marquer. De la même manière, en cyberdéfense, les défenseurs du réseau peuvent investir dans des outils de détection de signatures de logiciels malveillants (un nouvel équipement) pour empêcher un acteur de cybermenace de percer le réseau. Ils peuvent aussi recourir à l'analyse heuristique, à des systèmes de détection d'intrusion ou à la connaissance des techniques, tactiques et procédures pour repérer certains acteurs de menace, atténuer la menace ou améliorer les délais d'intervention. Dans cet exemple, l'équipe doit prendre des mesures défensives précises pour se protéger contre l'autre équipe. Cependant, contrairement à un match de hockey, la cyberdéfense et la cybersécurité sont des activités soutenues, menées en tout temps, qui ne prennent jamais vraiment fin. La différence entre les deux notions sera aussi utile pour la section suivante, qui présente le continuum des cyberévénements, des cyberincidents et des compromissions.

Distinguer les cyberévénements des cyberattaques : comprendre l'échelle des activités

Certaines activités ou anomalies dans le cyberspace sont parfois regroupées dans un même « panier » sous l'étiquette de *cyberattaque*. Toutefois, sur le plan technique, il existe des différences. Nous devons distinguer les types d'activités pour pouvoir ajuster l'ampleur des mesures d'intervention. Par exemple, si vous venez d'arriver dans une équipe et que vous recevez un courriel d'hameçonnage (auquel vous ne répondez pas) et que vous affirmez qu'il y a eu une cyberattaque, cette qualification est erronée et amplifie indûment l'incident. Le gouvernement canadien utilise les définitions énoncées dans le *Plan de gestion des événements de cybersécurité du gouvernement du Canada* pour distinguer les différents types d'activités.²² La principale différence entre les catégories tient au degré de gravité et au niveau de certitude quant à la compromission.

À l'extrémité la moins grave de l'échelle, on trouve l'événement de sécurité, c'est-à-dire tout événement qui *peut* avoir entraîné

une compromission.^{23,24} Parmi les exemples d'événements de sécurité, mentionnons un courriel d'hameçonnage ciblé sur lequel la cible n'a pas cliqué ou des requêtes inhabituelles bloquées par un pare-feu. Même si certains de ces événements peuvent être malveillants, il est essentiel de reconnaître qu'un événement n'est pas la même chose qu'une compromission. Si une organisation traite chaque événement comme une atteinte à la sécurité, elle sera submergée par le nombre d'alertes, ce qui mènera à une lassitude face aux alertes et étirera les ressources déjà limitées.

Un événement de sécurité peut devenir un *incident de sécurité* lorsqu'il y a atteinte à la sécurité et que le système est compromis.²⁵ Par exemple, si un acteur de cybermenace envoie un courriel de harponnage à un employé et que l'employé clique sur un lien malveillant incorporé au courriel ou ouvre une pièce jointe infectée et télécharge un logiciel malveillant, l'événement de sécurité (le courriel) devient un incident de sécurité (téléchargement réussi du logiciel malveillant). L'événement devient un incident dès que le réseau est compromis.

Conclusion

Nous avons rédigé le présent article à l'intention des personnes qui se joignent à la communauté de la cybersécurité du gouvernement du Canada, dans l'espoir de les aider à reconnaître les idées fausses courantes auxquelles elles pourraient être confrontées. Après avoir lu cet article, nous estimons que tous

les lecteurs devraient posséder les mêmes connaissances de base. Les lecteurs devraient comprendre que le cyberspace est un objet physique, aussi banal et peu enthousiasmant que cela puisse paraître à certains. Le cyberdomaine correspond au cyberspace et à tout ce qui l'entoure. Il s'agit également de l'un des cinq domaines reconnus de la guerre que les FAC s'emploient activement à opérationnaliser.

Cet article ne cherche-t-il qu'à couper les cheveux en quatre? Pourquoi consacrer un article entier à des définitions que l'on retrouve déjà dans un enchevêtrement de notes de doctrine interarmées, de documents politiques, d'annexes, de glossaires et de présentations? Pourquoi est-il important de dire *cyberopération* plutôt qu'*opération d'information* si la plupart des gens comprennent de toute façon ce que l'on veut dire? En réalité, les FAC et le MDN se trouvent dans une situation particulière. Contrairement aux États-Unis, à la Chine et à la Russie, les FAC et le MDN sont en train de bâtir les assises de cybercapacités militaires essentielles. À mesure que le COMCYBERFAC sera pleinement opérationnel et que plusieurs équipes interagiront avec cette capacité, il sera important que tous parlent le même langage et emploient les termes avec justesse, afin d'éviter la confusion et les malentendus. Nous espérons que les explications simplifiées présentées ici auront permis de mieux comprendre la façon dont le cyberdomaine est structuré, ses liens avec les autres domaines et les raisons pour lesquelles il est peut-être plus simple à appréhender que ne le croient certains.

Notes

- Gouvernement du Canada, « Cyberopérateur : Nouvel insigne de métier des Forces armées canadiennes », La Feuille d'érable, 11 janvier 2022, source originale : <https://www.canada.ca/fr/ministere-defense-nationale/feuille-derable/defense/2022/01/cyberopérateur-nouvel-insigne-metier-forces-armees-canadiennes.html>.
- Gouvernement du Canada, « Félicitations aux premiers cyberopérateurs diplômés de l'EECF », La Feuille d'érable, 21 septembre 2021, source originale : <https://www.canada.ca/fr/ministere-defense-nationale/feuille-derable/defense/2021/09/felicitations-premiers-cyberopérateurs-diplomés-eeccf.html>.
- Gouvernement du Canada, « Mars 2020 - Forces armées canadiennes 101 », Défense 101 - cahier de transition mars 2020, s.d., 2, source originale : <https://www.canada.ca/fr/ministere-defense-nationale/organisation/rapports-publications/transition-ministerielle/defense-101/2020/03/defense-101/fac-101.html>.
- Gouvernement du Canada, « Cyberopérateur : Nouvel insigne de métier des Forces armées canadiennes ».
- Statistique Canada, « Protéger nos foyers et nos droits : servir dans les Forces armées canadiennes », (Gouvernement du Canada, 13 juillet 2022), source originale : <https://www150.statcan.gc.ca/n1/daily-quotidien/220713/dq220713c-fra.htm>.
- Gouvernement du Canada, « Cyber Mission Assurance », dans Banque de terminologie de la défense, s.d., source originale : https://www.btb.termiumplus.gc.ca/tpv2alpha/alpha-fra.html?lang=fra&i=1&srchtxt=cyber%20mission%20assurance&context2nd_wet=1&index=alt.
- Bruce Schneier, « Security and Cheap Complexity », Schneier on Security, blogue, 26 août 2022, source originale : <https://www.schneier.com/blog/archives/2022/08/security-and-cheap-complexity.html>.
- « Heightened DDoS Threat Posed by Mirai and Other Botnets », CISA, s.d., source originale : <https://www.cisa.gov/news-events/alerts/2016/10/14/heightened-ddos-threat-posed-mirai-and-other-botnets>.
- Scott J. Shackelford et Scott O. Bradner, « Have You Updated Your Toaster? Transatlantic Approaches to Governing the Internet of Everything », Hastings Law Journal 72, no 2 (2021), source originale : https://repository.uchastings.edu/cgi/viewcontent.cgi?article=3921&context=hastings_law_journal.
- Gouvernement du Canada, « Information Environment », dans Banque de terminologie de la défense, s.d., source originale : [dtb.termiology.mil.ca](https://www.dtb.termiology.mil.ca).
- « Glossary », dans Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press, 2013, 282.
- Gouvernement du Canada, « Information Operation », TERMIUM Plus, s.d.
- Gouvernement du Canada, « Cyber Operation », TERMIUM Plus, s.d.
- « Glossary », op.cit.
- Deborah A. Frincke et Matt Bishop, « Guarding the Castle Keep: Teaching with the Fortress Metaphor », IEEE Security & Privacy 2, no 3 (2004) : 69-72.
- Gouvernement du Canada, « Defensive Cyber Operation - Response Action », TERMIUM Plus, s.d.
- Gouvernement du Canada, « Offensive Cyber Operation », TERMIUM Plus, s.d.
- Gouvernement du Canada, « Network Operations », dans Banque de terminologie de la défense, s.d.
- Christian Leuprecht, David B. Skillicorn et Victoria E. Tait, « Beyond the Castle Model of Cyber-Risk and Cyber-Security », Government Information Quarterly 33, no 2 (s.d.) : 250-257.
- Christian Leuprecht et al., op.cit.
- National Institute of Standards and Technology, « NIST Special Publication 1800-26A », National Cybersecurity Center of Excellence, 2020, source originale : <https://www.nccoe.nist.gov/publication/1800-26/VolA/index.html>.
- Gouvernement du Canada, « Plan de gestion des événements de cybersécurité du gouvernement du Canada (PGEC GC) », 2019, source originale : <https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/securite-confidentialite-ligne/orientations-politiques-matiere-cybersecurite/gestion-incidents-securite/plan-gestion-evenements-cybersecurite-gouvernement-canada.html>.
- Gouvernement du Canada.
- National Institute of Standards and Technology, « Cadre pour l'amélioration de la cybersécurité des infrastructures critiques », NIST, s.d., source originale : <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018fr.pdf>.
- National Institute of Standards and Technology.



Le 435^e Escadron de transport et de sauvetage procède à l'évacuation de résidents de Norway House, au Manitoba, pendant les feux de forêt, au cours de l'opération LENTUS, dans le nord du Manitoba, le 30 mai 2025.

Aviateur Nicholas Zahari, Service d'imagerie du 17^e Escadron de soutien aux opérations, Winnipeg

Le lien entre le renseignement d'origine électromagnétique et le cyberdomaine au sein des Forces armées canadiennes

LIEUTENANTE-COLONELLE L. J. REDIGER

La lieutenant-colonelle (Lcol) Leslie Rediger a intégré les Forces armées canadiennes en 2001 à titre d'officière du génie électronique et des communications. Elle a obtenu, en 2006, un baccalauréat en génie mécanique du Collège militaire royal du Canada. Au cours des 15 premières années de sa carrière, elle a appuyé les opérations aériennes en qualité d'officière des systèmes de communications et d'information au sein de différentes escadres de l'Aviation royale canadienne et au Quartier général de la 1^{re} Division aérienne du Canada. Elle a été déployée à plusieurs reprises à l'appui des opérations ATHENA et REASSURANCE. En 2016, la Lcol Rediger est passée aux opérations de renseignement d'origine électromagnétique (SIGINT). Elle a alors occupé les fonctions de commandante de l'Escadron de soutien et de commandante adjointe à la Station des Forces canadiennes Leitrim, ainsi que celles de chef d'état-major du SIGINT au Quartier général du Groupe des opérations d'information des Forces canadiennes. Promue à son grade actuel en 2020, elle a commandé la Station des Forces canadiennes Leitrim, de juin 2023 à octobre 2025. À l'heure actuelle, elle est officière de liaison du COMCYBERFAC, au Royaume-Uni. La Lcol Rediger détient une maîtrise ès arts en leadership de l'Université Royal Roads ainsi qu'une maîtrise en études de la défense du Collège des Forces canadiennes.

Protection, Sécurité, Engagement : La politique de défense du Canada, publiée en 2017, présente « l'évolution rapide de la technologie » comme l'un des principaux facteurs de transformation du contexte de sécurité mondial, qui modifie la nature des conflits.¹ Elle souligne également que l'utilisation du cyberspace et des technologies émergentes par les Forces armées canadiennes (FAC) « apporte de nombreux avantages opérationnels, mais engendre aussi des vulnérabilités critiques ».² Ainsi, pour demeurer concurrentielles et défendre les intérêts du Canada, les FAC doivent être en mesure de protéger leurs biens, préserver leur liberté de manœuvre dans le cyberspace et être en mesure de tirer parti de ce contexte opérationnel, tout en étant prêtes à le faire, afin d'exécuter le mandat qui leur est confié.³

Pour « maximiser l'efficacité du Canada dans le cyberspace » dans *Notre Nord, fort et libre : Une vision renouvelée pour la défense du Canada*, le gouvernement du Canada a ordonné aux FAC de créer le Cybercommandement des Forces armées canadiennes (COMCYBERFAC).⁴ Ce nouveau commandement vise à « améliorer la capacité des Forces armées canadiennes à mener des cyberopérations » et « seront ainsi capables de mettre sur pied et d'employer des cyberforces ainsi que d'autres capacités spécialisées sur court préavis, et de contribuer à la promotion des intérêts canadiens ainsi qu'à la protection de l'armée canadienne et des forces alliées et partenaires sur le territoire national et à l'étranger ».⁵

Le COMCYBERFAC a été créé le 26 septembre 2024. Le Groupe des opérations d'information des FAC a alors été élevé du statut de formation de niveau 3 à celui de commandement. Soutenu sur le plan administratif par le Groupe des services numériques, il relève directement du chef d'état-major de la défense.⁶ À titre d'autorité de la défense en matière de cyberopérations, il est chargé de l'emploi, de la mise sur pied, du maintien, de la gestion et du développement des cyberforces qui lui sont attribuées, y compris le renseignement d'origine électromagnétique (SIGINT) et la guerre électronique interarmées.⁷

Quoique ce soit relativement bien connu dans la communauté de la défense que le Centre de la sécurité des télécommunications Canada (CST) est l'organisme du gouvernement du Canada chargé du SIGINT étranger,⁸ on sait moins que les FAC disposent de leur propre unité intégrée de SIGINT. Depuis près de 85 ans, la Station des Forces canadiennes Leitrim mène des opérations de SIGINT pour défendre le Canada.⁹ À première vue, l'intégration de l'organisation de SIGINT des FAC au nouveau commandement des cyberopérations peut sembler inhabituelle, puisqu'il s'agit d'une fonction du renseignement et que les FAC disposaient déjà d'un commandement du renseignement. Toutefois, le SIGINT entretient des liens particulièrement étroits avec les cyberopérations. Ces liens ne cessent de se renforcer et de gagner en importance dans le monde interconnecté et riche en technologies au sein duquel les FAC mènent leurs opérations. Le SIGINT et le cyberdomaine sont les deux faces d'une même médaille : malgré leurs objectifs, leurs pouvoirs et leurs capacités distincts, ils sont indissociables et se

renforcent mutuellement. Le présent article propose une introduction à la relation entre le SIGINT et les cyberopérations dans un contexte militaire. Il vise à illustrer leurs interdépendances et leur caractère complémentaire au sein du nouveau COMCYBERFAC.

Lexique

Pour amorcer cette réflexion, il importe d'abord de définir la terminologie. Les progrès technologiques dans le domaine des renseignements devancent souvent l'évolution de la doctrine. Ainsi, il n'existe aucune définition universellement reconnue de termes comme « cyberspace », « cyberopérations » ou « cyberdomaine ». L'OTAN, les alliés et les partenaires les interprètent de manière quelque peu différente et les emploient souvent de manière interchangeable. Aux fins de la présente discussion, pour garantir la cohérence terminologique, le présent article s'appuie sur la *Banque de la terminologie de la défense* (BTD) du ministère de la Défense nationale.

Le cyberspace et le cyberdomaine

Le terme « cyberspace » désigne l'« environnement physique comprenant toutes les ressources qui traitent, stockent ou communiquent des données numériques ».¹⁰ Contrairement aux autres milieux opérationnels au sein desquels les FAC mènent leurs activités, la terre, la mer, l'air et l'espace, le cyberspace est « omniprésent dans tous les autres environnements ».¹¹ Le cyberdomaine est une notion plus vaste qui intègre non seulement le cyberspace, mais également l'infrastructure qui l'appuie et le rend possible, de même que ses utilisateurs et les activités connexes.¹²

Le cyberspace comprend la couche des cyberpersonnages, qui intègre les profils en ligne et les autres moyens par lesquels les personnes et les objets sont représentés en ligne, tandis que le cyberdomaine s'étend aux humains qui interagissent réellement avec le cyberspace. De même, le cyberspace comprend la couche physique, notamment l'ensemble du matériel informatique, des téléphones, des capteurs et des dispositifs de stockage de données. Le cyberdomaine intègre cette couche ainsi que la couche géographique, qui représente les emplacements physiques où se trouvent les dispositifs du réseau et leur environnement immédiat.¹³

Cyberopérations

Le terme « cyberopération » ou cyberop désigne un vaste éventail d'activités, menées dans le cyberspace afin d'atteindre des objectifs stratégiques et tactiques. Ces activités se divisent en cyberopérations défensives et offensives. Les cyberops défensives visent à préserver et à assurer la liberté d'action dans le cyberspace,¹⁴ notamment en défendant les réseaux et les données contre les adversaires. Les cyberops offensives, en revanche, visent à projeter la puissance dans le cyberspace

afin de produire des effets précis.¹⁵ Elles ont pour objet de perturber, de dégrader ou de détruire la liberté de mouvement de l'adversaire dans le cyberspace, ou encore d'avoir d'autres répercussions, par l'intermédiaire du cyberspace, sur ses activités ou ses capacités.

La dépendance croissante des acteurs étatiques et non étatiques à l'égard du cyberspace, de ses systèmes informatiques intégrés et de ses capteurs a exigé un accroissement proportionnel des capacités en matière de cyberopérations des FAC. Il est essentiel que les FAC puissent défendre leur territoire dans le cyberspace et tirer parti de ce milieu pour atteindre leurs adversaires et agir contre eux. *Protection, Sécurité, Engagement : La politique de défense du Canada* établit comme attente que les cyberforces des FAC soient en mesure « de cibler, d'exploiter, d'influencer et d'attaquer [dans le cyberspace] à l'appui des opérations militaires »,¹⁶ en s'appuyant sur des plateformes émergentes dans les milieux terrestre, maritime, aérien et spatial afin d'intégrer les systèmes de capteurs.¹⁷ La politique de défense souligne également la nécessité d'empêcher l'adversaire d'avoir une incidence sur les capacités C4ISR des FAC (commandement, contrôle, communications, informatique, renseignement, surveillance et reconnaissance), lesquelles sont indispensables à la conduite des opérations des FAC à l'échelle mondiale.¹⁸

Renseignement d'origine électromagnétique

Le terme « renseignement d'origine électromagnétique » intègre tant la discipline du renseignement elle-même que les activités de collecte de renseignements menées dans le cyberspace et dans d'autres parties du spectre électromagnétique, ainsi que les produits qui alimentent le système de renseignement dans son ensemble.¹⁹ Essentiellement, le SIGINT consiste à intercepter, recueillir, décrypter, traduire et analyser des signaux de communication ou des signaux autres que des signaux de communication, puis à produire des rapports qui contribuent au processus général de collecte du renseignement.²⁰ Compte tenu du caractère délicat de ces activités, les processus, les capacités et les produits exigent des mesures particulières de protection et de traitement; ainsi, ils ne peuvent faire l'objet de discussions publiques.²¹

Le SIGINT se divise en trois sous-catégories : le renseignement sur les communications (COMINT), le renseignement électronique (ELINT) et le renseignement tiré de signaux d'instrumentation étrangers (FISINT). Le COMINT est constitué de renseignements recueillis par l'interception de communications électromagnétiques, vocales ou textuelles par exemple, autrement que par leur destinataire prévu.²² L'ELINT est axé sur les émissions électromagnétiques autres que les communications, notamment celles des systèmes radars.²³ Ces émissions peuvent révéler des renseignements sur leur source, notamment la fréquence utilisée, la fréquence de répétition et la direction d'arrivée, entre autres caractéristiques.²⁴ Enfin, le FISINT, domaine plus spécialisé, désigne le « renseignement technique tiré de

l'interception d'émissions électromagnétiques d'origine étrangère associées à l'essai et à l'utilisation de systèmes aérospatiaux, de surface et sous-marins ». ²⁵ Il sert notamment à recueillir des renseignements sur les émissions et les données provenant de systèmes de missiles et de systèmes de contrôle.²⁶ Ensemble, ces trois sous-catégories fournissent les renseignements essentiels à l'atteinte des objectifs de défense nationale et continentale ainsi qu'à l'orientation des opérations de sécurité nationale, de la politique étrangère et de la cybersécurité.²⁷

Le SIGINT a un long historique de clandestinité. Étroitement protégé par les personnes chargées de l'exécuter, il appuie dans l'ombre les opérations des FAC depuis la Seconde Guerre mondiale.²⁸ Pierre angulaire des opérations militaires, le SIGINT permet de mieux comprendre les intentions, les capacités et les activités de l'adversaire. Il appuie ainsi la prise de décisions stratégiques, la défense du continent et la connaissance de la situation des forces déployées à l'échelle mondiale.²⁹

À l'instar des cyberopérations, le SIGINT a pris une importance accrue au sein des opérations des FAC dans le contexte de la guerre moderne, où les progrès technologiques ont transformé le champ de bataille, la stratégie militaire et les activités de collecte du renseignement. L'environnement d'information, de plus en plus interconnecté, crée des vulnérabilités. Il permet à l'entreprise de SIGINT d'accéder aux communications, aux capteurs et aux systèmes d'armes de l'adversaire afin de produire des renseignements essentiels sur ses capacités et ses intentions. L'utilisation considérablement accrue des systèmes des technologies de l'information, des capteurs intégrés et des systèmes de commandement et contrôle a renforcé l'importance du SIGINT pour la défense des biens des FAC et l'exploitation des vulnérabilités de l'adversaire. Elle ouvre ainsi la voie à des cyberactivités défensives et offensives actives qui exploitent ces mêmes vulnérabilités.

Le lien entre le SIGINT et le cyberdomaine

Les opérations de SIGINT tirent parti du cyberspace et des technologies qui y sont intégrées pour exploiter la dépendance de l'adversaire à l'égard des communications numériques, des appareils interconnectés et de l'emploi généralisé de capteurs. Elles permettent ainsi de produire du renseignement dans tous les milieux opérationnels, y compris le cyberspace. Le renseignement issu de ces processus appuie les opérations des FAC à tous les égards, tant sur le plan tactique que sur le plan stratégique. L'interception des communications et des données provenant des capteurs de l'adversaire fournit, en temps réel, du renseignement sur ses positions et ses mouvements dans tous les milieux (aérien, terrestre, maritime, spatial et cyberspatial), ce qui éclaire les évaluations de la menace et les cycles de ciblage des décideurs. Sur le plan stratégique, elle façonne la connaissance de la situation en révélant les intentions, les capacités et les menaces émergentes de l'adversaire.³⁰

Quoique le SIGINT et les cyberopérations reposent tous deux sur des technologies numériques et s'exercent dans le cyberdomaine, leur portée, leurs méthodes et leurs objectifs diffèrent. Le SIGINT est principalement axé sur la collecte passive de renseignements et l'analyse de transmissions, tandis que les cyberopérations peuvent être passives ou actives. Les cyberopérations défensives visent à protéger les systèmes informatiques et les systèmes de communication contre les intrusions, à garantir leur protection proactive et à intervenir en cas d'attaque. Les cyberopérations offensives, quant à elles, cherchent à pénétrer, à manipuler et à exploiter les systèmes de l'adversaire. La conduite de cyberopérations exige toutefois une compréhension approfondie des auteurs de la menace, de l'infrastructure numérique et de ses vulnérabilités éventuelles. Le SIGINT peut appuyer ces activités en fournissant le renseignement requis pour identifier les cibles et évaluer les menaces.

Cyberopérations appuyées par le SIGINT

Qu'elles soient défensives ou offensives, les cyberopérations reposent largement sur un renseignement exact et obtenu en temps opportun. Le SIGINT constitue un élément fondamental de l'appui aux cyberopérations : l'interception et l'analyse de signaux de communication et d'autres transmissions permettent de cerner les vulnérabilités des systèmes, de détecter des tendances dans les cyberactivités et de mieux comprendre les auteurs de la menace. Les cyberopérateurs des FAC doivent être en mesure de comprendre la topologie des réseaux ciblés, notamment l'interconnexion des systèmes, les protocoles employés ainsi que l'emplacement et la nature des vulnérabilités au sein de ces réseaux.³¹

Dans le cadre des cyberopérations défensives, le SIGINT peut révéler la structure et le comportement de l'environnement numérique, de même que les intentions et les capacités des adversaires et d'autres auteurs de la cybermenace. Par ailleurs, il peut contribuer au renseignement sur les menaces, en repérant des indicateurs de compromission, ce qui permet aux FAC de renforcer la sécurité des systèmes, de déployer des contre-mesures et d'intervenir en cas d'intrusion. Dans le cadre des cyberopérations offensives, le SIGINT peut éclairer le choix des cibles, le moment d'intervention et les tactiques à employer afin que les cyberactions soient précises et efficaces.

Le SIGINT peut également faciliter l'attribution, c'est-à-dire le processus qui consiste à déterminer l'auteur d'une cyberattaque. L'attribution repose sur la corrélation entre les communications interceptées et les comportements connus des auteurs de la menace. Cette fonction revêt une importance particulière dans le contexte actuel des menaces, où les acteurs étatiques et non étatiques utilisent des méthodes perfectionnées pour dissimuler leur identité.

Le SIGINT est essentiel à la cartographie de la topologie des réseaux et à la compréhension des cybermenaces. Son rôle dans le cadre des cyberopérations va au-delà de l'interception,

car il permet une analyse approfondie qui éclaire la planification stratégique et renforce la connaissance de la situation des décideurs. Pour les FAC, ce lien est mis en évidence par le regroupement des unités de SIGINT et des cyberunités au sein d'un même commandement. La création du COMCYBERFAC favorise une meilleure communication et une coopération accrue entre ces capacités essentielles sur le plan stratégique.

Soutien des cyberopérations au SIGINT

L'évolution initiale du SIGINT au Canada reposait sur deux objectifs principaux : tirer parti de sa situation géographique particulière pour assurer la défense souveraine du pays, et utiliser cette même situation géographique, de concert avec des initiatives nationales de collecte, afin de participer au partenariat de renseignement du Groupe des cinq avec les États-Unis, le Royaume-Uni, l'Australie et la Nouvelle-Zélande, tout en tirant parti de ce partenariat.³² Ces impératifs existent encore à l'heure actuelle. Le SIGINT est une activité fondamentalement collective, car l'omniprésence des systèmes d'information, des capteurs et des émetteurs rend presque impossible le traitement du déluge de données numériques provenant de toutes ces sources. Repérer, décrypter, analyser et communiquer les renseignements pertinents afin de répondre aux besoins en renseignement et d'appuyer les opérations des FAC représente un défi considérable. La mise en commun de ce fardeau avec des pays partenaires qui partagent les mêmes intérêts accroît le volume de données pouvant être traitées et exploitées. Sans la collaboration des alliés du Canada, ce défi serait vraisemblablement insurmontable, particulièrement lorsque les opérations se déroulent dans le cyberspace. La superficie du Canada et sa proximité avec des pays adverses lui procurent un avantage géographique. Le pays peut ainsi offrir des apports particuliers, accroître sa pertinence dans ce domaine, faciliter l'accès au renseignement de ses partenaires et tirer pleinement parti des capacités du Groupe des cinq afin d'appuyer les opérations des FAC à l'échelle mondiale.³³ Dans un environnement numérique en constante évolution, ce partenariat est plus que jamais essentiel. En investissant à la fois dans des infrastructures souveraines de SIGINT et dans des infrastructures intégrées, le Canada veille à ce que ses apports ne soient pas seulement complémentaires, mais qu'ils fournissent également des renseignements distincts et utiles aux opérations des FAC et du Groupe des cinq. Ces capacités souveraines permettent au Canada d'aligner ses opérations sur les priorités en matière de sécurité nationale, ce qui renforce la pertinence et l'incidence de son renseignement. Leur caractère intégré permet également au Canada de renforcer la défense collective et la mise en commun de renseignements au sein de l'alliance.

Les opérations de SIGINT dépendent fortement d'infrastructures de réseau sécurisées, des télécommunications et des communications radioélectriques, des flux de données provenant de capteurs, de fonctions informatiques complexes, de

l'automatisation, de l'analyse de données et, surtout, de l'intégration et de la communication avec les partenaires et les alliés. Comme cette infrastructure est répartie à l'échelle du pays et du monde, cela pose un défi technique et de sécurité considérable et durable. Toutes ces activités tirent parti du cyberspace et aucune ne serait possible sans l'appui des cyberopérations. Les cyberopérations de l'adversaire constituent une menace importante pour les opérations des FAC, y compris le SIGINT, notamment en refusant ou en manipulant l'information, en menant une collecte rapide ou soutenue, ou en exécutant des activités de tromperie.³⁴

Ce sont les cyberopérations défensives qui garantissent aux opérations de SIGINT la liberté de manœuvre dans le cyberspace, tout en protégeant les biens, les systèmes et les installations essentiels à la recherche, à la détection, à l'analyse et à la diffusion du SIGINT. Par ailleurs, le SIGINT et les cyberopérations offensives concourent à repérer les points d'accès et à comprendre le terrain dans le cyberspace, ce qui permet de recueillir du renseignement et de produire des effets. Ce lien essentiel entre les cyberopérations et le SIGINT garantit l'efficacité et la pérennité de ces deux capacités.

Conclusion

La création du COMCYBERFAC témoigne de la reconnaissance délibérée, par le gouvernement du Canada et les FAC, que le

cyberspace est un milieu opérationnel contesté au sein duquel les FAC doivent pouvoir manœuvrer, défendre leurs positions et produire des effets. Dans ce contexte, l'intégration des capacités de SIGINT et des cybercapacités au sein d'un même commandement constitue une réponse logique aux réalités des conflits modernes. Comme le démontre le présent article, le SIGINT et les cyberopérations sont étroitement interdépendants. Le SIGINT fournit le fondement de renseignement nécessaire à la conduite efficace des cyberopérations défensives et offensives, tandis que les cybercapacités protègent, facilitent et amplifient la collecte et l'analyse du SIGINT. Ensemble, ces deux éléments forment un cycle de renforcement mutuel qui améliore la connaissance de la situation, appuie la prise de décisions, préserve la liberté d'action des FAC dans tous les milieux et facilite la projection de la puissance militaire au moyen du cyberspace.

À mesure que les menaces gagnent en ampleur, en perfectionnement et en rapidité, l'importance de cette relation entre le SIGINT et les cyberopérations ne peut que croître. Le regroupement, au sein du COMCYBERFAC, de l'expertise, des pouvoirs et des capacités permet aux FAC de mieux intégrer le renseignement d'origine électromagnétique et les cyberopérations, de renforcer leurs partenariats avec les alliés et d'intervenir avec détermination dans le cyberdomaine omniprésent. En fin de compte, l'efficacité des cyberforces des FAC ne reposera pas sur la puissance de capacités isolées, mais sur la puissance de la collaboration, de l'intégration et de l'innovation.

Notes

- Gouvernement du Canada, *Protection, Sécurité, Engagement : La politique de défense du Canada* (Ottawa : ministère de la Défense nationale, 2017), 14.
- Ibid.*, 72.
- Gouvernement du Canada, Joint Doctrinal Note (JDN): Cyber Operations 2017-02 2-0, Ottawa : ministère de la Défense nationale, 2017, 1-1.
- Gouvernement du Canada, *Notre Nord, fort et libre : Une vision renouvelée pour la défense du Canada*, Ottawa : ministère de la Défense nationale, 2024, 26.
- Ibid.*, 26.
- Forces armées canadiennes, Military Organization Order 2025001-2025006, 14 juillet 2025.
- Ministère de la Défense nationale, « Message de la SM et de la CEMD : Une nouvelle ère pour le domaine cybernétique : Lancement du Commandement Cyber des Forces armées canadiennes », La Feuille d'érable, 26 septembre 2024. Tiré de <https://www.canada.ca/fr/ministere-defense-nationale/feuille-derable/defense/2024/09/nouvelle-ere-domaine-cybernetique-lancement-commandement-cyber-forces-armees-canadiennes.html>.
- Centre de la sécurité des télécommunications, « Mandat », Gouvernement du Canada, dernière modification le 7 avril 2021. Tiré de <https://www.cse-cst.gc.ca/fr/renseignements-organisationnels/mandat>.
- George T. Fraser et Robert Lynn Wortmann, *History of Canadian Signals Intelligence & Direction Finding*, publié à compte d'auteur, 2005.
- « Cyberspace », Banque de la terminologie de la défense, fiche 694338, consulté le 6 février 2026.
- Canada, JDN: Cyber Operations, 2-1.
- « Cyber Domain », Banque de terminologie de la défense, fiche 694360, consulté le 6 février 2026.
- Canada, JDN: Cyber Operations, 2-3-2.4.
- « DCO », Banque de terminologie de la défense, fiche 693742, consulté le 18 septembre 2025.
- « OCO », Banque de terminologie de la défense, fiche 693752, consulté le 18 septembre 2025.
- Canada, *Protection, Sécurité, Engagement*, 65.
- Ibid.*, 39, 109.
- Ibid.*, 56.
- Gouvernement du Canada, CAF SIGINT Primer, ministère de la Défense nationale, avril 2021, 1.
- Gouvernement du Canada, B-GJ-005-200/FP-001, PIFC 2-0, Le renseignement, Ottawa : ministère de la Défense nationale, 2011, 1-16.
- Gouvernement du Canada, CAF SIGINT Primer, 1.
- Gouvernement du Canada, « COMINT », Banque de la terminologie de la défense, fiche 3843, consulté le 18 septembre 2025.
- « ELINT », Banque de la terminologie de la défense, fiche 507, consulté le 18 septembre 2025.
- Canada, CAF SIGINT Primer, 21.
- « FISINT », Banque de terminologie de la défense, fiche 695891, consulté le 18 septembre 2025.
- Gouvernement du Canada, CAF SIGINT Primer, 21.
- Gouvernement du Canada, B-GJ-005-200/FP-001, PIFC 2-0, Le renseignement, 1-4.
- George T. Fraser et Robert Lynn Wortmann, op.cit.
- Gouvernement du Canada, Centre de la sécurité des télécommunications, « Renseignement étranger », dernière modification le 6 avril 2023. Tiré de <https://www.cse-cst.gc.ca/fr/mission/renseignement-etrange>.
- Centre de la sécurité des télécommunications, « Renseignement étranger ».
- Gouvernement du Canada, JDN: Cyber Operations, 5-14.
- Wesley Wark, « Favourable Geography: Canada's Arctic Signals Intelligence Mission », *Intelligence and National Security* 35, no 3 (2020) : 319-330, DOI : 10.1080/02684527.2020.1724629.
- Maria A. Robson, « The Third Eye: Canada's Development of Autonomous Signals Intelligence to Contribute to Five Eyes Intelligence Sharing », *Intelligence and National Security* 35, no 7 (2020) : 954-969, DOI : 10.1080/02684527.2020.1768477.
- Gouvernement du Canada, JDN: Cyber Operations, 1-1.



Un soldat de Caméra de combat des Forces canadiennes, filme les mouvements du Système non classifié de connaissance de la situation par télédétection (URSA), à Manama, Bahreïn, le 26 janvier 2017.

Caporal-chef Mathieu Gaudreault, Caméra de combat des Forces canadiennes IS04-2017-0001-004

Forger l'avenir : un écosystème intégré d'intelligence artificielle de défense au Canada

LIDIA KORCZYNSKA

Lidia Korczynska est directrice du Centre d'IA du MDN et des FAC ainsi que directrice – Politique sur les données et gouvernance. Elle a auparavant travaillé aux Affaires du Parlement et réglementaires à l'Agence des services frontaliers du Canada.

Le ministère de la Défense nationale (MDN) et les Forces armées canadiennes (FAC) entrent dans une phase déterminante de leur parcours vers l'opérationnalisation de l'intelligence artificielle (IA). L'IA transforme tous les aspects de nos vies et se trouve au cœur de la défense moderne. Elle sous-tend des plateformes comme le F-35 et le destroyer de classe *River*, en plus d'être essentielle dans la cyberguerre, la désinformation et les armes autonomes. L'IA offre aussi une occasion unique de transformer la défense, mais seulement si nous sommes prêts à saisir ce moment. Or, toute occasion comporte sa part de risque, et le plus grand risque que nous pourrions prendre serait de maintenir le statu quo.

Pour suivre le rythme de ses alliés et de ses adversaires, le Canada doit transformer l'IA de défense et passer d'une expérimentation fragmentée à une capacité intégrée et prête pour la mission. Dans cette optique, nous alignerons les talents, les infrastructures de données, l'approvisionnement et les partenariats partout à la défense afin d'être habilités par l'IA d'ici 2030. Pour y parvenir, nous traçons une voie pratique à suivre : chaque N1 demeure responsable de ses systèmes d'IA, tandis que le Centre d'IA établit des garde-fous organisationnels clairs, des fondations communes en matière de données et de calcul, ainsi que des voies d'approvisionnement permettant la mise en œuvre rapide de projets pilotes et leur expansion. Nous maintenons également l'engagement avec l'industrie, le milieu universitaire et les alliés pour accélérer la prestation, renforcer les options de cas d'utilisation et garantir que nos investissements contribuent aux résultats de l'OTAN.

Intelligence artificielle et rendement du capital investi

Un rapport récemment publié par le *Massachusetts Institute of Technology* (MIT) souligne que 95 % des projets pilotes en IA générative échouent en raison d'une mauvaise intégration et de développements internes inadéquats.¹ Pour le domaine de la défense, l'IA représente une occasion de surmonter certaines dettes techniques, mais seulement si l'Équipe de la Défense accepte d'effectuer le travail difficile là où cela compte. Briser les anciens silos et favoriser la transparence et la collaboration ne sont pas seulement de bonnes pratiques de leadership : ce sont, selon moi, des facteurs qui détermineront la réussite ou l'échec de nos efforts de transformation numérique. Nous devons être prêts à effectuer le travail exigeant de recenser les règles opérationnelles trop lourdes ou obsolètes, et avoir le courage de collaborer et l'humilité de reconnaître que personne ne peut réussir seul.

Une transformation à l'échelle de l'organisation, qui prend des années, doit aussi être découpée en projets pilotes et sprints plus courts, car la technologie évolue rapidement et la mise en œuvre de nouvelles capacités numériques peut révéler d'autres lacunes. Le MDN et les FAC peuvent mettre en œuvre le changement plus efficacement en concevant des capacités d'IA organisationnelle qui commencent modestement, mais qui sont conçues pour grandir à l'échelle de l'organisation. Cette approche permet à l'Équipe de la Défense de tirer rapidement des leçons des projets pilotes, de faire évoluer les solutions réussies et de s'adapter continuellement aux exigences opérationnelles et commerciales en évolution. Dans le même esprit, nous devons cesser de voir les capacités numériques comme de simples facilitateurs et plutôt les positionner comme le noyau des opérations, soutenues par la force motrice du capital humain. L'Équipe de la Défense peut concevoir cette approche délibérée et mesurée de l'innovation

grâce à la *Stratégie industrielle de la Défense* et d'autres cadres collaboratifs.

La vision d'un MDN et de FAC habilités par l'intelligence artificielle

La *Stratégie d'IA du MDN et des FAC*² engage l'Équipe de la Défense à devenir une organisation habilitée par l'IA d'ici 2030, en utilisant une IA responsable de manière à renforcer les résultats opérationnels et à moderniser les fonctions ministérielles tout en maintenant la confiance. Elle met l'accent sur l'application pratique plutôt que sur l'expérimentation pour faire en sorte que les solutions d'IA soient développées avec et pour le personnel de la défense, et ainsi répondre aux véritables besoins opérationnels et de la mission. Cette vision souligne l'engagement du MDN et des FAC envers l'interopérabilité avec les alliés et une culture prête à l'innovation.

Pour concrétiser cette vision, la *Stratégie d'IA du MDN et des FAC* définit cinq principaux axes de travail qui traduiront cette vision en un avantage décisionnel : déployer et utiliser des capacités d'IA; favoriser la gestion du changement en vue de l'intégration de l'IA dans les flux de travail réels; ancrer l'éthique, la sécurité et la confiance dans l'ensemble du cycle de vie de l'IA; perfectionner les talents et former une main-d'œuvre prête pour l'IA; et approfondir les partenariats avec les alliés, l'industrie et le milieu universitaire. Ensemble, ces efforts visent à livrer et à opérationnaliser des capacités d'IA pour le personnel des FAC.

L'IA touche toutes les couches de la fondation numérique, des appareils utilisateurs aux réseaux, en passant par l'hébergement et la cybersécurité. Pour tirer parti des occasions qu'elle offre, l'Équipe de la Défense a besoin de données de qualité, de systèmes interopérables, de processus de développement et d'exploitation bien orchestrés, de supercalculateurs et de compétences techniques et partenariats de haut niveau. Toutefois, les organisations de la défense sont, par nature, hautement décentralisées et formées de nombreuses composantes autonomes, ce qui rend la coordination et l'intégration difficiles et complexes.

De nombreuses difficultés pourraient nous empêcher d'être habilités par l'IA d'ici 2030, notamment : des efforts fragmentés et des TI parallèles; des pénuries de talents; des infrastructures manquantes; l'absence d'intégration des données pour des plateformes de nouvelle génération; notre retard par rapport aux alliés et aux adversaires.

En tant qu'organisation publique, le MDN et les FAC rivalisent pour les mêmes talents que le secteur privé et pour la même innovation technologique que nos alliés et nos adversaires. L'écosystème fédéral comporte également un réseau complexe de responsabilités matricielles, de mandats qui se chevauchent et d'objectifs parfois contradictoires.

Heureusement, le MDN ne part pas de zéro. Notre écosystème civil d'IA, de calibre mondial, est porté par trois instituts

nationaux, Mila, Vector et Amii, nommés dans la *Stratégie pan-canadienne en matière d'IA*.³ À l'international, nos alliés les plus proches ont démontré ce qui est possible : le *Defence AI Centre* (DAIC) du Royaume-Uni a démontré comment un seul pôle, appuyé par un institut de sécurité de l'IA, des normes officielles d'IA et des manuels transparents, peut unifier des efforts fragmentés, accélérer l'approvisionnement et instaurer la confiance grâce à un déploiement responsable.⁴ Son AI Model Arena évalue de multiples systèmes d'IA dans des scénarios de défense, ce qui fournit des données objectives qui réduisent les risques et éclairent l'approvisionnement fondé sur les données probantes. Parallèlement, le DAIC mobilise des experts du domaine et des universitaires de façon à accélérer l'innovation tout en intégrant dès le départ des normes éthiques et opérationnelles. Le Canada doit maintenant tirer parti de ces initiatives, les adapter au contexte canadien, consolider ses activités, éviter le dédoublement des efforts et démontrer des contributions mesurables aux objectifs d'investissement en défense de l'OTAN.

Combattre à partir du prototype

Le Centre d'IA du MDN et des FAC permet de développer des capacités prêtes à la mission grâce à un modèle fédéré ou en franchise, où chaque partie de l'organisation conserve la propriété et la responsabilité de ses systèmes d'IA, tout en respectant des garde-fous organisationnels clairs. À partir de 2025-2026, le Centre d'IA a dépassé la simple rédaction de politiques pour les mettre en œuvre, démontrer leur valeur grâce à des projets pilotes opérationnels et étendre leur adoption dans l'ensemble de l'Équipe de la Défense.⁵

Nous travaillons avec les FAC pour cerner les besoins en IA ou les lacunes de capacités et trouver des solutions potentielles, y compris mettre à l'essai de nouvelles capacités afin de comprendre leur rendement dans des scénarios opérationnels. Le Centre d'IA travaille également en partenariat avec Recherche et développement pour la défense Canada (RDDC) et le milieu universitaire pour amener la recherche et le développement vers la production afin que les FAC puissent tester des capacités d'IA innovantes.

En 2026-2027, les projets pilotes deviendront des capacités. Cela signifie que des projets pilotes souverains en IA seront déployés et testés dans les fonctions opérationnelles des FAC, démontrant visiblement que le Canada ne dépend pas de solutions étrangères pour ses applications les plus sensibles. Parallèlement, toutes les voies d'approvisionnement disponibles seront mobilisées afin que les projets prometteurs puissent passer à une production à grande échelle. De nouvelles solutions utilisant des technologies d'IA émergentes auront été introduites, et l'année se conclura par un rapport officiel sur les leçons apprises, preuve que nos cadres ont été testés dans la pratique et sont prêts à guider la croissance future.

