Défense nationale | National Defence

FORCES ARMÉES CANADIENNES

# LA STRATÉGIE D'INTELLIGENCE ARTIFICIELLE

## DU MINISTÈRE DE LA DÉFENSE NATIONALE ET DES FORCES ARMÉES CANADIENNES

Canada

Pour de plus amples renseignements :

Courrier :
Ministère de la Défense nationale
101, promenade du Colonel By
Ottawa (Ontario)  K1A 0K2

Téléphone : 1-888-995-2534

Courriel : information@forces.gc.ca

© 2024 Sa Majesté le Roi du chef du Canada, représentée par le ministre de la Défense nationale.

Titre du document - La Stratégie d'intelligence artificielle du ministère de la Défense nationale et des Forces armées canadiennes

N° de cat. : D2-633/2024F-PDF (fichier PDF, Français)
ISBN : 978-0-660-45123-7

N° DGM : DGM-21422-HVD

# AVANT-PROPOS

## du sous-ministre et du chef d'état-major de la Défense

Nous vivons dans un monde doté de l'intelligence artificielle (IA). Lorsque nous déverrouillons nos téléphones intelligents à l'aide de la reconnaissance faciale, que nous effectuons des recherches sur Internet, que nous acceptons des suggestions offertes par un correcteur automatique ou que nous interagissons avec un agent conversationnel ou un assistant virtuel, nous utilisons l'IA. Ces technologies sont aujourd'hui omniprésentes, si bien que nous oublions qu'il s'agit d'IA et qu'aucune d'entre elles n'existait il y a à peine vingt-cinq ans.

Tout comme elle a transformé rapidement nos activités quotidiennes, l'IA transforme également l'environnement de la Défense. Elle a rendu possibles de nouvelles capacités opérationnelles et organisationnelles pour nous aider à continuer de respecter nos obligations de protéger et de défendre le Canada ainsi que les Canadiennes et Canadiens, mais a aussi entraîné de nouveaux risques contre lesquels nous devons les protéger. En outre, l'IA n'est pas une technologie indépendante, elle s'inscrit plutôt dans le cadre d'une vaste révolution technologique encore plus transformatrice qui découle de la convergence des données et du numérique avec l'IA.

La Stratégie d'intelligence artificielle du MDN et des FAC (Stratégie d'IA) engage l'Équipe de la Défense à adopter de manière intégrée l'IA d'ici 2030, conformément à nos objectifs liés à une transformation numérique globale d'ici cette date. Il s'agit d'un objectif ambitieux, mais que nous devons atteindre. Nous sommes arrivés à un point d'inflexion technologique. Nos alliés progressent rapidement dans leurs engagements à l'égard de l'IA et de son adoption. Nous devons agir maintenant pour nous assurer de pouvoir continuer de partager une perspective opérationnelle commune avec eux, de détecter, de décider et d'agir à un rythme soutenu par l'IA, afin de ne pas perdre notre crédibilité et notre pertinence en tant que force combattante.

La technologie n'attendra pas que nous agissions. Chaque jour qui passe, elle devient plus accessible à nos concurrents et adversaires potentiels et ce, à moindre coût, et la convergence de la technologie quantique et de l'IA approche à grands pas. En prenant du retard maintenant sur le plan de l'adoption de l'IA, nous risquerions de perdre notre avantage opérationnel.

Le fait d'adopter l'IA nous offre aussi la possibilité de répondre à l'appel à la modernisation et à la reconstitution : devenir de meilleurs intendants des ressources que les Canadiennes et Canadiens nous ont confiées, tout en obtenant de meilleurs résultats. Cela nous offre la possibilité de répondre aux attentes de notre personnel qui veut travailler et combattre dans le même monde numérique, stimulé par l'IA, dans lequel il vit. En même temps, nous devons nous assurer que notre utilisation de l'IA est à la hauteur des attentes des Canadiennes et Canadiens et de nos membres à notre égard. Nous devons nous assurer qu'elle répond à leurs attentes concernant une mise en œuvre sûre, responsable et éthique tout en préservant une culture inclusive et diversifiée.

La Stratégie d'IA offre une vision et une orientation relatives au développement et à l'intégration de l'IA et de systèmes décisionnels automatisés au sein de l'Équipe de la Défense. Les capacités et les besoins opérationnels du ministère de la Défense nationale et des Forces armées canadiennes (MDN/FAC) dans l'environnement moderne de sécurité sont au cœur de cette approche et orientent la priorisation et la nécessité de la présente Stratégie. Celle-ci communique notre intention et notre orientation à nos membres, à nos partenaires du gouvernement du Canada, du milieu universitaire et de l'industrie ainsi qu'à nos alliés.