Si ces objectifs ne sont pas atteints dans les délais prévus, nous risquons de prendre du retard dans l'adoption de l'IA,

ce qui pourrait éroder notre avantage opérationnel et notre interopérabilité avec des alliés clés. Pour atténuer ce risque, les N1 doivent intégrer des indicateurs flexibles et des évaluations de maturité qui permettent des ajustements de trajectoire et un apprentissage continu issu de l'expérience.

Au sein du Groupe des services numériques, le Centre d'IA établit des liens entre, d'une part, les FAC et, d'autre part, l'industrie, le milieu universitaire et les alliés afin de déployer des capacités d'IA souveraines prêtes à la mission. Ces efforts incluent la mise en place d'une fondation numérique robuste qui soutient les environnements sur site et infonuagiques dans des domaines non classifiés et classifiés, permettant des opérations conjointes grâce à des services infonuagiques opérationnels unifiés, des données, du calcul, de la cybersécurité et du développement d'applications. Pour l'avenir, le Centre d'IA jouera un rôle essentiel dans les efforts pangouvernementaux visant à créer une base industrielle de défense et à moderniser l'approvisionnement au chapitre de la défense.

L'objectif stratégique du Centre d'IA du MDN et des FAC est d'être une force de cohérence qui appuie les N1 des FAC. Le Centre d'IA permettra des voies de déploiement sécurisées, appuiera la gouvernance de l'IA, intégrera temporairement du personnel qualifié en IA dans chaque N1, et fournira des données, des conseils personnalisés et du soutien. En retour, les N1 bénéficieront de l'interaction avec le Centre d'IA avant la création de leurs propres solutions d'IA; il se peut que le Centre ait déjà un modèle déployé prêt à l'emploi.⁶ Pour se préparer à l'IA, les N1 doivent aussi collaborer à la conception des plateformes et des outils organisationnels, et faire le nécessaire pour que les données soient bien gouvernées, utilisables et interopérables, tout en respectant les normes de l'OTAN.

Ce cycle—mettre à l'essai, évaluer, augmenter la production—est ce qui transforme les cadres théoriques en doctrine opérationnelle.

Collaboration avec l'industrie et le milieu universitaire

Le MDN ne peut pas innover en vase clos. Le Centre d'IA réalise une cartographie exhaustive des partenaires, industriels et universitaires, et élabore un plan de participation, permettant de nous assurer que nos interactions sont structurées et ciblées. Parallèlement, il collabore avec l'Université Carleton pour organiser la toute première conférence sur l'IA en défense, qui réunira la communauté de la défense, l'industrie, le milieu universitaire et des partenaires de confiance pour faire progresser l'adoption responsable de l'IA par le MDN et les FAC.⁷ Cette conférence permettra au MDN et aux FAC de convenir avec l'industrie d'une feuille de route quinquennale en ce qui a trait aux capacités en IA et en données.

Les forums comme la prochaine conférence sur l'IA en défense au début de l'année 2027 prouvent que l'Équipe de la

Défense est connectée à l'écosystème élargi. Des partenariats durables démontreront que l'Équipe de la Défense n'est pas simplement un consommateur d'innovation, mais un contributeur à la réussite canadienne en IA.

Ensemble, le Centre d'IA et nos organisations doivent repérer les talents en leur sein et leur donner les moyens de nous aider. Du point de vue du recrutement et de la rétention, nous devons explorer toutes les options pour attirer les meilleurs talents. Nous bénéficierons tous de la création de partenariats collaboratifs et, surtout, nous devons tous examiner attentivement nos processus opérationnels et nous demander comment nous pourrions les adapter à l'ère de l'IA.

Habiliter l'approvisionnement et les contributions à l'OTAN

À la base de chaque volet de cette stratégie se trouve l'approvisionnement. Sans voies adaptées à l'IA, les projets pilotes prometteurs resteront bloqués au stade expérimental. En 2026-2027, le Centre d'IA permettra la mise en place de nouvelles voies d'approvisionnement numérique pour créer un cycle continu de projets pilotes à petite échelle qui favorisera le déploiement et la mise à l'essai rapides de nouvelles technologies. Les membres des FAC pourront collaborer avec l'industrie pour développer conjointement des technologies innovantes avec les utilisateurs finaux et acquérir celles qui démontrent leur efficacité dans les projets pilotes. Nous gérerons également un répertoire de fournisseurs pour éviter les doublons et informer les diverses équipes sur les travaux déjà réalisés et les leçons apprises, ainsi que sur les pratiques exemplaires pour des projets aux idées semblables. Ces étapes à court terme créeront un élan, avec des lots prêts à être classés et un approvisionnement dynamique.

En parallèle, nous veillerons à ce que chaque investissement en IA soit suivi avec précision. Chaque projet sera associé à des codes de capacité de l'OTAN,⁸ pour permettre aux investissements du Canada en IA d'être reconnus comme des contributions à la défense. Nous pourrions ainsi rapporter non seulement le nombre de projets en cours, mais aussi la proportion des investissements en IA qui répondent aux catégories d'investissement en défense de l'OTAN : une démonstration visible du sérieux du Canada en matière de technologies émergentes.

Coordination dans tout l'écosystème fédéral

Dans l'ensemble de l'écosystème fédéral, la réussite exigera une tolérance au risque calculé et des bacs à sable réglementaires permettant l'expérimentation. L'industrie doit avoir davantage de certitude quant à l'avenir de ses relations avec le MDN. Rien de tout cela ne se fera du jour au lendemain : il faudra des progrès graduels et des leçons apprises en cours de route.

Notre élan soutenu a posé une base solide pour la réussite; la priorité est maintenant de fournir des voies claires et accessibles

et une vision cohérente qui permettent une collaboration fluide entre le personnel des FAC et l'industrie. Pour y parvenir, il faudra maintenir une concentration rigoureuse et surmonter des obstacles clés, notamment des processus d'approvisionnement lents et complexes, ainsi qu'une préparation numérique et des données inégales. Nous pouvons surmonter ces défis grâce à des orientations claires et à une coordination d'entreprises.

Conclusion

L'année à venir s'annonce très stimulante, alors que le Centre d'IA passe de la conception de cadres et de politiques à la mise en œuvre de ceux-ci. La gouvernance et les outils d'IA responsables seront intégrés dans les NI, des projets pilotes souverains seront menés, des voies d'approvisionnement seront activées, l'industrie et le milieu universitaire seront mobilisés, et notre main-d'œuvre sera prête. Le Canada pourra montrer à l'OTAN et à ses alliés que nous ne faisons pas que parler d'IA en défense : nous l'adoptons de manière responsable, à grande échelle et de façon percutante.

Le Royaume-Uni a montré ce qui est possible lorsque l'ambition rencontre la structure. Le Canada est maintenant prêt à rattraper son retard, avec un plan qui lui est propre : un plan ancré dans la souveraineté, harmonisé avec l'OTAN et axé sur la prestation de capacités fiables aux militaires au combat.

Notes

- 1 Sheryl Estrada, « MIT Report: 95% of Generative AI Pilots at Companies Are Failing », Fortune, 18 août 2025. Tiré de <https://fortune.com/2025/08/18/mit-report-95-percent-generative-ai-pilots-at-companies-failing-cfo/>.
- 2 Gouvernement du Canada, La Stratégie d'intelligence artificielle du ministère de la Défense nationale et des Forces armées canadiennes, 22 mars 2024. Tiré de <https://www.canada.ca/fr/ministere-defense-nationale/organisation/rapports-publications/mdn-fac-strategie-intelligence-artificielle.html>.
- 3 Gouvernement du Canada, Stratégie pancanadienne en matière d'intelligence artificielle, 31 octobre 2025. Tiré de <https://ised-isde.canada.ca/site/ised/fr/strategie-pancanadienne-matiere-dintelligence-artificielle>.
- 4 Ministère de la Défense du Royaume-Uni, Defence Artificial Intelligence (AI) Playbook, publié le 1^{er} février 2024. Tiré de <https://www.gov.uk/government/publications/defence-artificial-intelligence-ai-playbook>; Ministère de la Défense du Royaume-Uni, JSP 936: Dependable Artificial Intelligence (AI) in Defence (Part 1: Directive), Joint Service Publication, 13 novembre 2024. Tiré de https://assets.publishing.service.gov.uk/media/6735fc89f6920bfb5abc7b62/JSP936_Part1.pdf.
- 5 Voir la p. 48 du Plan ministériel du MDN et des FAC pour une description de la mise en œuvre de la stratégie d'IA par le MDN et les FAC en 2025-2026. Ministère de la Défense nationale et Forces armées canadiennes, Plan ministériel 2025-2026 (Ottawa : Publications du gouvernement du Canada, 2025). Tiré de https://publications.gc.ca/collections/collection_2025/mdn-dnd/D3-37-2025-fra.pdf.
- 6 Quelques-uns de nos outils d'IA communs sont accessibles dans le Registre de l'IA du gouvernement du Canada. Gouvernement du Canada, Registre de l'IA du gouvernement du Canada (produit minimum viable), 28 novembre 2025. Tiré de <https://ouvert.canada.ca/data/fr/dataset/fcb0200-79ba-4fa4-94a6-00e32facea6b>.
- 7 Institut canadien des affaires mondiales, « AI in Defence Conference | Conférence sur l'IA en défense », événement tenu les 9 et 10 février 2026. Tiré de https://www.cqai.ca/ai_in_defence_conference.
- 8 OTAN, « Le rôle de l'OTAN dans le développement des capacités », dernière mise à jour le 26 juin 2025. Tiré de <https://www.nato.int/fr/what-we-do/deterrence-and-defence/natos-role-in-capability-development>.

L'intelligence artificielle et la concurrence technologique entre la Chine et les États-Unis : Répercussions sur la défense canadienne et alliée

JENNIFER GEAREY ET MAJOR TYLER CURRIE

Jennifer Gearey dirige l'équipe Stratégie, capacités et intelligence artificielle responsable au Centre d'IA du ministère de la Défense nationale. Elle a été cadre à la Commission canadienne de sûreté nucléaire, à Santé Canada, au ministère de la Justice et au Conseil du Trésor, et est une ancienne journaliste.

Tyler Currie est l'agent d'intégration et d'accélération de l'IA des FAC qui travaille au Centre d'IA du MDN et des FAC. Tyler a passé 16 ans au sein de la Branche des services du renseignement et a participé à des déploiements en Afghanistan et dans un contexte international avec le Commandement allié de forces interarmées de Naples. Tyler détient une maîtrise en études politiques de Queen's ainsi qu'une maîtrise en gestion en matière d'IA de la Queen's Smith School of Business.

L'intelligence artificielle (IA) est passée de la curiosité des laboratoires à un moteur clé de la stratégie en moins d'une décennie. Elle contribuera à l'amélioration des chaînes logistiques, des flux de travail de renseignement, de la cyberguerre, du jeu de guerre virtuel, du ciblage, de l'entretien préventif des véhicules, de l'administration du personnel, de la gestion des données et de l'orchestration d'opérations complexes.

Contrairement aux plateformes à usage unique, l'IA est une capacité polyvalente. Une fois les bases établies, à savoir les données, la capacité de calcul et les habitudes organisationnelles pour les utiliser, de nouvelles fonctions militaires peuvent être « écrites » dans un logiciel et exécutées à la vitesse du logiciel. C'est pourquoi l'IA est essentielle pour obtenir un avantage décisionnel. Les nations capables de traduire les données en décisions rapides et fiables sur le champ de bataille bénéficieront d'avantages croissants; celles qui ne le peuvent pas découvriront que le fait de disposer de matériel haut de gamme sans cohésion numérique représente un risque coûteux. Les États-Unis et la Chine, l'Union européenne (UE) ou le Canada : les pays ont maintenant mis en œuvre des stratégies d'IA pour maximiser le potentiel de l'IA en défense.¹

La concurrence technologique entre la Chine et les États-Unis illustre cette réalité. Elle couvre les puces et l'infonuagique, les normes et les chaînes d'approvisionnement, les écosystèmes de recherche et les plateformes d'entreprise. Cette concurrence ne concerne pas seulement les parts de marché; il s'agit de la capacité à établir le rythme des opérations et les règles d'interopérabilité pendant des décennies.

La Chine cherche à compresser le temps—adopter et étendre l'IA au service de la « guerre intelligentisée », intégrer la surveillance et l'automatisation des commandements à travers les domaines et exporter la gouvernance numérique clé en main au moyen de sa Route de la soie numérique.² Les États-Unis, avec leurs alliés, possèdent toujours les points d'étranglement les plus importants—des équipements avancés de fabrication de puces, des modèles et cadres de pointe, une infonuagique à grande

échelle et une grande partie des meilleurs talents mondiaux en IA, mais les cycles d'approvisionnement démocratiques et l'ambivalence des entreprises peuvent freiner cette avance.³

Pour le Canada, les enjeux sont exceptionnellement concrets. En tant que puissance intermédiaire imbriquée dans les architectures d'alliances (OTAN, NORAD, Groupe des cinq) et dépendante de l'informatique importée et de l'infonuagique commerciale, le Canada doit faire des choix qui détermineront s'il demeure interopérable à la vitesse et à la fidélité exigées par l'IA. Les Forces armées canadiennes (FAC) combattront de plus en plus au sein de groupes de travail multidomains et de coalitions qui relient capteurs, armes et données dans tous les domaines.⁴

Cet avenir n'est plausible que si le Canada peut protéger et mobiliser ses données, garantir un accès fiable aux capacités de calcul et chaînes d'outils, réformer les institutions pour déployer l'IA de manière responsable et rapide, et attirer et retenir les talents nécessaires pour concrétiser ces trois éléments. Au sein de chacun de ces moteurs, l'adoption de l'IA doit rester ancrée dans la prise de décision plaçant l'humain dans la boucle, avec une reddition de comptes clairement attribuée et la préservation d'un jugement humain significatif dans des contextes de défense conséquents. La solution de rechange est une dérive induite par la technologie—des lacunes de capacités qui se développent discrètement en temps de paix et se révèlent au pire moment possible.

Pour demeurer un allié de premier ordre à l'ère de l'IA, le Canada devrait faire des investissements délibérés et des démarches institutionnelles qui transforment les valeurs



Un membre de l'Unité des capacités navales avancées basée à Victoria, en Colombie-Britannique, en poste à l'intérieur d'une tente de contrôle, utilise un ordinateur Toughbook en collaboration avec le contrôleur pour commander le drone G15 Sentinel afin de tester l'interopérabilité en conditions arctiques dans le cadre de l'opération NANOOK-NUNALIVUT, à Inuvik, dans les Territoires du Nord-Ouest, le 27 février 2025.

Caporale-chef Alana Morin, Force opérationnelle interarmées (Nord) - Yellowknife

démocratiques en avantages opérationnels. Cet impératif repose déjà sur une base solide, puisque le Canada est depuis longtemps un investisseur précoce et durable en IA, avec un écosystème de recherche reconnu mondialement dans ce domaine. La tâche consiste maintenant à s'assurer que cette force est convertie en un avantage opérationnel durable.

L'IA en tant que défi stratégique

Au niveau opérationnel, l'IA harmonise l'espace aérien, aligne les activités là où la coordination est requise et fusionne les données dispersées en un tableau opérationnel cohérent. Au niveau stratégique, elle favorise une reconnaissance cybernétique persistante et façonne les opérations à la vitesse des machines. Ensemble, ces capacités compressent et accélèrent les cycles de décision.

Trois caractéristiques de l'IA en font un problème de sécurité particulièrement difficile pour les démocraties. Premièrement, elle sert un double usage poussé à l'extrême.⁵ Le même modèle qui aide à rédiger des notes juridiques peut générer des troupes d'hameçonnage ciblées; le même pipeline d'images synthétiques qui génère des données d'entraînement bénignes peut produire des hypertrucages plausibles; le même moteur d'optimisation qui achemine les camions peut planifier des essais de systèmes autonomes. Les mesures de contrôle gouvernementales à l'exportation—des règles qui restreignent la vente de technologies sensibles comme les puces informatiques avancées et les logiciels d'IA à certains pays—peuvent ralentir l'accès des adversaires à du matériel et des modèles de pointe.⁶ Les idées, et même le code, se sont rapidement diffusés à travers

les publications universitaires et les communautés de source ouverte. Les FAC devraient donc supposer que des adversaires compétents obtiendront des outils d'IA générative quasi de pointe, même s'ils ne peuvent pas produire eux-mêmes les puces les plus récentes.

Deuxièmement, l'IA évolue avec les données et la capacité de calcul, pas seulement avec les budgets. Les super-applications commerciales et la surveillance intérieure de la Chine produisent des océans de données à haute granularité sur les personnes, les lieux et les modes de vie; l'alignement entre l'État et l'industrie permet de réutiliser ces données à des fins de sécurité sans trop de friction.⁷ Par ailleurs, l'accès à l'informatique est inégal et de plus en plus coûteux. Lorsque la demande mondiale pour les UTG explose, les entraînements coûtant des millions de dollars deviennent courants pour les grands fournisseurs de nuages—et hors de portée pour d'autres.⁸ Cela crée un monde où ceux qui peuvent financer un entraînement soutenu et un ajustement fin obtiennent des avantages cumulés en termes de capacité et d'alignement du modèle.

Troisièmement, l'IA rend la dissuasion et le recours hiérarchique plus difficiles à gérer. Lorsque les machines agissent avec un certain degré d'autonomie, il devient moins clair qui est responsable de leurs décisions.⁹ Si les adversaires manipulent les systèmes d'IA, ils peuvent déclencher des défaillances inattendues. En même temps, l'IA peut maintenant générer de fausses voix, images et vidéos de façon si convaincante que tout l'espace d'information devient un champ de bataille. La dissuasion dépend de signaux clairs et d'une compréhension partagée des lignes rouges, mais cela s'effondre lorsque l'espace d'information lui-même est dégradé par la désinformation, la manipulation et le bruit du signal. Dans un tel monde, la confiance entre alliés n'est pas optionnelle; elle est essentielle.

Pour le Canada, l'IA influencera tous les types de missions.¹⁰ Dans l'Arctique et l'Atlantique Nord, où les communications sont limitées, les forces auront besoin d'une IA capable de traiter les signaux faibles et dispersés directement sur les navires et les avions, car il n'y a ni le temps ni la bande passante pour tout renvoyer au quartier général. En ce qui concerne la modernisation du NORAD, de nouveaux radars et systèmes de capteurs ne seront utiles que si l'IA aide à trier le flot de données pour mettre en lumière les menaces réelles. Lors des opérations à l'étranger, les postes de commandement devraient pouvoir fonctionner même lorsque les communications sont coupées, dégradées ou peu fiables, en utilisant des modèles d'IA capables de fonctionner sur du matériel robuste et portable sur le terrain.

Dans toutes les missions, les adversaires exploiteront l'IA pour mener des campagnes de désinformation, lancer des cyberattaques activées par l'IA, compromettre des modèles grâce à l'apprentissage automatique adverse, et même donner des ordres clonés par voix destinés à semer le doute à l'égard du leadership. Des incidents récents, comme les hypertrucages par IA d'images diffusant de la désinformation sur les feux de forêt en

Colombie-Britannique, montrent que les attaques activées par l'IA sont une réalité d'aujourd'hui.¹¹

La *Stratégie d'IA du ministère de la Défense nationale (MDN) et des FAC* offre un point de départ solide, notamment par son accent sur la mise en vente d'applications d'IA et la création de garanties éthiques.¹² La nouvelle *Stratégie industrielle de défense du Canada*, dévoilée en février 2026, renforce également cette orientation en donnant la priorité aux technologies numériques comme l'IA et l'infonuagique sécurisée, ce qui fait progresser davantage les capacités d'IA en défense.¹³ À mesure que la Stratégie d'IA passe de la vision à l'exécution, le MDN et les FAC devraient s'assurer que ces principes se traduisent par des réalités opérationnelles (combler les écarts en matière de talents, éliminer le travail en silos, améliorer la préparation des données et accélérer les voies d'approvisionnement) afin que l'IA puisse être adoptée de manière responsable, à grande échelle et avec un impact.

Les grandes entreprises technologiques, l'agence d'entreprise et la défense de la démocratie

À des époques précédentes, les gouvernements possédaient ou dirigeaient les technologies décisives de la guerre : physique nucléaire, décryptage de codes, aérospatiale, lancement spatial, etc. Aujourd'hui, les outils d'IA les plus importants—comme les plus grands modèles, les plateformes en nuage massives, les logiciels sécurisés de travail d'équipe et les systèmes qui vérifient si le contenu est vrai ou faux—sont tous développés et contrôlés par seulement quelques grandes entreprises mondiales. Alibaba, Tencent, Microsoft, Amazon, Google et Meta possèdent les nuages et les accélérateurs; ces entreprises contrôlent les plateformes de collaboration et d'identité sur lesquelles le travail gouvernemental se déroule réellement. Il s'agit là à la fois d'une opportunité et d'une vulnérabilité.

Cela est une opportunité parce que les grandes entreprises technologiques peuvent avancer rapidement, embaucher des talents que les gouvernements ont du mal à attirer et répartir les coûts sur leurs vastes marchés commerciaux. Lorsque leurs produits s'alignent sur les objectifs des alliés, les forces armées peuvent gagner du temps. Au lieu de construire tous les systèmes d'IA à partir de zéro, un ministère de la Défense peut acheter des versions sécurisées et conformes aux politiques des plateformes commerciales, puis se concentrer uniquement sur les parties spécifiques à la mission.¹⁴ Des fonctionnalités telles que des régions d'infonuagique avec des mesures de contrôle nationales, des systèmes de connexion avec des règles d'accès strictes, et des pipelines logiciels qui vérifient l'intégrité du code sont des exemples pour lesquels quelques choix intelligents peuvent générer des avantages majeurs en matière de sécurité à l'échelle de l'entreprise.

Les plateformes commerciales sont aussi une source de vulnérabilité parce qu'elles sont mondiales. Leurs revenus et leur croissance dépendent d'opérations multijuridictionnelles, y compris dans les pays dont les régimes juridiques imposent la coopération avec les services de sécurité de l'État.¹⁵ Leurs feuilles de route pour les produits devraient trouver un équilibre entre le rendement pour les actionnaires, le risque pour la marque et la politique interne des employés, ainsi que les demandes gouvernementales en matière de sécurité nationale. Le résultat est une ambivalence structurelle. Une entreprise peut être un partenaire crucial pour le département de la Défense des États-Unis (DoD) tout en maintenant une présence de recherche en Chine ou en vendant des logiciels d'entreprise à des pays tiers qui les utilisent de manière non conforme aux intérêts des alliés. Il existe des cas récents où des universités américaines menant des recherches financées par le DoD ont involontairement soutenu des technologies plus tard liées à des institutions militaires chinoises, ce qui a poussé le Pentagone à réduire leurs possibilités de financement.¹⁶ Ces enchevêtrements peuvent être légaux et même transparents, mais ils créent une exposition pour toute entité dont la mission repose sur ces plateformes.

Pour le Canada, la leçon consiste à traiter les grandes entreprises technologiques non pas comme un « allié » monolithique, mais comme des acteurs ayant de l'autonomie et dont les incitatifs devraient être façonnés. Trois choix de conception suivent.

D'abord, inscrire la sécurité et la voie sortie dans le contrat. L'approvisionnement en défense devrait exiger une journalisation des audits juricomptables, tels que des journaux d'activités détaillés, une séparation stricte des clés gérées par les clients et une résidence par défaut des données dans les juridictions alliées.¹⁷ Cela devrait aussi nécessiter des voies de sortie pratiques, comme garantir un accès indépendant aux modèles de fondation, utiliser des systèmes d'IA facilement transférables entre fournisseurs infonuagiques, et s'assurer que tout logiciel personnalisé fonctionne sur de nombreuses plateformes.¹⁸ Il ne s'agit pas d'afficher un comportement hostile envers les vendeurs, mais plutôt de reconnaître que l'interopérabilité et la continuité constituent des exigences de combat. Si un choc géopolitique force la migration rapide des services, les FAC ne devraient pas être menottées par des liens propriétaires. Ces mécanismes, tels que les clauses de voie de sortie, pourraient être intégrés dans de grandes initiatives d'approvisionnement en IA pour la défense afin de se prémunir contre d'éventuelles contingences.

Deuxièmement, traiter la gouvernance comme quelque chose de concret, pas seulement comme une promesse. Chaque système d'IA devrait être accompagné d'une « trousse de gouvernance » de base, incluant des éléments comme des cartes modèles expliquant comment le système d'IA a été construit et testé, des résumés de l'origine des données d'entraînement, des résultats des essais de l'équipe rouge pour cerner les faiblesses du système face aux menaces activées par l'IA, des limites connues,

des vérifications des biais, et un processus clair pour gérer les incidents ou revenir en arrière si nécessaire.¹⁹

En ce qui concerne l'authenticité du contenu, exiger des normes ouvertes, telles que des signatures numériques prouvant d'où provient le contenu, ainsi que des pistes de vérification qui montrent si quelque chose a été modifiée. Pour les logiciels, exiger des listes de documents, listant tous les composants, une preuve d'intégrité de la chaîne d'approvisionnement et des compilations reproductibles pour le code critique.²⁰ Ces outils transforment les affirmations des vendeurs en faits vérifiables et permettent aux alliés de collaborer en toute confiance.

Troisièmement, diversifier intelligemment sans créer une complexité inutile. Utiliser plusieurs plateformes en nuage simplement pour le fait de le faire peut rendre les systèmes fragiles et plus difficiles à gérer. Le véritable objectif consiste à éviter des points de défaillance uniques, pas à répartir le travail de façon égale entre les fournisseurs. Une bonne approche consiste à s'appuyer sur une plateforme principale pour les opérations quotidiennes, tout en gardant les plateformes secondaires en attente pour les augmentations subites ou les urgences. Les normes ouvertes, telles que les identifiants d'identité courants, les trousseaux logicielles, pouvant fonctionner partout, et les systèmes de messagerie, respectant les normes de l'OTAN, facilitent le basculement ou la connexion au besoin.

Ce qui compte le plus, c'est la façon dont le Canada est relié à ses alliés, à l'industrie et à ses partenaires. S'appuyer trop fortement sur quelques grandes plateformes technologiques—fournisseurs infonuagiques, modèles d'IA ou suites logicielles—crée un risque pour la plateforme, ce qui signifie que le Canada pourrait devenir dépendant de systèmes qu'il ne contrôle pas. Si ces entreprises modifient leurs politiques, limitent l'accès, subissent des pannes ou doivent se conformer aux autorités juridiques étrangères, la sécurité et les opérations du Canada pourraient être compromises.²¹ Mais si le Canada utilise des contrats, des normes et des pratiques claires pour aligner ces plateformes organisationnelles sur les besoins nationaux, cela peut transformer cette dépendance en un avantage. Sinon, le risque posé par la plateforme deviendra simplement une autre forme de vulnérabilité stratégique. Pour remédier à ces vulnérabilités, le MDN et les FAC soutiennent l'écosystème canadien de l'IA de défense et acquièrent des capacités d'IA alignées sur la stratégie d'IA de l'OTAN.

Les quatre champs de bataille du pouvoir de l'IA – et les choix du Canada

Les États-Unis et la Chine sont engagés dans une lutte pour obtenir l'avantage en matière d'IA. La concurrence n'est pas abstraite—tout se résume à des aspects très pratiques : qui contrôle les bonnes données, qui a accès à la puissance de calcul, qui peut transformer les politiques en systèmes fonctionnels, et qui peut attirer et retenir les bonnes personnes. Ces

quatre champs de bataille détermineront qui est un chef de file en matière d'IA. Pour le Canada, le succès dépendra des choix que nous ferons maintenant.

Les données représentent le premier champ de bataille. Le modèle chinois repose sur le volume et la contrainte : des flux sans fin provenant de capteurs, et un accès étatique à l'information par défaut.²² Les démocraties comme le Canada ne peuvent pas et ne devraient pas copier cette approche. L'avantage du Canada devrait reposer sur la préparation des données, pas sur l'accumulation compulsive. Cela signifie savoir quels ensembles de données sont importants pour la défense—comme les voies aériennes et maritimes, les dossiers logistiques ou les flux satellitaires—et les organiser pour qu'ils puissent réellement être utilisés par l'IA. Trop souvent, les organisations de défense se noient sous des pétaoctets de données inutilisables sans étiquettes claires, sans information traçant leurs origines et sans politiques sur leur utilisation.²³ La tâche du Canada revient à transformer cette botte de foin en une bibliothèque bien organisée, prête à être utilisée par les systèmes d'IA. Parfois, lorsque les données sont rares ou sensibles, la réponse sera des exemples synthétiques ou simulés—comme entraîner des modèles de détection de sous-marins sur des signaux sonar simulés, plutôt que de risquer de révéler de véritables tactiques. La disponibilité opérationnelle signifie aussi faire preuve de retenue : les alliés ne communiqueront leurs données que si le Canada peut aussi prouver qu'il sait les supprimer ou les réduire au minimum de manière responsable.

La capacité de calcul représente le deuxième champ de bataille. Les puces informatiques les plus avancées et l'accès à l'équipement de fabrication restent concentrés dans les écosystèmes alliés et partenaires, bien que la capacité de fabrication de la Chine soit solide, mais reste en retard. Les contrôles à l'exportation restreignent principalement l'accès des adversaires aux calculs les plus performants tout en permettant des flux continus au sein des chaînes d'approvisionnement fiables. L'accès aux systèmes d'IA les plus avancés et leur exploitation à grande échelle sont toujours façonnés par l'usage de puces de pointe. Cela n'a d'importance que si le Canada peut réellement accéder à la puissance de calcul dont il a besoin lorsque nécessaire. Les marchés infonuagiques sont volatils, et les charges de travail en défense peuvent facilement être éclipsées par la demande commerciale.²⁴ Des centres de données en sol canadien, connectés à des réseaux sécurisés; et des ordinateurs en périphérie robustes capables d'exécuter des modèles d'IA sur le terrain, même lorsque les communications sont coupées. L'objectif n'est pas d'élaborer le prochain GPT-4 à partir de zéro, mais de s'assurer que le Canada peut s'adapter et faire fonctionner des modèles compatibles sans faire la queue. La capacité de calcul, en ce sens, est comme un carburant : quelque chose de rare, stratégique et qui doit être soigneusement planifié, budgété et conservé.

Les organisations représentent le troisième champ de bataille. La puissance de l'IA ne se limite pas à rédiger des

principes; il s'agit aussi de mettre les outils de travail entre les mains des opérateurs rapidement et en toute sécurité. Cela signifie établir des habitudes qui manquent souvent aux organisations de défense : expérimentations rapides, essais continus, pipelines d'approbation rapides mais responsables, et budgets qui permettent de transformer les projets pilotes en véritables programmes.²⁵ Le Centre d'IA de la défense du Canada devrait être le point névralgique, mais chaque formation a besoin de petites équipes qui rassemblent opérateurs, ingénieurs, avocats et éthiciens pour transformer des idées en systèmes déployables. Les voies réparties en fonction du risque sont essentielles. Un assistant utilisant l'IA qui effectue des recherches concernant la doctrine n'a pas besoin de la même surveillance qu'un modèle qui informe les décisions de ciblage. L'approvisionnement doit aussi évoluer—acheter les résultats par incréments, financer les personnes qui maintiendront et adapteront les modèles, et supposer que les systèmes auront besoin de mises à jour régulières, pas seulement de livraisons ponctuelles.

À mesure que le MDN et les FAC accélèrent le déploiement de l'IA, il faut intégrer l'assurance dès la conception grâce à des essais automatisés, des bacs à sable d'IA, ainsi que des modèles de déploiement modulaires et par étapes qui permettent aux capacités de s'étendre rapidement des projets pilotes aux opérations. Parallèlement, il faut développer des ressources de calcul d'IA souveraines pouvant être réutilisées dans de nombreux projets et tirer parti d'un écosystème d'IA canadien fiable, ce qui garantit que les capacités de défense sensibles peuvent être déployées rapidement sans dépendance stratégique.

Enfin, les talents représentent le dernier champ de bataille. Peu d'entités peuvent dépenser plus que celles de la Silicon Valley, en embauchant des centaines d'ingénieurs expérimentés, et elles n'ont pas à le faire. Ce dont nous avons besoin, c'est d'une approche pyramidale : un petit groupe d'experts chevronnés pour résoudre les problèmes les plus difficiles, une large base d'opérateurs numériquement fluides capables d'utiliser les outils d'IA dans leur travail quotidien, et des traducteurs intermédiaires qui relient la politique à l'ingénierie et les opérations aux données. Cela nécessite aussi des systèmes d'IA modulaires et de source ouverte afin que les capacités puissent être adoptées plus facilement, ainsi qu'une formation permettant aux opérateurs des FAC d'acquérir les compétences nécessaires pour les maintenir et les améliorer au fil du temps. Au-delà des spécialistes techniques, les viviers de talents devraient explicitement renforcer la capacité et la formation des éthiciens, des commandants, des concepteurs centrés sur l'humain et des experts en communication afin que l'adoption de l'IA demeure sécuritaire et bien ancrée. Le MDN et les FAC achèvent déjà certaines de ces étapes, car le talent et la formation constituent l'un des piliers fondamentaux de la Stratégie d'IA de la Défense.

Le MDN et les FAC peuvent réaliser des gains rapides grâce à des bourses liées au service, des détachements auprès de grands instituts d'IA, des habilitations de sécurité simplifiées pour les

compétences clés et des formations pour promouvoir la connaissance en IA. Des initiatives plus ambitieuses devraient suivre sous forme d'investissements à moyen et à long terme. Un exemple clé est la création d'un corps de réserve numérique qui permettrait aux experts de l'industrie d'intervenir lors d'exercices ou de crises. Le MDN et les FAC pourraient cultiver un noyau protégé de spécialistes principaux en IA avec une variété d'expertises soutenues par des flux de travail et des outils modernes compatibles avec l'IA, ainsi qu'une reconnaissance qui ne nécessite pas de laisser de traces techniques à la gestion. Retenir ces talents exige ultimement autonomie, raison d'être et reconnaissance—ainsi qu'un système qui valorise l'expertise approfondie comme un atout stratégique. Par-dessus tout, les talents doivent être protégés, car ceux qui travaillent sur l'IA de défense pourraient être ciblés par des campagnes d'espionnage et de harcèlement.

Le choix du Canada est clair : nous pouvons soit traiter ces quatre champs de bataille comme des problèmes distincts—données, capacité de calcul, organisations et talents—soit les aborder comme une seule posture stratégique. Le succès repose sur la préparation, l'accès, la rapidité et les personnes.

Huawei, la Route de la soie numérique et le défi de l'interopérabilité

Huawei est souvent considérée comme une simple entreprise de télécommunications, mais son rôle est plus large. Grâce à ses plateformes de « villes sûres » et à l'initiative plus large de la Route de la soie numérique en Chine, Huawei regroupe des caméras, des capteurs, des analyses et des logiciels de commande dans des ensembles technologiques prêts à l'emploi.²⁶ Ces outils sont commercialisés comme des outils de modernisation. Pour les gouvernements travaillant avec des budgets serrés, il est difficile d'ignorer le discours : financement à faible coût, déploiement rapide, et l'apparence d'un contrôle plus strict sur la sécurité et les infrastructures.

La difficulté pour les alliés n'est pas seulement la possibilité d'espionnage, mais aussi la diffusion d'architectures conçues pour une surveillance hautement centralisée. Une fois intégrés, ces systèmes tendent à façonner les pratiques qui les entourent.²⁷ Lorsque ces architectures entrent dans les réseaux partenaires, les opérations alliées peuvent hériter de leurs contraintes.

La décision du Canada d'exclure Huawei des réseaux 5G représentait une étape importante, mais des difficultés subsistent. Les risques proviennent désormais de l'exposition indirecte : des sous-traitants qui intègrent des composants Huawei dans des systèmes autrement « propres »; des nations partenaires dans des régions telles que l'Indo-Pacifique, l'Afrique ou l'Europe de l'Est qui adoptent des réseaux basés sur Huawei et accueillent plus tard des exercices alliés; des achats locaux au Canada qui intègrent des technologies de surveillance dans les infrastructures critiques.²⁸ Dans un environnement partagé, l'interopérabilité n'est aussi forte que son maillon le plus faible. Un

seul fournisseur avec des canaux de mise à jour opaques peut créer une incertitude persistante.

La réponse pratique du MDN et des FAC devrait se concentrer sur trois domaines. Premièrement, il ne suffit pas de vérifier le fournisseur principal; nous devons aussi savoir quelles pièces et quels logiciels proviennent de leurs sous-traitants. Des règles de divulgation de base et des outils simples peuvent rendre visibles les risques cachés avant qu'ils ne causent des problèmes.²⁹

Deuxièmement, offrir de vraies solutions de rechange. Dire à d'autres pays de ne pas utiliser un certain fournisseur ne fonctionne pas s'il n'y a pas d'options abordables parmi lesquelles choisir. Le Canada devrait collaborer avec ses alliés pour offrir des forfaits technologiques fiables, respectueux des principes de confidentialité et offrant un soutien à long terme.

Troisièmement, se présenter là où les règles sont écrites. Les normes internationales décident quels systèmes peuvent être connectés et fonctionner ensemble. Le Canada devrait être présent à ces tables de négociations, poussant pour l'adoption de règles ouvertes et transparentes qui rendent l'infrastructure de confiance l'option la plus facile.

En prenant ces mesures, le MDN, les FAC et leurs partenaires peuvent réduire les risques, renforcer la coopération et soutenir un écosystème numérique ouvert, sécuritaire et résilient, sans augmenter inutilement les tensions.

Approvisionnement, volatilité du marché et économie de la rapidité

Le MDN et les FAC avec leurs alliés peuvent avoir un avantage en ce qui concerne les puces avancées et les plateformes info-nuagiques, mais cet avantage ne vaut pas grand-chose si les gouvernements ne peuvent pas acheter et déployer rapidement de nouveaux outils. Aujourd'hui, l'approvisionnement est souvent le goulot d'étranglement. Les processus concurrentiels lents pour l'achat des grands systèmes universels peuvent prendre tellement de temps que la technologie devient obsolète avant même d'être obtenue. Au Canada, les grands cycles d'approvisionnement dans le domaine de la défense peuvent durer sept ou huit ans.³⁰ Les méthodes d'évaluation ont tendance à récompenser les fournisseurs familiers plutôt que ceux qui innovent³¹. Les contestations juridiques peuvent retarder les progrès pendant des mois, voire des années. Pendant ce temps, la technologie de l'IA évolue tous les trois à six mois, et non chaque décennie.³²

Le MDN et les FAC peuvent combler l'écart entre la vitesse de l'innovation commerciale et le rythme plus lent de l'approvisionnement en défense grâce à des mesures concrètes, tirant parti de leur écosystème dynamique de recherche et d'innovation en IA.³³

Pour y parvenir, on peut acheter par petites quantités plutôt que de miser sur des projets massifs, une approche démontrée par le service d'adoption rapide de l'Accélérateur d'innovation de défense pour l'Atlantique Nord (DIANA) de l'OTAN lors d'essais opérationnels alliés.³⁴ Diviser les programmes en éléments

gérables, chacun associé à des contrôles du rendement clairs, réduit les risques et permet des ajustements en cours de route.³⁵ Les paiements devraient être liés à des jalons mesurés par des indicateurs montrant une analyse des données plus rapide ou des cycles de décision plus courts, plutôt que simplement la livraison des logiciels. Une autre étape consiste à se préparer à la volatilité du marché. L'accès à la puissance de calcul est habituellement chose courante, jusqu'à ce qu'il ne le soit soudainement plus. Les contrats devraient inclure des clauses garantissant un accès prioritaire en cas de crise et le plafonnement des prix pour un usage de base, et offrir au Canada la flexibilité de déplacer les charges de travail entre les régions.³⁶ Le fait de maintenir de petits contrats stables avec plusieurs fournisseurs peut servir d'assurance contre les pénuries ou les perturbations soudaines.³⁷

L'évaluation doit aussi être considérée comme centrale, et non secondaire. Le vrai coût d'un système d'IA n'est pas la licence logicielle, mais le travail continu d'essai, de surveillance et de réentraînement. L'Équipe de la Défense a besoin de ressources consacrées aux exercices de l'équipe rouge, aux outils pour détecter la dérive ou la manipulation et à des registres clairs sur les limites d'un système.³⁸ Si les commandants doivent s'appuyer sur l'IA pour des décisions à enjeux élevés, ils devraient pouvoir démontrer comment l'outil a été testé et quelles sont ses limites. Des alliés comme les États-Unis et le Royaume-Uni utilisent déjà des mesures pour évaluer la fiabilité et la sécurité de leurs modèles d'IA en matière de défense, notamment la fréquence à laquelle les systèmes prennent les bonnes décisions, s'ils accélèrent les opérations, et la sécurité et la prévisibilité de leur rendement lors d'essais réalistes, notamment lorsque les conditions sur le champ de bataille changent.³⁹

Le MDN et les FAC doivent aussi traverser la « vallée de la mort », l'endroit où les prototypes fructueux échouent à devenir des outils déployés. Trop souvent, les projets pilotes meurent parce qu'aucune unité n'est prête ou ne dispose du financement pour les adopter.⁴⁰ Aux États-Unis, par exemple, seul 16 % du financement pour l'innovation en défense passe à la production à temps plein.⁴¹ Un financement exclusif pourrait permettre la mise en service des projets pilotes réussis, grâce à une organisation réceptrice désignée dès le départ. Les projets pilotes eux-mêmes devraient être conçus en tenant compte des réalités du déploiement—telles que les exigences de classification, la gestion des identités et la consignation des événements liés à la sécurité—afin qu'ils puissent passer à la phase de production sans encombre.

Enfin, la gestion des coûts devrait être considérée comme une partie intégrante de la sécurité. Des dépenses cachées, comme les frais de transfert dans le nuage, l'expansion des outils d'IA à l'ensemble de l'organisation ou le gonflement du stockage, peuvent discrètement consommer des budgets.⁴² Intégrer directement la supervision financière au sein des équipes techniques permet de maintenir des coûts prévisibles, de rendre les

compromis transparents et d'empêcher que des factures imprévues ne fassent dérailler l'adoption.

Prises ensemble, ces mesures peuvent aider le MDN et les FAC à adapter l'approvisionnement pour la défense au rythme rapide du développement de l'IA, de sorte que l'avantage technologique se traduise par un avantage opérationnel.

Implications pour le Canada et l'OTAN : un ordre du jour contenu

Transformer l'analyse en action signifie se concentrer sur ce qui peut réellement être fait maintenant et sur ce qui devrait être construit pour l'avenir. Pour le Canada, l'horizon immédiat correspond aux 12 à 18 prochains mois. Au-delà de cela, il faut penser aux deux à quatre années suivantes.

À court terme, la priorité du Canada est de créer les conditions pour que l'IA soit adoptée rapidement, mais de façon sécuritaire.

Plutôt que de suivre le rythme de l'IA commerciale, la priorité du MDN et des FAC consiste à éliminer les retards évitables et à aligner les rythmes d'approvisionnement et d'essai sur ceux des alliés grâce à des projets pilotes rapidement déployables qui évoluent à mesure que les capacités mûrissent. Cela commence par des directives claires à l'ensemble de l'Équipe de la Défense. Toutes les utilisations de l'IA n'entraînent pas le même niveau de risque, et les décideurs ont besoin d'un cadre simple qui facilite l'approbation des applications à faible risque tout en réservant des processus plus stricts aux usages à plus haut risque. Parallèlement, le Canada bénéficierait d'un centre consacré aux essais, à l'évaluation et l'approche de l'équipe rouge; un endroit où de nouveaux systèmes peuvent être poussés à leurs limites, leurs vulnérabilités exposées et leur performance surveillée dans des conditions réelles. Pour bâtir un écosystème d'IA souverain, le MDN et les FAC ont demandé au Centre canadien d'IA de la Défense de renforcer la capacité de recherche et d'expérimentation en IA tout en contribuant à des solutions innovantes en IA.

L'accès à la puissance de calcul constitue un autre besoin urgent. Le MDN et les FAC ne peuvent pas se permettre d'attendre alors que la demande pour des puces avancées explose. Cela signifie sécuriser les ressources infonuagiques avec des droits prioritaires, développer une capacité modeste sur place pour le travail sensible, et certifier des dispositifs portatifs en périphérie capables de fonctionner même dans des environnements de communication dégradés.⁴³ Cela signifie aussi s'assurer que le MDN et les FAC disposent de ressources de calcul suffisantes pour réduire la dépendance aux fournisseurs étrangers. En même temps, le Canada devrait commencer à préparer ses données. Certaines zones de mission, telles que la surveillance dans l'Arctique, les images de renseignement ou les dossiers d'entretien de l'équipement, devraient être élevées à la norme d'excellence, avec des métadonnées appropriées, des garanties de confidentialité et des

données synthétiques au besoin. Ces exemples peuvent donner le ton pour le reste de l'organisation.