Aujourd'hui, nous sommes confrontés à un monde plus instable et dangereux qu'à toute autre période depuis la fin de la guerre froide. Nous devons nous attendre à ce que les exigences imposées aux FAC, tant à l'échelle nationale qu'à l'échelle internationale, ne fassent qu'augmenter. Nous devons nous moderniser rapidement pour relever les défis de demain. L'impératif est clair et l'urgence est réelle — mais nous sommes à la hauteur. Nous devons agir — et agir maintenant — pour que notre organisation intègre pleinement l'IA.

**Le général Wayne Eyre**

Chef d'état-major de la Défense
Forces armées canadiennes

**Bill Matthews**

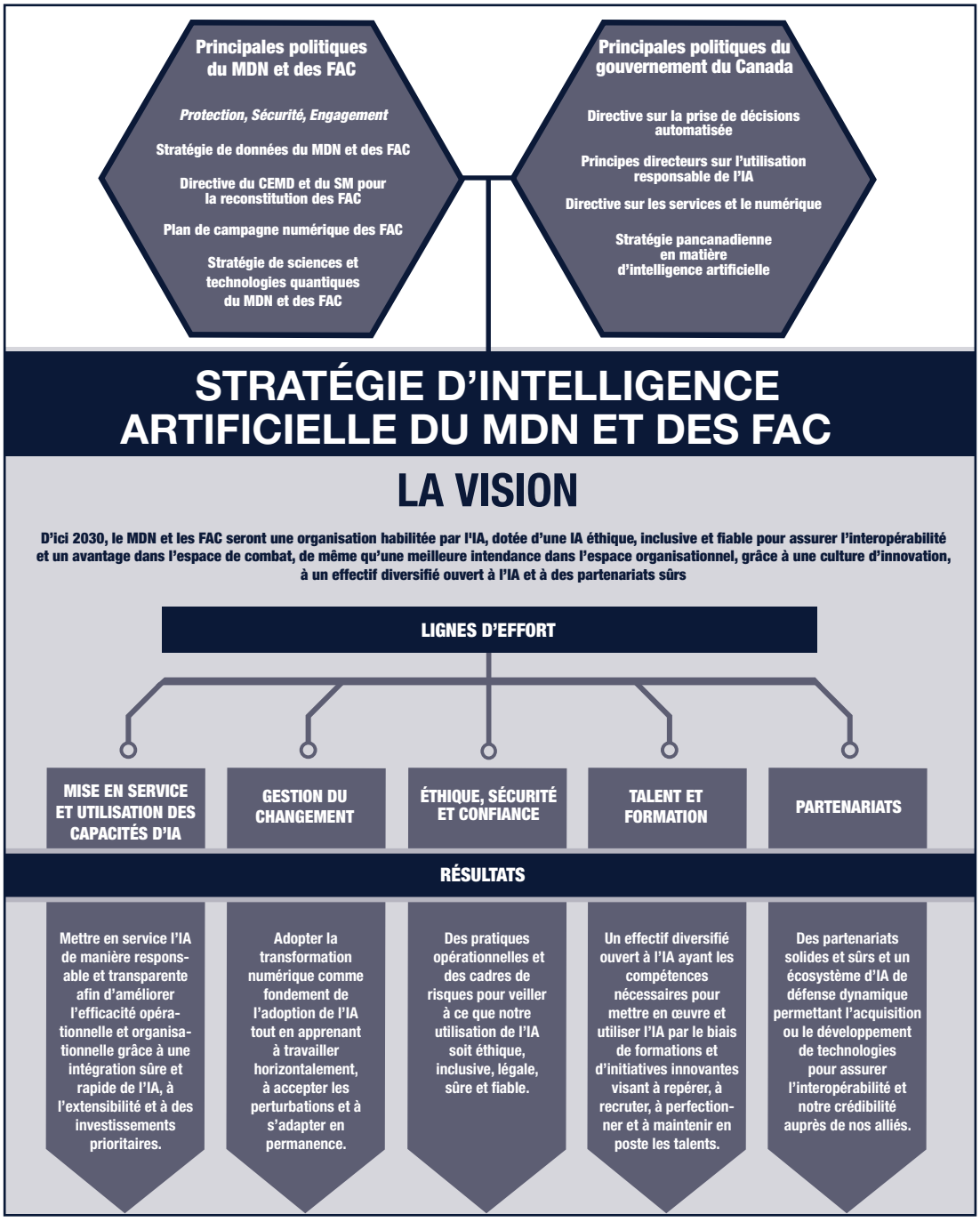
Sous-ministre
Ministère de la Défense nationale

# TABLE DES MATIÈRES

# INTRODUCTION

## HARMONISATION STRATÉGIQUE

La Stratégie d'IA est harmonisée avec les politiques et les stratégies relatives à la modernisation et à la transformation numérique du MDN et des FAC ainsi qu'avec leur engagement à appliquer l'Analyse comparative entre les sexes Plus (ACS Plus) dans le cadre de l'élaboration et de l'exécution de ses opérations, de ses politiques et de ses programmes. Plus particulièrement, la Stratégie d'IA doit être lue et mise en œuvre conjointement avec la Stratégie de données et le plan de mise en œuvre de la Stratégie de données (PMOSD) afin de garantir qu'une base solide de gestion des données soutiendra la mise en œuvre de l'IA. Cette Stratégie est également harmonisée avec les lois canadiennes et le droit international applicables ainsi qu'avec les politiques et les lignes directrices du gouvernement du Canada relatives à l'utilisation du numérique et de l'IA.