La gouvernance doit aussi devenir une partie intégrante du produit, et non une réflexion après coup. Chaque outil d'IA acquis pour la défense devrait être accompagné d'une documentation de base : sur quoi il a été entraîné, comment il fonctionne, où il rencontre des difficultés et comment il peut être désactivé en toute sécurité si quelque chose tourne mal. Les exercices devraient aussi évoluer. Les principaux exercices de l'OTAN ou du Groupe des cinq devraient désormais inclure des hypertrucages générés par l'IA et une manipulation narrative, offrant aux équipes des affaires publiques la possibilité de pratiquer la détection rapide et de mettre en place des réponses coordonnées.⁴⁴

Si l'on regarde plus loin, le programme à moyen terme porte sur le changement organisationnel. Le système actuel d'approbations uniques pour les logiciels ne peut pas suivre le rythme de l'IA, qui évolue chaque semaine. Le MDN et les FAC devront évoluer vers des modèles d'assurance continue, selon lesquels la sécurité est surveillée et appliquée en temps réel. Les États-Unis et l'UE fournissent des indicateurs d'assurance de l'IA que le MDN et les FAC pourraient envisager d'adopter, ce qui pourrait inclure le développement de modèles d'IA ayant une conception robuste, surveillant en continu les comportements anormaux, démontrant des protocoles de recours hiérarchique centrés sur l'humain clairs et ayant des pipelines de modèles segmentés. En travaillant avec leurs alliés, le MDN et les FAC devraient aussi aider à créer un échange de modèles partagé, avec des trousseaux et une documentation mis en commun afin que les partenaires puissent utiliser le travail des autres plutôt que de le réinventer.⁴⁵

Il y a aussi une dimension géopolitique. De nombreux pays adoptent des technologies axées sur la surveillance dans le cadre de programmes de sécurité urbaine. Le Canada, en collaboration avec les partenaires du Groupe des sept (G7), pourrait développer des solutions de rechange qui sont abordables, protègent les renseignements personnels et démontrent un modèle démocratique de technologie de « ville sécuritaire ».⁴⁶ Parallèlement, la dimension humaine ne peut pas être négligée. Le MDN et les FAC auront besoin d'habilitations plus rapides pour les compétences critiques, ainsi que de parcours de carrière permettant aux spécialistes techniques d'évoluer sans être forcés à occuper des postes de gestion. Le MDN et les FAC peuvent conserver l'accès à leur main-d'œuvre critique en IA, en assurant l'accès à la capacité de calcul grâce à un approvisionnement partagé avec la fonction publique et en construisant des cadres de vérification partagés. La protection des chercheurs grâce à des programmes de contre-espionnage adaptés sera également essentielle.⁴⁷ Il faudra notamment s'assurer que les chercheurs agissent avec une diligence raisonnable pour comprendre les sources de financement et savoir avec qui ils interagissent. S'ils développent de nouveaux produits, ils doivent être formés à prendre les précautions de base, comme limiter l'exposition à des renseignements de nature

délicate ou propriétaires, déposer des brevets avant la divulgation ou utiliser des accords de confidentialité.⁴⁸

Enfin, des alliances comme l'OTAN dépendent de l'interopérabilité. Cela nécessite des lignes budgétaires explicitement réservées à l'intégration : adaptateurs, environnements d'essai et essais interalliés. Sans cela, l'ambition dépasse la réalité. Et à mesure que les systèmes d'IA deviennent plus puissants, l'approche de l'équipe rouge devrait être institutionnalisée. Les modèles devraient être soumis à des simulations de crise non seulement par des ingénieurs, mais aussi par des linguistes, des psychologues et des opérateurs capables de repérer des faiblesses que les adversaires pourraient exploiter. Des initiatives axées sur les essais et l'évaluation existent déjà—le programme DIANA de l'OTAN a ouvert 16 centres d'essais et deux accélérateurs à l'échelle du Canada, axés sur le développement de technologies à double usage comme l'IA. Pris ensemble, cet agenda ne consiste pas à développer les capacités canadiennes à tout prix. Il s'agit de séquencer les étapes pratiques que le MDN et les FAC peuvent entreprendre aujourd'hui, tout en posant les bases pour que l'OTAN et ses partenaires alliés intègrent l'IA de manière responsable à long terme.

Conclusion

Le duel entre la Chine et les États-Unis en matière d'IA n'est pas un spectacle lointain; c'est le contexte dans lequel les choix de défense du Canada vont soit devenir un avantage pour les alliés, soit se transformer en vulnérabilité. Le Canada et d'autres démocraties disposent des bases institutionnelles et collaboratives pour faire progresser l'IA appliquée à la défense, mais leur efficacité dépend du maintien de la confiance publique, d'une gouvernance agile et d'écosystèmes d'innovation résilients.⁴⁹ Les

démocraties possèdent aussi des forces mesurables : elles possèdent les meilleurs écosystèmes de capacité de calcul au monde, et le talent pour continuer à repousser les frontières—mais l'avantage est périssable. Les rivaux autocratiques agiront rapidement là où la loi et l'éthique nous contraignent; les plateformes organisationnelles pencheront vers le profit à moins que nous n'adaptions les mesures incitatives en direction de la sécurité; et les achats seront lents à moins que les dirigeants ne favorisent délibérément la vitesse.

La tâche du MDN et des FAC ne consiste pas à rivaliser avec les superpuissances puce par puce ou modèle par modèle. Il s'agit d'être interopérable sur des échéanciers qui correspondent au rythme de nos alliés et à nos besoins opérationnels, de protéger et de mobiliser les données qui comptent, de garantir un accès aux capacités de calcul, de réformer les organisations afin que les bonnes idées atteignent les troupes avant qu'elles ne s'épuisent, et de cultiver les talents qui rendent tout cela possible. Ce faisant, le MDN et les FAC défendront non seulement leurs propres intérêts, mais renforceront aussi la logique de coalition sur laquelle repose la sécurité du Canada. L'IA ne remplacera pas la stratégie, mais elle récompensera ceux qui la considèrent comme stratégique, en transformant les valeurs en gouvernance, la gouvernance en capacité, et la capacité en un effet combiné.

En agissant délibérément, le MDN et les FAC peuvent s'assurer que l'IA renforce la prise de décision, protège la résilience dans le domaine de l'information et renforce une dissuasion crédible. Si cela est bien fait, ces capacités renforceront la sécurité du Canada et de ses alliés et démontreront que les technologies avancées peuvent être intégrées de manière responsable au service des sociétés libres et démocratiques.

Notes

- 1 Les avancées en matière d'IA dans le domaine de la défense visent à trouver un équilibre entre innovation et développement responsable et éthique, tandis que d'autres acteurs s'attachent à l'utiliser pour obtenir un avantage décisionnel. Voir : Mind Foundry, « Defence and National Security AI Strategies – The Global Landscape », 27 novembre 2025.
- 2 Meredith Chen, « China's Growing Civilian-Defence AI Ties Will Challenge US, Report Says », South China Morning Post, 8 septembre 2025. Tiré de <https://www.scmp.com/news/china/military/article/3324727/chinas-growing-civilian-defence-ai-ties-will-challenge-us-report-says>.
- 3 Cullen O'Keefe, « Chips for Peace: How the U.S. and Its Allies Can Lead on Safe and Beneficial AI », Lawfare, 10 juillet 2024. Tiré de <https://www.lawfaremedia.org/article/chips-for-peace-how-the-u.s.-and-its-allies-can-lead-on-safe-and-beneficial-ai>.
- 4 Ministère de la Défense nationale du Canada, Commandement et contrôle pan-domaine (C2PD) Document de conception, Gouvernement du Canada, 9 décembre 2024. Tiré de <https://www.canada.ca/fr/ministere-defense-nationale/organisation/rapports-publications/commandement-contrôle-pan-domaine.html>.
- 5 Branka Marijan, « The Dilemma of Dual-Use AI », The Ploughshares Monitor, 18 septembre 2023. Tiré de <https://ploughshares.ca/the-dilemma-of-dual-use-ai/>.
- 6 Karen M. Sutter, U.S. Export Controls and China: Advanced Semiconductors, CRS Report R48642, Congressional Research Service, 19 septembre 2025. Tiré de <https://www.congress.gov/crs-product/R48642>.
- 7 Enrique Dans, « Super Apps: A Path to Surveillance in China and Russia », Center for European Policy Analysis, 12 septembre 2025. Tiré de <https://cepa.org/article/super-apps-a-path-to-surveillance-in-china-and-russia/>.
- 8 KPMG, « Future Forward: Following the Money in AI », 2025. Tiré de <https://kpmg.com/xx/en/our-insights/value-creation/future-forward.html>.
- 9 Erica Stanford, « Autonomous AI: Who Is Responsible When AI Acts Autonomously and Things Go Wrong? », Global Legal Insights, 15 mai 2025. Tiré de <https://www.globallegalinsights.com/practice-areas/ai-machine-learning-and-big-data-laws-and-regulations/autonomous-ai-who-is-responsible-when-ai-acts-autonomously-and-things-go-wrong/>.
- 10 Ministère de la Défense nationale et Forces armées canadiennes, La Stratégie d'IA, Gouvernement du Canada, 7 mars 2024. Tiré de <https://www.canada.ca/content/dam/dnd-mdn/documents/reports/ai-ia/mdn-fac-strategie-ia.pdf>.
- 11 Akshay Kulkarni, « AI-Generated Wildfire Images Spreading Misinformation in B.C., Fire Officials Warn », CBC News, 6 août 2025.
- 12 Ministère de la Défense nationale, « La Stratégie d'IA du ministère de la Défense nationale et des Forces armées canadiennes », 7 mars 2024. Tiré de <https://www.canada.ca/content/dam/dnd-mdn/documents/reports/ai-ia/dndcaf-ai-strategy.pdf>.
- 13 Ministère de la Défense nationale, Sécurité, souveraineté et prospérité : la Stratégie industrielle de défense du Canada, février 2026. Tiré de <https://www.pm.gc.ca/fr/nouvelles/communiqués/2026/02/17/premier-ministre-carney-lance-la-premiere-strategie-industrielle>.
- 14 Nicolas Chaillan, « The Fast Track to Mission-Ready

- AI: Buy What Works, Skip the Build », Government Technology Insider, 8 juillet 2025. Tiré de <https://governmenttechnologyinsider.com/the-fast-track-to-mission-ready-ai-buy-what-works-skip-the-build/>.
- 15 Margarida Silva, Jasper van Teeffelen et Çağrı Çavuş, « Big Tech Acquires a New Company Every 11 Days », SOMO, 15 avril 2025, <https://www.somo.nl/big-tech-acquires-a-new-company-every-11-days/>.
 - 16 Didi Tang et Collin Binkley, « Pentagon-Funded Research at Colleges Has Aided the Chinese Military, a House GOP Report Says », AP News, 5 septembre 2025. Tiré de <https://apnews.com/article/china-pentagon-funding-research-military-bf8640d0e04c01614af513350078d58c>.
 - 17 U.S. National Security Agency et Cybersecurity and Infrastructure Security Agency, Use Secure Cloud Key Management Practices, mars 2024. Tiré de <https://media.defense.gov/2024/Mar/07/2003407858/-1/-1/0/CSI-CloudTop10-Key-Management.PDF>.
 - 18 Office of the Under Secretary of Defense for Research and Engineering, Software Engineering for Continuous Delivery of Warfighting Capability, U.S. Department of Defense, avril 2023. Tiré de <https://www.cto.mil/wp-content/uploads/2023/07/SWE-Guide-April2023.pdf>.
 - 19 James Kavanagh, « AI Model Lifecycle Governance », Ethos AI, 23 juin 2025. Tiré de <https://www.ethos-ai.org/p/ai-model-lifecycle-governance?>
 - 20 Cybersecurity and Infrastructure Security Agency, Securing the Software Supply Chain: Recommended Practices for Suppliers, Department of Homeland Security, septembre 2022. Tiré de https://www.cisa.gov/sites/default/files/2024-08/SECURING_THE_SOFTWARE_SUPPLY_CHAIN_SUPPLIERS_508.pdf.
 - 21 Par exemple, la loi américaine CLOUD Act impose aux prestataires relevant de la juridiction des États-Unis de conserver et de communiquer les données, dont ils ont la possession, la garde ou le contrôle, que ces données se trouvent ou non sur le territoire américain.
 - 22 Forum économique Mondial et Accenture, Blueprint to Action: China's Path to AI-Powered Industry Transformation, janvier 2025. Tiré de https://reports.weforum.org/docs/WEF_Blueprint_to_Action_Chinas_Path_to_AI-Powered_Industry_Transformation_2025.pdf.
 - 23 Robert O. Work et Tara Murphy Dougherty, « It's Time for the Pentagon to Take Data Principles More Seriously », War on the Rocks, 6 octobre 2020. Tiré de <https://warontherocks.com/2020/10/its-time-for-the-pentagon-to-take-data-principles-more-seriously/>.
 - 24 Harry Davies et Yuval Abraham, « Revealed: Microsoft Deepened Ties with Israeli Military to Provide Tech Support During Gaza War », The Guardian, 23 janvier 2025. Tiré de <https://www.theguardian.com/world/2025/jan/23/israeli-military-gaza-war-microsoft>.
 - 25 Brodi Kotila et al., Strengthening the Defense Innovation Ecosystem, RAND Corporation, 7 mars 2023. Tiré de https://www.rand.org/content/dam/rand/pubs/research_reports/RR1300/RR1352-1/RAND_RRA1352-1.pdf.
 - 26 Stefan Vladislavjev, « Surveying China's Digital Silk Road in the Western Balkans », War on the Rocks, 3 août 2021. Tiré de <https://warontherocks.com/2021/08/surveying-chinas-digital-silk-road-in-the-western-balkans/>.
 - 27 Thomas Morley et Matthew Schrader, « Huawei Espionage Arrests in Poland: A Wake-Up Call to Europe », German Marshall Fund of the United States, consulté le 25 septembre 2025. Tiré de <https://www.gmfus.org/news/huawei-espionage-arrests-poland-wake-call-europe>.
 - 28 Innovation, Sciences et Développement économique Canada, « Énoncé de politique - Sécuriser le système de télécommunications au Canada », Gouvernement du Canada, 19 mai 2022. Tiré de <https://www.canada.ca/fr/innovation-sciences-developpement-economique/nouvelles/2022/05/enonce-de-politique--securiser-le-systeme-de-telecommunications-au-canada.html>.
 - 29 Darren Death, « Understanding and Addressing Supply Chain Risks in AI Systems », LinkedIn, 8 janvier 2025, <https://www.linkedin.com/pulse/understanding-addressing-supply-chain-risks-ai-systems-death-kz2jc>.
 - 30 Chambre des communes du Canada, Comité permanent de la défense nationale, Témoignages, 45^e législature, 1^{re} session, réunion n° 9, 23 octobre 2025. Tiré de <https://www.noscommunes.ca/documentviewer/fr/45-1/NDDN/reunion-9/temoignages>.
 - 31 Chloe Autoio, Kate Cummings, Brinson S. Elliott et Beth Simone Noveck, A Snapshot of Artificial Intelligence Procurement Challenges: Diagnosing Perceived and Actual Risks Impeding Responsible AI Acquisition, The GovLab, 2023. Tiré de <https://files.thegovlab.org/a-snapshot-of-ai-procurement-challenges-june2023.pdf>.
 - 32 Akhil Gupta, « Government AI Adoption: Unique Challenges in Pricing and Procurement », Agentic AI Pricing, 6 janvier 2025. Tiré de <https://www.agenticai-pricing.com/government-ai-adoption-unique-challenges-in-pricing-and-procurement/>.
 - 33 Recherche et développement pour la défense Canada (RDDC) mène depuis longtemps des travaux sur l'IA, notamment dans les domaines de la connaissance de la situation, de la surveillance, de la cyberdéfense et de la détection des menaces. Parmi les initiatives susceptibles de soutenir le développement et la commercialisation de solutions canadiennes d'IA pour la défense figurent le programme Innovation pour la défense, l'excellence et la sécurité (IDEES) et le Bureau de recherche, d'ingénierie et de leadership avancés en matière d'innovation et de science (BOREALIS). Le programme Mobilisation des idées nouvelles en matière de défense et de sécurité (MINDS) joue un rôle distinct, axé sur la recherche, l'expertise externe et l'élaboration des politiques.
 - 34 Par l'intermédiaire du service d'adoption rapide du DIANA de l'OTAN, le MDN et les FAC sont en voie d'acquiescer un véhicule autonome sans équipage auprès d'une entreprise appelée HonuWorx. Ce véhicule sera contrôlé au moyen d'une plateforme de mission infonuagique et contribuera à la capacité du MDN et des FAC d'entretenir, d'exploiter et de manipuler des infrastructures en eaux profondes ainsi que d'autres objets sous-marins.
 - 35 Alex McPhail, Alexander Rudolph et Philippe Lagassé, rapport final du projet « Aperçu et analyse de l'approvisionnement agile de la Défense (AAAAD) », EXA Consulting Group, 10 juillet 2025. Tiré de <https://static1.squarespace.com/static/5cd08376797f7421f5ea7c-c/t/68af61b380a0f3571c695ae9/1756324275338/Final+Report++Defence+Agile+Procurement+Insights+and+Analysis.pdf>.
 - 36 Carlo Munoz, « Le Pentagone lance l'initiative d'accélération de l'infonuagique de la JWCC », Janes, 31 octobre 2024. Tiré de <https://www.janes.com/osint-insights/defence-news/defence/pentagon-rolls-out-jwcc-cloud-accelerator-initiative>.
 - 37 U.S. Defense Innovation Board, Scaling Nontraditional Defense Innovation, U.S. Department of Defense, 8 janvier 2025. Tiré de <https://innovation.defense.gov/Portals/63/DIB%20Scaling%20Nontraditional%20Defense%20Innovation%20250113%20PUBLISHED.pdf>.
 - 38 MITRE Corporation, AI Red Teaming: Advancing Safe and Secure AI Systems, juillet 2024. Tiré de <https://www.mitre.org/sites/default/files/2024-07/PR-24-01820-4-AI-Red-Teaming-Advancing-Safe-Secure-AI-Systems.pdf>.
 - 39 Pour obtenir d'autres lignes directrices sur ces pratiques d'évaluation, voir le *Responsible AI Toolkit* du département de la Défense des É.-U., qui propose des outils d'évaluation du cycle de vie et d'assurance pour les systèmes d'IA; voir aussi le JSP 936 du ministère de la Défense du R.-U., qui établit les exigences pour des capacités d'AI de défense fiables, sécuritaires et robustes. Voir : Department of Defense, *Responsible Artificial Intelligence (RAI) Toolkit*, Chief Digital and Artificial Intelligence Office, 14 novembre 2023, <https://rai.tradewindai.com/>; Ministry of Defence, JSP 936: *Dependable Artificial Intelligence (AI) in Defence (Part 1: Directive)*, 13 novembre 2024. Tiré de <https://www.gov.uk/government/publications/jsp-936-dependable-artificial-intelligence-ai-in-defence-part-1-directive>.
 - 40 U.S. Congress, Senate Committee on Small Business and Entrepreneurship, Golden Age of American Innovation: Reforming SBIR-STTR for the 21st Century, S. Hrg. 119-20, 119th Cong., 1st sess., 5 mars 2025. Tiré de <https://www.digitaljournal.com/business/canadas-innovation-pipeline-is-stalling-sir-michael-houghton-calls-for-a-vc-mind-set-shift/article>.
 - 41 U.S. Congress, Senate Committee on Small Business and Entrepreneurship, Golden Age of American Innovation: Reforming SBIR-STTR for the 21st Century, S. Hrg. 119-20, 119th Cong., 1st sess., 5 mars 2025. Tiré de <https://www.congress.gov/event/119th-congress/senate-event/LC74425/text>.
 - 42 IBM, « Qu'est-ce que la gestion des coûts liés au cloud? », 5 octobre 2023. Tiré de <https://www.ibm.com/fr-fr/think/topics/cloud-cost-management>.
 - 43 Secrétariat du Conseil du Trésor du Canada, *Livre blanc du gouvernement du Canada sur la souveraineté des données et le nuage public*, Gouvernement du Canada, 2018. Tiré de <https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/innovations-gouvernementales-numeriques/services-informatique-nuage/souverainete-numerique/qc-livre-blanc-souverainete-donnees-nuage-public.html>.
 - 44 Organisation du Traité de l'Atlantique Nord, « Approche de l'OTAN pour la lutte contre les menaces informationnelles », 3 février 2025. Tiré de <https://www.nato.int/fr/what-we-do/wider-activities/natos-approach-to-counter-information-threats>.
 - 45 Ann M. Fitz-Gerald, Carsten Maple et Halyna Padalko, « Collaborative AI Governance: A Policy Roadmap for Canada and the UK », Royal United Services Institute, 13 novembre 2024. Tiré de <https://www.rusi.org/explore-our-research/publications/commentary/collaborative-ai-governance-policy-roadmap-canada-and-uk>.
 - 46 Steve Feldstein, « The Global Expansion of AI Surveillance », Carnegie Endowment for International Peace, 17 septembre 2019. Tiré de <https://carnegieendowment.org/research/2019/09/the-global-expansion-of-ai-surveillance?lang=en>.
 - 47 Centre canadien pour la cybersécurité, Évaluation des cybermenaces nationales 2025-2026, Gouvernement du Canada, 2024. Tiré de <https://www.cyber.gc.ca/sites/default/files/evaluation-cybermenaces-nationales-2025-2026-f.pdf>.
 - 48 Service canadien du renseignement de sécurité, « Protection des jeunes pousses technologiques : exploitation des concours de pitch internationaux », 8 septembre 2025.
 - 49 Pew Research Center, Representative Democracy Remains a Popular Ideal, but People Around the World Are Critical of How It's Working, Washington, DC : Pew Research Center, 28 février 2024. Tiré de https://www.pewresearch.org/global/wp-content/uploads/sites/2/2024/02/gap_2024.02.28_democracy-closed-end-report.pdf.



Les contrôleurs interarmées de la finale de l'attaque (CIFA) canadiens et français installent des lasers pour les frappes aériennes et regardent à travers les jumelles pour s'assurer que la zone de largage est dégagée pendant l'ex MAPLE STRIKE dans la zone de largage Shaver à Jimmy Lake, en Alberta.

Caporale Connie Valin, photo des Forces armées canadiennes

L'interopérabilité des alliés sous pression : l'IA, l'approvisionnement et l'avenir de la cohésion en matière de défense

SAMUEL PAQUETTE ET MAJOR TYLER CURRIE

Samuel Paquette exerce les fonctions d'analyste des politiques au sein du Centre d'IA du MDN et des FAC. Il a récemment obtenu une maîtrise en affaires internationales à l'Université Carleton. Auparavant, il a travaillé comme chercheur diplômé auprès de l'État-major interarmées stratégique à Recherche et développement pour la défense Canada (RDDC).

Tyler Currie occupe le poste d'agent d'intégration et d'accélération de l'IA des FAC au Centre d'IA du MDN et des FAC. Tyler a passé 16 ans au sein de la Branche des services du renseignement et a participé à des opérations de déploiement en Afghanistan ainsi qu'à des missions internationales auprès du Commandement allié de forces interarmées de Naples. Il est titulaire d'une maîtrise en études politiques de l'Université Queen's ainsi que d'une maîtrise en gestion-option Intelligence artificielle (MMAI) de la Smith School of Business de l'Université Queen's.

L'intelligence artificielle (IA) s'impose progressivement comme le tissu unificateur des alliances de défense modernes.

Elle relie les données, les plateformes et la prise de décisions au-delà des frontières. Pour le ministère de la Défense nationale (MDN) et les Forces armées canadiennes (FAC), de même que pour l'Organisation du Traité de l'Atlantique Nord (OTAN), le principal défi consiste à s'assurer que l'adoption de l'IA renforce constamment l'interopérabilité, fondement essentiel de l'efficacité des opérations interarmées. Les alliés subissent une pression constante attribuable aux pénuries de semi-conducteurs de pointe, à l'évolution des marchés technologiques, à la rigidité des processus d'approvisionnement ainsi qu'à la diversité des règles et des normes encadrant l'IA. Ces contraintes rendent le renforcement de l'interopérabilité d'autant plus crucial. Elles influent sur la rapidité avec laquelle les alliés peuvent intégrer de nouvelles capacités, sur la fiabilité des communications entre les systèmes sur le terrain ainsi que sur l'efficacité du soutien que les outils fondés sur l'IA apportent aux commandants pendant les opérations. Les enjeux sont considérables. Grâce à des normes communes et à des stratégies d'approvisionnement résilientes, l'IA peut accélérer la prise de décisions, approfondir l'intégration et procurer un avantage décisif dans l'espace de combat.

L'OTAN qualifie l'IA de capacité transformatrice. Toutefois, sa pleine exploitation repose sur des environnements infonuagiques sécurisés conformes aux normes de l'OTAN, sur des réseaux alliés interconnectés sans rupture et sur des langages de données communs, permettant aux plateformes canadiennes de communiquer directement avec les systèmes de l'Alliance. Ces fondements permettent à l'IA de raccourcir les cycles décisionnels, d'améliorer la clarté du renseignement et de renforcer la dissuasion. L'obtention de cet avantage repose sur des normes communes, des activités conjointes d'essai et de certification ainsi que des architectures de données communes. La valeur opérationnelle de l'IA repose sur le maintien du jugement humain aux moments critiques, de sorte que les commandants demeurent responsables de l'emploi de la force et que la supervision humaine s'exerce durant tout le cycle décisionnel. En misant sur ces facteurs habilitants, le MDN et les FAC ainsi que l'OTAN peuvent faire en sorte que l'IA renforce l'interopérabilité au quotidien et transforme les progrès technologiques en avantage collectif.

Parallèlement, plusieurs facteurs compliquent les opérations des alliés. La volatilité des marchés des puces électroniques, des capacités infonuagiques et des minéraux critiques fragilise la disponibilité opérationnelle; les frictions persistantes liées à l'approvisionnement ralentissent la mise en service de capacités d'IA en évolution rapide; enfin, les normes et les cadres de gouvernance émergents de l'OTAN doivent gagner en maturité pour garantir des systèmes fiables et interopérables. Ensemble, ces pressions influent sur la posture d'approvisionnement du Canada et déterminent dans quelle mesure le pays peut demeurer en phase avec ses alliés à mesure que l'IA accélère le rythme de la guerre moderne.

Pour le Canada, puissance moyenne résolument engagée et voix digne de confiance au sein de l'OTAN, l'approvisionnement et la gouvernance constituent des leviers de première importance pour la sécurité. Ils joueront un rôle essentiel dans l'atteinte de l'objectif de la *Stratégie d'intelligence artificielle du MDN et des FAC*, soit devenir une organisation dotée de capacités d'IA d'ici 2030. Lorsque leur conception intègre l'interopérabilité, ils créent les conditions permettant au MDN et aux FAC de s'intégrer harmonieusement aux forces alliées, d'apporter des capacités distinctives et de demeurer un partenaire crédible de la défense collective. En intégrant des pratiques d'approvisionnement modulaires, en favorisant les normes ouvertes et en harmonisant les cadres de gouvernance avec les principes de l'OTAN, le MDN et les FAC peuvent contribuer à garantir la fiabilité, l'agilité et le déploiement rapide des nouveaux systèmes d'IA dans l'ensemble de l'Alliance. Ces choix font de l'IA un véritable multiplicateur de force, ce qui accroît la capacité du MDN et des FAC à contribuer à la dissuasion, approfondit la collaboration entre les alliés et préserve la pertinence du Canada dans l'espace de combat de demain.

La volatilité des marchés et la disponibilité opérationnelle

La course à l'adoption de l'IA dans le domaine de la défense ne se déroule pas en vase clos. Elle est directement tributaire de la volatilité des marchés mondiaux des composantes matérielles, des infrastructures et des talents qui rendent l'IA possible. L'accès sécurisé aux puces électroniques de pointe, aux capacités infonuagiques et aux compétences spécialisées est devenu une nécessité stratégique. Sans ces ressources, même les stratégies de défense les plus ambitieuses risquent de tourner court.

Cette problématique s'articule principalement autour de la chaîne d'approvisionnement mondiale des puces électroniques. L'entraînement de modèles d'IA avancés repose sur des processeurs à haut rendement, comme le modèle H100 de Nvidia. Ces puces sont produites presque exclusivement par une seule entreprise qui contrôle plus de 90 % de la production mondiale des semi-conducteurs les plus avancés.¹ Pour les forces armées alliées, cette situation crée une disparité dans l'accès à la puissance de calcul, ce qui risque de fragmenter le rythme auquel les pays peuvent déployer des capacités interopérables fondées sur l'IA. L'explosion de la demande dans les secteurs civils fait grimper les coûts et restreint la disponibilité.² Pour les forces armées, les retards dans l'acquisition des capacités de calcul se traduisent directement par des lacunes sur le plan opérationnel.

L'infrastructure infonuagique revêt une importance tout aussi cruciale, puisque l'accès combiné aux puces électroniques et aux services infonuagiques détermine la capacité d'un État à entraîner, à déployer et à faire évoluer les systèmes d'IA. Les centres de données sont eux-mêmes devenus des actifs de sécurité

nationale, à la fois indispensables et vulnérables aux cyberattaques, aux menaces internes et au sabotage. Les gouvernements et l'industrie investissent massivement pour protéger ces installations, conscients que les écosystèmes informatiques résilients confèrent des avantages durables dans les domaines comme les cyberopérations, les systèmes autonomes et la surveillance spatiale.³ Sans des capacités infonuagiques sécurisées et évolutives, les alliés ne peuvent ni entraîner des modèles communs, ni échanger des données opérationnelles, ni utiliser des outils fondés sur l'IA dans le cadre des missions multinationales.

Le contexte géopolitique accentue davantage cette volatilité. Les chaînes d'approvisionnement en minéraux critiques demeurent concentrées et les restrictions à l'exportation limitent parfois l'accès aux terres rares et à d'autres intrants essentiels. Ces perturbations font augmenter les coûts et retardent les projets d'infrastructure. Elles montrent à quel point il est important que le MDN et les FAC ainsi que leurs alliés renforcent la résilience des chaînes d'approvisionnement, diversifient leurs sources d'approvisionnement et investissent dans des capacités nationales et alliées afin de maintenir leur disponibilité opérationnelle à long terme.⁴ Pour le Canada, dont la capacité nationale de fabrication de semi-conducteurs demeure limitée, ces perturbations présentent un risque accru comparativement à celui auquel font face les alliés disposant d'une base industrielle plus diversifiée.

Au sein de l'OTAN, certains membres peuvent atténuer les chocs du marché, en subventionnant la production nationale de semi-conducteurs, en investissant dans les entreprises en démarrage spécialisées dans l'IA ou en constituant des réserves de minéraux critiques.⁵ D'autres apportent leur contribution en mettant leurs ressources en commun, en appuyant des initiatives multinationales ou en tirant parti de leurs forces régionales.⁶ L'essentiel réside dans le fait que ces approches différentes se complètent, ce qui garantit un développement équilibré des capacités et consolide l'intégration du commandement et du contrôle au sein de l'Alliance. En agissant collectivement, l'OTAN peut transformer la diversité des investissements nationaux en avantage commun.

Pour le Canada, les enjeux sont immédiats. Le pays est confronté à des défis persistants pour développer ses capacités sécurisées d'infonuagique et d'IA. Il dispose d'une capacité limitée de fabrication de matériel informatique de pointe et s'appuie sur un secteur des technologies de défense de taille modeste, mais en croissance constante. En tant que puissance moyenne, il ne peut compter uniquement sur sa taille ou ses dépenses. Il doit plutôt consolider sa position en s'appuyant sur la résilience et la collaboration. Alors que les alliés de grande taille peuvent absorber les chocs par la seule force de leurs investissements, le Canada devrait privilégier la planification de la résilience, la constitution de réserves de composantes critiques, la diversification des chaînes d'approvisionnement et le renforcement des partenariats avec ses alliés dans le domaine de la capacité de calcul. Cet effort est déjà en cours. Depuis 2016, le Canada

a consacré plus de 4,4 milliards de dollars à la recherche en IA et aux infrastructures numériques, notamment dans le cadre de la *Stratégie canadienne sur la capacité de calcul souveraine pour l'IA de 2025*, qui prévoit un investissement de 2 milliards de dollars pour l'établissement d'une infrastructure infonuagique souveraine, à l'expansion de la capacité nationale de calcul et à la réduction de la dépendance envers les plateformes appartenant à des intérêts étrangers.⁷ Le Canada possède également l'une des plus importantes réserves mondiales d'éléments des terres rares. Une gestion responsable de ces ressources peut contribuer à la sécurité de l'approvisionnement des alliés pendant de nombreuses années.⁸

La préparation à l'IA commence par la sécurisation des fondements de l'écosystème numérique. Les processeurs de pointe, une infrastructure infonuagique résiliente et un approvisionnement fiable en minéraux critiques sont aussi essentiels à la défense que les navires, les aéronefs ou les satellites. Ils déterminent la capacité des outils fondés sur l'IA à fonctionner à grande échelle et en coordination avec les alliés. Pour le Canada, cela signifie qu'il doit utiliser stratégiquement les leviers dont dispose une puissance moyenne : investir au pays, collaborer avec les partenaires étrangers et anticiper les cycles du marché avant qu'ils ne dégénèrent en crises. En renforçant ainsi cette résilience, le MDN et les FAC peuvent faire en sorte que l'adoption de l'IA consolide la cohésion de l'Alliance et préserve leur rôle de partenaire fiable et compétent au sein de l'OTAN.

Les frictions liées à l'approvisionnement

Même lorsque les fonds sont disponibles, les systèmes d'approvisionnement peinent à suivre le rythme rapide de l'innovation en matière d'IA. Les processus traditionnels d'approvisionnement en défense ont été conçus pour des navires et des aéronefs dont le développement s'échelonne sur des décennies, et non pour des algorithmes susceptibles de devenir obsolètes en quelques mois. Par conséquent, les organisations peuvent cerner des besoins urgents, mais mettre des années à passer de la définition des exigences à l'attribution des contrats puis à la livraison des capacités. Lorsqu'elles sont finalement mises en service, ces capacités peuvent déjà être dépassées.

La modernisation de l'infrastructure infonuagique du ministère de la Défense des États-Unis illustre bien cette vulnérabilité. Annoncée pour la première fois en 2017, l'initiative *Joint Enterprise Defense Infrastructure* (JEDI) visait à regrouper les services infonuagiques dans le cadre d'un contrat unique de 10 milliards de dollars américains attribué à une seule entreprise.⁹ Des années de contestations judiciaires ont suivi et, en 2021, le contrat a été annulé, étant devenu obsolète avant même sa mise en œuvre. Le projet *Joint Warfighter Cloud Capability* (JWCC), un modèle plus souple à fournisseurs multiples, l'a remplacé en 2022.¹⁰ La leçon est claire : les contrats rigides attribués à un fournisseur unique risquent d'enfermer les forces armées

dans des solutions peu flexibles qui ne peuvent pas évoluer au même rythme que les changements technologiques.

Le même phénomène s'observe dans d'autres domaines de l'IA en mutation rapide. Au terme d'un processus d'approvisionnement, des versions plus performantes peuvent déjà avoir supplanté les modèles ou les capteurs initialement précisés. Dans les domaines comme les drones autonomes, la cyberdéfense et le traitement du langage naturel, les cycles d'acquisition pluriannuels risquent d'aboutir à des systèmes nouveaux pour les combattants, mais déjà surpassés par les nouvelles capacités d'adversaires, dont les cycles d'acquisition sont plus courts.¹¹

Toutefois, d'autres États se heurtent à moins de contraintes. La stratégie centralisée de fusion civilo-militaire de la Chine transpose rapidement l'IA de la recherche civile aux applications militaires, sans examen public ni mise en concurrence transparente. Les entreprises d'État ayant des liens directs avec l'Armée populaire de libération de la Chine obtiennent ces contrats, qui accélèrent le développement de capacités, telles que les véhicules autonomes, la guerre électronique et la reconnaissance automatisée des cibles.¹² Même si le MDN et les FAC ainsi que les alliés rejettent, à juste titre, cette approche pour des raisons d'ordre éthique et de gouvernance, la rapidité avec laquelle les adversaires peuvent déployer les capacités d'IA montre à quel point il est urgent de moderniser les processus d'approvisionnement afin de demeurer concurrentiels.

Pour le MDN et les FAC, cette réalité se traduit par des défis bien connus, mais persistants. Comme chez de nombreux alliés, la culture de l'approvisionnement est marquée par une forte aversion au risque et par de multiples niveaux d'examen et de vérification de la conformité, ce qui peut prolonger les délais sur plusieurs décennies.¹³ Ces processus visent à assurer une reddition de comptes rigoureuse dans le cas de grandes plateformes à longue durée de vie, mais ils ne correspondent pas au rythme de l'innovation en IA. Par conséquent, l'intégration de capacités qui évoluent rapidement, au même rythme que chez les partenaires qui expérimentent des approches plus agiles et que chez les concurrents capables de déployer rapidement de nouveaux systèmes, demeure un défi constant.

L'approvisionnement agile est essentiel non seulement pour suivre le rythme de l'innovation en IA, mais aussi pour garantir que tous les fournisseurs respectent les normes de cybersécurité de la défense. Les modèles d'approvisionnement traditionnels reposent sur des contrats monolithiques qui aboutissent souvent à la livraison de systèmes fermés, de type « boîte noire », accumulant au fil du temps une dette technique importante : les logiciels sont difficiles à mettre à jour, les vulnérabilités persistent et les chaînes opaques de sous-traitance compliquent l'évaluation des risques liés à la chaîne d'approvisionnement. À l'inverse, les architectures modulaires et ouvertes permettent l'application continue de correctifs, la modernisation des composants au fur et à mesure ainsi qu'une plus grande transparence dans l'évaluation des fournisseurs. Plutôt que de concentrer les

risques dans un seul écosystème propriétaire, ces architectures permettent de les répartir et de les gérer au moyen de composants interopérables. Ainsi, l'approvisionnement agile renforce la résilience, favorise l'adoption de solutions à code source ouvert par les fournisseurs et veille à ce que ceux-ci respectent un niveau de cybersécurité commun conforme aux exigences du secteur de la défense. Le MDN et les FAC appuient activement l'évolution des processus d'approvisionnement afin de permettre l'intégration de l'IA au rythme exigé par les opérations modernes. Cette démarche comprend l'essai d'approches plus agiles, la mise en place de mécanismes, favorisant le prototypage rapide, et l'amélioration continue. Ainsi, les nouvelles capacités demeurent pertinentes dans le temps, elles peuvent être actualisées au gré des avancées technologiques et être conçues dès le départ pour être interopérables avec les systèmes des alliés.

Il existe toutefois des pistes prometteuses. Le MDN et les FAC ont également commencé à tester de nouvelles approches dans le cadre du programme canadien Innovation pour la défense, l'excellence et la sécurité (IDEES). Ce programme a recours à des concours, à des essais et à des environnements d'expérimentation pour accélérer l'innovation.¹⁴ Ces outils permettent de mettre rapidement de nouvelles idées à l'essai à faible coût, sans engager les FAC à long terme avant que les technologies aient démontré leur valeur. Certains experts soulignent également l'intérêt de mécanismes contractuels plus souples, comme les ententes de type « Other Transaction Authorities » (OTA) utilisés par la *Defense Innovation Unit* des États-Unis, qui facilitent le prototypage rapide et permettent de contourner bon nombre des lourdeurs administratives associées aux processus d'approvisionnement traditionnels.¹⁵

Pour le MDN et les FAC, l'objectif n'est pas d'aller vite à tout prix, mais d'avancer rapidement avec discernement. Les contrats agiles et les projets pilotes devraient s'appuyer directement sur des architectures communes de données, des mécanismes modulaires de certification et des cadres d'assurance de l'OTAN. Ainsi, l'approvisionnement devient un vecteur de cohésion, en veillant à ce que les nouvelles capacités d'IA soient non seulement livrées plus rapidement, mais également déployées de manière à renforcer la confiance entre les alliés et l'interopérabilité de leurs systèmes.

Les normes de l'OTAN et la cohésion

L'avantage de l'OTAN repose sur l'interopérabilité, c'est-à-dire sur la capacité des alliés à échanger des données, à se fier aux systèmes de leurs partenaires et à combattre comme une seule force. En pratique, cette capacité exige davantage que des équipements compatibles. Elle dépend de règles, de normes et de cadres de gouvernance communs qui permettent à chaque État membre d'avoir confiance dans la conception, les essais et le déploiement des systèmes d'IA. Comme les alliés adoptent des approches réglementaires différentes, l'Alliance a fait de l'élaboration de normes une priorité.

L'un des exemples de ces travaux émergents sur les normes est le concept « AI Exchange » actuellement à l'étude au sein de certains pays de l'OTAN. L'idée consiste à mettre en place un mécanisme commun, permettant de tester et de valider les systèmes d'IA en fonction de principes convenus à l'échelle de l'Alliance. S'il est mis en œuvre, ce « passeport » fonctionnerait un peu comme une cote de sécurité pour les technologies : lorsqu'un système est certifié par un pays allié, les autres pourraient l'adopter sans devoir reprendre tout le processus de validation. Cette approche permettrait de réduire les coûts et les délais tout en donnant aux forces armées l'assurance que les outils fondés sur l'IA répondent aux exigences de l'OTAN en matière de sécurité, de responsabilité et de fiabilité.

Pour le MDN et les FAC, cette initiative présente un double avantage. D'abord, elle offrirait un moyen d'éviter le doublement des processus de certification et de veiller à ce que les technologies développées au Canada soient prêtes à être utilisées par les alliés dès leur mise en service. Ensuite, elle donnerait au MDN et aux FAC l'occasion de contribuer à l'élaboration même du cadre de référence en mettant à profit leur expérience en matière d'IA responsable. Après avoir contribué à l'avancement des normes internationales par l'intermédiaire de l'Organisation de coopération et de développement économique (OCDE), du Processus d'Hiroshima du Groupe des sept (G7) et du Sommet sur l'intelligence artificielle responsable dans le domaine militaire, le MDN et les FAC sont bien placés pour transposer cette expérience dans le contexte opérationnel de l'OTAN. L'harmonisation des processus d'approvisionnement avec un tel mécanisme contribuerait à garantir que les systèmes canadiens, qu'il s'agisse d'outils de commandement infonuagiques ou de plateformes de surveillance reposant sur l'IA, s'intègrent harmonieusement à ceux des pays alliés.

Plus généralement, *AI Exchange* montre comment l'OTAN peut transformer les différences nationales en une force collective. Les États membres peuvent légiférer ou réglementer l'IA de différentes façons, mais ce « passeport » permettrait d'instaurer un langage commun de confiance. Il illustre la capacité de l'Alliance à coordonner ses activités sans compromettre la souveraineté nationale, de sorte qu'une innovation réalisée dans un pays puisse devenir une capacité accessible à tous.

Le mécanisme *AI Exchange* offre aux puissances moyennes comme le Canada un moyen concret d'éviter de dépendre de systèmes incompatibles avec leurs priorités en matière de défense, tout en réduisant le risque d'acquiescer des solutions souveraines qui ne seraient pas interopérables avec celles des alliés. Par exemple, des capacités souveraines de renseignement, de surveillance et de reconnaissance, de logistique ou d'aide à la décision fondées sur l'IA pourraient être difficiles à intégrer à d'autres systèmes lorsque les normes d'assurance diffèrent. En fournissant une norme commune d'assurance, *AI Exchange* permet aux puissances moyennes de conserver une certaine marge de manœuvre pour convenir de garanties techniques communes et évite que les

États les plus puissants n'imposent leurs normes uniquement en raison de leur taille. Ces travaux arrivent à point nommé, puisque les alliés mettent en place des modèles de gouvernance distincts. La *Loi sur l'intelligence artificielle* de l'Union européenne (UE) est la plus ambitieuse à ce jour. Elle établit un cadre exhaustif, fondé sur les risques qui s'applique à la quasi-totalité des usages de l'IA.¹⁶ Elle impose des exigences rigoureuses aux systèmes à haut risque, notamment ceux utilisés pour l'identification biométrique, les infrastructures essentielles et les soins de santé. Bien que les applications militaires soient exemptées de son champ d'application, cette loi influence néanmoins le développement des technologies à double usage, lesquelles franchissent souvent la frontière entre les secteurs civil et militaire.¹⁷ Pour l'OTAN, cela signifie que l'environnement réglementaire européen exercera une influence considérable sur la manière dont les entreprises développent les systèmes d'IA ainsi que sur les conditions dans lesquelles ces systèmes pourront être partagés entre les pays.