# CONTEXTE

***L'IA est un puissant outil qui pourrait perturber et transformer à la fois la conduite des opérations militaires et la gestion des fonctions organisationnelles.*** À tous les échelons de commandement, des technologies algorithmiques rendent possibles de nouvelles capacités qui sont plus rapides et plus puissantes que celles réalisables par de seuls agents humains. Activées par des volumes de données toujours croissants, ces technologies peuvent améliorer la connaissance de la situation et l'aide à la décision dans tous les domaines. Sur le plan opérationnel, l'IA et l'utilisation d'outils d'apprentissage automatique (AA) – ou « apprentissage machine » – peuvent accroître les capacités humaines permettant de surveiller, de prévoir, de cibler et d'accélérer l'aptitude à repérer un adversaire et à réagir face à celui-ci. En outre, l'IA peut aussi servir à automatiser la logistique et à prévoir la nécessité de réparations, améliorant ainsi l'état de préparation opérationnelle. Au niveau organisationnel, l'analytique avancée permet aux organisations de mieux se voir et de mieux se comprendre, elles ainsi que leurs processus, en identifiant des économies potentielles de coûts et de temps. L'automatisation augmentée par l'IA peut prendre en charge des tâches répétitives et ainsi libérer le personnel qui peut entreprendre des activités plus complexes et exigeantes.

***Tirer parti de l'IA est au cœur des priorités du MDN et des FAC, de leurs alliés et de leurs adversaires.*** La politique de défense du Canada, ***Protection, Sécurité, Engagement,*** et la ***Stratégie de données du MDN et des FAC*** décrivent un objectif final souhaité dans laquelle les données seront utilisées pour accroître l'efficacité et pour procurer un avantage en matière d'information sur le plan des opérations militaires et des applications organisationnelles. L'analyse et l'interprétation d'une grande quantité de données dépassent désormais largement la capacité des seuls agents humains et l'atteinte de cette situation finale nécessitera l'aide de l'IA et d'autres systèmes décisionnels automatisés. Les domaines prioritaires en matière de défense, notamment la modernisation du Commandement de la défense aérospatiale de l'Amérique du Nord (NORAD), le Centre des opérations et du renseignement de la Défense nationale (CORDN), la surveillance et la reconnaissance interarmées (RSRI) envisagent l'intégration de l'IA et des technologies connexes dans l'élaboration d'une structure modernisée de Commandement, contrôle, communications, informatique, cyberespace, renseignements, surveillance et reconnaissance (C3ICRSR). Les partenaires de défense du Canada définissent également rapidement leurs propres approches à l'égard de l'IA, tandis que la Chine a annoncé ses plans en vue d'atteindre la domination mondiale en matière d'IA d'ici 2030.

***Toutefois, le MDN et les FAC ne sont pas encore en mesure d'adopter l'IA et d'en tirer parti.*** À l'heure actuelle, les initiatives en matière d'IA au sein du MDN et des FAC sont fragmentées, chaque commandement et environnement abordant l'IA indépendamment. La maturité de l'IA varie à l'échelle du MDN et des FAC, avec d'importants groupes d'experts à certains endroits et de faibles niveaux de compétences et de capacité ailleurs. Il n'existe aucune feuille de route pour faire progresser l'organisation vers une exploitation efficace de l'IA aux fins de coordonner et de gérer convenablement les investissements ou de développer les capacités, l'attitude et les compétences nécessaires à la mise en œuvre efficace, sûre et responsable de l'IA. Sans une telle approche, le MDN et les FAC risquent de manquer de nombreuses occasions appropriées d'utiliser l'IA de manière responsable dans la conduite des opérations des FAC et ainsi de manquer l'occasion de concrétiser de nombreux avantages, y compris l'avantage opérationnel sur des adversaires potentiels. De même, ils risquent de créer ou de perpétuer des préjudices en raison de biais algorithmiques ou liés aux données et aux effets systémiques imprévus ainsi que de causer la perte de possibilités d'améliorer les activités de défense et notre gestion organisationnelle au moyen des capacités basées sur l'IA.