Les États-Unis ont choisi une approche différente, en privilégiant des orientations propres à certains secteurs, et des cadres fondés sur des principes plutôt qu'une loi unique. Le plan directeur *Blueprint for an AI Bill of Rights* de la Maison-Blanche et le cadre *AI Risk Management Framework* du *National Institute of Standards and Technology* (NIST) en sont des exemples marquants, auxquels s'ajoutent plusieurs décrets présidentiels demandant aux organismes fédéraux de protéger l'innovation tout en préservant les droits.¹⁸ Cette approche favorise le leadership du secteur privé et l'adoption rapide des technologies. Toutefois, parce qu'elle est décentralisée, elle exige souvent des mécanismes d'assurance supplémentaires de l'OTAN avant que les systèmes américains puissent être pleinement utilisés dans les opérations alliées.

L'évolution de cette réflexion au Canada s'est révélée plus complexe. Présentée en 2022, la *Loi sur l'intelligence artificielle et les données* (LIAD) visait à établir un cadre national de réglementation de l'IA fondé sur le niveau de risque. Inspirée en partie du modèle européen tout en conservant la souplesse de l'approche américaine, elle cherchait à concilier l'innovation et la surveillance réglementaire. Toutefois, la prorogation du Parlement, en janvier 2025, a entraîné la mort au Feuilleton du projet de la LIAD, laissant le Canada sans loi consacrée à l'IA.¹⁹ Cette expérience a néanmoins enrichi le débat national et permis de mieux définir les orientations futures. Le Canada continue d'appliquer les lois existantes en matière de droits de la personne, de protection des renseignements personnels et de protection des consommateurs, tout en renforçant sa crédibilité grâce à la *Stratégie d'intelligence artificielle du MDN et des FAC*, à la *Stratégie en matière d'intelligence artificielle pour la fonction publique fédérale* ainsi qu'à sa participation aux travaux de l'OTAN.

Ces approches divergentes montrent pourquoi des mécanismes comme *AI Nexus* sont essentiels. Sans eux, certaines technologies à double usage élaborées selon des normes commerciales pourraient ne pas satisfaire aux exigences de l'OTAN en

matière d'essai et d'évaluation, créant ainsi des failles de sécurité susceptibles de compliquer leur déploiement lorsqu'un autre pays les acquiert. Alors que l'UE met en œuvre un cadre juridique rigoureux, que les États-Unis privilégient une approche sectorielle et que le Canada redéfinit son orientation après la LIAD, l'OTAN a besoin d'un mécanisme commun de certification capable de faire le lien entre ces différents modèles. Pour le Canada, il s'agit d'une occasion d'agir comme trait d'union, en contribuant à harmoniser les pratiques transatlantiques d'une manière qui soit à la fois efficace sur le plan opérationnel et conforme aux principes de gouvernance démocratique.

À première vue, ces différences de gouvernance peuvent sembler purement techniques. En réalité, elles déterminent si les alliés peuvent se fier aux systèmes d'IA de leurs partenaires et les utiliser. Par exemple, une application à double usage comme un algorithme de navigation pour drone peut être parfaitement conforme dans un territoire de compétence, mais faire l'objet de restrictions dans un autre en raison de divergences en matière de certification. Les exigences relatives à la localisation des données peuvent limiter l'entraînement transfrontalier des modèles, tandis que des interprétations différentes de l'« IA responsable » risquent de compliquer les mécanismes communs d'assurance. Ces vulnérabilités peuvent provoquer des retards dans les chaînes d'approvisionnement, ralentir la mise à niveau des systèmes et le réentraînement des modèles utilisés par les alliés et, au bout du compte, miner la confiance. En l'absence d'approches communes, les alliés risquent d'hésiter au moment même où l'unité d'action est indispensable. Des mécanismes concrets sont donc essentiels pour garantir l'interopérabilité des systèmes d'un pays et d'un contexte à l'autre.

L'OTAN a déjà entrepris des démarches en ce sens. La *Stratégie OTAN sur l'intelligence artificielle* (2021, mise à jour en 2024) énonce cinq principes directeurs : la légalité, la responsabilité, la fiabilité, la gouvernabilité et l'atténuation des biais.²⁰ Bien qu'ils n'aient pas force de loi, ces principes établissent un socle commun d'attentes. Pour passer des principes à leur mise en œuvre, l'OTAN a créé des mécanismes comme le Comité d'examen des données et de l'intelligence artificielle (DARB), qui réunit des représentants des gouvernements, de l'industrie et du milieu universitaire afin d'élaborer des normes relatives aux essais, à la validation et à la certification, ainsi que les programmes Défis et innovation de l'Accélérateur d'innovation de défense pour l'Atlantique Nord (DIANA), qui mène des essais conjoints dans des centres d'essais répartis en Europe et en Amérique du Nord.²¹ Ensemble, ces initiatives témoignent de la volonté de l'Alliance d'instaurer un climat de confiance et d'assurer l'interopérabilité à grande échelle.

Pour le Canada, il importe de contribuer activement à cette mise en œuvre concrète des principes. Cela suppose d'harmoniser l'application nationale des principes de l'OTAN en matière d'IA tout en maintenant un équilibre entre le modèle réglementaire fondé sur les risques de l'UE et l'approche sectorielle des

États-Unis, de façon à permettre une certification adaptable d'un territoire de compétence à l'autre. Un cadre de gouvernance modulaire et commun faciliterait le déploiement transfrontalier des systèmes d'IA grâce à des architectures ouvertes et renforcerait la confiance opérationnelle entre les alliés. En contribuant à l'élaboration des cadres de certification, en intégrant l'interopérabilité aux processus d'approvisionnement et en veillant à ce que les mécanismes de gouvernance favorisent autant la confiance que la rapidité d'exécution, le MDN et les FAC peuvent aider l'OTAN à préserver son principal avantage : sa capacité d'agir collectivement, avec assurance et au rythme qu'exige l'environnement stratégique moderne.

La gouvernance comme catalyseur

On décrit souvent la gouvernance comme un frein à l'innovation. En pratique, elle rend l'innovation utilisable, fiable et digne de confiance à grande échelle au sein d'une alliance. Pour l'OTAN, la gouvernance s'apparente moins à un feu de circulation qu'à un système de navigation : elle ne ralentit pas les progrès, mais veille à ce que les États membres avancent dans la même direction et arrivent ensemble à destination. Cette fonction se manifeste dans des exercices comme *Steadfast Duel*, durant lesquels des outils fondés sur l'IA ont été intégrés aux structures multinationales de commandement et de contrôle, puis mis à l'essai au regard de doctrines communes, de principes d'IA responsable et de normes d'interopérabilité avant leur adoption.²² La gouvernance constitue le moteur qui assure une adoption de l'IA non seulement rapide, mais aussi responsable, interopérable et durable.

Les cadres communs donnent aux commandants la confiance nécessaire pour se fier aux systèmes de leurs partenaires. Pour que le personnel canadien, américain ou européen puisse s'appuyer sur des outils fondés sur l'IA dans le cadre d'opérations multinationales, il doit savoir que les données, les algorithmes et les mesures de protection sous-jacents respectent des normes convenues. Sans cette assurance, l'hésitation risque de s'immiscer dans le cycle décisionnel.²³ Grâce à elle, les commandants peuvent agir avec détermination, sachant qu'un plan d'action ou un produit du renseignement généré par l'IA d'un allié peut inspirer confiance à tous. Des approches communes pour les essais, la validation et la certification rendent cette confiance possible et transforment les capacités nationales en force collective.

En pratique, l'OTAN met la gouvernance en œuvre, en élaborant des doctrines conjointes, des normes techniques communes et des environnements d'essai coordonnés. Les accords de normalisation établissent des exigences communes pour l'échange de données et les interfaces, tandis que les publications interarmées alliées intègrent les technologies émergentes à des concepts opérationnels communs. Concernant l'IA, des mécanismes comme le DARB et DIANA visent à donner aux pays l'assurance commune que les outils fondés sur l'IA respectent les

principes de fiabilité et de sécurité de l'OTAN. Il faut maintenant approfondir et élargir ces efforts, en étendant la certification à un plus grand nombre de cas d'utilisation, en reliant les centres d'essai plus directement aux commandements opérationnels et en veillant à intégrer rapidement aux processus d'approvisionnement les leçons tirées des essais.

À l'extérieur de l'OTAN, la communauté du renseignement du Groupe des cinq, à laquelle participe le Canada par l'intermédiaire du Centre de la sécurité des télécommunications (CST), renforce ces efforts. En publiant des avis techniques interarmées sur le déploiement sécuritaire de l'IA et la cyberdéfense, ses membres fournissent des orientations communes concernant le renforcement des systèmes, l'intégrité des données et l'atténuation des risques.²⁴ Cette coordination aide les forces armées alliées à faire face aux mêmes menaces au moyen de mesures de défense cohérentes, qu'il s'agisse de l'empoisonnement des données, de la manipulation malveillante ou des cyberintrusions. Pris dans leur ensemble, ces travaux montrent comment la gouvernance peut se concrétiser non pas sous forme de déclarations générales, mais au moyen de mécanismes précis qui renforcent la confiance et rendent possible le déploiement des systèmes d'IA au-delà des frontières.

Le Canada a un rôle particulier à jouer dans le renforcement de ces initiatives. La Directive sur la prise de décisions automatisée et la *Stratégie d'intelligence artificielle du MDN et des FAC* intègrent déjà des valeurs comme la légalité, la transparence et la responsabilisation.²⁵ En reliant ces cadres nationaux aux processus de certification et d'essai de l'OTAN, le Canada peut montrer comment des principes consacrés à l'échelle nationale peuvent renforcer directement l'interopérabilité de l'Alliance. Ce double ancrage garantit l'interopérabilité des systèmes canadiens dès leur conception et offre un modèle que d'autres puissances moyennes peuvent suivre.

La gouvernance doit également faire preuve d'agilité. Les normes ne peuvent rester figées alors que les technologies évoluent si rapidement. Il faut appliquer les principes de l'OTAN au moyen d'une certification modulaire, d'environnements d'expérimentation et de processus d'essai itératifs qui évoluent au même rythme que les technologies.²⁶ Une approche modulaire signifie qu'un système n'a pas à être certifié de nouveau dans son intégralité chaque fois qu'un de ses composants est mis à jour. Cette méthode permet de gagner du temps tout en préservant la confiance envers le système. Les environnements d'expérimentation offrent pour leur part un cadre contrôlé, permettant de mettre à l'essai de nouvelles idées, donnant aux innovateurs la liberté d'explorer de nouvelles possibilités tout en maintenant un niveau de sécurité adéquat. Quant aux essais itératifs, ils garantissent que les systèmes, une fois déployés, continuent de mériter la confiance qui leur est accordée dans des conditions d'utilisation réelles. Une telle approche permet aux alliés de déployer rapidement de nouvelles capacités fondées sur l'IA tout

en maintenant le niveau d'assurance commun qui constitue le fondement de l'interopérabilité.

La mise en œuvre concrète de la gouvernance exige également de s'attaquer aux menaces réelles qui pèsent sur les chaînes d'approvisionnement et sur la cybersécurité. Les systèmes de défense fondés sur l'IA sont exposés à des risques allant de l'altération des micrologiciels, des portes dérobées matérielles et des vulnérabilités des logiciels tiers aux techniques d'apprentissage automatique antagoniste, comme l'empoisonnement des données d'entraînement et les attaques par évasion, sans oublier les risques émergents liés au déchiffrement quantique. Sans mesures de gestion adéquates, ces vulnérabilités peuvent éroder la confiance et compromettre l'interopérabilité dans les réseaux alliés.

Leur atténuation exige l'intégration de mesures de protection dans la gestion des chaînes d'approvisionnement : des principes de confiance zéro qui vérifient continuellement les utilisateurs et les appareils; une surveillance continue fondée sur la détection des anomalies; l'échange de renseignements sur les cybermenaces entre les alliés; ainsi que des exercices réguliers d'équipe rouge et une certification conjointe selon les cadres d'assurance de l'OTAN. Des mesures concrètes, comme l'atténuation des attaques par injection de requête, l'assainissement des données d'entrée, la restriction des outils à risque élevé et le filtrage des données de sortie, peuvent réduire le risque d'utilisation abusive de l'IA et de compromission des systèmes.²⁷ En intégrant ces mesures aux processus d'approvisionnement et de certification, le MDN et les FAC peuvent faire en sorte que les systèmes fondés sur l'IA demeurent sécurisés, résilients et dignes de confiance dans l'ensemble de l'Alliance. En somme, la gouvernance ne constitue pas une contrainte, mais un multiplicateur de force. Elle transforme un ensemble de projets nationaux en capacité commune et permet à l'OTAN d'avancer rapidement de façon concertée plutôt que de laisser chaque État membre progresser isolément. Pour le MDN et les FAC, promouvoir la gouvernance comme catalyseur permet de veiller à ce que les investissements dans l'IA soient non seulement responsables, mais aussi interopérables, pertinents sur le plan stratégique et solidement ancrés dans la confiance qui caractérise l'Alliance.

Qu'est-ce que cela signifie pour la posture d'approvisionnement du Canada?

La *Stratégie d'intelligence artificielle du MDN et des FAC* fixe un objectif ambitieux : devenir une force dotée de capacités d'IA d'ici 2030 grâce à « une IA éthique, inclusive et fiable pour l'interopérabilité et l'avantage dans l'espace de combat et une meilleure intendance dans l'espace de l'entreprise²⁸ ». L'atteinte de cet objectif ne repose pas uniquement sur des documents stratégiques. Elle nécessite un changement à la fois culturel et structurel. L'approvisionnement doit être considéré dès le départ comme un levier essentiel de l'interopérabilité, et non comme un

élément secondaire dont on tient compte une fois les décisions prises. Chaque décision d'acquisition doit garantir que les systèmes canadiens s'intègrent sans rupture aux plateformes alliées et conservent leur capacité d'adaptation au fil de l'évolution technologique.

Pour relever ce défi, il faut délaisser les modèles d'approvisionnement conventionnels et rigides au profit d'approches modulaires, agiles et axées sur les compétences. La modularité permet de moderniser les capacités sans devoir les remplacer. Au lieu de s'enfermer dans des systèmes fermés fournis par une seule entreprise et qui deviennent rapidement désuets, les FAC devraient privilégier des architectures ouvertes permettant des mises à niveau progressives à mesure qu'apparaissent de nouveaux algorithmes, capteurs et outils de communication. Cette orientation correspond à celle de nombreuses forces armées alliées, qui adoptent des systèmes prêts à l'emploi afin de réduire leur dépendance envers un fournisseur unique et d'accroître leur souplesse. Une intégration agile tout au long du cycle de vie revêt une importance tout aussi grande. Les systèmes d'IA ne restent jamais statiques : ils apprennent, dérivent et doivent faire l'objet d'un nouvel entraînement. Les processus d'approvisionnement doivent tenir compte de cette réalité au moyen d'essais itératifs, d'exigences souples et d'un dialogue continu avec les fournisseurs.²⁹ Au lieu d'attendre plusieurs années la livraison d'une capacité, les FAC peuvent recourir à des mises à niveau successives pour maintenir les systèmes au rythme de l'innovation. Par exemple, le modèle d'approvisionnement intégré du Royaume-Uni prévoit la mise en service rapide d'une capacité minimale déployable, suivie d'améliorations apportées au fil du temps. Cette approche réduit les délais applicables aux systèmes numériques et intègre des mises à niveau continues à l'ensemble du cycle d'acquisition.³⁰

Le personnel compte autant que les plateformes. Les cadres de gouvernance ne donnent de résultats que si le personnel possède les compétences nécessaires pour les appliquer. Le Canada manque de spécialistes de l'IA, de la cybersécurité et des données, ce qui limite la rapidité avec laquelle le MDN et les FAC peuvent déployer et évaluer les systèmes d'IA. La concurrence du secteur privé complique le recrutement et le maintien en poste du personnel technique.

Pour atténuer ces difficultés, les FAC doivent créer des cheminements de carrière destinés aux spécialistes de l'IA et aux scientifiques des données, constituer un corps de réserve technique capable de fournir rapidement une expertise pour des projets de courte durée et doter les opérateurs de compétences pratiques. Il faut donc mettre en place des parcours de formation qui associent les connaissances techniques au contexte militaire. Il pourrait s'agir, par exemple, d'intégrer des modules d'IA au perfectionnement professionnel des officiers et des militaires du rang, d'établir des partenariats avec des instituts canadiens spécialisés en IA et d'offrir des détachements permettant au personnel militaire d'acquérir de l'expérience dans l'industrie et dans

des laboratoires universitaires.³¹ Ces échanges renforceraient les compétences tout en favorisant une culture de collaboration. La formation devrait également porter sur les applications pratiques, les usages responsables et la gestion des risques liés à la cybersécurité, notamment le contrôle de l'accès aux systèmes d'IA. Qu'il s'agisse de gérer les chaînes de traitement des données ou de formuler des requêtes à l'intention de grands modèles de langage, les opérateurs doivent avoir la certitude que les outils d'IA leur permettent de gagner du temps et d'améliorer la prise de décisions plutôt que d'accroître la complexité.³² L'établissement d'un lien de confiance entre les humains et les machines revêtira autant d'importance que le rendement technique des systèmes eux-mêmes.

Enfin, les choix d'approvisionnement devraient renforcer la résilience du MDN et des FAC ainsi que la cohésion des alliés. Les économies à court terme que procurent des technologies peu coûteuses, mais impossibles à intégrer ou jugées indignes de confiance, peuvent sembler attrayantes. Elles finissent toutefois par nuire à la souveraineté et à l'interopérabilité.³³ Cette leçon vaut autant pour le matériel que pour les modèles logiciels. Les systèmes fermés ou opaques conçus par des fournisseurs de pays non alliés peuvent introduire des vulnérabilités cachées ou limiter la capacité du MDN et des FAC à mettre à jour et à certifier les outils. Le fait de privilégier des sources canadiennes et alliées de matériel et de logiciels, appuyées par des normes ouvertes et des pratiques de développement transparentes, contribue à la fois à la sécurité et à l'interopérabilité. Cette orientation renforce également la base industrielle de défense du Canada et donne aux entreprises canadiennes un rôle plus clair dans les chaînes d'approvisionnement de l'OTAN.

Le rôle du MDN et des FAC ne consiste pas simplement à acheter du matériel plus rapidement, mais à orienter le marché selon des principes d'ouverture, de résilience et de confiance. En participant à des initiatives conjointes d'approvisionnement avec les alliés, en regroupant la demande relative à une infrastructure infonuagique sécurisée et en tirant parti de l'avantage naturel que procurent au Canada ses éléments des terres rares, le MDN et les FAC peuvent exercer une influence qui dépasse largement ce que laisserait supposer la taille de leur budget. Ainsi, l'approvisionnement devient autant un outil stratégique qu'un outil logistique : il réunit l'industrie canadienne, les normes alliées et les besoins opérationnels dans un cadre cohérent.

Prises dans leur ensemble, ces mesures permettront au MDN et aux FAC de concilier la rigueur budgétaire avec les impératifs de rapidité et de confiance. Ils permettront également aux FAC d'intégrer l'IA à de nouvelles plateformes, comme les F-35, les destroyers de la classe Fleuves et rivières et les systèmes de modernisation du NORAD, d'une façon adaptable, résiliente et entièrement interopérable. Dans ce contexte, l'approvisionnement ne se limite plus à l'acquisition de matériel. Il consiste à intégrer l'interopérabilité, la résilience et la pertinence stratégique à chaque décision. Ce faisant, le MDN et les FAC renforcent non

seulement la défense nationale, mais aussi la capacité de l'OTAN à agir collectivement, tout en préservant l'influence du Canada comme partenaire digne de confiance au sein de l'Alliance.

Conclusion

L'adoption de l'IA façonnera l'avenir de la défense, et son succès dépendra de la capacité des alliés à progresser ensemble. Pour l'OTAN ainsi que pour le MDN et les FAC, l'enjeu ne consiste pas simplement à acquérir de nouvelles technologies, mais à les intégrer de manière à inspirer confiance, à renforcer l'interopérabilité et à maintenir la cohésion de l'Alliance. La gouvernance et l'approvisionnement ne constituent pas des obstacles à surmonter. Ils représentent les leviers qui rendent l'adoption de l'IA rapide, éthique et durable.

Les objectifs de modernisation du MDN et des FAC illustrent clairement cet enjeu. *La Stratégie d'intelligence artificielle du MDN et des FAC* (2024) fixe l'objectif de devenir une force dotée de capacités d'IA d'ici 2030. Pour concrétiser cette vision, il faudra traduire les principes en mesures concrètes dans l'ensemble des programmes et veiller à la mise en œuvre des principes d'une IA éthique et des mécanismes de gouvernance de l'IA dans toute l'organisation. De nouvelles plateformes, comme les destroyers de la classe Fleuves et rivières et les F-35, produiront d'importants volumes de données opérationnelles, créant à la fois des possibilités nouvelles et un besoin accru d'analyses fondées sur l'IA.³⁴ La modernisation du NORAD, grâce à ses capacités de commandement et de contrôle infonuagiques, montre déjà comment l'IA peut raccourcir les cycles décisionnels, proposer aux commandants des plans d'action en temps réel et renforcer la défense commune de l'Amérique du Nord.³⁵ Ces initiatives mettent en évidence une réalité fondamentale : l'interopérabilité n'est pas facultative; elle constitue le fondement de la sécurité continentale et alliée.

Pour relever ce défi, il faudra investir de façon soutenue dans trois domaines.³⁶ D'abord, il faut développer des normes communes qui rendent les outils fondés sur l'IA dignes de confiance d'un pays à l'autre, afin qu'un système canadien puisse être adopté sans difficulté par un commandant américain ou

européen sur le terrain. Ensuite, il faut s'engager dans des pratiques d'approvisionnement ouvertes et souples permettant d'intégrer de nouveaux algorithmes, capteurs et logiciels sans s'enfermer dans des architectures fermées. Enfin, il faut favoriser des chaînes d'approvisionnement résilientes qui garantissent au Canada et à ses alliés un accès sécurisé aux puces électroniques, aux minéraux critiques et aux infrastructures infonuagiques sur lesquels reposent les systèmes numériques.

Pour le Canada, cela signifie intégrer l'interopérabilité à l'ensemble des acquisitions, mettre à profit sa réputation en matière de gouvernance responsable de l'IA et collaborer étroitement avec les alliés afin d'harmoniser les cadres de certification et d'assurance. Cela signifie également renforcer les atouts nationaux, qu'il s'agisse de l'écosystème canadien de recherche en IA, des ressources en minéraux critiques ou des programmes d'innovation en matière de défense, afin que la contribution du Canada demeure à la fois distinctive et indispensable à l'Alliance. En conjuguant résilience nationale et collaboration internationale, le MDN et les FAC peuvent faire en sorte que les nouvelles capacités soient non seulement avancées sur le plan technologique, mais aussi pertinentes sur le plan stratégique, dignes de confiance et pleinement utilisables dans l'ensemble de l'OTAN.

L'objectif du MDN et des FAC de devenir une force dotée de capacités d'IA à l'horizon de 2030 ne pourra se concrétiser que si chaque décision relative à l'approvisionnement, à la gouvernance, à la formation et aux investissements est prise dans une perspective d'interopérabilité. Le succès ne se mesurera pas au nombre de systèmes d'IA que le MDN et les FAC mettront en service de façon autonome, mais à leur capacité de les intégrer efficacement aux capacités collectives de l'Alliance.

En harmonisant son ambition pour 2030 avec les cadres adoptés par les alliés, le MDN et les FAC assurent non seulement leur propre avenir en tant que force dotée de capacités d'IA, mais renforcent également la cohésion qui permettra à l'OTAN de relever les défis de l'espace de combat numérique. Ce faisant, le MDN et les FAC contribuent à préserver le principal avantage stratégique de l'Alliance : la capacité d'agir collectivement, avec confiance et rapidité, pour défendre la démocratie.

Notes

1 Karen Hui, « Taiwan, Canada, and the Global Semiconductor Race », *Asia Pacific Foundation of Canada*, 10 février 2025, à l'adresse : <https://www.asiapacific.ca/publication/taiwan-canada-and-global-semiconductor-race>.

2 Koc Cagan, Ian King et Jillian Deutsch, « ASML, Europe's Most Valuable Tech Firm, Is at the Heart of the US-China Chip War », *Bloomberg*, 26 avril 2023, à l'adresse : <https://www.bloomberg.com/news/articles/2023-04-26/asml-europe-s-most-valuable-tech-firm-to-define-us-china-chip-war>.

3 Janet Egan, « Global Compute and National Security: Strengthening American AI Leadership Through Proactive Partnerships », *Center for a New American Security*, 29 juillet 2025, à l'adresse : <https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/AE-Report-Global-ComputeFINALv2.pdf>.

4 Gracelin Baskaran et Meredith Schwartz, « The Consequences of China's New Rare-Earths Export Restrictions », *Center for Strategic & International Studies*, 14 avril 2025, à l'adresse : <https://www.csis.org/analysis/consequences-chinas-new-rare-earths-export-restrictions>.

5 Peter Flory, « EIES Insights – NATO Summit », *Secure Energy Europe*, 7 juillet 2025, à l'adresse : <https://www.secureenergyeurope.org/eies-insights-nato-summit>.

6 Daniella Cheslow, « NATO Sparks an AI Gold Rush », *Politico*, 30 juin 2025, à l'adresse : <https://www.politico.com/newsletters/digital-future-daily/2025/06/30/nato-sparks-an-ai-gold-rush-00433756>.

7 Premier ministre du Canada, « Nous renforçons nos partenariats transatlantiques et assurons un avantage canadien en matière d'intelligence artificielle », gouvernement du Canada, 12 février 2025, à l'adresse : <https://www.pm.gc.ca/fr/nouvelles/>

- communiqués/2025/02/12/nous-renforcons-nos-partenariats-transatlantiques-et-assurés; Innovation, Sciences et Développement économique Canada, *Stratégie canadienne sur la capacité de calcul souveraine pour l'IA*, gouvernement du Canada, 6 mai 2025, <https://ised-isde.canada.ca/site/ised/fr/strategie-canada-puissance-calcul-souveraine-pour-lia>.
- 8 Ressources naturelles Canada, « Faits sur les éléments des terres rares », Gouvernement du Canada, 19 septembre 2025, à l'adresse : <https://ressources-naturelles.canada.ca/mineraux-exploitation-miniere/donnees-statistiques-analyses-exploitation-miniere/faits-mineraux-metallurgiques-faits-elements-terres-rares>.
 - 9 Joe Walsh, « Pentagon Scrams Microsoft's \$10 Billion Cloud Computing Deal After Lawsuit from Amazon », *Forbes*, 6 juillet 2021, publié initialement à l'adresse : <https://www.forbes.com/sites/joewalsh/2021/07/06/pentagon-scrams-microsofts-10-billion-cloud-computing-deal-after-lawsuit-from-amazon/>.
 - 10 U.S. Department of War, « Department of Defense Announces Joint Warfighting Cloud Capability Procurement », 7 décembre 2022, à l'adresse : <https://www.defense.gov/News/Releases/Release/Article/3239378/departement-of-defense-announces-joint-warfighting-cloud-capability-procurement/>.
 - 11 Kateryna Bondar, « Unleashing U.S. Military Drone Dominance: What the United States Can Learn from Ukraine », *Center for Strategic & International Studies*, 18 juillet 2025, à l'adresse : <https://www.csis.org/analysis/unleashing-us-military-drone-dominance-what-united-states-can-learn-ukraine>.
 - 12 Jacob Stokes, « Military Artificial Intelligence, the People's Liberation Army, and U.S.-China Strategic Competition », *Center for a New American Security*, 1^{er} février 2024, à l'adresse : <https://www.cnas.org/publications/congressional-testimony/military-artificial-intelligence-the-peoples-liberation-army-and-u-s-china-strategic-competition>.
 - 13 Comité permanent de la défense nationale de la Chambre des communes, *L'heure du changement a sonné : Réforme de l'approvisionnement en matière de défense au Canada*, juin 2024, à l'adresse : <https://www.noscommunes.ca/documentviewer/fr/44-1/NDON/rapport-12/page-126>.
 - 14 Ministère de la Défense nationale, « Innovation pour la défense, l'excellence et la sécurité (IDEES) », Gouvernement du Canada, 22 juillet 2025, à l'adresse : <https://www.canada.ca/fr/ministere-defense-nationale/programmes/idees-defense.html>.
 - 15 Derek Dobson, « Modernizing the Defence Procurement Ecosystem », LinkedIn, 25 avril 2023, à l'adresse : <https://www.linkedin.com/pulse/modernizing-defence-procurement-ecosystem-canada-derek-dobson->.
 - 16 Matt Kosinski et Mark Scapicchio, « The EU AI Act: What You Need to Know », IBM, 20 septembre 2024, à l'adresse : <https://www.ibm.com/think/topics/eu-ai-act>.
 - 17 Ian Reynolds et Yasir Atalan, « Calibrating NATO's Vision of AI-Enabled Decision Support », *Center for Strategic and International Studies*, 8 juillet 2024, à l'adresse : <https://www.csis.org/analysis/calibrating-natos-vision-ai-enabled-decision-support>.
 - 18 Service de recherche du Parlement européen, « US approach to artificial intelligence », Parlement européen, 2024, à l'adresse : [https://www.europarl.europa.eu/RegData/etudes/ATAG/2024/757605/EPRS_ATAG\(2024\)757605_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2024/757605/EPRS_ATAG(2024)757605_EN.pdf).
 - 19 Innovation, Sciences et Développement économique Canada, *La Loi sur l'intelligence artificielle et les données (LIAD) - document complémentaire*, gouvernement du Canada, 31 janvier 2025, à l'adresse : <https://ised-isde.canada.ca/site/innover-meilleur-canada/fr/loi-intelligence-artificielle-donnees-liad-document-complementaire>.
 - 20 Zoe Stanley-Lockman et Edward Hunter Christie, « An Artificial Intelligence Strategy for NATO », 25 octobre 2021, à l'adresse : <https://www.nato.int/docu/review/articles/2021/10/25/an-artificial-intelligence-strategy-for-nato/index.html>.
 - 21 OTAN, « NATO's Data and Artificial Intelligence Review Board », 17 octobre 2022, à l'adresse : https://www.nato.int/cps/en/natohq/official_texts_208374.htm; OTAN, « DIANA | Accelerator », 2025, à l'adresse : <https://www.diana.nato.int/accelerator-programme.html>.
 - 22 L'exercice Steadfast Duel 2025 a utilisé le *Project Maven Smart System*, qui fait appel à de grands modèles de langage et à l'apprentissage automatique pour améliorer la fusion du renseignement et accélérer la prise de décisions. Voir : Agence OTAN d'information et de communication, « NCIA enables Steadfast Duel 25, NATO's largest computer-assisted command post exercise », OTAN, 29 octobre 2025. À l'adresse : <https://www.ncia.nato.int/newsroom/news/ncia-enables-steadfast-duel-25-natos-largest-computer-assisted-command-post-exercise>.
 - 23 Zoe Stanley-Lockman, « Responsible and Ethical Military AI », *Center for Security and Emerging Technology*, août 2021, à l'adresse : <https://cset.georgetown.edu/publication/responsible-and-ethical-military-ai/>.
 - 24 Cybersecurity and Infrastructure Security Agency, « Joint Guidance on Deploying AI Systems Securely », Department of Homeland Security, 15 avril 2024, à l'adresse : <https://www.cisa.gov/news-events/alerts/2024/04/15/joint-guidance-deploying-ai-systems-securely>.
 - 25 Secrétariat du Conseil du Trésor du Canada, *Directive sur la prise de décisions automatisée*. Gouvernement du Canada, 24 juin 2025, à l'adresse : <https://www.tbs-sct.canada.ca/pol/doc-fra.aspx?id=32592>; ministère de la Défense nationale et Forces armées canadiennes, *La Stratégie d'intelligence artificielle du ministère de la Défense nationale et des Forces armées canadiennes*, gouvernement du Canada, 3 mars 2024, à l'adresse : <https://www.canada.ca/content/dam/dnd-mdn/documents/reports/ai-ia/dndcaf-ai-strategy.pdf>.
 - 26 Daniel Fata, « NATO's Evolving Role in Developing AI Policy », *Center for Strategic and International Studies*, 8 novembre 2022, à l'adresse : <https://www.csis.org/analysis/natos-evolving-role-developing-ai-policy>.
 - 27 Centre canadien pour la cybersécurité, « Les 10 mesures de sécurité en matière d'intelligence artificielle : Introduction - ITSAP10.049 », mars 2026, à l'adresse : <https://www.cyber.gc.ca/fr/orientation/10-mesures-securite-matiere-dintelligence-artificielle-introduction-itsap10049>.
 - 28 Ministère de la Défense nationale et des Forces armées canadiennes, *La Stratégie d'intelligence artificielle du ministère de la Défense nationale et des Forces armées canadiennes*, Gouvernement du Canada, 2024, à l'adresse : <https://www.canada.ca/content/dam/dnd-mdn/documents/reports/ai-ia/mdnfac-strategie-ia.pdf>.
 - 29 Alex McPhail, Alexander Rudolph, et Philippe Lagassé, *Defence Agile Procurement: Insights and Analysis (DAPIA) Report*, *EXA Consulting Group*, 10 juillet 2025, à l'adresse : <https://static1.squarespace.com/static/5cd08376797f74215eaa7cc/t/68af61b380a0f3571c695ae9/1756324275338/Final+Report+-+Defence+Agile+Procurement+Insights+and+Analysis.pdf>.
 - 30 Ministère britannique de la Défense, « Integrated Procurement Model: Driving pace in the delivery of Military Capability », 28 février 2024, à l'adresse : <https://www.gov.uk/government/publications/integrated-procurement-model-driving-pace-in-the-delivery-of-military-capability/integrated-procurement-model-driving-pace-in-the-delivery-of-military-capability>.
 - 31 Ministère de la Défense nationale et des Forces armées canadiennes, *La Stratégie d'intelligence artificielle du ministère de la Défense nationale et des Forces armées canadiennes*, Gouvernement du Canada, 3 mars 2024, à l'adresse : <https://www.canada.ca/content/dam/dnd-mdn/documents/reports/ai-ia/mdnfac-strategie-ia.pdf>.
 - 32 Alexander Salt, « Reflections on Artificial Intelligence and Canadian Defence », *Institut canadien des affaires mondiales*, août 2025, à l'adresse : https://www.cgai.ca/th_pp_reflections_on_artificial_intelligence_and_canadian_defence.
 - 33 Joshua Kurlantzick, « Assessing China's Digital Silk Road », Council on Foreign Relations, 18 décembre 2020, à l'adresse : <https://www.cfr.org/blog/assessing-chinas-digital-silk-road-transformative-approach-technology-financing-or-danger>.
 - 34 Alexander Salt, « Reflections on Artificial Intelligence and Canadian Defence », *Institut canadien des affaires mondiales*, août 2025, à l'adresse : https://www.cgai.ca/th_pp_reflections_on_artificial_intelligence_and_canadian_defence.
 - 35 Ministère de la Défense nationale, « Le Secteur de la défense aérienne du Canada présente un nouveau système de commande et contrôle infonuagique », Gouvernement du Canada, 26 janvier 2024, à l'adresse : <https://www.canada.ca/fr/ministere-defense-nationale/feuille-derable/arc/2024/01/secteur-defense-aerienne-canada-presente-nouveau-systeme-commande-contrôle-infonuagique.html>.
 - 36 Ian Bremmer et Mustafa Suleyman, « The AI Power Paradox: Can States Learn to Govern Artificial Intelligence—Before It's Too Late? » *Foreign Affairs*, 16 août 2023, à l'adresse : <https://www.foreignaffairs.com/world/artificial-intelligence-power-paradox>.



Le membre de l'élément du contrôle aérien tactique (ECAT) saisit les coordonnées pour la prochaine frappe aérienne effectuée pendant l'ex MAPLE STRIKE dans la zone de largage Shaver à Jimmy Lake, en Alberta.

Caporale Connie Valin, photo des Forces armées canadiennes

Navigation au sextant et à l'astrocompas : une approche des FAC pour l'adoption de l'IA¹

COLONEL ADAM MOORE ET MATTHEW DA MOTA

Le colonel Adam Moore a été commissionné dans le régiment Princess Patricia's Canadian Light Infantry et sert comme officier d'infanterie dans les Forces armées canadiennes depuis 1996. La carrière du colonel Moore comprend divers rôles de commandement et d'état-major, notamment comme commandant du troisième bataillon, PPCLI, de 2018 à 2020. Il a été déployé à l'international à quatre reprises, notamment en Bosnie-Herzégovine, en Afghanistan et en Irak, ainsi que lors de cinq opérations nationales. Diplômé du Collège militaire royal du Canada, il détient un baccalauréat en génie et une maîtrise en études de la défense. Il a suivi une instruction militaire professionnelle au Collège de commandement et d'état-major de l'Armée canadienne ainsi qu'au Collège des Forces canadiennes. Le colonel Moore est boursier au Centre for International and Defence Policy de l'Université Queen's depuis 2024-2025 et il est actuellement chef d'état-major de la 4^e Division du Canada.

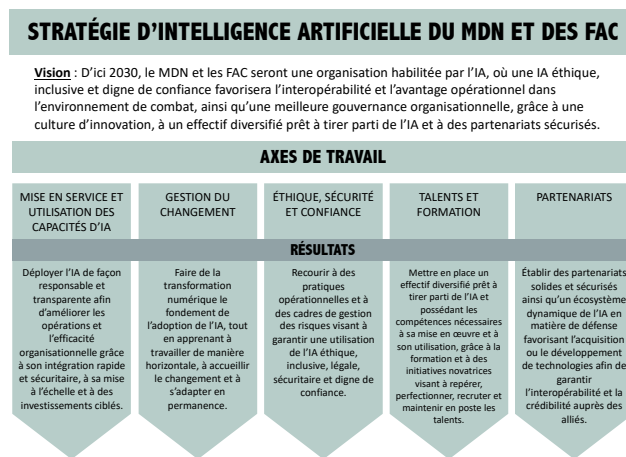
Matthew da Mota est directeur de la recherche, Technologies émergentes et sécurité nationale au Canadian Shield Institute for Public Policy. Son travail explore comment les technologies émergentes et les dynamiques géopolitiques changeantes redéfinissent la sécurité, la gouvernance, la connaissance et la souveraineté, en mettant l'accent sur les implications de l'IA et des infrastructures numériques. Matthew a auparavant travaillé sur la gouvernance et la sécurité de l'IA internationale au Centre pour l'innovation dans la gouvernance internationale. Ses recherches de doctorat portaient sur la relation entre le récit historique, les preuves écrites et le pouvoir politique. Matthew est également chercheur en technologie et sécurité au Centre for International and Defence Policy de l'Université Queen's, et siège dans plusieurs comités techniques de normalisation.

Cet article se concentre précisément sur la perturbation causée par l'IA dans les processus décisionnels militaires. D'autres aspects de l'IA dans les forces armées, comme l'intégration de l'IA à la robotique, sont importants, mais distincts, et ne sont pas abordés dans cet article. Les lecteurs devraient considérer cet article comme présentant l'état du développement de l'IA à la mi-2025, qui pourrait avoir évolué depuis dans des domaines clés.

Les plus grandes institutions de sécurité nationale du Canada, soit l'organisation conjointe du ministère de la Défense nationale (MDN) et des Forces armées canadiennes (FAC), font face à un impératif institutionnel : être habilitées à l'IA d'ici 2030 ou risquer de devenir non pertinentes du point de vue stratégique. Pourtant, l'intégration de l'IA introduit des dangers (déqualification cognitive, dilution de la responsabilité, biais d'automatisation) qui restent mal compris dans des environnements militaires, confrontés à des enjeux élevés. L'environnement mondial des menaces est en évolution rapide—caractérisé par la compétition stratégique, les instabilités régionales et les perturbations non étatiques—ce qui intensifie ce défi et exige une adoption rapide jumelée à une gestion efficace des risques opérationnels.^{2,3}

La *Stratégie d'intelligence artificielle du MDN et des FAC* exprime cette ambition par cinq axes de travail interconnectés : (1) mise en service et utilisation des capacités d'IA, (2) gestion du changement, (3) éthique, sécurité et confiance, (4) talents et formation, et (5) partenariats.⁴ Bien que l'échéance de 2030 semble lointaine, cela représente un défi immédiat en matière d'approvisionnement pour la défense, nécessitant une transformation organisationnelle et culturelle qui relie l'expertise technique aux connaissances institutionnelles.⁵

Figure 1 : Axes de travail de la Stratégie d'IA du MDN et des FAC⁶



Cet article explore l'intégration de l'IA par la métaphore de la navigation au sextant et à l'astrocompas—soulignant l'importance d'ancrer l'innovation dans des cadres professionnels établis. S'appuyant sur la hiérarchie cognitive des FAC, le modèle Autorité, responsabilité et reddition de comptes (ARR) et le langage d'évaluation des risques institutionnels, l'analyse traite l'IA non pas comme une solution, mais comme un ensemble d'outils puissant, mais incomplet qui doit rester subordonné au jugement professionnel, à la logique institutionnelle et aux réalités de la prise de décision militaire.

L'article soutient qu'une adoption significative de l'IA nécessite une action délibérée et informée par les risques, ainsi qu'une double fluidité : la capacité d'opérer efficacement à la fois dans des environnements habilités à l'IA et des environnements privés de technologie. En utilisant la Stratégie d'IA comme document-cadre pour comprendre les plans du MDN/FAC en la matière, il examine comment les cadres décisionnels établis des FAC peuvent guider une intégration responsable, en concluant par des recommandations politiques pour soutenir une avancée éclairée dans la logique institutionnelle existante.

Étoiles de repérage pour l'intégration de l'IA

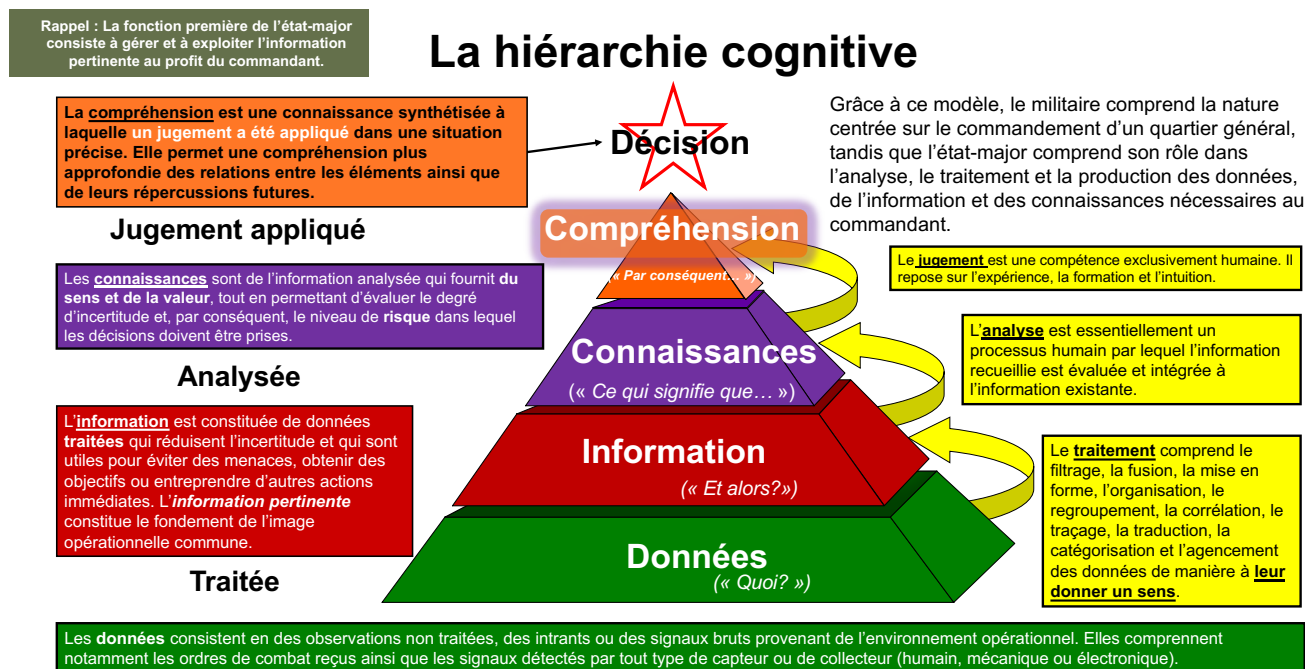
Tout comme la navigation céleste sur l'océan, l'intégration de l'IA au sein du MDN et des FAC nécessite des points de référence fixes pour maintenir le cap et l'azimut. Le sextant mesure les angles entre les corps célestes connus et l'horizon; l'astrocompas aide à déterminer le vrai nord. En ce qui concerne l'adoption de l'IA au sein de l'entreprise de défense, trois constantes institutionnelles devraient servir d'étoiles guides : le modèle de hiérarchie cognitive des FAC; le cadre ARR; et la logique structurante du risque qui concerne tous les paliers du MDN et des FAC. Bien que ces cadres ne soient pas propres à l'IA, ils régissent la manière dont les militaires interagissent et utilisent l'information dans tous les contextes, ce qui les rend essentiels pour comprendre comment l'IA, une suite fondamentalement basée sur l'information, s'intégrera dans les systèmes du MDN et des FAC existants et émergents.