***Pour avancer dans le domaine de l'IA, le MDN et les FAC ont besoin d'une Stratégie d'IA afin d'orienter et de coordonner les efforts vers des opérations habilitantes et des activités de défense au moyen de l'IA***. La présente Stratégie d'IA établit cinq lignes d'efforts pour accélérer l'adoption d'une IA responsable au sein du MDN et des FAC. Ces lignes d'effort décrites dans le présent document comprennent des activités connexes pour faire avancer la mise en œuvre à court terme, y compris la création d'un Centre d'IA du MDN et des FAC (CIAMF) en tant que centre d'excellence du MDN et des FAC. La Stratégie d'IA sera suivie d'un plan de mise en œuvre établissant les responsabilités et les échéanciers relatifs à la mise en œuvre de la Stratégie.

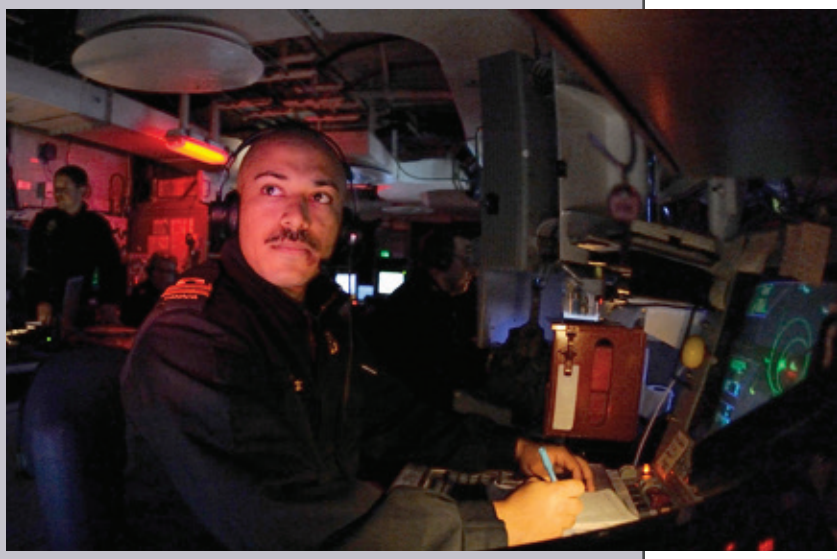
# L'APPRENTISSAGE AUTOMATIQUE PEUT PRÉDIRE LES DÉFAILLANCES DU SYSTÈME À BORD DES NAVIRES DE LA MARINE ROYALE CANADIENNE

**Capacité d'IA nécessaire :** détecter les défaillances imminentes des systèmes de navires à l'aide de données de capteurs

**Techniques d'IA utilisées :** apprentissage automatique supervisé et non supervisé, analytique prédictive

**Valeur ajoutée par l'IA :** prédiction des défaillances de systèmes à l'aide de données de capteurs d'un système de contrôle intégré de plateforme (SCIP)

Les défaillances des machines peuvent entraîner des événements tragiques à bord des navires en compromettant la sécurité des marins et le succès des opérations en mer. Par conséquent, la capacité de prédire des défaillances des systèmes de marine et de remplacer l'équipement avant qu'une défaillance ne survienne offre des avantages opérationnels importants aux utilisateurs pour la Marine royale canadienne (MRC).



C'est pourquoi en 2018, la MRC a communiqué avec le Centre d'analyse et de recherche opérationnelle (CARO) de Recherche et développement pour la défense Canada (RDDC) afin d'examiner si des données fournies par le SCIP pourraient être utilisées pour prédire les défaillances à bord des navires de la MRC. Le SCIP a été installé lors d'un carénage de demi-vie pour aider à surveiller la propulsion, les circuits électriques et les machines de lutte contre les avaries. Ses capteurs en réseau enregistrent des données chaque 0,5 seconde et fournissent des billions de points de données concernant l'état et la performance de chaque navire.

Le CARO a utilisé les données recueillies sur trois ans à partir de quatre systèmes à bord de navires sélectionnés de la MRC : le moteur diesel de propulsion, le groupe électrogène diesel, la ligne d'arbres et les hélices à pas variable et réversible et la boîte de vitesses. Il a agrégé les données sur une échelle de cinq minutes et les a jugées normales ou précédant une défaillance. Le CARO a ensuite utilisé des journaux de maintenance corrective et des rapports de défaillance opérationnelle pour corroborer les événements de défaillance.

Le CARO a utilisé ces données pour former et entraîner des algorithmes de réseau neuronal auto-encodeur afin de localiser les anomalies du système associées aux événements de défaillance. Les premiers résultats ont montré que les algorithmes pouvaient prédire le besoin en maintenance corrective jusqu'à une semaine à l'avance 75 p. 100 du temps.

La performance du système n'était pas parfaite, des faux positifs ayant été générés, mais les premiers résultats étaient suffisamment prometteurs pour justifier des mises à l'essai plus poussées.

# EN QUOI CONSISTE L'IA?


***Il est difficile de définir l'IA, et il n'existe aucune définition reconnue.*** Les technologies incluses dans le terme évoluent et se développent constamment à mesure que la science de l'IA progresse, alors que de nombreuses technologies plus anciennes, autrefois incluses, ne sont plus du tout considérées comme de l'IA.