À mesure que les systèmes d'IA commencent à influencer les environnements décisionnels au sein du MDN et des FAC, ces modèles fondamentaux de prise de décisions et de production de connaissances continuent de servir d'aides essentielles à la navigation. Ils veillent à ce que l'innovation technologique reste ancrée dans une logique institutionnelle éprouvée et selon un jugement professionnel.

Hiérarchie cognitive

Le modèle de hiérarchie cognitive des FAC (figure 2) offre un cadre structuré pour transformer les données brutes en éléments exploitables. Le modèle repose sur quatre étapes ascendantes : données, information, connaissances et compréhension, dont chacune représentant une étape qualitative dans le traitement cognitif. Bien que l'IA puisse enrichir cette hiérarchie, elle ne peut pas remplacer le rôle fondamental du jugement humain.

Figure 2 : La hiérarchie cognitive⁷



Les outils d'IA peuvent considérablement améliorer cette hiérarchie en aidant à nettoyer et étiqueter les données, en automatisant la désignation réciproque⁸ et en extrayant les informations pertinentes pour soutenir la collecte et le traitement des données. Des systèmes plus avancés peuvent soutenir l'analyse pour générer des connaissances et même offrir des entrées structurées qui éclairent le jugement humain dans la recherche d'une compréhension partagée. Néanmoins, le jugement demeure une fonction distinctement humaine, façonnée par l'expérience, l'intuition et le discernement éthique. Dans un environnement centré sur le commandement, où le personnel gère et interprète l'information pertinente au nom des commandants, la hiérarchie cognitive renforce la mentalité de commandement de mission des FAC, mettant l'accent sur la prise de décision décentralisée et la confiance. Tout soutien à la décision habilité à l'IA doit donc être subordonné et ancré dans un jugement humain expert et éthique.

Le cadre ARR au sein du MDN et des FAC

La triade Autorité, Responsabilité et Reddition de comptes (ARR) est l'épine dorsale décisionnelle du MDN et des FAC qui s'applique tant aux composantes militaires que civiles de l'institution conjointe.⁹ Tout comme la relation entre le vrai nord et les corps célestes demeure fixe, ces concepts maintiennent des positions relatives constantes même lorsque les contextes changent.

La *reddition de comptes*, c'est-à-dire l'obligation de rendre compte des responsabilités assumées, est non déléguables, résidant dans les structures juridiques et institutionnelles de l'organisation d'appartenance de la personne. La *responsabilité* est l'obligation d'accomplir les tâches assignées, qui peuvent être déléguées mais jamais totalement abandonnées. L'*autorité* désigne le droit de prendre des décisions, de donner des ordres ou instructions formels et de diriger des actions, que ce soit dans une capacité de commandement, administrative ou fonctionnelle.

Le cadre ARR prend un caractère unique dans l'attribution des fonctions de commandement, où chaque élément est indivisiblement confié à une seule personne exerçant l'autorité légale pour diriger les opérations militaires. Les fonctions de commandement font porter

le fardeau légal et moral exclusif de la prise de décision; le commandant assume la responsabilité personnelle du succès ou de l'échec de la mission. Tous les autres participants—état-major, personnel du quartier général, organisations de soutien—tirent leur autorité par délégation délimitée par des paramètres établis par celui ou celle à qui incombe la reddition de comptes.

Cette structure hiérarchique assure l'unité de commandement et la clarté de la reddition de comptes, renforcée par la double structure MDN et FAC, au sein de laquelle les militaires des FAC et les employés du MDN opèrent en vertu de chaînes distinctes avec des autorités juridiques distinctes, où la reddition de comptes légale revient à l'organisation de chacun, assurant ainsi une délimitation claire des responsabilités.¹⁰

Les systèmes d'IA interagiront principalement au niveau du personnel et des postes de commandement, où l'information est traitée, fusionnée et convertie en éléments exploitables. Ces couches gèrent les entrées, effectuent des analyses et génèrent des recommandations. L'introduction de l'IA soulève des questions importantes, surtout dans les échelons supérieurs de la hiérarchie cognitive des FAC, sur la possible dilution ou le déplacement du jugement humain. Ces questions sont abordées et explorées plus en profondeur dans la section « Dangers de l'intégration de l'IA ».

Le risque comme logique structurante au sein du MDN et des FAC

Le risque est une logique fondamentale dans les domaines opérationnels et institutionnels du MDN et des FAC. Deux cadres complémentaires guident son application : *Gestion des risques aux fins des opérations des FC* fournit la base doctrinale du risque militaire dans les contextes tactiques et opérationnels, tandis que les *Lignes directrices sur la gestion du risque d'entreprise de la Défense* régissent les considérations au niveau de l'organisation.¹¹ Bien que distincts par ce qu'ils mettent en évidence, les deux cadres renforcent une logique commune : le risque n'est pas simplement un calcul—c'est une discipline de jugement professionnel ancrée dans le contexte, l'autorité et la responsabilité.

Au sein des forces armées, les commandants utilisent le risque pour orienter la prise de décision. Le personnel joue un rôle consultatif essentiel dans la détermination des dangers, la proposition de mesures d'atténuation et la définition des compromis liés aux risques. Le risque se caractérise non seulement par la probabilité et la gravité, mais aussi par des facteurs tels que l'urgence et la contrôlabilité. Le risque ne peut être accepté que par des personnes qui détiennent à la fois une autorité déléguée sur les mesures d'atténuation proposées et qui opèrent dans le cadre de leur autorité résiduelle d'acceptation du risque définie.

La reddition de comptes concernant les risques au sein du MDN et des FAC est personnelle, non procédurale, et elle représente plus qu'une simple protection bureaucratique. Les processus ne peuvent pas être tenus responsables; seules les

personnes le peuvent. Le principe persistant est que *la reddition de comptes incombe à la personne qui accepte le risque*. Cela soulève d'importantes questions institutionnelles : lorsque le risque accepté dans le passé se matérialise dans le présent, qui doit rendre des comptes? Cette reddition de comptes est-elle transférée aux successeurs et, si oui, ces personnes sont-elles pleinement conscientes des risques dont elles sont maintenant responsables?

Le MDN et les FAC auraient avantage à traiter le risque comme une monnaie commune de communication, en promouvant un langage commun entre les fonctions opérationnelles et institutionnelles afin d'améliorer la cohérence et la clarté décisionnelle. Tous les membres du MDN et des FAC n'utilisent pas les cadres de risque de cette façon. Par conséquent, une utilisation cohérente du langage propre aux risques pourrait aider à normaliser et à harmoniser la conscience des risques autour de l'IA dans tous les contextes.¹² La plus grande difficulté consiste à reconnaître que des risques apparemment discrets et à faible enjeu peuvent s'accumuler entre les systèmes et, par des effets de capitalisation, créer des profils de risque agrégés qui dépassent la somme de leurs parties, restant invisibles pour n'importe quel gestionnaire de risques, mais capables de mettre en péril toute l'organisation.¹³

Ces étoiles de repérage aident à orienter l'institution dans un espace inexploré, mais elles n'éliminent pas l'incertitude. Avec ces points de référence établis, l'attention peut désormais se tourner vers les dangers à venir—non pas le long d'un itinéraire prédéterminé, mais avec la discipline de navigation que les sextants et les astrocompas exigeaient autrefois : observation, calcul et orientation avant le mouvement.¹⁴

Risques de l'intégration de l'IA

Comme dans tous les parcours, l'intégration de l'IA au sein du MDN et des FAC a une destination grossièrement tracée telle que définie dans la Stratégie d'IA, mais le processus de navigation doit être agile et adaptable face aux risques connus et émergents, capable de changer de cap au besoin tout en trouvant le chemin.

Premièrement, il est essentiel de reconnaître que l'IA, en particulier les modèles génératifs, ne comprend rien dans le sens humain. Ces systèmes fonctionnent comme des moteurs de reconnaissance de motifs très sophistiqués, capables de générer des extrants plausibles basés sur des régularités statistiques dans les données d'entraînement.¹⁵ Bien qu'ils puissent atteindre une précision surhumaine dans des contextes bien définis, leur fiabilité se dégrade fortement lorsqu'ils sont confrontés à des cas particuliers—le soi-disant *1 % des problèmes*—lorsque des entrées atypiques sortent des schémas appris.¹⁶ Cette limitation ne constitue pas un risque en soi, mais devient un facteur à considérer lors de l'évaluation de l'adéquation des outils d'IA pour des tâches ou domaines spécifiques.

Les dangers suivants sont regroupés selon les dynamiques cognitives et institutionnelles plutôt que les domaines techniques, reflétant la façon dont l'intégration de l'IA va transformer les processus décisionnels à l'échelle de l'organisation de la défense.

Déchargement cognitif, déqualification et érosion du jugement

Les systèmes d'IA promettent de réduire la charge cognitive, en automatisant les tâches gourmandes en données, permettant théoriquement au personnel de passer du mode production au mode évaluation—accéléralant ainsi la progression dans la hiérarchie cognitive vers la compréhension et le jugement. Ce déchargement cognitif reflète des pratiques familières selon lesquelles les humains délèguent des tâches mentales à des systèmes algorithmiques.¹⁷

Cependant, le recours par habitude introduit un compromis crucial. Lorsque la délégation devient une dépendance, une déqualification cognitive se produit, c'est-à-dire la perte progressive de la capacité de raisonnement indépendant, qui est distincte de la décharge en ce qu'elle peut entraîner une érosion à long terme du jugement.¹⁸ Le recours persistant aux outils compatibles avec l'IA peut éroder le jugement individuel et institutionnel en refusant l'exposition aux activités subjectives, basées sur l'expérience aux niveaux inférieurs de la hiérarchie cognitive. Le résultat peut comprendre des dirigeants techniquement compétents qui manquent du jugement intuitif nécessaire pour naviguer dans des environnements ambigus ou dégradés.

Dans les contextes militaires, cela signifie que le personnel doit à la fois exceller dans l'interprétation des résumés de renseignements, générés par l'IA, et posséder l'expérience nécessaire pour détecter que les données sources ont été compromises ou que des tendances ont été manipulées. Mais dans un futur où les systèmes d'IA gèrent la plupart des tâches de traitement et de synthèse, que se passe-t-il lorsque l'humain concerné n'a pas l'expérience personnelle nécessaire pour vérifier l'extrait? Que se passe-t-il lorsque le volume de données dépasse la capacité d'un opérateur humain à effectuer un examen significatif? Les FAC devraient-elles délibérément conserver des produits générés par des humains non habilités par l'IA, aussi inférieurs soient-ils, pour former le personnel selon un jugement indépendant? Bien qu'une telle délégation puisse être acceptable dans des contextes bénins, comment la responsabilité devrait-elle être imputée lorsqu'une décision habilitée à l'IA contribue à l'application illégale de la force létale : la responsabilité est-elle imputable au développeur, au programmeur sous contrat? Qui est accusé du crime de guerre? Un résumé de décision en 2035 pourrait impliquer des extraits générés par l'IA, présentés avec une grande conviction, mais si ces données ont été empoisonnées ou le modèle saboté, et que l'humain présent manque de connaissances approfondies pour les contester, le résultat pourrait non seulement être erroné—il pourrait être erroné d'une manière indétectable. Dans

de tels environnements, la confiance envers l'automatisation doit être accompagnée d'un engagement tout aussi fort à former des dirigeants capables de faire preuve de jugement.

L'adoption de l'IA en défense ne réduit pas le fardeau du perfectionnement professionnel; elle l'augmente. Pour opérer dans des environnements technologiquement dégradés et technologiquement améliorés, le personnel des FAC devra avoir une double maîtrise du jugement centré sur l'humain et de l'analyse assistée par machine. Tout comme pour naviguer sur les mers, la capacité à reconnaître quand quelque chose sort de sa trajectoire dépend moins de l'amélioration des instruments que de la capacité à les utiliser.¹⁹

Biais d'automatisation et aversion aux algorithmes

Le soutien à la décision habilitée à l'IA introduit un double danger : le recours non critique aux extraits algorithmiques (biais d'automatisation) et leur rejet pur et simple, même lorsqu'ils sont statistiquement supérieurs (aversion aux algorithmes).²⁰ Les deux existent sur un continuum, avec une incidence particulièrement aiguë sous la pression du temps au sein des organisations axées sur l'action.

La prise de décision militaire dépend depuis longtemps d'intermédiaires—officiers d'état-major, conseillers, cellules de planification—qui filtrent l'information et cadrent les choix. Le soutien offert par l'IA représente une bureaucratie numérique, structurée par des règles et des réseaux de neurones.²¹ Cependant, les commandants ont toujours compris que le personnel apporte des biais implicites, des intérêts et des limites analytiques. Le risque distinctif de l'IA est le biais induit par les algorithmes : des distorsions intégrées dans les données d'entraînement, les hypothèses du modèle ou les entrées environnementales, souvent cachées aux utilisateurs finaux et difficiles à détecter. Les solutions au biais algorithmique sont incertaines, mais une solution claire en attendant consiste à mettre en place un système de freins et contrepoids avec des humains dans la boucle pour vérifier les extraits de l'IA.

La traçabilité, à savoir la capacité de comprendre comment une recommandation a été générée, est devenue une préoccupation majeure dans ce contexte.²² Pourtant, cela aussi a un précédent. Le jugement expert humain repose souvent sur une connaissance tacite qui résiste à l'articulation formelle.

Au sein du MDN et des FAC, la difficulté ne réside pas dans l'élimination des biais ou de l'aversion, mais dans leur gestion par des processus solides et une supervision humaine délibérée.²³ Si la surveillance humaine des recommandations de l'IA se traduit par de simples cases à cocher pour accélérer le processus, l'utilité du soutien décisionnel est perdue.²⁴ Inversement, si le scepticisme mène à la paralysie, l'avantage de l'IA n'est jamais réalisé. Le succès exige des autorités et des responsabilités clairement définies pour déterminer qui vérifie les extraits, quand

faire une pause pour une analyse plus approfondie, et comment acheminer un problème au commandement supérieur lorsqu'il semble anormal.

Zones de déformation morale et illusion de responsabilité

Le concept de *zones de déformation morale*, présenté par Madeline Elish, fait référence à la tendance humaine à absorber le blâme lorsque les systèmes autonomes échouent, peu importe le contrôle ou l'auteur véridique.²⁵ La personne « dans la boucle » qui vérifie les extrants d'un système automatisé devient le visage de la reddition de comptes, même lorsque la prise de décision a été largement déléguée à un système opaque et distribué. Cette illusion de reddition de comptes devient de plus en plus problématique à mesure que la complexité du système augmente et que l'explication devient moins accessible.²⁶

En regardant vers une organisation du MDN et des FAC habilitée à l'IA d'ici 2030, cette préoccupation passe de la théorie à la réalité. Si les futurs outils d'IA continuent de fonctionner comme des boîtes noires, produisant des extrants sans raisonnement transparent ou interprétable, les structures de reddition de comptes doivent être réévaluées. Le développement rapide de l'IA, la complexité et l'autonomie croissantes des systèmes, ainsi que le potentiel d'amélioration récurrente et d'auto-modification des systèmes d'IA menacent de pousser ces systèmes au-delà de la compréhension humaine.²⁷ À mesure que la frontière entre autorité et responsabilité s'estompe, dans des systèmes de plus en plus automatisés, le fardeau de rendre des comptes reste fortement concentré, souvent de manière disproportionnée, sur l'humain le plus proche.

Cela soulève des questions pressantes pour le travail d'équipe humain-machine : qui est tenu responsable quand quelque chose tourne mal?²⁸ L'opérateur, le commandant tactique, le gestionnaire de projet, la compagnie sous contrat ou l'équipe d'entraînement du modèle? Bien que les défaillances puissent être rares, leur gravité peut être considérable tant pour les personnes touchées que pour la confiance institutionnelle.

En pratique, il est très probable qu'une personne soit blâmée pour des échecs liés à l'IA, mais les conséquences ultérieures de ce reproche méritent d'être retenues. Si le MDN et les FAC souhaitent rester ancrés dans l'éthique tout en étendant l'intégration de l'IA, ils doivent doter tout le personnel concerné non seulement d'outils pour prendre des décisions, mais aussi de cadres pour partager la reddition de comptes et la complexité morale des processus.

Propriété institutionnelle et propriété intellectuelle générative

La décision *Lukits c. MDN* de 2019 rendue par la Commission des relations de travail et de l'emploi dans le secteur public

fédéral a confirmé le droit d'un professeur du Collège militaire royal du Canada de conserver la propriété de notes de cours manuscrites.²⁹ Bien que la décision *Lukits* ait justement confirmé la liberté académique,³⁰ elle révèle aussi une vulnérabilité institutionnelle dans la manière dont la Couronne revendique la propriété des connaissances produites par son personnel. Quelle est la position du MDN et des FAC pour gérer la propriété intellectuelle à l'ère de l'IA?

Les outils d'IA générative compliquent encore plus la situation. Contrairement aux notes de cours manuscrites, les extrants de l'IA générative sont façonnés par des prédictions statistiques, informés par des consignes de l'utilisateur et traités par l'infrastructure commerciale. Les produits résultants—texte, images, code, concepts de conception—peuvent être affinés par l'utilisateur, mais ils ne sont pas facilement traçables pour ce qui est de l'auteur ou du détenteur. Les directives du Conseil du Trésor visant à ce que les employés consultent les services juridiques, examinent les modalités de licence et restent informés de l'évolution du droit de l'IA³¹ sont bien intentionnées, mais peu pratiques. Tous les membres du MDN et des FAC ne sont pas des spécialistes en propriété intellectuelle, et aucune capacité n'a été allouée pour garantir que l'utilisateur moyen de l'IA au MDN et dans les FAC peut gérer ce fardeau. La responsabilité de gérer le risque de propriété intellectuelle ne devrait pas être transférée aux utilisateurs individuels.

On ne peut présumer que la Couronne est propriétaire des extrants de l'IA générative codéveloppés. Si les données ou les artefacts de conception générés au sein du MDN et des FAC sont absorbés ou monétisés par des fournisseurs commerciaux au moyen d'accords de licence peu clairs,³² les répercussions résultantes pourraient être considérables. Le problème n'est pas l'absence de politiques, mais le défaut de fournir une orientation claire et sans ambiguïté.

Une autorité désignée, comme le Centre d'IA du MDN et des FAC, devrait être habilitée à émettre des directives exécutoires sur la propriété, la licence et l'utilisation des données à l'ensemble de tous les outils d'IA adoptés. Il s'agit d'une exigence immédiate, pas un sujet d'étude à approfondir. Il est déraisonnable de s'attendre à ce que le personnel militaire ou civil gère lui-même la conformité légale. Une situation qui entraîne le risque de perdre le contrôle institutionnel sur les connaissances critiques pour la mission et ouvre la porte à l'érosion de l'intégrité de l'information.

Évaluation des données : signification contextuelle et aveuglement systémique

Les systèmes d'IA déduisent la valeur statistiquement, mais la planification militaire repose souvent sur des renseignements rares et spécifiques au contexte.³³ Cela devient complexe à mesure que les modèles sont entraînés sur de grands volumes de données non structurées et gouvernées de manière

incohérente.³⁴ Le paragraphe d'intention d'un ordre d'opérations peut apparaître une fois tandis que les détails administratifs se répètent tout au long. Toutefois, l'IA peut surévaluer la répétition plutôt que le contenu critique pour le jugement. Sans la capacité d'entreprise à signaler les intrants faisant autorité, les systèmes ne peuvent pas distinguer l'autorité déléguée du bruit administratif, ce qui augmente considérablement le risque.

Il demeure une incertitude à savoir si la capacité d'entreprise actuelle du MDN et des FAC existe pour indiquer que certains intrants devraient être traités comme supérieurs à d'autres. Comment les FAC s'assurent-elles qu'une directive révisée par le Chef d'état-major de la Défense ou un ordre modifiant les règles d'engagement d'une force opérationnelle déployée est enregistré comme un changement significatif plutôt qu'un simple document de plus? Comment s'assurer que le contenu supplanté ne continue pas à influencer les résultats simplement parce qu'il apparaît plus fréquemment dans les ensembles de données?

L'importance des données est contextuelle, elle évolue dans le temps, tandis que les modèles d'IA sont optimisés pour détecter les tendances, et non l'importance. Le même point de données peut être crucial dans un contexte, sans importance dans un autre, et trompeur dans un troisième.³⁵ Le MDN et les FAC doivent soit développer des mécanismes qui reconnaissent et préservent le contexte changeant au fil du temps, soit formaliser des rôles humains dans la boucle spécifiquement destinés à préserver le sens contextuel dans les processus habilités par l'IA.³⁶

Avancer malgré l'incertitude³⁷

Le MDN et les FAC devraient considérer l'IA comme une technologie d'usage général, nécessitant une préparation immédiate. La trajectoire du développement de l'IA et sa convergence avec des domaines militaires clés suggèrent fortement qu'elle remodelera à la fois le champ de bataille et l'environnement institutionnel dans lequel le MDN et les FAC opèrent. Cela justifie un changement de cap délibéré vers la préparation à l'IA : institutionnelle, procédurale et culturelle. Se préparer maintenant pose les bases essentielles pour affronter les perturbations futures causées par d'autres technologies émergentes, y compris les menaces de l'ère quantique.

Les préoccupations de souveraineté devraient être vues comme une contrainte à gérer, et non comme un obstacle à surmonter. L'échelle des infrastructures requises pour les modèles d'IA actuels et futurs est vaste et il est peu probable qu'il soit possible pour le Canada de développer un ensemble d'IA souverain à court terme.³⁸ Un certain degré de dépendance, envers les infrastructures d'infonuagique et de données privées et étrangères existantes, restera nécessaire. Cependant, toutes les données ou tous les processus ne nécessitent pas une classification ou un contrôle maximal.³⁹ Pour ceux dont c'est le cas, des centres de données souverains sécurisés peuvent être construits, s'ils n'existent pas déjà. Pour ceux qui se situent dans la zone grise entre les deux, le MDN et les FAC peuvent utiliser

des technologies d'amélioration de la confidentialité (TAC), des enclaves de données et d'autres outils pour maximiser la souveraineté et la protection des données tout en continuant d'utiliser des infrastructures privées de haute qualité hébergées dans les pays alliés.⁴⁰ Tant que l'on sait clairement ce qui doit rester souverain et ce qui peut être externalisé de manière responsable avec des garanties, un degré raisonnable de protection peut être assuré.⁴¹

L'interopérabilité numérique est désormais stratégique. Dans un environnement où les alliés intègrent rapidement l'IA dans les opérations, le Canada doit suivre le rythme pour conserver son influence et sa crédibilité.⁴² Un pays en retard risque de devoir suivre les normes plutôt que les façonner. Si le Canada veut façonner l'utilisation éthique et opérationnelle de l'IA, le MDN et les FAC doivent maintenir une présence crédible dans ces discussions grâce à une capacité significative et à des expérimentations démontrées.

L'écosystème intérieur canadien de l'IA représente un avantage national.⁴³ L'expertise universitaire, la capacité d'innovation et l'industrie existent déjà. L'axe de travail 5 de la Stratégie d'IA appelle au développement de partenariats basés sur la confiance qui assurent la mission et servent les intérêts nationaux canadiens.

Recommandations stratégiques

Les recommandations suivantes tracent une orientation délibérée vers une intégration responsable de l'IA au sein du MDN et des FAC, reflétant les axes de travail intégrés définis dans la Stratégie d'IA et guidés par des points de référence institutionnels durables :

1. Considérer l'IA comme une technologie polyvalente à des fins de planification et commencer une mise en œuvre structurée en conséquence.
2. Considérer le Plan de campagne numérique des FAC et la Stratégie d'IA comme des guides de réinvention de l'organisation, et non comme des initiatives distinctes.
3. Institutionnaliser le risque comme un langage partagé entre les sphères opérationnelle et institutionnelle, afin d'améliorer la capacité à suivre et gérer l'accumulation globale des risques, particulièrement lorsque l'IA introduit la prise de décision distribuée.
4. Développer une double capacité : le personnel doit opérer efficacement à la fois dans des environnements habilités par l'IA et des environnements privés de technologie.
5. Distinguer de manière pragmatique les exigences de souveraineté en ce qui concerne les données et les processus nécessitant un contrôle gouvernemental total et ceux permettant une externalisation sécurisée.
6. Exploiter l'interopérabilité comme un vecteur d'influence stratégique, et non seulement pour la compatibilité technique, afin d'aider le Canada à façonner les normes émergentes de l'IA appliquée à la défense.

Intégrer l'adoption de l'IA au sein du MDN et des FAC dans la planification globale de l'écosystème, afin de s'assurer que les contextes de défense informent la gouvernance gouvernementale générale concernant l'IA.

Conclusion

Ces étoiles-repères, à savoir la hiérarchie cognitive, le cadre ARR et la logique structurante du risque, brillent davantage dans un environnement habilité à l'IA, non pas malgré la transformation technologique, mais précisément grâce à celle-ci. Dans un cadrage doctrinal Fins-Méthodes-Moyens, l'IA modifie fondamentalement les *moyens* de prendre les décisions grâce à des modèles basés sur les données, le raisonnement probabiliste et des systèmes capables d'une adaptation exponentiellement plus rapide. Ces nouveaux moyens exigent de nouvelles *méthodes* (processus révisés, doctrine adaptée, perfectionnement des compétences et littératie numérique) permettant au personnel de remettre en question la fiabilité, la traçabilité et la pertinence

pour la mission des extrants générés par l'IA. Les *fins*, à savoir la prise de décision efficace dans des environnements volatils, incertains, complexes et ambigus, demeurent constantes.

L'avantage stratégique du Canada réside dans une adoption efficace de l'IA, alignée sur les valeurs canadiennes et sensible aux besoins du pays. La légitimité du Canada découle de la recherche de calibre mondial, d'une instruction militaire professionnelle et de partenariats solides, mais fondamentalement du respect des droits et des valeurs. Le fait de canaliser ces principes dans des cadres d'IA permet de créer des outils supérieurs et des extrants plus souhaitables.

Le sextant et l'astrocompas métaphoriques nous rappellent que, bien que les outils évoluent, la discipline de la navigation perdure. La voie à suivre par le Canada exige un progrès délibéré, guidé par la sagesse institutionnelle et les valeurs démocratiques, des principes de navigation qui tracent une trajectoire dans des eaux incertaines tout en gardant une véritable orientation.

Notes

- Rédigé par le colonel Adam Moore pendant un congé sabbatique dans le domaine de la défense (août 2024-mai 2025), alors qu'il était chercheur invité à l'Université Queen's. Une version plus longue a paru au Centre for International and Defence Policy (CIDP) de l'Université Queen's en 2025.
- Service canadien du renseignement de sécurité, Rapport public du SCRS 2023, 2024, source d'origine : <https://www.canada.ca/fr/service-renseignement-securite/organisation/publications/rapport-public-du-scrs-2023.html>; ministère de la Défense nationale, Commandement et contrôle pandomaine (C2PD) : document de conception, 2024, source d'origine : <https://www.canada.ca/fr/ministere-defense-nationale/organisation/rapports-publications/commandement-contrôle-pan-domaine.html>. Voir Lily Jamali, « DeepSeek AI Shakes American Swagger and Upends Assumptions », BBC News, 28 janvier 2025, source d'origine : <https://www.bbc.com/news/articles/cd643wx888qo>.
- Voir Ron Lloyd, « Public Service Culture, Risk Management and Governance: The Prerequisite of Effective Strategic Governance to Realizing Our Digital Ambition », Institut canadien des affaires mondiales, 2024, source d'origine : <https://www.cgai.ca/public-service-culture-risk-management-and-governance-the-prerequisite-of-effective-strategic-governance-to-realizing-our-digital-ambition>.
- Ministère de la Défense nationale (MDN), La Stratégie d'intelligence artificielle du ministère de la Défense nationale et des Forces armées canadiennes, 2024, source d'origine : <https://www.canada.ca/fr/ministere-defense-nationale/organisation/rapports-publications/mdn-fac-strategie-intelligence-artificielle.html>.
- Inspiré de la sélection de l'École de la fonction publique du Canada comprenant M. Stewart-Weeks et S. Cooper, « We're Missing the Point of Digital Government - Here's Why. Opinion: Digital Experts Understand Tech - but Do They Understand Government? », Apolitical, 13 août 2019. Source d'origine : <https://apolitical.co/solution-articles/en/why-were-missing-the-point-in-digital-government>.
- Reproduction d'une image tirée de MDN, La Stratégie d'intelligence artificielle du ministère de la Défense nationale et des Forces armées canadiennes, 2024, p. 1.
- Représentation adaptée par l'auteur, inspirée du Mission Command Training Program de l'U.S. Army. Cette représentation concorde avec les explications relatives à la hiérarchie cognitive des FAC dans MDN, B-GL-300-003/FP-002, Le commandement dans les opérations terrestres, 2007; MDN, B-GL-331-001/FP-002, Soutien au commandement dans les opérations terrestres, 2008; et MDN, Publication interarmées des Forces canadiennes 01 : Doctrine militaire canadienne, 2e éd., 2024. L'image source figure dans U.S. Army, FY 24 Mission Command Training Program Key Observations, Center for Army Lessons Learned, 2025, figure 2-1, « Cognitive Hierarchy », p. 10. Source d'origine : <https://api.army.mil/e2/c/downloads/2025/02/24/aea2698e/25-04-946-fy-24-mctp-key-observations-feb-25.pdf>.
- L'utilisation en croisé des détecteurs « implique la transmission d'information relative à la détection, à la géolocalisation et à l'acquisition de cibles d'un capteur à un autre », ce qui permet d'améliorer l'efficacité. MDN, Doctrine de l'Aviation royale canadienne : renseignement, surveillance et reconnaissance, 2017, p. 2-2.
- MDN, *Accountabilities, Responsibilities, and Authorities*, Secrétariat général, 2024.
- MDN, Publication interarmées des Forces canadiennes 01 : Doctrine militaire canadienne, 2e éd., 2024.
- MDN, Gestion des risques aux fins des opérations des Forces canadiennes, 2007. MDN, Lignes directrices sur la gestion du risque d'entreprise de la Défense, 2018.
- L'Institut national des normes et des technologies (NIST), AI Risk Management Framework, NIST AI 100-1, 2023, source d'origine : <https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf>, fournit des orientations utiles pour l'analyse institutionnelle des risques.
- Voir Lloyd (note iii).
- L'outil d'évaluation de l'incidence algorithmique (EIA) du Conseil du Trésor met l'accent sur la gravité des incidences plutôt que sur leur probabilité, ce qui cadre mal avec les modèles de gestion des risques de la défense, qui exigent la prise en compte de ces deux facteurs. Comme de nombreuses applications du MDN et des FAC comportent peu de renseignements personnels canadiens, une application stricte de l'EIA pourrait retarder inutilement des applications opérationnelles à grande utilité. Un modèle d'évaluation adapté ou des exceptions contrôlées pourraient mieux répondre aux besoins de la défense tout en maintenant une supervision éthique. Secrétariat du Conseil du Trésor du Canada, « Stratégie en matière d'intelligence artificielle pour la fonction publique fédérale 2025-2027 », 4 mars 2025, source d'origine : <https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/innovations-gouvernementales-numeriques/utilisation-responsable-ai/gc-ai-strategie-apercu.html>.
- Shannon Vallor, *The AI Mirror: How to Reclaim Our Humanity in an Age of Machine Thinking*, Oxford University Press, 2024.
- Max Lamparth et Jacquelyn Schneider, « Why the Military Can't Trust AI », Foreign Affairs, 2024, <https://www.foreignaffairs.com/united-states/why-military-cant-trust-ai>. Karine Perset et Sara Fialho Esposito, How Are AI Developers Managing Risks? Insights from Responses to the Reporting Framework of the Hiroshima AI Process Code of Conduct, OECD Artificial Intelligence Papers, Paris : Éditions OCDE, 2025, p. 33, source d'origine : https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/09/how-are-ai-developers-managing-risks_fbab3ad6/658c2ad6-en.pdf.

- 17 Sandra Grinschgl, Frank Papenmeier et Hauke S. Meyerhoff, « Consequences of Cognitive Offloading: Boosting Performance but Diminishing Memory », *Quarterly Journal of Experimental Psychology*, vol. 74, n° 9 (2021), p. 1477-1496. Source d'origine : <https://doi.org/10.1177/17470218211008060>.
- 18 Leslie Paul Thiele, « Rise of the Centaurs: The Internet of Things Intelligence Augmentation », dans *Towards an International Political Economy of Artificial Intelligence*, sous la direction de Tugrul Keskin et Ryan David Kiggins, p. 39-61, Springer International Publishing, 2021, source d'origine : <https://link.springer.com/book/10.1007/978-3-030-74420-5>. La déqualification cognitive est étroitement liée au concept d'érosion des compétences morales. Pour une analyse approfondie de ce dernier, voir Shannon Vallor, « Moral Deskillling and Upskilling in a New Machine Age: Reflections on the Ambiguous Future of Character », *Philosophy & Technology*, vol. 28, n° 1 (2015), p. 107-124.
- 19 Des recherches supplémentaires sont nécessaires sur l'incidence de l'IA sur les connaissances tacites au sein des FAC. Comme les systèmes d'IA fonctionnent à partir de données structurées et explicites, tandis que l'expertise militaire repose largement sur des connaissances expérientielles non consignées, un recours excessif à l'IA risque d'éroder le jugement expert si les systèmes remplacent l'expérience humaine plutôt que l'augmenter. Pour en savoir plus sur la dévalorisation du jugement professionnel, voir Tom M. Nichols, *The Death of Expertise: The Campaign against Established Knowledge and Why It Matters*, Oxford University Press, 2017.
- 20 L'expression « biais d'automatisation » s'appuie ici directement sur Anna Nadibaidze, Ingvild Bode et Qiaochu Zhang, *AI in Military Decision Support Systems: A Review of Developments and Debates*, 2024, source d'origine : https://findresearcher.sdu.dk/ws/portals/portal/275893410/Al_DSS_report_WEB.pdf; l'« aversion algorithmique » est définie de façon plus souple d'après Ekaterina Jussupow, Izak Benbasat et Armin Heinzl, « Why Are We Averse Towards Algorithms? A Comprehensive Literature Review on Algorithm Aversion », dans ECIS 2020 Proceedings, conférence virtuelle, Association for Information Systems, 2020, source d'origine : https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1167&context=ecis2020_rp.
- 21 Inspiré d'une extrapolation logique de l'idée suivante : « if the economy is an information processing system, does that mean that every corporation is an artificial intelligence? »; Dan Davies, *The Unaccountability Machine: Why Big Systems Make Terrible Decisions—and How the World Lost Its Mind*, Profile Books, 2024, p. 63.
- 22 Mariarosaria Taddeo, David McNeish, Alexander Blanchard et Elizabeth Edgar, « Ethical Principles for Artificial Intelligence in National Defence », *Philosophy & Technology*, vol. 34, n° 4 (2021), p. 1707-1729, source d'origine : <https://doi.org/10.1007/s13347-021-00482-3>, p. 1717-1718; Stratégie d'IA du MDN et des FAC, 2024, p. 18.
- 23 Davies, *The Unaccountability Machine*, p. 78-79.
- 24 Nadibaidze, Bode et Zhang, *AI in Military Decision Support Systems*, p. 33.
- 25 Madeleine Clare Elish, « Moral Crumple Zones: Cautionary Tales in Human-Robot Interaction », *Engaging Science, Technology, and Society*, vol. 5 (23 mars 2019), p. 40-60, source d'origine : <https://doi.org/10.17351/ests2019.260>.
- 26 S. Kate Devitt, « Bad, Mad, and Cooked: Moral Responsibility for Civilian Harms in Human-AI Military Teams », dans *Responsible Use of AI in Military Systems*, sous la direction de Jan Maarten Schraagen, p. 248-277, Chapman and Hall/CRC, 2024, source d'origine : <https://doi.org/10.1201/9781003410379-16>.
- 27 Mustafa Suleyman a mis en garde contre ces risques (Mustafa Suleyman et Michael Bhaskar, *The Coming Wave: Technology, Power, and the Twenty-First Century's Greatest Dilemma*, Crown, 2023), et Dan Davies formule une observation semblable : lorsque l'explication devient impossible, l'examen du code source n'apporte aucun éclairage réel sur les causes ou les conséquences (Davies, *The Unaccountability Machine*, p. 76).
- 28 Voir Elish, « Moral Crumple Zones: Cautionary Tales in Human-Robot Interaction », p. 54; Nadibaidze, Bode et Zhang, *AI in Military Decision Support Systems*, p. 40-41.
- 29 Lukits c. Conseil du Trésor (ministère de la Défense nationale), 2019 CRTESP 32 (CanLII), Commission des relations de travail et de l'emploi dans le secteur public fédéral, 13 mars 2019. Source d'origine : <https://decisions.fpslreb-crtespf.gc.ca/fpslreb-crtespf/d/fr/item/407680/index.do>.
- 30 Secrétariat du Conseil du Trésor du Canada, « Enseignement universitaire (UT) : Convention entre le Conseil du Trésor et l'Association des professeurs des collèges militaires du Canada », source d'origine : <https://www.canada.ca/fr/secretariat-conseil-tresor/sujets/remuneration/conventions-collectives.html>.
- 31 Secrétariat du Conseil du Trésor du Canada, « Guide sur l'utilisation de l'intelligence artificielle générative », 20 février 2024, source d'origine : <https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/innovations-gouvernementales-numeriques/utilisation-responsable-ai/guide-utilisation-intelligence-artificielle-generative.html>.
- 32 Voir, par exemple, Sean McManus, « Why Employees Smuggle AI into Work », *BBC News*, 3 février 2025, source d'origine : <https://www.bbc.com/news/articles/cn7rx05xq2go>.
- 33 Avi Goldfarb et Jon R. Lindsay, « Prediction and Judgment: Why Artificial Intelligence Increases the Importance of Humans in War », *International Security*, vol. 46, n° 3 (2022), p. 7-50, source d'origine : https://doi.org/10.1162/isec_a.00425.
- 34 Avi Goldfarb et Jon R. Lindsay, « Artificial Intelligence in War: Human Judgment as an Organizational Strength and a Strategic Liability », *Foreign Policy at Brookings*, 2020, source d'origine : https://www.brookings.edu/wp-content/uploads/2020/11/tp_20201130_artificial_intelligence_in_war.pdf.
- 35 Vallor, *The AI Mirror*, p. 26-27; Nadibaidze, Bode et Zhang, *AI in Military Decision Support Systems*, p. 36-38.
- 36 Sur les données contextuelles dans le déploiement de l'IA, voir M. da Mota, « Toward an AI Policy Framework for Research Institutions », Centre pour l'innovation dans la gouvernance internationale, 2024, source d'origine : <https://www.cigionline.org/publications/toward-an-ai-policy-framework-for-research-institutions/>.
- 37 Réflexion de l'auteur fondée sur les connaissances acquises pendant le congé sabbatique dans le domaine de la défense; aucune source publique ou universitaire n'est citée.
- 38 Pour en savoir plus sur les débats entourant une « pile souveraine » canadienne pour l'IA, voir les travaux émergents du Canadian AI Sovereignty and Innovation Cluster, source d'origine : <https://caisic.ca/>; du Conseil canadien des innovateurs <https://www.canadianinnovators.org/fr-ca/>; de la Canadian AI Adoption Initiative, source d'origine : <https://www.aiadoption.ca/>; ainsi que d'Innovation, Sciences et Développement économique Canada, Stratégie canadienne sur la capacité de calcul souveraine pour l'IA, 2025, source d'origine : <https://ised-isde.canada.ca/site/ised/fr/strategie-canada-puissance-calcul-souveraine-pour-lia>.
- 39 Pour un examen critique du cadre de classification du Canada sous l'angle numérique, voir : Ron Lloyd, « Canada's Security Classification Framework: The Biggest Impediment to Realizing Our Digital Ambition », Institut canadien des affaires mondiales, 2024. Source d'origine : https://www.cgai.ca/canadas_security_classification_framework_the_biggest_impediment_to_realizing_our_digital_ambition.
- 40 Pour en savoir plus sur les technologies renforçant la protection de la vie privée qui favorisent la souveraineté de l'IA, voir : OCDE, « Sharing Trustworthy AI Models with Privacy-Enhancing Technologies », *OECD Artificial Intelligence Papers*, n° 38, 2025, source d'origine : https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/06/sharing-trustworthy-ai-models-with-privacy-enhancing-technologies_5df6fd05/a266160b-en.pdf.
- 41 Services partagés Canada et le Centre de la sécurité des télécommunications ont mis en place, et continuent de développer, l'infrastructure et de définir les paramètres nécessaires à la mise en œuvre de ces politiques.
- 42 Par exemple, voir : OTAN, « Stratégie OTAN pour l'intelligence artificielle - synthèse pour mise en lecture publique », 2024, source d'origine : <https://www.nato.int/fr/about-us/official-texts-and-resources/official-texts/2024/07/10/summary-of-natos-revised-artificial-intelligence-ai-strategy>.
- 43 MDN, « Songer à la sécurité lorsqu'on adopte l'intelligence artificielle », DDN2-V46, École de la fonction publique du Canada, 2024, source d'origine : <https://www.cspc-efpc.gc.ca/video/ai-security-fra.aspx>.



Des membres de la compagnie Talon des Forces armées canadiennes effectuent une mission de reconnaissance (Reco) au cours de l'exercice Wolverine Shield/Strike, au Camp Adazi, en Lettonie, le 7 mars 2023.

Technicien en imagerie des Forces armées canadiennes

L'authenticité comme arme : l'avantage des Forces armées canadiennes dans la guerre de l'information à l'ère de l'IA

ALI MANOUCHEHRI ET MAJOR TYLER CURRIE

Ali Manouchehri est actuellement conseiller principal au Centre d'IA du MDN et des FAC. Avant de se joindre au GSN, il occupait le poste de gestionnaire des données et de l'analytique au sein du SMA (Svc Ex) du MDN.

Le major Tyler Currie occupe le poste d'agent d'intégration et d'accélération de l'IA des FAC au Centre d'IA du MDN et des FAC. Tyler a passé 16 ans au sein de la Branche des services du renseignement et a participé à des opérations de déploiement en Afghanistan ainsi qu'à des missions internationales auprès du Commandement allié de forces interarmées de Naples. Il est titulaire d'une maîtrise en études politiques de l'Université Queen's ainsi que d'une maîtrise en gestion—option Intelligence artificielle (MMAI) de la Smith School of Business de l'Université Queen's.

Le ministère de la Défense nationale (MDN) et les Forces armées canadiennes (FAC) évoluent dans un environnement informationnel où, en situation de crise, la certitude est la première victime.

Par exemple, au cours d'un incident aérospatial relevant du Commandement de la défense aérospatiale de l'Amérique du Nord (NORAD), alors que les forces assurent le suivi d'un aéronef non identifié et interviennent, les commandants et les équipes des affaires publiques peuvent devoir composer simultanément avec une autre menace : des fichiers audio, des vidéos et des textes manipulés au moyen de l'IA qui circulent à la vitesse des machines.¹ Ce qui exigeait autrefois des studios, des budgets importants et plusieurs semaines de travail peut maintenant être produit en quelques minutes au moyen de services d'IA et d'applications de montage largement accessibles, puis diffusé rapidement auprès du public.

Cette réalité opérationnelle met en évidence un autre type de défi, lié à la confiance. L'intelligence artificielle générative accélère la production de contenus convaincants, mais mensongers. Une situation qui fausse les perceptions du public dès les premiers instants d'un incident et complique la gestion de crise au moment le plus critique. Lorsque la confiance s'effrite, la transmission et l'exécution des ordres prennent plus de temps, la coordination ralentit et le risque de conséquences graves augmente.

Dans ce contexte, le Canada est confronté aux mêmes pressions dans l'ensemble de ses missions. À l'étranger, nous menons des opérations avec les alliés, où l'étroite coordination des messages et des décisions est essentielle au maintien de l'unité d'action dans les opérations de coalition. Au pays, le MDN et les FAC viennent en aide à la population canadienne lors de situations de crise—feux de forêt, inondations, opérations de recherche et sauvetage—souvent sous l'œil attentif du public, où les communications doivent être rapides, exactes et dignes de confiance.

Dans le Nord, les grandes distances, les conditions météorologiques rigoureuses et les infrastructures limitées influencent la façon dont l'information circule et dont les collectivités perçoivent le danger. Dans chacun de ces contextes, la capacité d'authentifier un message officiel, de rassurer la population avec calme face à des affirmations trompeuses et de garder une longueur d'avance dans la bataille de l'information est essentielle à la réussite de la mission.

Le raisonnement est simple. Le Canada, de concert avec ses alliés, peut rivaliser efficacement avec ses adversaires sur les plans de la sophistication technologique et de la puissance de calcul, et même les dépasser dans certains domaines technologiques émergents grâce à une main-d'œuvre hautement qualifiée et diversifiée sur le plan culturel, ainsi qu'à une approche fondée sur la collaboration avec ses alliés. L'essentiel consiste à démontrer que nos communications proviennent bien de nous, à vérifier les nouvelles informations avant d'agir et à informer rapidement le public lorsque nous sommes confrontés à la mésinformation ou à la désinformation. En faisant de ces pratiques une norme dans les politiques, la formation, l'approvisionnement et le leadership, le MDN et les FAC préservent leur crédibilité et leur rythme opérationnel face aux acteurs étatiques, aux groupes

mandataires et aux individus opportunistes qui cherchent à exploiter le chaos informationnel à des fins stratégiques.

Nous n'avons pas besoin de surpasser nos adversaires en programmation. En revanche, nous devons être capables de démontrer que nos communications proviennent bien de nous, de vérifier les nouvelles informations avant d'agir et d'informer rapidement le public lorsque nous sommes confrontés à la mésinformation ou à la désinformation.

Les nouvelles conditions de la déception

Les systèmes génératifs apprennent à partir de vastes ensembles de textes, d'images et d'enregistrements audio, puis produisent de nouveaux contenus qui reproduisent les caractéristiques observées. Ils ne raisonnent pas comme les êtres humains.² Parce qu'ils sont conçus pour imiter un style plutôt que pour vérifier les faits, ils peuvent produire des contenus fluides qui paraissent exacts et crédibles, même lorsqu'ils sont faux. Lorsque ces contenus reprennent des éléments familiers, comme une voix connue, une formulation officielle ou une image réaliste, le public est naturellement porté à les considérer comme crédibles.

Les organisations de défense canadiennes doivent désormais composer avec des adversaires capables de produire des imitations convaincantes de contenus officiels en quelques minutes plutôt qu'en plusieurs semaines.³ Ce qui exigeait autrefois du temps, des ressources financières et du matériel spécialisé est désormais peu coûteux et largement accessible. Un article fabriqué de toutes pièces, une image falsifiée ou un enregistrement vocal cloné peuvent être créés rapidement puis diffusés sur de multiples plateformes à un coût négligeable.

Pour les praticiens de la défense, ces changements entraînent trois pressions qui se renforcent mutuellement :

- **La rapidité.** Les adversaires peuvent introduire des contenus manipulés dans l'environnement informationnel alors même que les événements sont encore en cours. Un extrait audio falsifié d'un ordre d'évacuation peut se propager sur les réseaux sociaux avant même que les autorités provinciales aient eu le temps de rédiger le véritable message.⁴ Dans un contexte opérationnel, un fragment d'ordre fabriqué de toutes pièces peut parvenir à une unité avant que le quartier général n'ait confirmé l'ordre réel. La rapidité constitue l'avantage de l'adversaire, puisqu'un simple moment d'hésitation suffit à briser le rythme des opérations et à semer le doute.
- **Le coût.** Les outils génératifs sont largement accessibles, faciles à utiliser et peu coûteux. Ce qui nécessitait auparavant des suites de montage professionnelles et du personnel spécialisé peut aujourd'hui être réalisé à l'aide d'un ordinateur portable et d'un simple abonnement à un logiciel. Ainsi, des États hostiles, des groupes mandataires ou même des acteurs isolés peuvent agir à grande échelle. La défense doit donc faire face non seulement à la

désinformation orchestrée par des États, mais aussi à des tentatives opportunistes d'ingérence menées par des acteurs qui ont peu à perdre.⁵

- **La précision.** Les adversaires peuvent tester et affiner leurs messages en temps quasi réel, en fonction de ce qui trouve un écho auprès de publics précis. Une séquence vidéo manipulée qui ne suscite pas la réaction souhaitée dans une collectivité peut être rapidement reformulée et diffusée de nouveau auprès d'une autre.⁶ Cette précision itérative leur permet d'adapter leurs contenus non seulement selon la langue ou la région, mais aussi en exploitant les récits ou les craintes propres à des groupes ciblés, notamment les familles des militaires, les communautés issues de la diaspora ou les partenaires alliés.

Pour le MDN et les FAC, il en résulte un environnement opérationnel où il est possible de créer l'incertitude plus rapidement, à moindre coût et avec davantage de précision que jamais auparavant. Un ordre retardé, un message discrédité par le doute ou une directive concurrencée par une imitation convaincante contribuent tous à éroder la confiance. Les adversaires n'ont plus besoin de tromper tout le monde. Il leur suffit de semer le doute chez un nombre suffisant de personnes, à des moments clés, pour perturber la coordination.

Pour contrer cette menace, l'authentification doit devenir une pratique courante des communications militaires, renforcée par la formation et le leadership jusqu'à devenir un réflexe. Dans le contexte actuel, l'authentification désigne la vérification de l'origine et de l'intégrité d'un message dans la chaîne de commandement. La perception plus générale de l'authenticité, c'est-à-dire la confiance que le public accorde aux communications officielles, demeure essentielle, mais elle relève d'une notion distincte des mécanismes techniques de protection.

Lorsque l'authentification devient une pratique habituelle, qu'il s'agisse de confirmer les ordres dans la chaîne de commandement, d'intégrer des marqueurs d'authenticité aux communications publiques ou de mettre les procédures de vérification en pratique durant les exercices, le rythme des opérations et la crédibilité demeurent entre les mains de l'institution plutôt que de ceux qui cherchent à les perturber.⁷ Ainsi, l'authentification ne constitue pas seulement une pratique de communication; elle représente une mesure de sécurité opérationnelle. Elle protège le rythme des opérations, préserve l'unité d'action et maintient l'avantage décisionnel.

La vérité mise à l'épreuve dans une démocratie

Les dynamiques qui compliquent la prise de décisions sur le plan opérationnel ne se limitent pas au niveau tactique. Elles s'étendent à l'environnement plus vaste dans lequel le MDN et les FAC doivent expliquer leurs décisions à la population canadienne,

rendre des comptes au Parlement et coordonner leurs activités avec leurs alliés. Lorsque des contenus synthétiques brouillent la distinction entre le vrai et le faux, les conséquences dépassent largement une simple perturbation temporaire sur le terrain. La confiance du public envers les institutions chargées de protéger la population canadienne s'en trouve ébranlée.⁸ La crédibilité des dirigeants s'affaiblit lorsque leurs propos et leurs gestes peuvent être présentés de façon plausible comme des fabrications. Enfin, elle introduit des frictions au sein de la coopération alliée. Une hésitation passagère peut quand même ralentir la coopération entre les alliés ou altérer la perception de la fiabilité du Canada. En ce sens, la manipulation par l'utilisation de contenus synthétiques n'est pas simplement une nuisance sur le champ de bataille, mais une menace stratégique qui vise les fondements mêmes de la confiance dont la défense démocratique a besoin.⁹

Les systèmes génératifs compliquent l'établissement de la confiance, en produisant des imitations convaincantes de contenus officiels. Le problème plus profond réside dans le fait qu'une fois que le public sait que de telles falsifications existent, les documents authentiques peuvent eux aussi être remis en cause. Une vidéo montrant réellement une faute, un document consignait véritablement une infraction ou un extrait audio capturant une remarque malvenue peuvent tous être rejetés comme étant des montages. C'est ce que les chercheurs appellent le « dividende du menteur »—la capacité des acteurs malveillants à échapper à leurs responsabilités en prétendant que des preuves authentiques ont été manipulées.¹⁰

Pour relever ce défi, les vérifications techniques ne suffisent pas. Les institutions doivent renforcer leur résilience grâce à des pratiques de communication cohérentes, à une correction transparente des erreurs et à des activités de sensibilisation, permettant au public de reconnaître les communications authentiques et les voies par lesquelles elles sont diffusées. Lorsque le MDN et les FAC reconnaissent rapidement leurs erreurs, les corrigent ouvertement et expliquent leurs processus, ils démontrent que la crédibilité repose sur la transparence et la responsabilisation, et non sur une image artificielle d'inafaillibilité. Lorsqu'ils expliquent à l'avance comment les communications officielles seront authentifiées et diffusées, ils donnent à la population canadienne les moyens de reconnaître les tentatives d'usurpation. Ces pratiques n'éliminent pas complètement le dividende du menteur, mais elles en atténuent les effets, en faisant de l'authenticité une attente constante plutôt qu'une considération secondaire.

L'environnement informationnel propre au Canada

Les défis, posés par les systèmes génératifs, dépassent la seule dimension technique. Ils soulèvent une question de confiance qui influe directement sur les opérations dans des contextes propres au Canada.

Les enjeux auxquels sont confrontés le MDN et les FAC sont influencés par la géographie du Canada et par ses institutions. En raison de sa géographie, le pays doit composer avec de vastes distances, des conditions climatiques rigoureuses et des infrastructures limitées, particulièrement dans le Nord. À ces défis s'ajoutent des réalités institutionnelles propres au Canada : il s'agit d'une fédération où les responsabilités sont partagées entre différents ordres de gouvernement, où les dirigeants autochtones exercent une autorité reconnue et où la défense continentale s'appuie sur des mécanismes binationaux comme le NORAD. Ces caractéristiques influencent la circulation de l'information, déterminent les sources d'autorité perçues comme légitimes et façonnent les conditions dans lesquelles la confiance s'établit.

Contrairement à celui d'États plus centralisés, le système de gouvernance à plusieurs niveaux du Canada fait en sorte qu'aucune institution ne contrôle à elle seule le discours public en période de crise. Un ordre d'évacuation lié à un feu de forêt peut provenir d'une administration municipale, être relayé par une province et recevoir l'appui des Forces armées canadiennes. Dans un tel contexte, la clarté des communications est essentielle, car des acteurs malveillants peuvent exploiter le moindre décalage entre les administrations ou les autorités compétentes afin de semer le doute.

Les crises nationales montrent comment ces pressions s'intensifient lorsque plusieurs administrations et d'importantes populations sont concernées. Les feux de forêt, les inondations et les urgences de santé publique exigent une intervention coordonnée entre les administrations municipales, provinciales, territoriales et fédérales. Dans ces circonstances, une fausse alerte qui paraît officielle ou un faux avis d'annulation d'un ordre d'évacuation peut se propager rapidement dans les médias sociaux.¹¹ Quelques minutes d'hésitation suffisent à rendre les voies d'évacuation plus dangereuses ou à compliquer la coordination des services d'urgence.

Les crises nationales révèlent également la fragilité des systèmes sur lesquels la population canadienne compte. Les feux de forêt peuvent endommager les tours de télécommunications, les inondations interrompre l'alimentation électrique et les pointes de demande surcharger les réseaux locaux. Pour le MDN et les FAC, l'appui aux autorités civiles suppose de se préparer à la fois aux perturbations physiques et à l'arrivée simultanée de contenus synthétiques trompeurs. Un faux message, concernant la fermeture de routes ou la qualité de l'eau, peut combler le vide pendant que les véritables alertes peinent à atteindre la population.

Dans le Nord canadien, les communications présentent des caractéristiques particulières et les conséquences de la confusion peuvent être immédiates. Les collectivités sont de petite taille, très soudées et souvent éloignées des grands centres. Les infrastructures demeurent limitées et les communications peuvent être perturbées par les conditions météorologiques, la géographie ou une capacité de transmission restreinte.¹²

Dans de nombreuses collectivités, le bouche-à-oreille, la radio locale et les pages Facebook communautaires demeurent les principaux moyens de communication.¹³ Cette proximité constitue une force, mais elle accroît également la vulnérabilité des collectivités nordiques. Les rumeurs circulent rapidement parce que les gens se soucient profondément de leurs voisins et réagissent sans délai lorsqu'ils croient qu'ils sont en danger. Un faux message, annonçant la disparition d'une personne, un déversement de matières dangereuses ou un ordre d'évacuation, peut se propager à la vitesse d'une conversation, bien avant qu'une communication officielle soit vue ou jugée crédible.

Pour le MDN et les FAC, cela signifie que la crédibilité dans le Nord ne peut pas reposer uniquement sur des solutions techniques. Elle dépend de relations humaines établies bien avant qu'une situation d'urgence ne survienne. Dans les faits, les aînés autochtones, les radiodiffuseurs locaux et les dirigeants communautaires exercent souvent une influence plus grande que les représentants des autorités éloignées.¹⁴ Lorsque le MDN et les FAC collaborent avec ces acteurs pour promouvoir des pratiques de communication authentiques et les mettent en application durant les patrouilles de routine, les exercices d'entraînement et les opérations saisonnières, ils renforcent un réseau de confiance propre au contexte canadien. Ces réseaux ne se contentent pas de transmettre l'information; ils l'adaptent aux réalités culturelles et linguistiques de la collectivité afin qu'elle soit à la fois comprise et utile.¹⁵

La force de cette approche ne repose pas uniquement sur des éléments visuels comme les logos ou l'image de marque, qui peuvent être imités, mais surtout sur des personnes reconnues et respectées qui communiquent une information crédible. Il s'agit notamment des détenteurs de savoirs reconnus, qui possèdent souvent une expertise particulière et savent le mieux comment rejoindre le plus grand nombre de personnes au sein de leur collectivité.

Lorsque les résidents savent à quoi ressemble un message officiel et où il sera diffusé, et lorsqu'ils ont pu observer ces procédures mises en pratique dans des circonstances normales, ils sont davantage enclins à écarter les captures d'écran ou les messages transférés. Pour le MDN et les FAC, il ne s'agit pas seulement d'une question de technique de communication, mais aussi de respect envers les collectivités nordiques, de reconnaissance du leadership autochtone et de partenariat avec les organisations locales qui bénéficient d'un niveau de confiance que les autorités fédérales ne peuvent atteindre à elles seules.

Le point de vue nord-américain et allié

Dans le contexte de la défense aérospatiale binationale, la capacité de diffuser des mises à jour crédibles en temps quasi réel est essentielle. Par exemple, lorsqu'un ballon ou un aéronef suscite l'attention du public, la population canadienne et américaine s'attend à recevoir rapidement des renseignements rassurants.

Le NORAD repose sur le principe selon lequel le Canada et les États-Unis réagissent comme une seule entité, et cette unité doit être perceptible tant pour les citoyens que pour les dirigeants politiques et les adversaires. Des communications rapides et crédibles ne constituent donc pas un simple complément à la défense continentale; elles en représentent un élément essentiel.¹⁶ Tout comme les réseaux radar offrent une vision commune de l'espace aérien, des mises à jour cohérentes et faisant autorité permettent d'établir une compréhension commune des événements.

Le même principe s'applique aux alliances auxquelles le Canada participe. Les exercices et les déploiements menés en coalition sont particulièrement vulnérables, puisqu'ils exigent un niveau élevé de confiance et de synchronisation entre des partenaires aux profils variés. Les adversaires le savent.¹⁷ Une seule provocation synthétique, un faux rapport après action faisant état d'une défaillance des capacités, une image falsifiée laissant croire à une inconduite ou un faux message évoquant des dissensions entre commandants, peuvent être diffusés au moment précis où une décision importante doit être prise. Même si la supercherie est démasquée quelques heures plus tard, elle mobilise inutilement des ressources, retarde la coordination et mine la confiance au sein de la coalition.

Ces perturbations ne brisent généralement pas les alliances, mais leur effet cumulatif réduit la marge de manœuvre et complique l'action collective. Les différences entre les priorités nationales sont naturelles au sein d'une coalition. Toutefois, les contenus synthétiques malveillants exploitent ces différences, alimentent la méfiance et freinent l'unité d'action.¹⁸

Lorsque le Canada et les États-Unis utilisent des méthodes d'authentification reconnues, comme l'utilisation de repères visuels uniformes dans leurs communications et de signatures cryptographiques intégrées aux images et aux vidéos ainsi que le recours systématique aux canaux officiels, le public apprend à reconnaître les communications authentiques et les journalistes peuvent rendre compte des événements avec davantage d'assurance, même sous pression.¹⁹ Ainsi, l'authentification ne constitue pas seulement une protection contre la confusion; elle devient un atout stratégique qui renforce la crédibilité de la défense continentale.

Pour le Canada, la crédibilité au sein des opérations alliées dépend non seulement du professionnalisme de ses forces, mais aussi de la rapidité et de la clarté avec lesquelles leurs actions sont présentées aux partenaires et au public. Dans cette perspective, l'authentification devient une véritable monnaie opérationnelle : elle permet de maintenir le rythme des opérations, de renforcer la confiance et d'empêcher les adversaires de transformer le doute en retard. Que ce soit dans le contexte de la défense continentale, des collectivités nordiques ou des opérations internationales, les FAC doivent acquérir des habitudes de communication rigoureuses bien avant qu'une crise ne survienne.

Les affaires publiques et la voix crédible du Canada

Les pratiques de vérification qui protègent la chaîne de commandement doivent également s'appliquer à la façon dont le MDN et les FAC communiquent avec le public. La culture d'une organisation se manifeste dans le ton, le moment choisi et la clarté de ses communications. Les affaires publiques commencent donc bien avant une crise. Si le MDN et les FAC expliquent en termes simples que les faux contenus convaincants font désormais partie de l'environnement informationnel, montrent comment reconnaître les communications authentiques et adoptent une communication régulière lorsque les enjeux sont limités, la population saura à quoi s'attendre lorsque les enjeux deviendront importants.²⁰ En situation de crise, la population canadienne réagit mieux lorsque les processus sont expliqués clairement : quelles mesures sont prises pour vérifier l'information, à quel moment la prochaine mise à jour sera diffusée et comment éviter de propager de faux renseignements pendant que les faits sont en cours de vérification.²¹

La voix du Canada doit également représenter son identité. La population canadienne accorde de l'importance à l'équité et à un langage direct. Une courte vidéo diffusée rapidement sur une plateforme officielle par un commandant peut avoir une forte portée morale, puisqu'elle revêt à la fois un caractère personnel et institutionnel. De même, un communiqué indiquant clairement quelles informations seront rendues publiques et selon quel échéancier renforce la crédibilité de l'institution, puisqu'il engage le MDN et les FAC à respecter un calendrier précis et permet au public de savoir à quoi s'attendre. Dans les communications bilingues, le fait de s'exprimer avec la même clarté dans les deux langues officielles témoigne d'un souci d'inclusion et contribue à renforcer la confiance. Lorsque des communautés autochtones sont concernées, un dialogue direct avec leurs dirigeants, mené de manière culturellement adaptée et, au besoin, par l'intermédiaire de personnes de confiance, renforce la légitimité des messages diffusés et favorise l'adoption de réflexes de vérification de l'information.

La vérification dans la chaîne de commandement

Les contenus synthétiques n'ont pas besoin de tromper l'ensemble d'une formation pour produire leurs effets. En situation opérationnelle, même un bref instant de doute peut perturber une action coordonnée. Lorsque de nombreux éléments doivent se déplacer de concert, l'hésitation d'une seule unité peut briser l'élan, accroître les risques et offrir à l'adversaire une marge de manœuvre. Le danger ne réside pas dans une désinformation à grande échelle, mais dans les petites fissures de confiance qui peuvent se propager au sein d'une formation lorsque l'on ne peut pas se fier immédiatement à l'information. Ce risque n'a rien de nouveau.

Les forces armées ont toujours dû s'assurer de l'authenticité des ordres. Par le passé, les unités recouraient à des indicatifs d'appel, à des mots de code ou même à des émissaires pour confirmer les instructions. Pendant la Seconde Guerre mondiale, par exemple, les procédures d'authentification par sommation et réponse constituaient une mesure de sécurité courante. Aujourd'hui encore, les contrôles radio demeurent une discipline de base.²² Le principe est demeuré le même : peu importe l'urgence de la situation, les unités doivent avoir la certitude que les ordres reçus sont authentiques. Les moyens de communication modernes ont accéléré la circulation de l'information, mais ils ont également multiplié les points d'entrée par lesquels un message faux ou qui a été manipulé peut s'introduire dans le système. À l'ère des contenus synthétiques, la différence tient au réalisme des faux ordres et au peu de temps dont disposent les destinataires pour en vérifier l'authenticité.²³

Un ordre inattendu reçu au cours d'une manœuvre illustre bien cette réalité. Le message peut sembler authentique, tant par sa forme que par son contenu. Toutefois, si son moment de diffusion soulève des doutes et qu'aucune procédure de vérification n'a été prévue, la décision la plus prudente consiste souvent à suspendre l'action jusqu'à ce qu'une autorité supérieure confirme l'ordre.²⁴ Si l'ordre s'avère authentique, cette attente aura déjà fait perdre un temps précieux. S'il est faux, l'unité aura évité une erreur, mais au prix d'un ralentissement et d'une perte d'initiative. Dans les deux cas, l'incertitude a un coût. Dans un environnement où le rythme des opérations est soutenu, quelques secondes d'hésitation peuvent modifier l'issue d'un engagement, faire basculer l'initiative ou créer une occasion dont l'adversaire peut tirer parti.

Les pratiques de la défense doivent donc privilégier des méthodes de confirmation simples et rapides. Un signal convenu à l'avance, un bref échange au moyen d'un canal secondaire ou toute autre procédure préétablie peuvent dissiper le doute en quelques secondes. Ces mesures de protection ne sont pas nouvelles. Les contrôles radio, les procédures d'authentification par sommation et réponse ainsi que la confirmation au moyen de canaux secondaires font depuis longtemps partie des pratiques courantes. Ce qui a changé, c'est le contexte opérationnel. L'IA générative soulève de nouveaux défis auxquels les procédures existantes n'ont pas été conçues pour répondre : des enregistrements audio synthétiques reproduisant avec une grande fidélité la voix d'un commandant, des vidéos truquées montrant en apparence la transmission d'ordres ou encore des messages texte qui imitent avec précision le style et la présentation des communications légitimes.

Les procédures actuelles du MDN et des FAC reposent sur l'hypothèse selon laquelle les communications sont généralement fiables, à moins qu'un motif précis ne justifie le doute. Dans un contexte où des contrefaçons convaincantes peuvent être produites rapidement et à grande échelle, cette hypothèse ne tient plus. Le problème ne réside pas dans l'absence de procédures

de vérification, mais dans le fait qu'elles ne sont pas appliquées de façon systématique lorsque l'information provient de canaux familiers. La formation met souvent l'accent sur la vérification d'ordres manifestement suspects, comme ceux qui arrivent par des moyens inhabituels ou qui contredisent les plans connus, mais elle ne prévoit pas toujours des exercices portant sur des instructions plausibles qui auraient été subtilement manipulées.

De plus, les contraintes opérationnelles peuvent réduire l'efficacité des procédures existantes. Durant des urgences au pays, comme les inondations ou les feux de forêt, les dommages causés aux infrastructures peuvent compromettre les canaux de communication secondaires et rendre plus difficile la confirmation indépendante des ordres. De la même façon, des contenus, manipulés au moyen de l'IA générative, peuvent diffuser de faux renseignements qui nuisent aux opérations des FAC, notamment de fausses alertes concernant une catastrophe, ce qui ralentit les interventions.²⁵ Dans les opérations de coalition, les différences entre les procédures nationales ou les barrières linguistiques peuvent ralentir les vérifications au moment où la rapidité est la plus essentielle. Enfin, dans les opérations de combat menées à un rythme élevé, la pression d'agir rapidement peut l'emporter sur le réflexe de vérifier un ordre, surtout lorsqu'il semble provenir d'une source digne de confiance.

Il ne s'agit donc pas d'inventer de nouvelles procédures, mais d'intégrer systématiquement les procédures existantes aux pratiques courantes, en les adaptant aux menaces que présentent les contenus synthétiques. Cela suppose de mettre en pratique les procédures de vérification non seulement pour les ordres manifestement suspects, mais aussi pour les instructions apparemment ordinaires reçues au cours des exercices. Cela suppose également de vérifier et d'entretenir les canaux de communication secondaires avec la même rigueur que les canaux principaux. Enfin, cela exige de former le personnel à reconnaître que, dans le contexte actuel, la vérification n'est pas un signe d'hésitation, mais de professionnalisme, au même titre que le maniement des armes ou la navigation.

Le leadership joue un rôle déterminant dans cette discipline. Les commandants doivent établir clairement que tout ordre inhabituel doit être vérifié et que la vérification sous pression témoigne non pas d'une faiblesse, mais d'un comportement professionnel.²⁶ Les unités qui répètent ces procédures durant les exercices les appliqueront naturellement en opération. Lorsque les dirigeants rappellent constamment que la vérification fait partie des attentes et qu'ils la reconnaissent comme un signe de bon jugement plutôt que d'hésitation, la culture de toute la formation évolue progressivement. Il en résulte non seulement une diminution des erreurs, mais aussi le maintien de la confiance au sein de la chaîne de commandement lorsque des adversaires cherchent à semer la confusion.

L'intégration de la confiance aux politiques, à la formation et au leadership

La crédibilité ne peut pas reposer uniquement sur la technologie. Elle doit être renforcée par l'ensemble des leviers de la défense : les politiques, la formation et les pratiques de leadership. Pour demeurer utiles, les lois et les politiques n'ont pas à suivre chaque évolution technologique. Elles doivent surtout donner des orientations claires et inspirer confiance à ceux qui prennent des décisions et qui communiquent au nom de l'institution. Pour le MDN et les FAC, cela signifie que la doctrine, les directives et les procédures opérationnelles normalisées doivent tenir compte du fait que les contenus synthétiques ne constituent plus une anomalie, mais une caractéristique permanente de l'environnement informationnel. Les politiques qui reposaient autrefois sur l'hypothèse que l'information était digne de confiance jusqu'à preuve du contraire doivent désormais partir du principe qu'elle peut être contestée.

Les politiques, à elles seules, ne suffisent toutefois pas. C'est grâce à la formation que les principes deviennent des réflexes. De la même façon que les militaires apprennent à effectuer des contrôles radio ou à effectuer des exercices de routine, le personnel du MDN et des FAC peut apprendre à réagir sans hésitation devant une information ambiguë. Un officier de quart confronté à une vidéo suspecte devrait immédiatement savoir à qui signaler l'incident et quelles mesures prendre. Un commandant qui reçoit un ordre inhabituel devrait avoir le réflexe d'en confirmer l'authenticité au moyen d'un canal secondaire.

Le problème n'est pas l'absence de ces connaissances, mais plutôt le fait qu'elles ne sont pas mises en pratique de façon régulière dans des conditions réalistes. À l'heure actuelle, la formation traite souvent la vérification de l'information comme une préoccupation secondaire, abordée en salle de classe plutôt qu'intégrée dans les exercices sur le terrain. Le personnel peut savoir, en théorie, à qui s'adresser lorsqu'il est confronté à un contenu suspect, mais sans mise en pratique régulière dans des situations de stress, cette connaissance ne se transforme pas en réflexe. Les comptes rendus après action d'exercices récents ont relevé des cas où des unités ont hésité ou pris des décisions à partir d'informations non vérifiées parce que les procédures de vérification, bien que connues, n'étaient pas suffisamment ancrées dans les habitudes de travail.²⁷

Ces situations ne devraient pas être laissées à l'improvisation sur le terrain. Les procédures de vérification devraient être intégrées à tous les niveaux de formation, depuis l'instruction de base jusqu'aux grands exercices interarmées, afin que les membres des FAC les appliquent aussi spontanément que les manœuvres de combat, la navigation ou les procédures radio.

Les officiers des affaires publiques devraient également disposer, à l'avance, de messages préapprouvés, leur permettant d'intervenir rapidement lorsque des contenus faux ou trompeurs circulent. Ainsi, ils n'auraient pas à attendre des autorisations

juridiques ou stratégiques en pleine crise, mais pourraient immédiatement signaler l'existence de contenus contestés, avertir le public que leur authenticité ou leur exactitude n'a pas encore été établie et l'orienter vers des sources officielles fiables où seront publiées les mises à jour. La préparation préalable de ces messages évite que le silence soit interprété comme une confirmation et permet au MDN et aux FAC d'intervenir d'emblée avec clarté et assurance. Pris isolément, ces gestes peuvent sembler modestes. Ensemble, ils créent un état de disponibilité opérationnelle qui permet aux opérations et aux communications de se poursuivre avec constance, même lorsque des adversaires cherchent à semer la confusion. Des exercices reproduisant des communications falsifiées et des contenus synthétiques permettraient aux équipes des affaires publiques d'intégrer les procédures de vérification avec autant d'aisance que les fantasmes maîtrisent le maniement des armes.

Le leadership constitue le lien qui transforme les principes en habitudes. Lorsque les officiers supérieurs et les dirigeants démontrent, par leur exemple, une vérification rigoureuse sous pression, leurs subordonnés y voient un comportement professionnel plutôt qu'un signe d'hésitation. Un commandant qui exige une confirmation rapide avant d'exécuter un ordre inhabituel établit une norme qui se diffuse dans toute la formation. Un responsable des affaires publiques qui corrige une déclaration avec la même rapidité et la même visibilité que lors de sa diffusion initiale montre que la crédibilité repose sur la franchise. Dans une culture militaire, où le ton et le rythme donnés par les dirigeants influencent l'ensemble de la chaîne hiérarchique, ces exemples se propagent rapidement.

En définitive, la confiance doit être intégrée à tous les échelons de la défense : inscrite dans la doctrine, renforcée par une formation régulière et incarnée par les dirigeants, tant en période normale qu'en situation de crise. Ensemble, ces trois piliers, soit les politiques, la formation et le leadership, permettent aux FAC d'aborder les interférences fondées sur des contenus synthétiques non pas comme une menace improvisée, mais comme une réalité opérationnelle à laquelle elles sont pleinement préparées.

La mesure d'une norme canadienne de réussite

Le MDN et les FAC possèdent une longue expérience de l'évaluation de la disponibilité opérationnelle, et cette même rigueur doit s'appliquer à l'environnement informationnel.²⁸ Le premier indicateur est le temps. L'institution doit mesurer le délai nécessaire pour classer un contenu suspect, fournir une évaluation interne du degré de confiance qu'il inspire et diffuser une mise à jour publique crédible. Elle doit également mesurer le temps requis pour confirmer ou écarter des ordres inhabituels au moyen des procédures établies, ainsi que la fréquence à laquelle ces procédures sont mises en pratique durant les exercices. De la même façon que les rapports sur la disponibilité opérationnelle



Un observateur-contrôleur-entraîneur (OCE) responsable de l'évaluation de l'ex GLOBAL RESOLVE, suit et met à jour les mouvements des troupes dans le secteur d'entraînement au moyen d'une tablette de la trousse d'assaut tactique (TAK), ce qui permet la communication en temps réel entre différents éléments d'OCE sur le terrain. Image prise dans la zone d'entraînement du Yukon près de Fairbanks, en Alaska, le 17 février 2026.

Cpl Dustin LeVasseur Pearce

mesurent les réserves de munitions, l'état de service des équipements ou les effectifs disponibles, le MDN et les FAC peuvent évaluer leur préparation informationnelle en fonction de la rapidité et de la fiabilité avec lesquelles ils valident ou rejettent des contenus contestés.²⁹

Le rendement doit s'améliorer de façon constante, comme dans les autres domaines de la disponibilité opérationnelle. Par exemple, si une formation met actuellement vingt minutes à transmettre un ordre suspect au niveau supérieur et à le confirmer, les exercices devraient viser à réduire ce délai à dix minutes, puis à cinq, sans compromettre l'exactitude ni la sécurité. Si les équipes des affaires publiques ont besoin d'une heure pour coordonner une première déclaration lors d'une urgence au pays, l'objectif devrait être de ramener ce délai à quelques minutes grâce à des messages préapprouvés, à une délégation claire des pouvoirs et à des mécanismes d'escalade bien établis. Chaque exercice devient ainsi une occasion de raccourcir les délais tout en renforçant la confiance.

Des sondages et des mécanismes de rétroaction peuvent également enrichir cette évaluation. Il conviendrait notamment de demander à la population canadienne si elle sait où trouver les communications réelles du MDN et des FAC et si elle est en mesure de les reconnaître. Les journalistes et les partenaires de la société civile pourraient également être consultés afin de déterminer si les outils de vérification sont accessibles et fiables. Les alliés pourraient, quant à eux, indiquer si les méthodes canadiennes sontinteropérables avec les leurs et s'ils accordent immédiatement leur confiance aux communications canadiennes dans un contexte multinational. Bien que qualitatives, ces formes d'évaluation sont aussi essentielles à la résilience que les indicateurs quantitatifs. Les travaux des chercheurs qui étudient

la confiance envers les institutions et leur crédibilité offrent d'ailleurs des cadres utiles pour mesurer ces dimensions.³⁰

Le succès ne se traduira pas par la disparition des faux contenus. Ils continueront d'apparaître, et les adversaires continueront d'innover. Le succès se mesurera plutôt à la capacité du Canada de réagir avec calme, de communiquer rapidement et de préserver la confiance lorsque des messages falsifiés apparaissent. Concrètement, cela signifie moins d'interruptions opérationnelles causées par des ordres non authentifiés, moins de situations où de fausses alertes circulent plus vite que les communications officielles lors d'urgences au pays et moins d'occasions où des récits fabriqués détournent l'attention des objectifs d'un exercice ou d'un déploiement allié. Lorsqu'ils sont suivis de façon constante, ces indicateurs permettent à la défense de déterminer non seulement si elle est prête, mais aussi si la population canadienne et les alliés ont confiance dans cet état de préparation.

Conclusion

L'intelligence artificielle générative a transformé les conditions dans lesquelles la vérité doit se frayer un chemin pour capter l'attention. Elle a rendu les faussetés peu coûteuses, rapides à produire et convaincantes. Cette réalité touche au cœur même de l'efficacité militaire.³¹ Lorsqu'un message falsifié peut ralentir une prise de décision, lorsqu'une vidéo fabriquée de toutes pièces peut fragiliser l'unité des alliés ou lorsqu'une fausse alerte peut exposer des Canadiens à un danger, les adversaires ont atteint leur objectif sans avoir à tirer un seul coup de feu. C'est dans cet environnement concurrentiel que les FAC évoluent désormais. Le Canada n'est pas démuni dans cette lutte. La défense n'a pas à éliminer chaque faux contenu; elle doit démontrer l'authenticité de l'information avant que les faussetés ne se propagent. Cela exige des commandants qui s'attendent à ce que l'information soit vérifiée avant toute manœuvre, des équipes des affaires publiques qui communiquent rapidement et avec franchise, ainsi que des politiques et des outils qui font de l'authentification une pratique courante. Cela exige également des dirigeants qui appliquent la même rigueur à leurs communications qu'à la conduite des opérations. Enfin, cela signifie de faire en sorte que la voix du MDN et des FAC soit immédiatement reconnaissable dans tous les contextes, que ce soit dans les postes de commandement du NORAD, dans les collectivités nordiques, lors de crises au pays ou au cours d'opérations menées en coalition à l'étranger.

Le MDN et les FAC ont toujours fondé leur identité sur le professionnalisme, l'intégrité et la capacité d'agir sous pression.³² Dans les luttes informationnelles qui se déroulent aujourd'hui, ces mêmes qualités constituent le fondement de leur avantage. En démontrant l'authenticité de leurs communications, en préservant le rythme des opérations et en s'exprimant d'une voix qui représente les valeurs canadiennes d'honnêteté et de respect, le MDN et les FAC doivent se protéger contre la tromperie et défendre la démocratie qu'ils servent.

Notes

- 1 Joseph Vossler, Gerald Mazur, Andre Slonopas, Danyl Miller, Edward Olbrych, Aaron Sweeney, et Jacob Strahan, « Artificial Intelligence as a Force Multiplier in U.S. Military Information Campaigns », *Cybersecurity and Information Systems Information Analysis Center (CSIAIC)*, 28 octobre 2024, à l'adresse : <https://csiac.dtic.mil/articles/artificial-intelligence-as-a-force-multiplier-in-u-s-military-information-campaigns/>.
- 2 Cole Stryker et Mark Scapicchio, « What Is Generative AI? », *IBM Think*, 22 mars 2024, à l'adresse : <https://www.ibm.com/think/topics/generative-ai>.
- 3 Service canadien du renseignement de sécurité, « Répercussions des hypertrucages sur la sécurité nationale », gouvernement du Canada, 14 juillet 2025, à l'adresse : <https://www.canada.ca/fr/service-renseignement-securite/organisation/publications/evolution-de-la-desinformation-un-avenir-hypertrucue-repercussions-des-hypertrucages-sur-la-securite-nationale.html>.
- 4 Akshay Kulkarni, « BC Wildfire Service Faces Challenges from AI-Generated Misinformation », *CBC News*, 6 août 2025, à l'adresse : <https://www.cbc.ca/news/canada/british-columbia/bc-wildfire-service-ai-misinformation-1.7602041>.
- 5 Centre canadien pour la cybersécurité, « Évaluation des cybermenaces nationales 2025-2026 », gouvernement du Canada, 30 octobre 2024, à l'adresse : <https://www.cyber.gc.ca/sites/default/files/evaluation-cybermenaces-nationales-2025-2026-f.pdf>.
- 6 « An existential threat: Disinformation 'single biggest risk' to Canadian Democracy », *Digital Forensic Research Lab (DFRLab)*, 19 mars 2024, à l'adresse : <https://dfrlab.org/2025/03/19/canada-disinfo-existential-threat/>.
- 7 National Security Agency, Federal Bureau of Investigation, et Cybersecurity and Infrastructure Security Agency, *Contextualizing Deepfake Threats to Organizations*, 12 septembre 2023, à l'adresse : <https://media.defense.gov/2023/Sep/12/2003298925/-1/1/O/CSI-DEEPPAKE-THREATS.PDF>.
- 8 *Increasing Threats of Deepfake Identities*, Department of Homeland Security, consulté le 29 septembre 2025, à l'adresse : https://www.dhs.gov/sites/default/files/publications/increasing_threats_of_deepfake_identities_0.pdf.
- 9 Di Cooke, Abigail Edwards, Alexis Day, Devi Nair, Sophia Barkoff, et Katie Kelly, *Crossing the Deepfake Rubicon: The Maturing Synthetic Media Threat Landscape*, Center for Strategic and International Studies, 1^{er} novembre 2024, à l'adresse : <https://www.csis.org/analysis/crossing-deepfake-rubicon>.
- 10 Bobby Chesney et Danielle Citron, « Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security », *California Law Review* 107, n° 6, décembre 2019, à l'adresse : <https://www.californialawreview.org/print/deep-fakes-a-looming-challenge-for-privacy-democracy-and-national-security>. Voir également Vaccari, Cristian et Andrew Chadwick, « Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News », *Social Media + Society*, 6(1), 2020.
- 11 Akshay Kulkarni, « AI-Generated Media and Misinformation of N.W.T. Wildfires Circulating, Fire Officials Warn », *CBC News*, 6 août 2025, à l'adresse : <https://www.cbc.ca/news/canada/north/ai-generated-media-and-misinformation-of-n-w-t-wildfires-circulating-fire-officials-warn-1.7623579>.
- 12 Alexander Dalziel et Daniel Nikoula, *Polarized: Climate Change, Geopolitics and Disinformation in the Arctic*, Laboratoire sur l'intégrité de l'information de l'Université d'Ottawa, juillet 2025, à l'adresse : <https://infolab.uottawa.ca/common/Uploaded%20files/PDI%20files/Polarized-EN-FINAL.pdf>.
- 13 Rob McMahon, Michael B. McNally, Eric Nitschke, Kyle Napier, María Alvarez Malvido, et Murat Akçayir, « Codesigning Community Networking Literacies with Rural/Remote Northern Indigenous Communities in Northwest Territories, Canada », *Journal of Computer-Mediated Communication* 29, n° 1, janvier 2024, à l'adresse : <https://doi.org/10.1093/jcmc/zmad042>.
- 14 Ministère de la Défense nationale, « Programme de réconciliation avec les peuples autochtones du ministère de la Défense nationale – Subventions et contributions », Gouvernement du Canada, 27 mars 2025, à l'adresse : <https://www.canada.ca/fr/ministere-defense-nationale/programmes/financement-reconciliation-autochtones.html>.
- 15 Jayde Lavoie, Jill Barclay, et Wilfrid Greaves, *Improving the Canadian Armed Forces' Recruitment and Retention of Indigenous People: Best Practices from the New Zealand Defence Force*, North American and Arctic Defence and Security Network, Queen's University, 8 septembre 2020, à l'adresse : https://www.naadsn.ca/wp-content/uploads/2020/09/20-September_Policy-Brief-CAF-1.pdf.
- 16 Ministère de la Défense nationale, « Déclaration conjointe sur la modernisation du NORAD », Gouvernement du Canada, 14 août 2021, à l'adresse : <https://www.canada.ca/fr/ministere-defense-nationale/houvelles/2021/08/declaration-conjointe-sur-la-modernisation-du-norad.html>.
- 17 Jill Goldenziel et Daniel Grant, « Information Resilience: Countering Disinformation and Its Threat to the U.S. Alliance System », *War on the Rocks*, 15 novembre 2023, à l'adresse : <https://warontherocks.com/2023/11/information-resilience-countering-disinformation-and-its-threat-to-the-u-s-alliance-system/>.
- 18 Patrick Samaha, « Weaponized AI, The New Frontline in Global Disinformation Warfare », *NATO Association of Canada*, 24 juin 2025, à l'adresse : <https://natoassociation.ca/weaponized-ai-the-new-frontline-in-global-disinformation-warfare/>.
- 19 Pour connaître les normes actuelles et les initiatives en cours, voir *Content Authenticity Initiative* (CAI), qui élabore des normes techniques relatives à la provenance des contenus (contentauthenticity.org), ainsi que Coalition for Content Provenance and Authenticity (C2PA), qui fournit des spécifications pour l'intégration de métadonnées cryptographiques aux médias numériques (c2pa.org). Le Centre d'excellence OTAN pour la communication stratégique a également publié des orientations sur la lutte contre la désinformation dans les contextes militaires (stratcomcoe.org).
- 20 Ministère de la Défense nationale, *Stratégie de communication de l'Armée canadienne 2024-2026*, gouvernement du Canada, 15 juillet 2025, à l'adresse : <https://www.canada.ca/fr/armee/services/pour-le-soldat/strategie-de-communication-de-l-armee-canadienne-2024-2026.html>.
- 21 Eric J.G. Storm, *Needing Unified Direction: Developing Capabilities for Operations in the Information Environment*, Collège des Forces canadiennes, 2025, à l'adresse : <https://www.cfc.forces.gc.ca/259/290/950/305/StormSF50DL.pdf>.
- 22 George I. Back et George Raynor Thompson, « Military Communication », *Encyclopaedia Britannica*, consulté le 29 septembre 2025, à l'adresse : <https://www.britannica.com/technology/military-communication>.
- 23 Di Cooke, Abigail Edwards, Alexis Day, Devi Nair, Sophia Barkoff, et Katie Kelly, *Crossing the Deepfake Rubicon: The Maturing Synthetic Media Threat Landscape*, Center for Strategic and International Studies, 1^{er} novembre 2024, à l'adresse : <https://www.csis.org/analysis/crossing-deepfake-rubicon>.
- 24 Daniel L. Byman, Chongyang Gao, Chris Meserole, et V. S. Subrahmanian, *Deepfakes and International Conflict*, Brookings Institution, janvier 2023, à l'adresse : https://www.brookings.edu/wp-content/uploads/2023/01/FP_20230105_deepfakes_international_conflict.pdf.
- 25 Des incidents récents montrent comment l'intelligence artificielle générative amplifie les risques de mésinformation : durant les feux de forêt de 2025 dans les Territoires du Nord-Ouest et en Colombie-Britannique, des images générées par l'IA ont exagéré l'ampleur des dégâts et ont largement circulé dans les médias sociaux. Voir : *N.W.T. fire officials warn of AI-generated images, misinformation circulating online* | CBC News; *AI-generated wildfire images spreading misinformation in B.C., fire officials warn* | CBC News. En 2022, une vidéo hypertrucquée, montrant le président Zelenskyy, exhortant les troupes ukrainiennes à se rendre, a circulé en ligne dans le but de miner le moral pendant les combats. Voir : *Une vidéo hypertrucquée montrant la capitulation de Volodymyr Zelenskyy inquiète les experts* : NPR.
- 26 Gen. Gary Brito, « Professionalism Is the Foundation of the Army and We Will Strengthen It », *War on the Rocks*, 18 mars 2024, à l'adresse : <https://warontherocks.com/2024/03/professionalism-is-the-foundation-of-the-army-and-we-will-strengthen-it/>.
- 27 Bien que les comptes rendus précis après action demeurent classifiés, cette observation concorde avec les conclusions d'exercices de l'OTAN, portant sur la lutte contre les menaces hybrides, selon lesquelles la vérification de l'information est un aspect auquel la formation devrait accorder une plus grande attention. Voir Centre d'excellence OTAN pour les communications stratégiques, *Hybrid Threats: A Strategic Communications Perspective*, 2019.
- 28 *Léthos des Forces armées canadiennes : Digne de servir*, ministère de la Défense nationale, 19 juillet 2023, à l'adresse : https://www.canada.ca/content/dam/dnd-mdn/documents/reports/Lethos_des_Forces_armees_canadiennes_-_digne_de_servir_FINAL.pdf.
- 29 Ministère de la Défense nationale, « Directive du CEMD/SM sur la posture de la force et la disponibilité opérationnelle (PF&DO) des FAC pour 2024-2025 », Gouvernement du Canada, 12 mars 2025. Protocole de transfert hypertexte sécurisé : <https://www.canada.ca/fr/ministere-defense-nationale/organisation/politiques-normes-directives-sm-cemd/directive-cemd-sm-posture-force-disponibilite-operationnelle-fac.html>.
- 30 Mayer, R. C., Davis, J. H., et Schoorman, F. D. An integrative model of organizational trust. *Academy of Management Review*, 20(3), 1995, 709-734; et Grimmelikhuijsen, S., et Knies, E. Validating a scale for citizen trust in government organizations. *International Review of Administrative Sciences*, 83(3), 2017, 583-601.
- 31 Austin Coombs, « Persuade, Change, and Influence with AI: Leveraging Artificial Intelligence in the Information Environment », *Modern War Institute*, 25 octobre 2024, à l'adresse : <https://mwi.westpoint.edu/persuade-change-and-influence-with-ai-leveraging-artificial-intelligence-in-the-information-environment/>.
- 32 *Léthos des Forces armées canadiennes : Digne de servir*, ministère de la Défense nationale, 19 juillet 2023, à l'adresse : https://www.canada.ca/content/dam/dnd-mdn/documents/reports/Lethos_des_Forces_armees_canadiennes_-_digne_de_servir_FINAL.pdf.