***Même l'IA la plus avancée de nos jours est restreinte :*** les outils sont axés sur des tâches précises telles que la reconnaissance de formes, la classification, l'optimisation des tâches et la détection d'anomalies. Les experts ne sont pas d'accord sur le moment ou même si l'IA générale — qui peut effectuer n'importe quelle tâche cognitive aussi bien ou mieux qu'un humain — sera un jour développée. Les systèmes d'IA générale sont donc en dehors de la portée de cette Stratégie. L'intelligence augmentée est également un sous-ensemble de l'IA dans lequel les technologies d'IA et d'AA, telles que les assistants virtuels, aideront les humains en analysant les requêtes et en fournissant des données pertinentes pour aider le demandeur à prendre de meilleures décisions.

**Pour le MDN et les FAC, l'IA s'entend de la capacité d'un ordinateur de faire des choses qui sont normalement associées au processus cognitif humain, comme le raisonnement, l'apprentissage et l'auto-amélioration.**

***L'AA est actuellement la technique dominante en IA, en termes d'application généralisée et d'efficacité.*** Plutôt que de définir des règles pour obtenir un résultat, comme le fait un logiciel conventionnel, l'AA utilise des données antérieures pour y relever des modèles, ce qui lui permet d'optimiser ses performances en vue d'atteindre un objectif prédéfini. Lorsqu'ils fonctionnent correctement, les outils d'AA peuvent aider à prévoir les besoins, les événements, les tendances et les risques futurs, ce qui permet aux utilisateurs de réaliser des gains d'efficacité importants dans des domaines tels que la maintenance, la logistique et la gestion des inventaires. Cependant, l'efficacité de l'AA dépend de l'accès à des données suffisantes, pertinentes et de haute qualité, sans lesquelles les résultats de l'outil ne seront pas fiables. Par conséquent, la quantité et la qualité des données utilisées pour les applications de l'AA sont une priorité clé pour le MDN et les FAC.

***L'IA générative est un sous-ensemble de l'AA qui peut produire une grande variété de nouveaux contenus, comme des images, des vidéos, de l'audio, du texte, du code et des modèles 3D, en réponse aux messages-guides des utilisateurs.***

Elle le fait en dégageant la structure et des modèles de grandes quantités de données existantes, puis en utilisant ces tendances pour générer de nouveaux résultats ayant des caractéristiques semblables. Les extrants de l'IA générative peuvent être complexes, très réalistes et parfois indiscernable du contenu créé par un humain. Les percées récentes dans le domaine, en particulier quant aux grands modèles linguistiques et à la génération d'images, ont considérablement amélioré les capacités de l'IA générative, ouvrant de nouvelles possibilités d'utilisation de la technologie pour résoudre des problèmes complexes, notamment pour la recherche scientifique.

***Dans la culture populaire, l'IA est souvent caractérisée comme une concurrente de l'intelligence humaine, mais dans la pratique, les deux types d'intelligence sont très complémentaires.*** Dans de nombreux domaines, l'intelligence humaine soutenue par l'IA peut fournir des résultats supérieurs à ceux obtenus séparément. À titre d'exemple, l'IA peut entreprendre des tâches répétitives ou qui exigent un niveau élevé de précision et une attention soutenue. Le personnel humain peut donc exécuter les tâches auxquelles il excelle, particulièrement celles qui nécessitent du jugement, de la créativité, de l'initiative et une compréhension du contexte stratégique dans son ensemble.

| | INTELLIGENCE HUMAINE | INTELLIGENCE ARTIFICIELLE |
|---|---|---|
| Forces | • Peut innover, imaginer et créer sans données<br>• Comprend la conversation, l'émotion et l'humour<br>• Peut tirer des conclusions avec peu de données<br>• Peut prévoir des résultats possibles mais incertains et comprendre les conséquences d'une décision<br>• Peut intégrer rapidement de nouvelles sources de données et adapter les interventions<br>• Très écoénergétique | • Capacité de calcul presque illimitée<br>• Entrées capteurs presque illimitées, avec une vitesse de signaux proche de la vitesse de la lumière<br>• Peut être mise en réseau avec d'autres IA/ordinateurs pour une communication directe<br>• Peut être mise à jour et mise à l'échelle<br>• Excelle dans les tâches nécessitant une attention soutenue<br>• Aucune limite biologique liée à la fatigue, à la faim ou à la mortalité<br>• L'apprentissage peut être transféré en fin de vie |
| Faiblesses | • Capacité limitée de travail et de mémoire à long terme et de calcul<br>• Entrées sensorielles limitées et vitesse de signaux lente<br>• Ne peut pas être reconfigurée, mise à jour, mise à niveau ou mise à l'échelle<br>• Communique indirectement par le langage et ne peut pas être mise en réseau avec d'autres humains ou machines<br>• Lutte pour maintenir l'attention et la précision dans des conditions monotones<br>• Les biais cognitifs nuisent à la rationalité et à la qualité de la décision<br>• Risque d'erreur : le rendement se dégrade lorsque l'on est fatigué, affamé ou stressé<br>• Pas de transfert de connaissances en fin de vie | • Ne peut pas apprendre en s'attaquant à des problèmes<br>• Peut être formée pour reconnaître, mais sans comprendre le langage et les émotions<br>• Nécessite des données pour l'apprentissage et, à l'heure actuelle, n'apprend pas bien avec des données limitées<br>• Impossible d'intégrer des faits en dehors des données de formation dans la prise de décision<br>• Ne peut pas comprendre les conséquences des décisions<br>• Incapable de juger l'importance ou la signification du problème qu'on lui demande de résoudre<br>• Soumis aux biais des données et des algorithmes<br>• Très inefficace sur le plan énergétique |

***En plus de ses promesses, l'IA et son utilisation des données entraînent des défis et des responsabilités.*** Si un modèle d'IA est formé sur des données biaisées, la prédiction qui en résulte peut refléter et perpétuer ces biais, entraînant des préjudices dans le monde réel. En outre, il se peut que les prédictions de l'IA basées sur des données passées ne représentent pas l'avenir, ce qui signifie que cette IA ne parviendrait pas à prévoir des événements peu probables, mais ayant d'importantes répercussions. Enfin, l'utilisation des données par l'IA peut également présenter des risques liés à la protection des renseignements personnels et à la sécurité, en particulier lorsque ces données comportent des renseignements permettant d'identifier une personne ou des renseignements gouvernementaux de nature sensible. Par conséquent, les résultats de l'IA doivent toujours être analysés par rapport au jugement humain expert et aux contraintes et attentes de l'organisation, en tenant compte des limites de l'IA. Sur la voie de l'habilitation de l'IA, il est essentiel que l'Équipe de la Défense établisse et respecte les exigences en matière d'éthique, d'équité et de sécurité pour l'utilisation de l'IA.

# CAPACITÉS D'IA

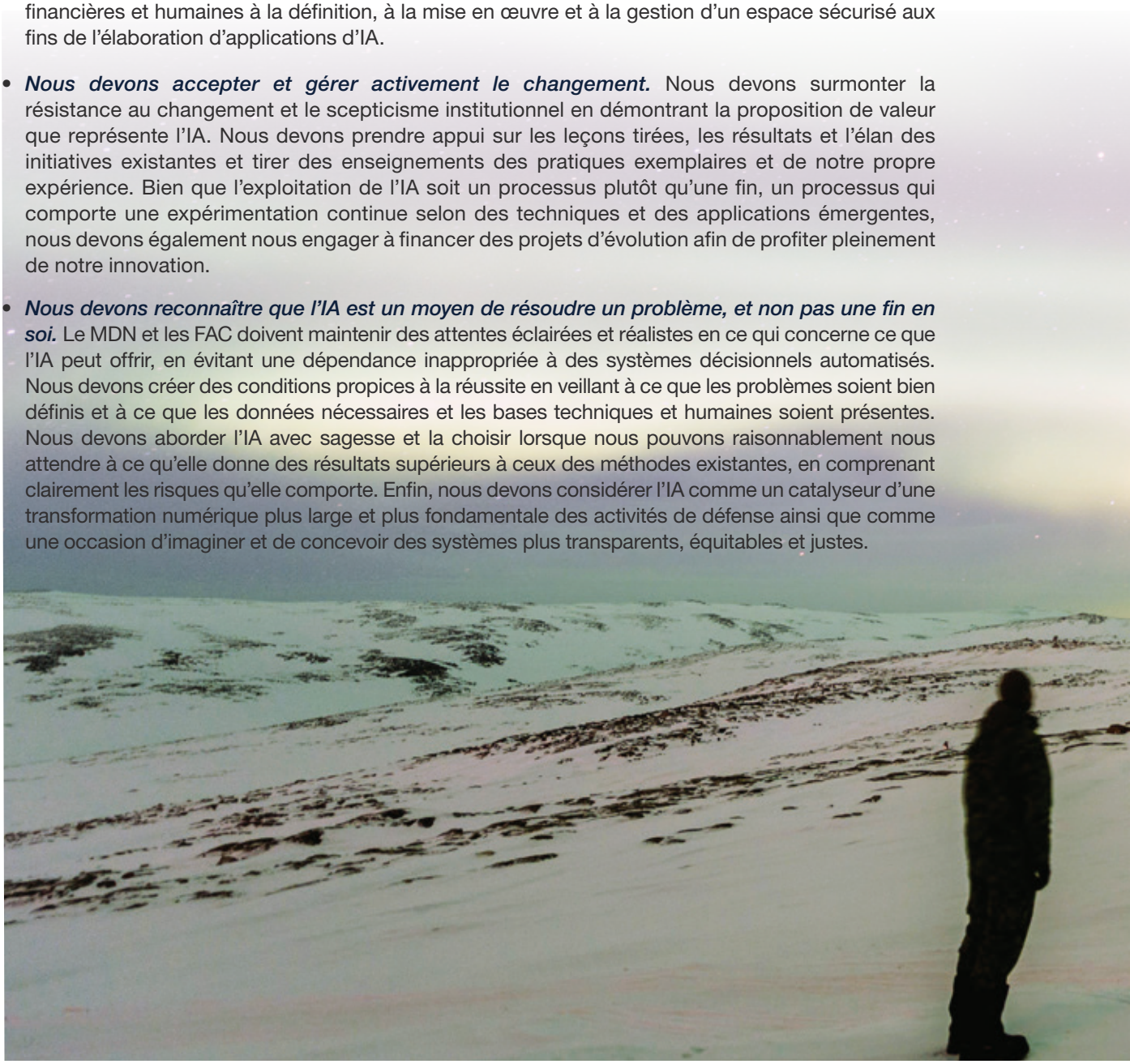
# PRINCIPES DIRECTEURS

Pour réussir la mise en œuvre de cette Stratégie d'ici 2030, le MDN et les FAC s'appuieront sur les principes suivants :

- ***Nous devons mettre en place les catalyseurs de données et techniques de l'IA. Le MDN et les FAC doivent mettre en œuvre la Stratégie de données du MDN et des FAC*** pour soutenir l'accès aux données de qualité supérieure, bien gérées, bien structurées et classifiées de manière appropriée dont l'IA dépend. Le MDN et les FAC doivent également créer l'infrastructure numérique sécurisée et interopérable nécessaire pour soutenir son application, y compris les investissements dans l'infrastructure infonuagique et la sécurité nécessaires pour faire évoluer l'IA. Cela doit être fait en tenant pleinement compte de la sécurité centrée sur les données, un aspect essentiel de la sécurité des données et de la cybersécurité. Le MDN et les FAC doivent affecter des ressources financières et humaines à la définition, à la mise en œuvre et à la gestion d'un espace sécurisé aux fins de l'élaboration d'applications d'IA.

- ***Nous devons accepter et gérer activement le changement.*** Nous devons surmonter la résistance au changement et le scepticisme institutionnel en démontrant la proposition de valeur que représente l'IA. Nous devons prendre appui sur les leçons tirées, les résultats et l'élan des initiatives existantes et tirer des enseignements des pratiques exemplaires et de notre propre expérience. Bien que l'exploitation de l'IA soit un processus plutôt qu'une fin, un processus qui comporte une expérimentation continue selon des techniques et des applications émergentes, nous devons également nous engager à financer des projets d'évolution afin de profiter pleinement de notre innovation.