La cybersécurité et la puissance aérienne : préserver l'intervention humaine

KRISTEN CSENKEY ET ALEXIS RAPIN

Kristen Csenkey, Ph.D. est boursière postdoctorale du Conseil de recherches en sciences humaines (CRSH) au Brian Mulroney Institute of Government de l'Université Saint-Francis Xavier. Elle est également chercheuse associée au Canadian Maritime Security Network, au Centre for Military, Security and Strategic Studies de l'Université de Calgary ainsi qu'au Réseau de défense de la sécurité de l'Amérique du Nord et de l'Arctique (RDSNAA), entre autres. Kristen Csenkey a dirigé plusieurs projets financés par le ministère de la Défense nationale portant sur les répercussions des technologies quantiques, des systèmes aéronautiques connectés et des véhicules électriques cyberrésilients sur la défense et la sécurité. Elle dirige actuellement un projet financé par une subvention d'engagement partenarial du CRSH, consacré à la gouvernance responsable des technologies quantiques à l'échelle mondiale. Elle est titulaire d'un baccalauréat spécialisé en sciences (H.B.Sc.), d'une maîtrise ès arts (M.A.), d'une maîtrise en administration publique (M.A.P.) et d'un doctorat (Ph. D.).

Alexis Rapin est chercheur associé à la Chaire Raoul-Dandurand en études stratégiques et diplomatiques de l'Université du Québec à Montréal (UQAM). Ses travaux de recherche portent sur la cybersécurité et sur les répercussions des technologies numériques sur la sécurité internationale. En 2023, il a témoigné devant le Comité permanent de la défense nationale de la Chambre des communes du Canada au sujet de la cyberdéfense et de la stratégie du Canada. Il est également membre du comité de rédaction de la plateforme francophone Le Rubicon, consacrée à l'analyse des affaires internationales et stratégiques.

Dans leur roman 2034 (publié en 2021), Elliot Ackerman et l'ancien amiral de la marine des États-Unis James G. Stavridis imaginent un conflit majeur opposant les États-Unis et la Chine.¹ Les premières pages s'ouvrent sur un incident au cours duquel un chasseur américain F-35 est soudainement capturé par l'Iran, après qu'une cyberattaque a permis à ce dernier de prendre le contrôle à distance de l'appareil. Plus loin dans le livre, confrontée à une situation désespérée, la Marine américaine décide de retirer sa flotte de F-35 du service et de remettre en service ses anciens F-18, dont la plupart des systèmes électroniques embarqués ont été retirés. Comme ses adversaires ont réussi à compromettre ses avions de haute technologie, les États-Unis sont contraints de revenir à des appareils d'une génération antérieure, jugés plus sûrs sur le plan numérique.

Bien qu'il s'agisse d'un scénario fictif fascinant,² la situation décrite dans 2034 renvoie à une idée qui gagne du terrain dans la littérature stratégique : les approches fondées sur la supériorité technologique, qui caractérisent les forces armées occidentales depuis près de quarante ans, pourraient désormais constituer une vulnérabilité.³ À mesure que les capacités de cyberguerre progressent, les adversaires semblent désormais en mesure d'exploiter les dépendances émergentes ainsi que les vulnérabilités potentielles associées aux technologies fortement interconnectées. En outre, des pratiques inégales de gestion collective des risques, la présence de systèmes existants vieillissants et l'élargissement de la surface d'attaque accroissent l'exposition aux cyberattaques sophistiquées ainsi qu'aux composants

électroniques, aux systèmes, aux processus, aux technologies et aux personnes susceptibles d'être compromis. Les conflits géopolitiques actuels illustrent déjà cette convergence et cette complexité. Ainsi, face à l'invasion russe toujours en cours, les forces armées ukrainiennes ont remis en service d'anciens téléphones de campagne le long de la ligne de front, craignant que leurs systèmes modernes de transmission ne soient compromis par l'adversaire.⁴

Dans le présent article, nous adoptons une conception large de la cyberguerre et des technologies connectées, qui englobe à la fois le cyberspace et la guerre électronique. Même si les opérations, menées dans le cyberspace et dans le spectre électromagnétique, présentent des caractéristiques distinctes, notamment en ce qui concerne les unités, les capacités et l'expertise mises en œuvre, nous nous intéressons principalement aux conséquences des vulnérabilités, des capacités et des activités humaines et technologiques qui leur sont associées. De façon plus générale, nous inscrivons cette réalité dans un concept global du cyberspace, où les moyens électromagnétiques, comme le brouillage des radiofréquences, et les tactiques cybernétiques, comme le piratage informatique, s'inscrivent dans un espace dynamique où les personnes et les technologies interagissent au sein d'un environnement à la fois numérique et physique.⁵ Cet environnement soulève des défis dans tous les domaines d'opérations. Nous soutenons donc qu'il faut agir tant sur les vulnérabilités humaines que sur les vulnérabilités techniques.

La problématique des technologies interconnectées et des menaces qui y sont associées revêt une importance particulière dans le domaine de l'aviation, où les avions, les drones, les hélicoptères⁶ ainsi que les infrastructures numériques et physiques qui les soutiennent sont désormais fortement numérisés et interconnectés. Dans un scénario qui a peut-être inspiré Ackerman et Stavridis, les États-Unis ont perdu, en 2011, un drone de surveillance après que l'Iran a piraté son système GPS afin de le faire atterrir sur une base iranienne.⁷ Les drones ne sont plus considérés comme les composantes d'une « force aérienne du pauvre »,⁸ surtout lorsqu'ils sont associés à de nouvelles tactiques⁹ et procédures¹⁰ cybernétiques ainsi qu'à des technologies commerciales de plus en plus accessibles.¹¹ D'autres auteurs ont également montré que le F-35, désormais utilisé par un nombre croissant de forces armées occidentales, représente l'exemple même d'un système d'armes fortement exposé aux cybermenaces.¹² Les cybermenaces ne relèvent plus de l'hypothèse. Elles constituent une réalité à laquelle les forces aériennes modernes doivent continuellement se préparer, répondre et s'adapter, tout en comprenant les liens étroits qui unissent désormais les environnements numériques et physiques. Le défi est clair : protéger les forces contre ces menaces sans sacrifier les avantages opérationnels que procurent les technologies de pointe.

L'un des principaux enjeux réside dans le fait que le « techno-solutionnisme » militaire, hérité des années 1990 et 2000,¹³ pourrait céder la place à un « techno-pessimisme », dans lequel les forces armées en général, et les forces aériennes en particulier, perdraient progressivement confiance dans leurs technologies de pointe et finiraient par en abandonner certaines, comme c'est le cas dans 2034. En effet, la grande force des capacités tient non seulement à leur capacité de compromettre la disponibilité et l'utilité des technologies militaires, mais aussi à leur aptitude à éroder la confiance que les décideurs leur accordent. En instillant simplement un doute quant à l'intégrité d'un système, une cyberattaque peut dissuader un acteur d'utiliser un éventail beaucoup plus large de capacités et produire ainsi des effets disproportionnés par rapport à son incidence réelle. Certains auteurs, dont Christopher Coker,¹⁴ avancent qu'une telle approche pourrait constituer une stratégie d'avenir pour des puissances étrangères comme la Chine. Plutôt que de chercher à égaler un adversaire technologiquement supérieur, un État pourrait tenter de le convaincre que certaines de ses technologies sont compromises ou devenues inefficaces, afin de le pousser à en réduire lui-même l'utilisation.

Dans cette perspective, maintenir et protéger la confiance que les forces armées occidentales accordent aux technologies qu'elles utilisent et dans lesquelles elles ont investi des ressources considérables constitue un enjeu stratégique de première importance.¹⁵ Cet enjeu devient encore plus crucial en période de crise, lorsque des décisions rapides et difficiles doivent être prises quant à la fiabilité des technologies de l'information. Le présent article propose des pistes de solution à ce défi. Nous préconisons

une approche qui place les personnes au cœur de la protection de la puissance aérienne contre les cybermenaces. Cette approche consiste à développer le capital humain et les structures organisationnelles nécessaires au maintien d'un haut niveau de confiance et de résilience technologique au sein d'une force aérienne. Alors que l'Aviation royale canadienne (ARC) célèbre son centenaire, adapte ses capacités afin de défendre et de protéger le Canada et continue de contribuer, avec les États-Unis, à la défense de l'Amérique du Nord, le moment est particulièrement propice pour examiner l'interconnexion croissante entre les domaines, les technologies et le rôle toujours essentiel des personnes dans un environnement en constante évolution.

BOYD 2.0 : RÉINVENTER LA BOUCLE

Pour bien comprendre l'enjeu, il faut d'abord revenir aux origines du paradigme du techno-solutionnisme, et plus particulièrement à l'un de ses concepts fondamentaux : la célèbre « boucle OODA » (observation, orientation, décision, action), élaborée par le colonel de l'United States Air Force, John Boyd, dans les années 1980.¹⁶ Conçue pour décrire le processus par lequel un acteur perçoit une situation, l'analyse, délibère, puis agit en conséquence, la boucle OODA a depuis acquis une notoriété considérable et a été appliquée, avec plus ou moins de succès, à une multitude de domaines non militaires, allant des affaires au sport. Dans le domaine militaire, le concept de la boucle OODA a progressivement donné naissance à une véritable théorie de la victoire, adoptée par plusieurs grandes forces armées occidentales,¹⁷ notamment celles des États-Unis, du Royaume-Uni et de la France.¹⁸ En résumé, le principe fondamental veut que l'acteur qui parvient à franchir les étapes de la boucle OODA le plus rapidement acquière un avantage sur son adversaire. Entre autres avantages, l'exécution rapide de cette boucle est censée procurer une meilleure connaissance de la situation et, ultimement, permettre de maîtriser le rythme des opérations.¹⁹ Au cours des années 1990, cette logique a conduit les forces armées à se doter de technologies de commandement, de contrôle, de communications, d'informatique, de renseignement, de surveillance et de reconnaissance (C4ISR) toujours plus perfectionnées afin d'accélérer l'exécution de la boucle OODA.

Toutefois, le paradigme de la boucle OODA paraît aujourd'hui fragilisé par la complexité croissante et le développement des capacités de guerre électronique et de cyberguerre. Puisque les cybermoyens peuvent compromettre les technologies de l'information, dont dépend largement la fluidité de la boucle OODA, ils semblent remettre en cause un mode de conduite de la guerre fondé en grande partie sur la supériorité technologique et informationnelle.²⁰ Certaines approches de conceptualisation des cyberopérations montrent qu'il est possible de neutraliser un adversaire dans un conflit ouvert, en compromettant ses capacités de collecte du renseignement ou ses systèmes de communication.²¹ À cet égard, les cybermenaces revêtent

une importance particulière dans le domaine aérien, où les technologies numériques sont non seulement omniprésentes et essentielles à l'accomplissement des missions, mais constituent également des vecteurs d'attaque potentiels. Les forces aériennes doivent désormais composer avec des cybermenaces, les risques associés à l'utilisation de technologies complexes et à leur interconnexion, ainsi qu'avec diverses formes d'intervention humaine, comme l'usurpation des signaux GPS,²² le piratage des logiciels embarqués²³ ou la compromission des liaisons de données,²⁴ sans oublier les menaces visant les bases aériennes et les infrastructures physiques. Ainsi, durant la crise du golfe d'Oman en 2019, les forces armées des États-Unis ont infiltré une base de données, exploitée par le Corps des gardiens de la révolution islamique, afin de neutraliser les capacités de ciblage de l'Iran, notamment celles utilisées pour les drones d'attaque.²⁵ Lorsqu'un adversaire exploite les vulnérabilités décrites précédemment, il peut ralentir considérablement, voire paralyser, l'exécution de la boucle OODA.

Malgré les nombreux usages - et mésusages - dont elle a fait l'objet au fil des ans, la boucle OODA demeure un cadre d'analyse utile pour notre propos, puisqu'elle met en évidence deux aspects essentiels de la gestion des cybermenaces. Premièrement, le principe de la boucle OODA s'applique aux situations liées aux cyberattaques, à la posture et à la planification. Lorsqu'une force armée est confrontée à un cyberincident, elle doit être en mesure d'observer les effets des activités de piratage, de *s'orienter* dans l'environnement perturbé par l'attaque, de *décider* avec assurance quelles capacités sont compromises et lesquelles demeurent opérationnelles, puis d'*agir* à partir de cette analyse. Le concept de la boucle OODA peut ainsi servir à comprendre les effets d'une attaque et à déterminer les mesures qui s'imposent. Certes, la boucle OODA ne constitue pas une méthode d'intervention en cas de cyberincident. Elle offre néanmoins un cadre utile pour renforcer la confiance envers les personnes et les technologies, comme nous le montrerons plus loin.²⁶

Deuxièmement, même si les technologies de l'information constituent d'importants facteurs facilitants et accélérateurs de la boucle OODA, elles n'en représentent nullement les seules composantes. Les processus par lesquels une force armée recueille et traite l'information reposent également sur des dimensions humaines et organisationnelles essentielles, dont l'importance est comparable à celle des technologies elles-mêmes.²⁷ Comme l'ont montré plusieurs auteurs, les forces armées modernes n'exploitent pas toujours pleinement les technologies les plus avancées, en raison d'une gestion insuffisante des facteurs humains et organisationnels.²⁸ Bien entendu, la rapidité d'exécution de la boucle OODA ne constitue pas, à elle seule, la clé du succès des opérations militaires contemporaines. Il n'en demeure pas moins que les facteurs humains et organisationnels jouent un rôle déterminant dans ce processus et doivent continuer à évoluer afin d'en préserver la fluidité. Le véritable défi consiste donc à déterminer comment tirer le meilleur parti des ressources

humaines et organisationnelles disponibles afin de maintenir, ou de rétablir, la fluidité de la boucle OODA dans un contexte où les technologies sont—ou semblent être—dégradées.

Dans les sections qui suivent, nous présentons des exemples tirés de l'expérience des alliés internationaux du Canada ainsi que des pistes visant à renforcer la résilience dans les environnements de conflit numériques et physiques. Enfin, nous regroupons notre analyse et nos recommandations dans le contexte de la modernisation du NORAD et de la coopération binationale, telles qu'elles sont mises en évidence dans la récente mise à jour de la politique de défense *Notre Nord, fort et libre : Une vision renouvelée pour la défense du Canada*. Ce faisant, nous mettons en lumière les liens étroits qui unissent les dimensions aérienne, humaine et du cyberspace de la puissance militaire.

S'ENTRAÎNER ET PLANIFIER : SE PRÉPARER AUX SCÉNARIOS DE CRISE

Les forces armées disposent de plusieurs moyens pour anticiper les cyberattaques majeures et s'y préparer. Parmi ceux-ci figurent les exercices simulant la compromission de systèmes militaires. Dès 1997, le ministère de la Défense des États-Unis (DoD) a mené un premier exercice de ce type, *Eligible Receiver 97*, au cours duquel une équipe rouge de la National Security Agency (NSA) a tenté d'infiltrer les réseaux du Commandement Indo-Pacifique des États-Unis.²⁹ Bien que les résultats se soient révélés catastrophiques pour les défenseurs, cet exercice a permis de mettre en évidence plusieurs cybervulnérabilités au sein du DoD et de démontrer différentes façons de renforcer les défenses. Depuis, ce type d'exercice est devenu beaucoup plus courant³⁰ et prend diverses formes.

Ces exercices sont souvent organisés chaque année. Ils peuvent faire intervenir plusieurs pays, réunir principalement des spécialistes du cyberspace et viser à simuler la défense active d'un réseau contre des acteurs hostiles fictifs. D'autres exercices mobilisent des forces conventionnelles afin de développer leur capacité à poursuivre leurs opérations dans un contexte de cyberattaque, dans le but de renforcer la résilience numérique des unités. La France, par exemple, organise de plus en plus d'exercices dans des « conditions de dégradation numérique » afin de mieux préparer ses unités à exécuter leurs missions même lorsque certaines technologies deviennent indisponibles ou inutilisables.³¹

Les exercices qui combinent des volets numériques et conventionnels, présentent un intérêt particulier, puisqu'ils réunissent des spécialistes du cyberspace et des militaires des forces conventionnelles et permettent aux unités de coordonner leurs opérations avec les activités de protection et de rétablissement des systèmes. Plusieurs auteurs qualifient cette synergie d'« assurance de la mission », concept selon lequel la capacité d'une organisation à accomplir sa mission est préservée grâce à des processus précis en cas de défaillance d'un système.³²

Ainsi, au début de 2024, l'armée française de l'Air et de l'Espace a simulé une cyberattaque, visant le système embarqué d'un avion d'avitaillement et de transport *Phénix*,³³ ainsi que son rétablissement, en réunissant des aviateurs et du personnel de cyberdéfense dans le cadre de l'exercice annuel majeur DEFNET.³⁴ Dans de tels exercices, il ne s'agit pas seulement d'entraîner un état-major à revenir à des technologies plus anciennes, comme dans 2034, mais aussi à s'exercer à déterminer avec assurance quels systèmes demeurent fiables et lesquels semblent compromis, ainsi qu'à évaluer la faisabilité et la rapidité de leur remise en service.³⁵ Autrement dit, ces exercices permettent de mettre en pratique les phases *observation* et *orientation* de la boucle OODA dans un contexte de cyberattaque.

Ces exercices permettent également aux forces armées de développer un autre élément essentiel de leur résilience : les plans de contingence. Des procédures préétablies peuvent préciser les mesures à prendre dans un scénario de crise, où certaines capacités technologiques sont dégradées. Dans le domaine aérien, l'United States Air Force teste actuellement des méthodes de navigation fondées sur l'analyse des anomalies du champ magnétique terrestre afin de permettre à ses pilotes de s'orienter même si leur système GPS est neutralisé.³⁶ Il ne s'agit là que de quelques exemples de procédures pouvant être élaborées et mises en œuvre en cas de cyberattaque. Toutefois, ces mesures doivent s'inscrire dans des plans de contingence complets, qui prévoient notamment une formation minimale permettant au personnel d'utiliser des méthodes de rechange ou des moyens « à faible composante technologique ». Lorsqu'ils sont bien conçus et largement diffusés, ces plans facilitent les phases *décision* et *action* de la boucle OODA. Ils offrent aux commandants des options éprouvées et potentiellement viables tout en veillant à ce que le personnel chargé de leur mise en œuvre dispose de toute l'information nécessaire.

S'ORGANISER : GARDER SES ALLIÉS À PROXIMITÉ

Un autre ensemble de mesures susceptibles d'accroître la résilience d'une force aérienne face aux cybermenaces concerne sa structure organisationnelle et administrative, plus particulièrement la place qu'y occupent les spécialistes de la cyberdéfense. À l'image d'un casse-tête, la cohérence d'une organisation militaire dépend non seulement de la présence de toutes les pièces, mais aussi de leur emplacement dans l'ensemble. Le défi consiste ici à organiser les « cyberpièces » d'une force aérienne de manière à lui permettre de réagir efficacement en situation de crise.

Comme dans bien des organisations, l'un des principaux défis tient au fait que les spécialistes et les unités de cyberdéfense demeurent souvent des éléments de soutien périphériques, relativement éloignés des centres décisionnels. Les commandants sur le terrain et les spécialistes de la cyberdéfense collaborent rarement et ne se *connaissent* pas vraiment sur le plan professionnel.

Pour compliquer davantage la situation, ces deux groupes peuvent avoir des parcours de formation différents ainsi que des façons distinctes d'aborder et de communiquer les problèmes opérationnels; ils ne se *comprennent* donc pas nécessairement bien. Comme le déplorait Michael Hayden, ancien général de l'United States Air Force et ancien directeur de la National Security Agency : « Après quelques phrases, l'exposé du spécialiste en cyberdéfense commence à évoquer vaguement *l'Homme de la pluie* pour la plupart des hauts dirigeants présents dans la salle. Après quelques phrases de plus, la plupart en sont convaincus ». ³⁷ Parler un langage commun et être capable de passer d'un langage à l'autre peut contribuer à combler les écarts entre la planification stratégique et la planification opérationnelle.

Cette situation est particulièrement problématique, parce que les cybermenaces peuvent profondément ébranler la confiance que les forces armées accordent à leurs technologies si les interactions complexes entre les composantes numériques et physiques sont mal comprises. Cette confiance repose notamment sur celle que les militaires des forces « conventionnelles » accordent aux spécialistes chargés de protéger leurs systèmes.³⁸ Il va de soi que la protection des systèmes ne relève pas uniquement des spécialistes de la cyberdéfense; les commandants et leurs états-majors ont eux aussi un rôle essentiel à jouer. Dans le milieu militaire, comme ailleurs, il est plus facile de faire confiance à une personne que l'on connaît et dont on a déjà pu apprécier les compétences. Il pourrait donc être opportun d'accorder une priorité organisationnelle à une intégration plus étroite des spécialistes de la cyberdéfense dans l'ensemble des opérations aériennes, tout en favorisant des relations de confiance réciproques permettant aux commandants de mieux comprendre leur dépendance envers le cyberspace. Les commandants devraient veiller à ce qu'eux-mêmes et leur état-major, y compris les spécialistes de la cyberdéfense, contribuent activement à la protection des systèmes. Le développement de cette confiance et de cette expertise revêt une importance particulière, puisque de nombreuses cyberattaques exploitent à la fois des vulnérabilités humaines et techniques.

Une intégration plus poussée pourrait notamment prendre la forme de mécanismes d'apprentissage réciproque, permettant au personnel de mieux comprendre le rôle des spécialistes de la cyberdéfense, leur façon de travailler et la contribution de leurs activités au fonctionnement stratégique, opérationnel et organisationnel d'une force aérienne. D'autres initiatives pourraient simplement consister à rapprocher physiquement les spécialistes de la cyberdéfense de certains secteurs d'opérations. Ainsi, dans le conflit qui se déroule actuellement en Ukraine, les forces ukrainiennes et russes auraient commencé à déployer des cyberéquipes près de la ligne de front afin d'améliorer leur coordination avec les unités avancées, une décision qui s'explique notamment par la nécessité d'assurer le fonctionnement efficace des drones.³⁹ En plus de raccourcir la chaîne de communication, le rapprochement des différentes équipes peut aider

les spécialistes de la cyberdéfense et le personnel des forces conventionnelles à mieux comprendre leurs besoins respectifs et à développer de meilleures synergies.⁴⁰ L'établissement de cette proximité et de cette connaissance mutuelle peut ainsi contribuer à accroître l'efficacité de la boucle OODA.

INSPIRER : CRÉER LES BONS INCITATIFS

L'isolement des spécialistes de la cyberdéfense ne découle pas uniquement de leur place dans l'organigramme; il s'enracine également dans des cultures organisationnelles qui influencent la façon dont la communauté militaire les perçoit. Qu'il s'agisse de l'armée de terre, de la marine ou de l'aviation, les organisations militaires entretiennent des normes, des valeurs et des traditions qu'elles perpétuent au fil du temps.⁴¹ Ces cultures ont une incidence directe sur le fonctionnement des organisations, mais elles peuvent aussi contribuer à certaines difficultés touchant la posture opérationnelle.

Dans un article, Rebecca Slayton montre que la persistance du culte de la « figure du guerrier » contribue directement à la marginalisation des spécialistes de la cyberdéfense au sein des forces armées des États-Unis.⁴² Le paradigme de la figure du guerrier renvoie à la valorisation institutionnelle de militaires, appartenant à certaines spécialités, notamment les forces spéciales ou les armes de combat, dont les fonctions sont jugées plus nobles parce qu'elles correspondent davantage à l'idéal martial de l'archétype du soldat.⁴³ Dans le domaine aérien, cette logique s'applique tout particulièrement à la figure du pilote, associée à une image d'autorité largement entretenue par la culture populaire.⁴⁴ Par conséquent, ces fonctions bénéficient souvent d'une plus grande crédibilité au sein de l'institution militaire, au détriment de spécialités perçues comme moins directement liées au combat, telles que la logistique ou les communications. Le culte de la figure du guerrier entraîne des conséquences concrètes. Par exemple, les fonctions considérées comme les plus prestigieuses donnent souvent un accès privilégié à certains postes ou commandements,⁴⁵ ce qui peut rendre certains parcours professionnels plus attrayants que d'autres.

Les spécialistes de la cyberdéfense, qui ne sont généralement pas perçus comme de « véritables guerriers », peuvent subir les effets négatifs de cette culture. Ces effets se traduisent notamment par une affectation plus fréquente à des tâches de moindre importance, par une progression plus lente dans la hiérarchie militaire et par un accès plus limité à certains commandements prestigieux.⁴⁶ Cette réalité pousse inévitablement de nombreux candidats potentiels vers d'autres spécialités militaires ou incite des spécialistes expérimentés à poursuivre leur carrière dans le secteur civil, où les perspectives d'emploi dans ce domaine sont nombreuses.⁴⁷ Aux États-Unis, l'United States Air Force est historiquement l'armée qui s'est montrée la plus accueillante envers les spécialistes de la cyberdéfense, sans doute en raison d'une culture institutionnelle de longue date fondée sur l'idée

que la victoire repose sur la supériorité technologique.⁴⁸ Même dans ce cas relativement favorable, le statut du cybercombattant demeure largement éclipsé par celui du pilote, qui continue d'incarner la figure idéale du guerrier. Dans une étude publiée en 2019, la RAND Corporation concluait que les pilotes de chasse, suivis des pilotes de bombardier, représentaient de loin les parcours les plus prometteurs pour accéder aux plus hauts échelons de l'United States Air Force.⁴⁹

Si une force aérienne veut relever efficacement les cybermenaces de demain, elle doit rehausser le statut des spécialistes de la cyberdéfense et mettre en place des incitatifs plus attrayants afin d'encourager le personnel à choisir cette spécialité. Cela peut passer par une réforme des mécanismes de recrutement, de formation et de maintien en poste existants, que Nicholas Romanow regroupe sous l'appellation de « triade de gestion des talents cybernétiques ».⁵⁰ Selon Romanow, même si les dirigeants militaires reconnaissent l'importance des cyberopérations, les effectifs demeurent insuffisants pour pourvoir les postes spécialisés, notamment en raison de la concurrence exercée par le secteur privé et d'une culture militaire peu attrayante pour la communauté cyber. Une façon de remédier à cette situation consiste à investir dans le développement de leaders solides en cyberdéfense tout en s'appuyant sur la culture de service propre aux forces armées.⁵¹ L'United States Air Force a récemment lancé un programme visant à accélérer l'octroi d'une commission d'officier aux spécialistes de la cyberdéfense.⁵² Dans le cadre d'une révision du parcours professionnel militaire traditionnel, ce programme vise notamment à mieux reconnaître les compétences liées au cyberspace par rapport à d'autres expériences militaires plus conventionnelles. Il cherche également à permettre aux spécialistes de la cyberdéfense d'accéder plus facilement à un grade et à une rémunération qui sont comparables à ceux offerts dans le secteur civil.

Comme l'ont montré des auteurs tels que Max Smeets, le développement des cybercapacités d'une force armée exige une combinaison judicieuse de compétences et de profils variés, qui dépasse largement le seul personnel technique.⁵³ Si le capital humain joue un rôle essentiel dans la confiance que les forces armées accordent à leurs technologies et s'il constitue une composante déterminante du bon déroulement de la boucle OODA, les spécialistes de la cyberdéfense doivent se sentir véritablement valorisés et pleinement associés à cet effort. Dans cette perspective, les programmes de formation et d'enseignement pourraient être élargis afin de s'adresser non seulement aux spécialistes de la cyberdéfense, mais également aux dirigeants et au personnel généraliste. En définitive, tous les militaires, et plus particulièrement ceux qui exercent des fonctions de commandement, doivent posséder les connaissances nécessaires pour comprendre dans quelle mesure leur mission dépend du cyberspace et pour jouer pleinement leur rôle dans la gestion des risques cybernétiques liés à cette mission.

CONCLUSION

Le maintien de la confiance envers les technologies numériques face aux cybermenaces doit aller de pair avec la confiance envers les personnes et leur capacité à travailler ensemble. Comme nous l'avons montré, la mise en pratique régulière de scénarios de cyberattaque et l'élaboration de plans de circonstance adaptés à ces situations contribuent à instaurer et à préserver cette confiance. Une autre approche consiste à agir sur les structures organisationnelles afin de mieux intégrer les spécialistes de la cyberdéfense et de favoriser une meilleure connaissance mutuelle ainsi que de plus grandes synergies avec les autres membres du personnel. L'évolution de la culture organisationnelle peut également jouer un rôle déterminant, en renforçant la confiance grâce à des incitatifs qui encouragent le personnel à choisir des fonctions liées au cyberspace.

Dans la récente mise à jour de la politique de défense, le ministère de la Défense nationale présente plusieurs projets, visant l'intégration de nouvelles technologies au sein du NORAD, notamment dans les domaines de l'information et des communications, en soulignant que les capacités de commandement et de contrôle doivent « être numérisées pour fonctionner à la vitesse de la machine ».⁵⁴ Dans cette perspective, le Canada a entrepris l'adoption et l'intégration de systèmes de commandement et de contrôle infonuagiques dans les installations canadiennes du NORAD.⁵⁵ Même si ces nouvelles technologies offrent des possibilités accrues en matière de circulation de l'information, de collecte de données et d'analyse pour améliorer la connaissance de la situation, elles doivent être considérées comme les composantes d'un système dont l'être humain demeure au cœur. Un autre élément mérite également une attention particulière : le NORAD repose sur un partenariat fondé sur l'interopérabilité et la confiance mutuelle. Par conséquent, la confiance envers les technologies de l'information revêt une importance fondamentale. De la même façon que le personnel des forces conventionnelles

doit avoir confiance dans la capacité des spécialistes de la cyberdéfense à protéger leurs systèmes, les deux partenaires doivent maintenir une confiance réciproque dans leur aptitude à préserver l'intégrité des réseaux liés au NORAD. Accorder une attention particulière à la dimension humaine de la cybersécurité pourrait également contribuer à résoudre les difficultés de recrutement et de maintien en poste auxquelles font face les Forces armées canadiennes (FAC).⁵⁶ Les FAC en général, et l'ARC en particulier, ont donc tout intérêt non seulement à demeurer un employeur attrayant pour les spécialistes de la cyberdéfense, mais aussi à tirer pleinement parti du potentiel d'innovation des personnes qui œuvrent déjà dans ce domaine.

Si les technologies de l'information constituent à la fois un élément essentiel et une source de vulnérabilité pour les forces armées modernes, les facteurs humains et organisationnels représentent des garanties indispensables au maintien de leurs capacités opérationnelles. Dans le présent article, nous avons cherché à situer les enjeux liés au cyberspace dans le contexte du domaine aérien. Les questions soulevées méritent l'attention des dirigeants de l'ARC, tant de façon autonome qu'en collaboration avec l'Armée canadienne et la Marine royale canadienne. La planification à long terme de la cybersécurité exige une approche, mobilisant l'ensemble des forces plutôt qu'une organisation en vase clos. Nous avons montré que divers outils existent déjà, ou sont en cours de développement, et qu'ils peuvent être mis à profit de manière concrète. À mesure que l'intégration des technologies émergentes devient une priorité pour la défense continentale et les autres partenariats de confiance,⁵⁷ les alliés devront veiller à préparer dès maintenant leurs capacités technologiques et humaines aux défis de demain afin de pouvoir assurer leur défense de manière concertée. Face au risque d'un techno-pessimisme excessif, les forces aériennes peuvent ainsi préserver la confiance envers leurs technologies numériques, en veillant à préserver l'intervention humaine.

Notes

- 1 Elliot Ackerman et amiral de l'USN James Stavridis (retraité), *2034*, Paris, Éditions Gallmeister, 2022.
- 2 Pour d'autres exemples de scénarios fictifs similaires, voir P. W. Singer et August Cole, *La flotte fantôme*, Gallimard, 2022. Pour un point de vue critique sur l'utilisation de la fiction spéculative, voir Col. Mark D. Jacobson, « The Uses and Limits of Speculative Fiction: Three Novels about a US-China War », *Journal of Indo-Pacific Affairs*, août 2023, 1-10.
- 3 Voir Bruce Schneier et Tara Wheeler, « Hacked drones and busted logistics are the cyber future of warfare », Brookings Institution, 4 juin 2021. Source d'origine : <https://www.brookings.edu/articles/hacked-drones-and-busted-logistics-are-the-cyber-future-of-warfare/>
- 4 Jonathan Beale, « Ukraine war: How old tech is helping Ukraine avoid detection », *BBC World*, 3 mai 2023. Source d'origine : <https://www.bbc.com/news/world-europe-65458263>
- 5 Pour une analyse de la distinction et de la convergence entre la cyberguerre et la guerre électronique, voir Ryan J. Worrell, *EW and Cyber Convergence: Beyond Information Warfare*, Air Force Fellows Program, 2020. Source d'origine : <https://apps.dtic.mil/sti/pdfs/AD112357.pdf>
- 6 Note terminologique : dans le contexte de l'aviation, les drones et les hélicoptères constituent tous deux des aéronefs. La classification des drones varie selon la doctrine nationale, qui peut notamment retenir les notions de système d'aéronef sans pilote, d'aéronef non habité ou d'aéronef télépilote. Chacune de ces catégories présente des caractéristiques et des vulnérabilités cybernétiques distinctes. Pour une analyse plus détaillée des différents types de classification des drones, voir Maj. Osman Aksu et al., *A Comprehensive Approach to Countering Unmanned Aircraft Systems*, Joint Air Power Competence Centre, janvier 2021.
- 7 Scott Peterson, Payam Faramarzi, « Iran hijacked US drone, says Iranian engineer », *Christian Science Monitor*, 15 décembre 2011. Source d'origine : <https://www.csmonitor.com/World/Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer>
- 8 Nick Waters, « The Poor Man's Air Force? Rebel Drones Attack Russia's Airbase in Syria », *Bellingcat*, 12 janvier 2018. Source d'origine : https://www.bellingcat.com/news/mena/2018/01/12/the_poor_mans_airforce/
- 9 Dan Black et Gabby Roncone, « The GRU's Disruptive Playbook », *Mandiant Blog*, 12 juillet 2023 [mise à jour : 3 avril 2024]. Source d'origine : <https://www.mandiant.com/resources/blog/gru-disruptive-playbook>
- 10 Mauro Gilli et Niklas Masuhr, « Drones enhance defences in the Ukraine war », *Binding Hook*, 10 janvier 2024. Source d'origine : <https://bindinghook.com/articles-hooked-on-trends/drones-enhance-defences-in-the-ukraine-war/>

- 11 Voir, par exemple, dans Sam Skove, « Army puts drones front and center in unfunded wishlist », *Defense One*, 22 mars 2024. Source d'origine : <https://www.defenseone.com/technology/2024/03/army-puts-drones-front-and-center-newly-obtained-budget-docs/395182/>. Sam Skove, « Army announces plan to help spread commercial drones across infantry units », *Defense One*, 27 mars 2024. Source d'origine : <https://www.defenseone.com/threats/2024/03/army-announces-plan-help-spread-commercial-drones-across-infantry-units/395260/>. Maxine Baen, « Army tests commercial satellite internet in pilot program », *U.S. Army*, 28 février 2022. Source d'origine : https://www.army.mil/article/254316/army_tests_commercial_satellite_internet_in_pilot_program
- 12 Daniel Moore, *Offensive Cyber Operations: Understanding Intangible Warfare*. Oxford University Press, 2022, 97-99.
- 13 Pour un aperçu du paradigme du techno-solutionnisme militaire, voir Jon R. Lindsay, « The Technology Theory of Victory », dans *Information Technology and Military Power*. Cornell University Press, 2020, 13-31.
- 14 Christopher Coker, *Future War*, Polity Press, 2015, 171-172.
- 15 Voir Martin C. Libicki, « Cyberwar as a Confidence Game », *Strategic Studies Quarterly* vol. 5, n° 1, 2011, 132-147.
- 16 Pour un aperçu des travaux de John Boyd, voir Robert Coram, *Boyd: The Fighter Pilot Who Changed the Art of War*, Little, Brown and Company, 2002.
- 17 Bien que la boucle OODA tire son origine de la puissance aérienne, ce concept a pris une importance croissante dans l'ensemble des domaines conventionnels de la guerre. Par exemple, voir Brian R. Price, « Colonel John Boyd's Thoughts on Disruption: A Useful Effects Spiral from Uncertainty to Chaos », *Journal of Advanced Military Studies*, vol. 14, n° 1, 2023, 98-117.
- 18 Pascal Venesson, « Fighting, Fast and Slow? Speed and Western Ways of War », dans Sten Rynning, Olivier Schmitt, Amelie Theussen, *War Time: Temporality and the Decline of Western Military Power*, Brookings Institution Press, 2021, 211-229.
- 19 Certes, la boucle OODA ne repose pas uniquement sur la rapidité. Comme le soutiennent notamment Luft et Kollars, elle repose également sur le rythme et le choix du moment. Voir Alastair Luft, « The OODA Loop and the Half-Beat », *The Strategy Bridge*, 17 mars 2020, et Nina A. Kollars, « War at Information Speed: Multi-Domain Warfighting Visions », dans Sten Rynning, Olivier Schmitt, Amelie Theussen, *op. cit.*, 230-252. Source d'origine : <https://thestrategybridge.org/the-bridge/2020/3/17/the-ooda-loop-and-the-half-beat>
- 20 Joseph Henrotin et Stéphane Taillat, « Military Operations: What If Digital Technologies Fail on the Battlefield? », dans Sten Rynning, Olivier Schmitt, Amelie Theussen, *op. cit.*, 275-291.
- 21 Daniel Moore, *op. cit.*, 186-200.
- 22 Shah Zahid Khan, Mujahid Mohsin, et Waseem Iqbal, « On GPS spoofing of aerial platforms: a review of threats, challenges, methodologies, and future research directions », *PeerJ Computer Science*, n° 7, 2021, e507.
- 23 Eduard Kovacs, « BAE Releases New Cybersecurity System for F-16 Fighter Aircraft », *Security Week*, 14 octobre 2022. Source d'origine : <https://www.securityweek.com/bae-releases-new-cybersecurity-system-f-16-fighter-aircraft/>
- 24 Kim Hartmann et Keir Giles, « UAV Exploitation: A New Domain for Cyber Power », 8th International Conference on Cyber Conflict: Cyber Power, Centre d'excellence OTAN pour la cyberdéfense en coopération, 2016, 205-221.
- 25 Julian E. Barnes, U.S. Cyberattack Hurt Iran's Ability to Target Oil Tankers, Officials Say », *The New York Times*, 28 août 2019. Source d'origine : <https://www.nytimes.com/2019/08/28/us/politics/us-iran-cyber-attack.html>
- 26 Le cadre de cybersécurité du National Institute of Standards and Technology (NIST) des États-Unis sert généralement à intervenir en cas de cyberincident. Ce cadre comprend les fonctions de déterminer, protéger, détecter, répondre et rétablir. Les liens entre ce cadre, une cybersécurité axée sur l'humain et la culture organisationnelle feront l'objet d'une analyse approfondie dans des travaux à paraître de Csenkey et Furlong.
- 27 Jon R. Lindsay, *op. cit.*, 32-70.
- 28 Jon Lindsay, *op. cit.*
- 29 Fred Kaplan, *Dark territory: The secret history of cyber war*, New York, Simon & Schuster, 2016, 68-71.
- 30 Pour une histoire plus approfondie des débuts des cyberconflits, notamment de l'exercice ELIGIBLE RECEIVER et d'autres événements, voir Jason Healey, *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*. Vienna, VA: Cyber Conflict Studies Association, 2013.
- 31 Comité d'éthique de la défense, *Avis sur l'environnement numérique des combattants*, ministère des Armées, 13 avril 2022. Source d'origine : https://www.defense.gouv.fr/sites/default/files/tronc_commun/20220413_Comit%C3%A9_d%C3%A9thique_de_la_d%C3%A9fense_-_Avis_sur_l%27environnement_num%C3%A9rique_des_combattants.pdf
- 32 Brad Bigelow, « Mission Assurance: Shifting the Focus of Cyber Defence », 2017 9th International Conference on Cyber Conflict (CyCon), CCD COE de l'OTAN, 2017, p. 1-12, <https://doi.org/10.23919/CYCON.2017.8240327>.
- 33 Airbus Defence and Space A330-200 Phénix Multi-Role Tanker Transport.
- 34 Commandement de la Cyberdéfense, *DEFNET 2024 : une cyberattaque simulée sur le plan de vol du Phénix*, ministère des Armées, 29 mars 2024. Source d'origine : <https://www.defense.gouv.fr/comcyber/actualites/defnet-2024-cyberattaque-simulee-plan-vol-du-phenix>
- 35 Daniel T. Sullivan, Edward J.M. Colbert, Blaine E. Hoffman et Alexander Kott, « Best practices for designing and conducting cyber-physical-system war games », *Journal of Information Warfare*, vol. 17, n° 3, 2018, 92-105.
- 36 David Roza, « C-17 Tests Magnetic Navigation System That Works When GPS Doesn't », *Air & Space Forces Magazine*, 7 juin 2023. Source d'origine : <https://www.airandspaceforces.com/air-force-magnetic-navigation-gps/>
- 37 Michael V. Hayden, *Playing to the Edge: American Intelligence in the Age of Terror*, Penguin Press, 2016, 147.
- 38 Diane Henshel, *et al.*, « Trust as a human factor in holistic cyber security risk assessment », *Procedia Manufacturing*, vol. 3, 2015, 1117-1124.
- 39 Gordon Corera, « Ukraine war: Cyber-teams fight a high-tech war on front lines », *BBC*, 5 septembre 2023. Source d'origine : <https://www.bbc.com/news/world-europe-66686584>
- 40 *Ibid.*
- 41 Joseph Soeters, « Organizational Cultures in the Military », *Handbook of the Sociology of the Military*, Springer, 2018, 251-272.
- 42 Rebecca Slayton, « What Is a Cyber Warrior? The Emergence of U.S. Military Cyber Expertise, 1967-2018 », *Texas National Security Review*, vol. 4, n° 1, 2021.
- 43 *Ibid.*
- 44 Voir Michael Wayne Hankins, *The Cult of the Lightweight Fighter: Culture and Technology in the U.S. Air Force, 1964-1991*, dissertation doctorale, Kansas State University, 2018.
- 45 Pour une analyse de cette dynamique dans le domaine aérien, voir Michael R. Worden, *Rise of the fighter generals: the problem of air force leadership, 1945-1982*, Air University Press, 1998.
- 46 Josh Lospinoso, « Fish Out of Water: How the Military Is an Impossible Place for Hackers, and What to Do About It », *War on the Rocks*, 12 juillet 2018. Source d'origine : <https://warontherocks.com/2018/07/fish-out-of-water-how-the-military-is-an-impossible-place-for-hackers-and-what-to-do-about-it/>
- 47 Lee Lunn, « Cyber Operator: Are you sure you want to do that? », *The Blue Knight Review*, 2021. Source d'origine : <https://www.cmrsj-rmcsj.forces.gc.ca/cb-bk/art-art/2021/art-art-2021-7-eng.asp>
- 48 Sarah P. White, *Subcultural Influence on Military Innovation: The Development of U.S. Military Cyber Doctrine*, dissertation doctorale, Harvard University, Graduate School of Arts & Sciences, 2019.
- 49 S. Rebecca Zimmerman, Kimberly Jackson, Natasha Lander, Colin Roberts, Dan Madden et Rebeca Orrie, *Movement and Maneuver: Culture and the Competition for Influence Among the U.S. Military Services*, RAND Corporation, 25 février 2019.
- 50 Nicholas Romanow, « Leadership, Culture, and the Military Cyber Workforce », *War on the Rocks*, 11 avril 2024. Source d'origine : <https://warontherocks.com/2024/04/leadership-culture-and-the-military-cyber-workforce/>
- 51 *Ibid.*
- 52 Air Force Recruiting Public Affairs, « Cyber Direct Commissioning Program enhancement to onboard future cyber officers », US Air Force, 19 avril 2023. Source d'origine : <https://www.af.mil/News/Article-Display/Article/3368057/cyber-direct-commissioning-program-enhancement-to-onboard-future-cyber-officers/>
- 53 Max Smeets, *No Shortcuts: Why States Struggle to Develop a Military Cyber-Force*, Oxford University Press, 2022, 75-79.
- 54 Ministère de la Défense nationale, *Notre Nord, fort et libre : Une vision renouvelée pour la défense du Canada*, 9 avril 2024. Source d'origine : <https://www.canada.ca/fr/ministere-defense-nationale/organisation/rapports-publications/nord-fort-libre-2024.html>
- 55 Maxime Cliché, *Canadian Air Defence Sector introduces new cloud-based command-and-control system*, Commandement de la défense aérospatiale de l'Amérique du Nord, 26 janvier 2024. Source d'origine : <https://www.norad.mil/Newsroom/Article/3657967/canadian-air-defence-sector-introduces-new-cloud-based-command-and-control-syst/>
- 56 Aaron D'Andrea, « Canada's military facing 'death spiral' on recruitment, minister says », *Global News*, 7 mars 2024. Source d'origine : <https://globalnews.ca/news/10341588/canadian-forces-recruitment-death-spiral/>
- 57 Kristen Csenkey et Nina Bindel, « Post-Quantum Cryptographic Assemblages and the Governance of the Quantum Threat », *Journal of Cybersecurity* vol. 9, n° 1, 2023, 1-14, <https://doi.org/10.1093/cybssec/tyad001>

Armes autonomes et cognition étendue

MAJOR ANDREW G. HOLT

Le major Andrew G. Holt est actuellement commandant du 5^e Régiment d'artillerie légère du Canada. Il est titulaire d'une maîtrise en histoire et philosophie des sciences et de la technologie de l'Université de Toronto et d'une maîtrise en études militaires de l'Université Deakin.