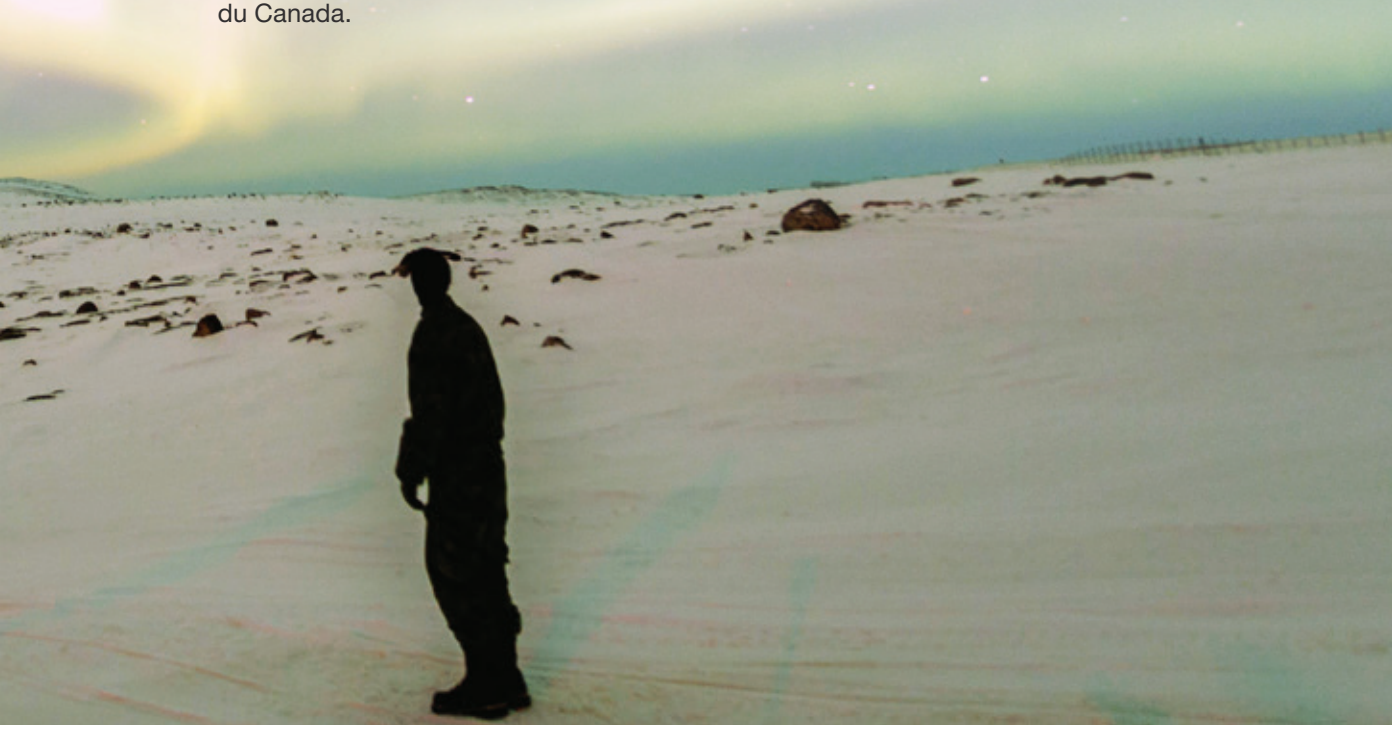
- ***Nous devons reconnaître que l'IA est un moyen de résoudre un problème, et non pas une fin en soi.*** Le MDN et les FAC doivent maintenir des attentes éclairées et réalistes en ce qui concerne ce que l'IA peut offrir, en évitant une dépendance inappropriée à des systèmes décisionnels automatisés. Nous devons créer des conditions propices à la réussite en veillant à ce que les problèmes soient bien définis et à ce que les données nécessaires et les bases techniques et humaines soient présentes. Nous devons aborder l'IA avec sagesse et la choisir lorsque nous pouvons raisonnablement nous attendre à ce qu'elle donne des résultats supérieurs à ceux des méthodes existantes, en comprenant clairement les risques qu'elle comporte. Enfin, nous devons considérer l'IA comme un catalyseur d'une transformation numérique plus large et plus fondamentale des activités de défense ainsi que comme une occasion d'imaginer et de concevoir des systèmes plus transparents, équitables et justes.



- ***Nous devons déployer l'IA pour accroître, et non pas remplacer, l'action humaine et la prise de décisions.*** Quels que soient les outils, la Défense sera toujours une entreprise fondamentalement humaine. Nous devons assurer une participation humaine appropriée dans les systèmes d'IA, calibrée en fonction des risques qu'ils présentent et de leur incidence. Bien que la participation puisse être minime dans le cas des applications à faible risque, une intervention humaine doit toujours être maintenue pour les applications impliquant une force létale. Dans la mesure du possible, les décisions et les résultats doivent être explicables et transparents, selon des mécanismes de responsabilisation appropriés en place.