Les pays se développent rapidement et mettent en œuvre des SALA. Ces armes font l'objet d'un débat dans les milieux universitaire, juridique et politique, où beaucoup soulèvent des objections éthiques en raison de lacunes perçues sur le plan de la responsabilisation. De telles lacunes pourraient entraver les poursuites contre les criminels de guerre, menacer la conduite morale de la guerre et réduire le respect du droit des conflits armés.¹ Beaucoup se concentrent sur le maintien des SALA sous contrôle humain, mais sans consensus sur la façon dont ce contrôle est défini ainsi que sur la façon dont il peut être exercé. La HCE, une vision de plus en plus populaire dans la science cognitive contemporaine, offre un moyen utile de comprendre le contrôle humain des SALA. J'aborde en premier lieu le débat en cours sur les SALA et la difficulté à définir le contrôle humain. Je résume ensuite la HCE et son application au contrôle humain des SALA, en examinant la façon dont les humains interagissent avec les technologies cognitives en général, en considérant les SALA comme des artéfacts cognitifs et en comparant le contrôle des SALA et des subordonnés humains. Je conclus que les SALA peuvent étendre la cognition et être sous le contrôle humain, même sans intervention humaine immédiate et consciente. Par conséquent, les processus militaires tels que l'instruction et la diffusion d'ordres pourraient permettre aux commandants d'exercer le contrôle des SALA de manière parallèle au contrôle des subordonnés humains.

Notions vagues de contrôle

Les universitaires débattent des répercussions éthiques des SALA depuis plus de dix ans. À la lumière de ce débat, la plupart d'entre eux adoptent des positions sceptiques à l'égard des SALA, sinon carrément opposées à leur utilisation. Une préoccupation commune est le manque de responsabilité humaine pour les SALA.² Une minorité d'auteurs, comme Simpson et Muller, ont un point de vue différent.³ Ils soutiennent que la responsabilité incombe aux commandants qui ont armé et déployé les SALA, et que le fait que les SALA se comportent de manière imprévisible n'empêche pas leur utilisation. Le débat n'est pas seulement théorique, mais mène à des appels à l'interdiction ou à la limitation des SALA en raison d'un manque de contrôle humain.⁴

Diverses organisations non gouvernementales ont adopté des positions fermes sur les SALA. L'International Committee for Robot Arms Control préconise que nous devons agir contre « les dangers pressants que [les SALA] posent à la paix et à la sécurité internationale ainsi qu'aux civils en temps de guerre⁵ » [TCO]. Le Comité international de la Croix-Rouge (CICR) a fait une présentation à une réunion des Hautes Parties contractantes et signataires de la Convention sur certaines armes classiques (CCAC) axée sur le contrôle humain des SALA, déclarant que : « il est essentiel que les États développent une compréhension commune des éléments

et critères du contrôle humain⁶ » [TCO]. Même les organisations qui s'intéressent de loin aux SALA, comme l'Institute of Electrical and Electronics Engineers (IEEE), recommandent que des mesures soient prises pour « aider à assurer un contrôle humain significatif des systèmes d'armes⁷ » [TCO].

Des États ont également commenté les répercussions juridiques et éthiques des SALA, bien que les positions énoncées puissent ne pas être exhaustives ni harmonisées avec les actions réelles desdits États.⁸ De nombreuses positions articulées se concentrent sur le contrôle humain des SALA, mais il n'y a pas de consensus sur ce que signifie réellement le contrôle humain.⁹ Le président du Groupe d'experts gouvernementaux a proposé une caractérisation de travail des SALA en 2025, mais le débat qui s'ensuit montre que la question du contrôle humain n'est toujours pas résolue. Certaines parties ont quand même demandé la qualification de « contrôle humain » avec des expressions telles que « contexte approprié » ou « significatif », mais il n'y a pas eu d'accord, car « les délégations ont réitéré leurs diverses positions partagées au cours des [précédents] échanges¹⁰ » [TCO].

Les discussions sur le contrôle humain font souvent référence à un cycle décision-action ou encore à l'exigence de la surveillance ou de l'intervention humaine. Le Canada utilise l'exigence de la surveillance ou de l'intervention humaine dans les documents officiels sur les SALA, en disant dans la stratégie

de modernisation de l'Armée canadienne que « l'exigence de la surveillance ou de l'intervention humaine demeurera pour toute application de la force létale¹¹ ». En 2013, Human Rights Watch a formulé les définitions suivantes :

- Armes semi-autonomes : Des robots qui peuvent sélectionner des cibles et fournir une force uniquement avec un commandement humain;
- Armes autonomes supervisées : Des robots qui peuvent sélectionner des cibles et fournir une force sous la supervision d'un humain qui peut passer outre les actions des robots;
- Armes autonomes : Des robots capables de sélectionner des cibles et de fournir une force sans intervention ou interaction humaine.¹²

Qu'est-ce qui constitue un « commandement humain » ou une « surveillance » en termes de temps, d'espace et de spécificité? Qu'en est-il d'une arme autonome « supervisée » pour rechercher et détruire la plus grande cible dans une zone donnée? La surveillance humaine doit-elle être constante et en temps réel? Tenter de définir le contrôle humain en faisant appel à des concepts comme « commandement » et « surveillance » ne fait que pousser le fardeau explicatif vers de nouveaux termes. Certains spécialistes soutiennent que le débat entourant les SALA demeure « truffé d'un manque de connaissances techniques et de rhétorique affective¹³ ». De plus, la surveillance humaine risque de produire un « biais d'automatisation » qui, selon Cummings, peut mener à de nouvelles erreurs si les capacités cognitives humaines ne sont pas prises en compte.¹⁴

La notion mal définie de contrôle humain entrave les progrès dans le débat sur les plans juridique et éthique sur les SALA. Le CICR note qu'« il y a un accord général entre les États sur le fait que le contrôle humain—qu'il soit qualifié de “significatif”, “substantiel”, “approprié”, “suffisant” ou “efficace”, ou “à des niveaux appropriés de jugement humain” ou “d'implication humaine”—doit être conservé par rapport aux systèmes d'armes et au recours à la force¹⁵ » [TCO]. Cette prolifération d'adjectifs révèle un manque de consensus et de clarté. Bode et Heulss font valoir que « [l]a compréhension multiple de ce qu'implique un contrôle humain significatif présente une complication¹⁶ » [TCO]. Les pays favorables à l'élaboration de SALA se demandent donc si et comment le contrôle humain peut être défini de manière utile, soutenant qu'« il est douteux que des critères permettant de déterminer un niveau d'importance attendu du contrôle humain sur la machine puissent être élaborés¹⁷ » [TCO]. Les mesures réglementaires sembleraient impossibles à mettre en œuvre sur la base d'une notion vague de contrôle, sans parler des mesures qui peuvent être appliquées de façon pratique dans le cadre d'opérations militaires.

Pour compliquer davantage le contrôle humain, les SALA peuvent être autonomes de différentes manières et à des degrés différents.¹⁸ Brian Cox, officier à la retraite de la U.S. Army,

propose que nous comprenions les SALA en termes de degré d'autonomie, de ce que cette autonomie apporte à leur fonction générale et de leur méthode de programmation.¹⁹ Même en 2012, avant de nombreuses avancées en matière d'IA, le département de la Défense des États-Unis a fait remarquer que « l'autonomie du système est un continuum allant du contrôle humain complet de toutes les décisions à des situations où de nombreuses fonctions sont déléguées à l'ordinateur²⁰ » [TCO]. Dans un rapport publié en 2017, les auteurs explorent les définitions de l'autonomie et décrivent l'autonomie des armes en termes de capacité accomplie de manière autonome.²¹ Ils constatent que divers systèmes (défense aérienne, protection active, munitions rôdeuses, etc.) peuvent être autonomes dans diverses fonctions (p. ex. mobilité, ciblage et gestion de la santé²²).

Il est utile, compte tenu de la grande variété des SALA, de concentrer mon analyse sur un type particulier. Les systèmes aériens sans pilote (UAS) ou « drones » qui sont autonomes dans la sélection et la poursuite de cibles sont les « robots tueurs » archétypaux au centre du débat des SALA. La discussion de ces systèmes n'est pas seulement hypothétique – un rapport des Nations Unies indique une première utilisation possible de ces SALA en Libye en mars 2020.²³ L'Ukraine a beaucoup utilisé les UAS dans la guerre en cours avec la Russie.²⁴ Certains effectuent des attaques de manière autonome.²⁵ C'est ce type de système, avec ce haut degré d'autonomie dans le ciblage, que j'examinerai en explorant la façon dont le contrôle humain des SALA pourrait être compris grâce à la HCE.

Hypothèse de la cognition étendue (HCE)

Les sciences cognitives et la philosophie de la cognition offrent un moyen utile de comprendre le contrôle humain significatif des SALA. L'examen de la manière dont les SALA pourraient étendre la cognition recoupe un ensemble de réflexions existantes sur l'IA, les artefacts cognitifs et la HCE. Les SALA constituent un exemple particulièrement intéressant et éthique de cognition étendue qui semble encore inexploré. Aucune des publications existantes sur les SALA ne tient compte des SALA par l'entremise de la HCE. Suchman et Weber font une référence intrigante à l'ouvrage fondateur de Knorr-Cetina, *Epistemic Cultures*, et à ses implications pour les relations sujet/objet,²⁶ mais n'explorent pas davantage la façon dont les SALA et les soldats pourraient faire partie d'un système cognitif.²⁷ C'est la lacune que j'essaie de combler. Avant d'examiner les SALA en particulier, il sera utile de donner un aperçu de la HCE.

La HCE possède un héritage intellectuel qui remonte à plusieurs décennies. Clark et Chalmers soutiennent que l'esprit humain peut s'étendre au monde physique et matériel, et qu'il le fait effectivement.²⁸ Leur théorie repose sur la parité fonctionnelle entre les rôles des processus internes (neuraux) et externes dans la cognition. Ils s'opposent aux tentatives visant à limiter l'esprit humain en se basant uniquement sur le lieu où se

déroule un processus cognitif. Un autre argument en faveur de la théorie de l'esprit étendu est que nos outils complètent souvent les processus cognitifs du cerveau, plutôt que de les imiter ou de les reproduire.²⁹ Ces deux arguments arrivent à la même conclusion : l'esprit ne réside pas seulement dans le cerveau. Les mécanismes physiques qui permettent nos processus cognitifs et, en fait, notre *esprit*, ne se limitent pas à nos processus neuronaux. Notre esprit peut parfois s'étendre aux outils que nous utilisons, nos cahiers de notes, télescopes, marteaux, ordinateurs portables et ainsi de suite. Bien que la HCE reste controversée, elle gagne en popularité dans les sciences cognitives. Comme le note Heersmink : « Le changement de paradigme, passant d'une conceptualisation de l'esprit en tant qu'affaire purement interne à la perception qu'il est incarné et façonné par l'environnement et fortement lié à celui-ci, est bien amorcé³⁰. » [TCO]. Je ne tente pas d'entrer pleinement dans le débat sur les HCE; il suffit d'avoir établi que la HCE est une théorie crédible.

Dans le cadre du paradigme de la HCE, les SALA pourraient être considérés comme des artefacts pouvant étendre la cognition humaine ou des artefacts cognitifs. Heersmink appelle les artefacts cognitifs « objets ou structures matériels d'origine humaine qui contribuent de manière fonctionnelle à l'exécution d'une tâche cognitive³¹ » [TCO]. Des auteurs tels que Sienknecht ont envisagé l'intégration d'artefacts cognitifs dans la guerre, où ces artefacts fournissent des intrants aux processus cognitifs biologiques (comme un système d'IA qui analyse les mouvements de l'ennemi et recommande à un commandant humain une frappe préventive³²). Un SALA permettrait plutôt d'étendre la cognition biologique à l'action. Si l'esprit s'étend dans les SALA, comme le permet la HCE, peut-être que cette extension reste sous contrôle humain.

Les SALA pour étendre la cognition

Les SALA, en tant qu'artefacts cognitifs, peuvent assumer certaines des tâches cognitives requises pour réaliser les intentions de leurs concepteurs et opérateurs. Pour comprendre comment, nous devons examiner les intentions plus en détail. Les intentions peuvent être hiérarchiques et exister à différents niveaux d'abstraction. Un commandant humain peut déployer des SALA avec l'intention plus abstraite, ou supérieure, de perturber les communications ennemies. Un SALA pourrait analyser le trafic radio ennemi, construire une représentation du réseau de communication ennemi ainsi que localiser et détruire les nœuds clés qui s'y trouvent. Il pourrait le faire en ciblant les radios elles-mêmes, les antennes de retransmission ou peut-être le carburant qui alimente leurs génératrices. Tout en fonctionnant de manière autonome en termes de sélection et de poursuite de cibles particulières, un tel SALA continue d'exercer une intention humaine. Les SALA permettent simplement aux humains de concentrer leurs intentions et pensées conscientes à un niveau plus élevé d'abstraction. C'est exactement le genre de délégation complémentaire des tâches cognitives qui, selon Heersmink,

caractérise un système cognitif étendu : « Le cerveau humain se développe dans un environnement riche en informations et doit apprendre à compléter ses lacunes en utilisant les fonctionnalités des artefacts pour effectuer des tâches cognitives de manière à ne pas gaspiller des ressources internes coûteuses³³. » [TCO]. Hernandez-Orallo et Vold parlent de technologies qui agissent comme des extensions de l'IA, qui existent « dans un continuum entre des systèmes complètement extériorisés, faiblement couplés à des humains, et des processus entièrement internalisés³⁴ » [TCO]. Les SALA semblent se situer sur ce spectre, même en l'absence d'un humain.

Une propriété intéressante des SALA avancés serait leur transparence³⁵ envers le commandant qui les emploie. Ce manque de conscience peut même justifier la *nécessité* de comprendre les SALA comme des extensions cognitives. Commentaires de Heersmink : « L'utilisation des artefacts peut être conceptualisée selon un spectre d'expertise. La première fois que nous utilisons un artefact, cela nécessite beaucoup d'efforts conscients et cognitifs, mais avec le temps, nous devenons plus aptes à l'utiliser et son utilisation devient plus procédurale³⁶. » [TCO]. Le philosophe Michael Wheeler soutient qu'une telle transparence peut être une indication de l'extension cognitive, mais aussi un motif de préoccupation.³⁷ Si les systèmes qui étendent notre cognition deviennent suffisamment transparents pour nous, nous pourrions ne plus réaliser que leurs catégorisations du monde ne correspondent pas aux nôtres.³⁸ Wheeler écrit :

« Si une application de réseau neuronal profond à laquelle je suis couplé de manière transparente se qualifie comme faisant partie de mon architecture cognitive et donc comme faisant partie de moi, alors les classifications en question—qui guident inconsciemment mon comportement—feront partie de ce que je crois inconsciemment être le cas, et aura donc vraisemblablement le même statut que mes croyances inconscientes plus familières, réalisées en interne³⁹. » [TCO]

Son objection est que ces machines « peuvent classifier régulièrement le monde d'une manière potentiellement dommageable et épistémique par rapport à nos pratiques technologiquement non augmentées⁴⁰ » [TCO]. Cette situation est particulièrement préoccupante pour les SALA qui utilisent l'IA et fonctionnent comme des « boîtes noires » dont le fonctionnement interne est inconnu de l'utilisateur. Il recommande donc que les technologies cognitives soient délibérément non transparentes, comme les appels à garder l'intervention d'un humain pour les SALA.

Les préoccupations au sujet des technologies cognitives ne sont pas nouvelles. Socrate s'inquiète du fait que l'écriture, en tant que technologie cognitive, agit en dehors de tout contrôle humain significatif, affirmant : « Et une fois qu'une chose est mise par écrit, la composition, quelle qu'elle soit, dérive dans tous les sens, tombant entre les mains non seulement de ceux qui la comprennent, mais aussi de ceux qui n'ont rien à voir avec elle; il ne sait pas comment s'adresser aux bonnes personnes, et ne sait pas s'adresser aux mauvaises⁴¹. » [TCO]. Ces mots font

écho aux objections modernes à l'égard des SALA qui interagissent involontairement avec les mauvaises personnes. Si nous acceptons que les intentions d'un auteur sont suffisamment intégrées dans une composition écrite pour qu'il n'ait pas besoin de contrôle humain actif lorsqu'il se propage sans supervision dans le monde, il devrait y avoir une certaine parité dans le degré et le type de contrôle que nous exigeons sur les SALA. Bien que les effets potentiellement mortels des SALA puissent limiter la comparaison directe avec la technologie civile, les SALA ne sont pas la seule technologie dont la défaillance présente un risque de décès (c.-à-d. ponts et automobiles).

La HCE, en permettant que l'esprit puisse s'étendre dans les SALA, remet en question toute insistance sur le fait qu'un cerveau doit superviser le contrôle. De plus en plus, l'apprentissage machine et l'IA permettront aux SALA d'avoir un effet non seulement sur une intention humaine spécifique, en assumant une infime partie de la cognition, mais aussi sur une intention humaine générale ou plus abstraite en assumant un fardeau beaucoup plus cognitif. Penser au contrôle simplement en termes d'implication immédiate et active d'un cerveau humain ne tient pas compte de la façon dont nous étendons systématiquement la cognition aux artefacts physiques sans céder le contrôle. Le CICR soutient qu'« un système d'armes doté d'une autonomie dans ses fonctions critiques *empêche le commandant ou l'opérateur humain de porter les jugements requis par le DIH [droit international humanitaire⁴²] [italiques ajoutés]* » [TCO]. Cependant, la HCE permet que l'esprit qui porte ces jugements *s'étende* aux SALA. Dans le cadre de la HCE, une force militaire pourrait instaurer des processus cognitifs soit dans un cerveau humain ou dans le monde physique, ou un mélange des deux.

La question de savoir si un SALA réalise l'intention humaine peut être plus importante que le fait qu'elle soit sous supervision humaine directe et immédiate. La présentation de 2018 des États-Unis à la CCAC fait avancer cette idée en énonçant ce qui suit : « La question clé de l'interaction homme-machine dans le développement, le déploiement et l'utilisation des technologies émergentes dans le domaine des systèmes d'armes autonomes létales est de s'assurer que, lorsqu'il est nécessaire de recourir à la force, cette force est utilisée pour réaliser les intentions des commandants et des opérateurs⁴³. » [TCO]. L'Australie adopte un point de vue similaire, déclarant que « l'expression "contrôle humain" utilisée par certains lors des discussions [du Groupe d'experts gouvernementaux] ne couvre pas adéquatement la multitude de contrôles pratiques ou de systèmes utilisés par les États et leurs forces armées⁴⁴ » [TCO]. Plutôt que de mandater la supervision par l'être humain, l'Australie articule plutôt son propre système de contrôle en neuf étapes applicable à toutes les armes, commandées par des humains et autonomes.

Conséquences pour les commandants

L'autonomie des subordonnés humains n'implique pas qu'ils soient hors du contrôle de leurs commandants. Les armées n'ont

pas besoin d'un commandant qui surveille un subordonné humain et autorise chaque action spécifique. James Kraska, du U.S. Naval War College, soutient qu'il n'y a pas d'écart de responsabilité avec les SALA, car les commandants demeurent ultimement responsables de tous les moyens de guerre qu'ils utilisent pour atteindre leurs objectifs militaires.⁴⁵ Certes, les SALA et les subordonnés humains ne sont pas identiques, les subordonnés humains ayant une responsabilité et un pouvoir moral que les SALA n'ont pas.⁴⁶ Malgré cette disparité, le contrôle des subordonnés humains peut encore influencer le contrôle des SALA à au moins deux égards : les ordres et l'instruction.

Les commandants donnent des ordres qui dirigent les actions de leurs subordonnés humains. Ces ordres peuvent comprendre à la fois une tâche et un but. Les ordres font généralement référence à l'intention du commandant supérieur, y compris des informations contextuelles qui permettent aux subordonnés humains d'agir conformément à ces intentions, même si la situation change si radicalement que leur tâche assignée n'est plus appropriée. Les intentions d'un commandant peuvent être exécutées de manière opaque pour ce dernier sans perte de contrôle. Même dans les armées modernes et professionnelles avec une communication avancée, il existe des exemples où des subordonnés ont agi de manière inattendue, sans supervision par les supérieurs, pour atteindre une intention supérieure.⁴⁷ Ces unités militaires ne sont pas considérées comme hors de contrôle, alors pourquoi les SALA devraient-ils l'être? Le cas échéant, les ordres peuvent contenir une variété de contraintes officielles (règles d'engagement, limites, échéanciers et exigences en matière de rapports) qui pourraient avoir des analogies directes pour les SALA. Il existe un nombre croissant de documents qui cherchent à « évaluer la fiabilité des humains et des systèmes automatisés pour décider s'il faut se fier à un mandataire donné pour effectuer une certaine tâche⁴⁸ » [TCO]. Un commandant humain peut avoir une confiance instrumentale suffisante dans les SALA pour appliquer une forme de commandement de mission et accepter des actions imprévues qui atteignent toujours l'intention.

L'analogie avec l'entraînement des humains fournit un moyen d'observer l'interaction entre les humains et les SALA et le contrôle des SALA utilisant l'IA ou l'apprentissage automatique. Les SALA qui utilisent des modèles génératifs sont « entraînés » sur un échantillon d'intrants simulant ce qu'ils pourraient rencontrer dans les opérations. Cette formation offrirait des possibilités de confirmation et de validation des SALA très semblables à ce qui est fait pour les unités militaires (humaines) avant le déploiement. Bien que Verbruggen soutienne qu'« il n'existe aucune technique permettant de valider et de vérifier l'IA, pour s'assurer que les systèmes fonctionneront comme prévu et éviteront les comportements imprévisibles⁴⁹ » [TCO]. Cette compréhension de la validation, qui vise une prévisibilité totale, est beaucoup plus stricte que ce qui est appliqué aux organisations humaines. L'Armée canadienne définit la confirmation comme « une évaluation qui montre à quel point une

entité tactique a satisfait à une [norme relative aux tâches de combat⁵⁰]. La validation sert à « vérifier que le programme d'[instruction collective] a bien préparé les unités ou les formations à remplir des tâches opérationnelles permettant d'atteindre des objectifs précis de l'Armée canadienne⁵¹ ». Les deux sont une responsabilité des commandants.

Un SALA bien entraîné peut être sous contrôle même s'il fonctionne en dehors de la conscience humaine et de la prise de décision, comme l'exécution inconsciente d'exercices humains. Dans certaines disciplines militaires, les réactions et les comportements nécessitant une réponse immédiate sont entraînés jusqu'à un point de quasi-inconscience. Avec un entraînement suffisant, cette manipulation d'une arme pour des fins potentiellement létales devient presque transparente. Wheeler décrit cela comme la transparence de l'utilisation des outils, en écrivant :

« Lorsque nous manipulons habilement de l'équipement sans accroc, nous n'avons aucune appréhension consciente des articles d'équipement utilisés en tant qu'objets indépendants, c'est-à-dire quelque chose comme des porteurs identifiables d'états et de propriétés déterminés. Ainsi, pour reprendre l'exemple le plus cité de Heidegger, pendant qu'il se livrait à un martelage sans problème, le menuisier qualifié n'a pas la reconnaissance consciente du marteau, des clous ou du banc de travail, comme on le ferait si on prenait du recul et y réfléchissait⁵². » [TCO]

Une arme peut être semblable à un marteau de menuisier habile. Étant libérée de la nécessité de se concentrer consciemment sur la façon de manipuler l'arme, la conscience humaine peut se concentrer sur des tâches cognitives plus abstraites, comme l'effet que cette manipulation vise à obtenir (c.-à-d. la suppression d'un tireur d'élite ennemi). Si l'entraînement d'un humain à répondre inconsciemment n'entraîne pas une abdication du contrôle significatif sur la force létale, la programmation ou l'entraînement d'un SALA artificiellement intelligent

pourrait-il également fournir le contrôle, même si les SALA opèrent en dehors de la conscience consciente humaine? Écarté des décisions individuelles concernant la sélection et la poursuite des cibles, un commandant militaire n'est pas détaché de l'usage de la force ni de ses responsabilités, mais il est plutôt libre de l'envisager à un niveau supérieur.

Conclusion

La notion de contrôle humain des SALA est complexe, et son examen par la HCE peut mener à des idées et des politiques utiles. Traiter les SALA comme des artéfacts cognitifs ouvre de nouvelles façons de comprendre et d'exercer le contrôle humain des SALA. Les SALA qui étendent la cognition humaine peuvent être sous contrôle même sans intervention immédiate et consciente par un cerveau humain. L'ouverture à l'expérimentation et à la formation avec les SALA pourrait produire des avantages imprévus pour les FAC. Carter et Nielsen soutiennent que les modèles génératifs peuvent permettre une augmentation de l'intelligence artificielle, écrivant ceci :

« [Les modèles génératifs] peuvent être utilisés pour explorer et découvrir, fournir de nouvelles représentations et opérations, qui peuvent être intériorisées dans le cadre de la pensée de l'utilisateur. Et bien que ces exemples en soient à leurs débuts, ils suggèrent que l'IA n'est pas seulement une externalisation cognitive. Une vision différente de l'IA est possible, une vision où elle nous aide à inventer de nouvelles technologies cognitives qui transforment notre façon de penser⁵³. » [TCO]

Si les SALA sont entraînés en collaboration avec leurs homologues humains, les solutions qu'ils emploient peuvent en fait fournir de nouvelles idées et de nouveaux outils cognitifs qui élargissent l'éventail de la pensée humaine. Cette valeur ne devrait pas être modifiée.

Notes

- 1 Mariarosaria Taddeo, *The Ethics of Artificial Intelligence in Defence*, New York, Oxford University Press, 2024, p. 181.
- 2 Robert Sparrow, « Killer Robots », *Journal of Applied Philosophy* 24, n° 1 (2007), p. 62 à 77.
- 3 Thomas Simpson et Vincent Müller, « Just War and Robots' Killings », *Philosophical Quarterly* 66, n° 263 (2016), p. 302 à 322.
- 4 Ingvild Bode et Hendrik Huelss, *Autonomous Weapons Systems and International Norms*, Kingston, McGill-Queen's University Press, 2022, p. 9.
- 5 International Committee for Robot Arms Control, consulté le 3 novembre 2025. Source originale : <https://www.icrac.net/about-icrac/>
- 6 Comité international de la Croix-Rouge, « The Element of Human Control », *Meeting of the High Contracting*

- Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects, 2018, p. 1. Source originale : https://reachingcriticalwill.org/images/documents/Disalibr-fora/ccw/2018/hcp-meeting/documents/ICRC_WP3.pdf, consulté le 3 novembre 2025.
- 7 IEEE, « Reframing Autonomous Weapons Systems », *The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems*, p. 113. Source originale : https://standards.ieee.org/content/dam/ieee-standards/standards/web/other/lead_reframing_autonomous_weapons_v2.pdf, consulté le 3 novembre 2025.
- 8 Michael Schmitt et Sean Watts, « The Decline of International Humanitarian Law Opinio Juris and the Law of Cyber Warfare », *Texas International Law Journal* 50, n° 2-3 (2015), p. 191.

- 9 Australie, « Australia's System of Control and Applications for Autonomous Weapon », *Group of Governmental Experts of the High Contracting Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects*, 2018. Source originale : <https://reachingcriticalwill.org/images/documents/Disalibr-fora/ccw/2019/gge/Documents/GGE.2-WP2.pdf>, consulté le 3 novembre 2025.
- 10 Group of Governmental Experts on Emerging Technologies, « Chair's summary - First 2025 session of the GGE on LAWS », *Group of Governmental Experts of the High Contracting Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects*,

- 2025, p. 7. Source originale : [https://docs-library.unoda.org/Convention_on_Certain_Conventional_Weapons-Group_of_Governmental_Experts_on_Lethal_Autonomous_Weapons_Systems_\(2025\)/CCW-GGE.1-2025-WP.1_-_Chair's_summary.pdf](https://docs-library.unoda.org/Convention_on_Certain_Conventional_Weapons-Group_of_Governmental_Experts_on_Lethal_Autonomous_Weapons_Systems_(2025)/CCW-GGE.1-2025-WP.1_-_Chair's_summary.pdf), consulté le 6 octobre 2025.
- 11 Quartier général de l'Armée canadienne, *Engagés vers l'avant : la stratégie de modernisation de l'Armée canadienne*, 2020, p. 54. Source originale : https://publications.gc.ca/collections/collection_2021/mdn-dnd/D2-438-2021-fra.pdf, consulté le 3 novembre 2025.
 - 12 Human Rights Watch, *Losing Humanity, The Case Against Killer Robots*, 2012. Source originale : <https://www.hrw.org/report/2012/11/19/losing-humanity/case-against-killer-robots>, consulté le 3 novembre 2025. Bien qu'elle soit désuète, cette typologie demeure influente et a été utilisée par Vincent Boulanin et Maakie Verbruggen dans *Mapping the Development of Autonomy in Weapon Systems*, Stockholm, Stockholm International Peace Research Institute, 2017, p. 26, pour caractériser les systèmes dans leur ensemble de données.
 - 13 Mary Cummings, « Lethal Autonomous Weapons : Meaningful Human Control or Meaningful Human Certification? [Opinion] », *IEEE Technology and Society Magazine* 38, n° 4 (1^{er} décembre 2019), p. 20-26. Source originale : <https://technologyandsociety.org/lethal-autonomous-weapons-meaningful-human-control-or-meaningful-human-certification/>, consulté le 28 février 2025.
 - 14 Missy Cummings, « Automation Bias in Intelligent Time Critical Decision Support Systems », *American Institute of Aeronautics and Astronautics 1st Intelligent Systems Technical Conference*, du 20 au 22 septembre 2004. Source originale : <https://arc.aiaa.org/doi/10.2514/6.2004-6313>, consulté le 9 juillet 2025.
 - 15 Comité international de la Croix-Rouge, « The Element of Human Control », *Meeting of the High Contracting Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects*, 2018, p. 1. Source originale : https://reachingcriticalwill.org/images/documents/Disalibr-fora/ccw/2018/hcp-meeting/documents/ICRC_WP3.pdf, consulté le 6 octobre 2025.
 - 16 Ingvild Bode et Hendrik Huels, *Autonomous Weapons Systems and International Norms*, Kingston, McGill-Queen's University Press, 2022, p. 159.
 - 17 Fédération de Russie, « Russia's Approaches to the Elaboration of a Working Definition and Basic Functions of Lethal Autonomous Weapons Systems in the Context of the Purposes and Objectives of the Convention », *Group of Governmental Experts of the High Contracting Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects*, 2018, p. 3. Source originale : <https://reachingcriticalwill.org/images/documents/Disalibr-fora/ccw/2018/gge/documents/GGE.1-WP6-English.pdf>, consulté le 6 octobre 2025.
 - 18 Noel Sharkey, « Staying in the Loop : Human Supervisory Control of Weapons », dans *Autonomous Weapons Systems: Law, Ethics Policy*, sous la dir. de N. Bhuta, S. Beck, R. Geiß, H.Y. Liu et C. Kreß, Cambridge, Cambridge University Press, 2016, p. 27.
 - 19 Brian Cox, « Why Binding Limitations on Autonomous Weapons Will Remain Elusive », *Articles of War*, 2022. Source originale : <https://lieber.westpoint.edu/binding-limitations-autonomous-weapons-elusive>, consulté le 6 avril 2022, exposé plus en détail par l'auteur lors d'une présentation à The Canadian National Group of the International Society for Military Law and the Law of War le 24 février 2022, à Ottawa (diffusion virtuelle sur MS Teams).
 - 20 DoD Defense Science Board, *The Role of Autonomy in DoD Systems*, 2012, p. 4. Source originale : <https://apps.dtic.mil/sti/pdfs/ADA566864.pdf>, consulté le 28 février 2025.
 - 21 Vincent Boulanin et Maakie Verbruggen, *Mapping the Development of Autonomy in Weapon Systems*, Stockholm, Stockholm International Peace Research Institute, 2024, p. 20.
 - 22 Vincent Boulanin et Maakie Verbruggen, *Mapping the Development of Autonomy in Weapon Systems*, Stockholm, Stockholm International Peace Research Institute, 2024, p. 36.
 - 23 Nations Unies, *Lettre datée du 8 mars 2021, adressée à la Présidente du Conseil de sécurité par le Groupe d'experts sur la Libye créé par la résolution 1973 (2011) du Conseil de sécurité*, 2021, p. 20. Source originale : <https://docs.un.org/fr/s/2021/229>, consulté le 25 octobre 2025.
 - 24 Jon-Wyatt Matlack, Sebastien Schwartz et Oliver Gill, *Ukraine's Drone Ecosystem and the Defence of Europe: Lessons Lost Can't Be Learned*, Londres, LSE, 2025. Source originale : <https://www.forbes.com/sites/davidhambling/2023/10/17/ukraines-ai-drones-seeking-and-attack-russian-forces-without-human-oversight/>, consulté le 21 septembre 2024.
 - 26 Lucy Suchman et Jutta Weber, « Human-Machine Autonomies », dans *Autonomous Weapons Systems: Law, Ethics Policy*, sous la dir. de N. Bhuta, S. Beck, R. Geiß, H.Y. Liu et C. Kreß, Cambridge, Cambridge University Press, 2016, p. 98.
 - 27 Karin Knorr-Cetina, *Epistemic Cultures : How the Sciences Make Knowledge*, Cambridge, Harvard University Press, 1999.
 - 28 Andy Clark et David Chalmers, « The Extended Mind », *Analysis* 58, 1998, p. 7-19.
 - 29 Richard Heersmink, « Dimensions of Integration in Embedded and Extended Cognitive Systems », *Phenomenology and the Cognitive Sciences* 14, 2015, p. 577 à 598.
 - 30 Richard Heersmink, « Varieties of Artifacts: Embodied, Perceptual, Cognitive, and Affective », *Topics in Cognitive Science* 13, 2021, p. 574.
 - 31 Heersmink, « Varieties of Artifacts », p. 580.
 - 32 Dennis Muller, Maurice Chiodo et Mitja Siemknecht, « Integrators at War : Mediating in AI-assisted Resort-to-Force Decisions », 12 janvier 2025, p. 7. Source originale : https://www.researchgate.net/publication/387976034_Integrators_at_War_Mediating_in_AI-assisted_Resort-to-Force_Decisions, consulté le 7 octobre 2025.
 - 33 Heersmink, « Dimensions of Integration », p. 582.
 - 34 Karina Vold et José Hernández-Orallo, « AI Extenders : The Ethical and Societal Implications of Humans Cognitively Extended by AI », *AIES '19 Session 9 : Interaction homme-machine*, 2019, p. 507.
 - 35 Il convient de noter que le terme « transparence » tel qu'il est utilisé par Wheeler fait référence à un outil qui échappe à la conscience de l'utilisateur. Cela diffère de l'utilisation du terme « transparence » dans la littérature sur l'IA, où il fait référence à la capacité de comprendre le fonctionnement interne d'une IA.
 - 36 Heersmink, « Varieties of Artifacts », p. 577.
 - 37 Michael Wheeler, « The Reappearing Tool: Transparency, Smart Technology, and the Extended Mind », *AI & Society* 34 (2019), p. 857 à 866.
 - 38 Wheeler, « The Reappearing Tool », p. 857-866.
 - 39 Wheeler, « The Reappearing Tool », p. 864.
 - 40 Wheeler, « The Reappearing Tool », p. 864.
 - 41 H. Fowler, *Platon : Phaedrus*, Loeb Classical Library, 1971, 275^e.
 - 42 Comité international de la Croix-Rouge, « The Element of Human Control », *Meeting of the High Contracting Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects*, 2018, p. 2. Source originale : https://reachingcriticalwill.org/images/documents/Disalibr-fora/ccw/2018/hcp-meeting/documents/ICRC_WP3.pdf, consulté le 6 octobre 2025.
 - 43 É.-U., « Human-machine Interaction in the Development, Deployment and Use of Emerging Technologies in the Area of Lethal Autonomous Weapons Systems » *Group of Governmental Experts of the High Contracting Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects*, 2018, p. 7. Source originale : <https://reachingcriticalwill.org/images/documents/Disalibr-fora/ccw/2018/gge/documents/GGE.2-WP4.pdf>, consulté le 6 octobre 2025.
 - 44 Australie, « Australia's System of Control and Applications for Autonomous Weapon Systems », *Group of Governmental Experts of the High Contracting Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects*, 2018, p. 5. Source originale : <https://reachingcriticalwill.org/images/documents/Disalibr-fora/ccw/2019/gge/Documents/GGE.2-WP2.pdf>, consulté le 6 octobre 2025.
 - 45 James Kraska, « Command Accountability for AI Weapon Systems in the Law of Armed Conflict », *International Law Study* 97 (2021), p. 408 à 445.
 - 46 Danièle Amoroso et Guglielmo Tamburrini, « Autonomous Weapons Systems and Meaningful Human Control: Ethical and Legal Issues », *Current Robotics Report* 1 (2020), p. 189.
 - 47 Douglas MacGregor, *Warrior's Rage : The Great Tank Battle of 73 Easting*, Annapolis, Brookings Institution Press, 2009.
 - 48 Markus Langer, Cornelius J. König, Caroline Back et Caroline Hemming, « Trust in Artificial Intelligence : Comparing Trust Processes Between Human and Automated Trustees in Light of Unfair Bias », *Journal of Business and Psychology* 38 (2023), p. 493.
 - 49 Maakie Verbruggen, « No, Not That Verification: Challenges Posed by Testing, Evaluation, Validation and Verification of Artificial Intelligence in Weapon Systems », dans *Armament, Arms Control and Artificial Intelligence: The Janus-Faced Nature of Machine Learning in the Military Realm*, sous la dir. de Thomas Reinhold et de Niklas Schörning, Springer International Publishing AG, 2022, *ProQuest Ebook Central*, <http://ebookcentral.proquest.com/lib/cvlibrary-ebooks/detail.action?docId=7108384>. Créé à partir de cvlibrary-ebooks le 2025-07-09 18:36:43, p. 242.
 - 50 Commandant de l'Armée canadienne, *INSTRUCTION POUR LES OPÉRATIONS TERRESTRES* (2014), 6-3-11.
 - 51 Commandant de l'Armée canadienne, *INSTRUCTION POUR LES OPÉRATIONS TERRESTRES*, 6-3-12.
 - 52 Wheeler, « The Reappearing Tool », p. 859.
 - 53 Shan Carter et Michael Nielsen, « Using Artificial Intelligence to Augment Human Intelligence », *Distill*, 2017. Source originale : <https://distill.pub/2017/aia>, consulté le 3 novembre 2025.