- ***Nous ne devons pas adopter l'IA sans les processus qu'elle exige.*** Les avancées technologiques ont fait passer les cycles d'innovation de décennies à des mois. Pour réussir en ce qui a trait à l'IA, le MDN et les FAC doivent être prêts à avancer à ce rythme. Nous devons faire évoluer nos systèmes et nos processus afin d'être en mesure d'acquérir, de développer, de mettre à l'essai et de déployer des technologies d'IA de manière sûre et à un rythme pertinent, tout en travaillant horizontalement pour atteindre nos objectifs en matière d'IA. À cette fin, nous devrons incorporer une gestion de projet agile, reconnaître les logiciels comme une capacité militaire tout autant que le matériel et intégrer la souplesse et la mise à niveau des logiciels à nos processus pour permettre l'amélioration des capacités. Nous devrons résoudre des contraintes relatives aux processus critiques et aux capacités en matière d'infrastructures et de données. Bref, nous devons être disposés à accepter une perturbation fondamentale afin de profiter de l'IA.

- ***Nous devons calibrer nos investissements en IA et assurer l'harmonisation avec les priorités du gouvernement.*** Le MDN et les FAC doivent déterminer et hiérarchiser les domaines d'investissement stratégique dans l'IA qui permettront le développement ou l'amplification de capacités clés pour les missions prioritaires, en particulier lorsque l'IA peut multiplier la force de combat. Dans la mesure du possible, ces domaines devraient prendre appui sur les forces existantes du MDN et des FAC et du Canada en matière d'IA et de défense afin de maximiser le rendement de nos investissements et d'assurer la souveraineté de nos fondements et de nos capacités en matière d'IA. Pour établir le rendement de nos investissements, nous devons toutefois tenir compte des coûts cachés de l'IA, y compris les coûts des données et de calcul et l'incidence sur les priorités et les objectifs généraux du Canada.



# DOMAINE D'EFFORT

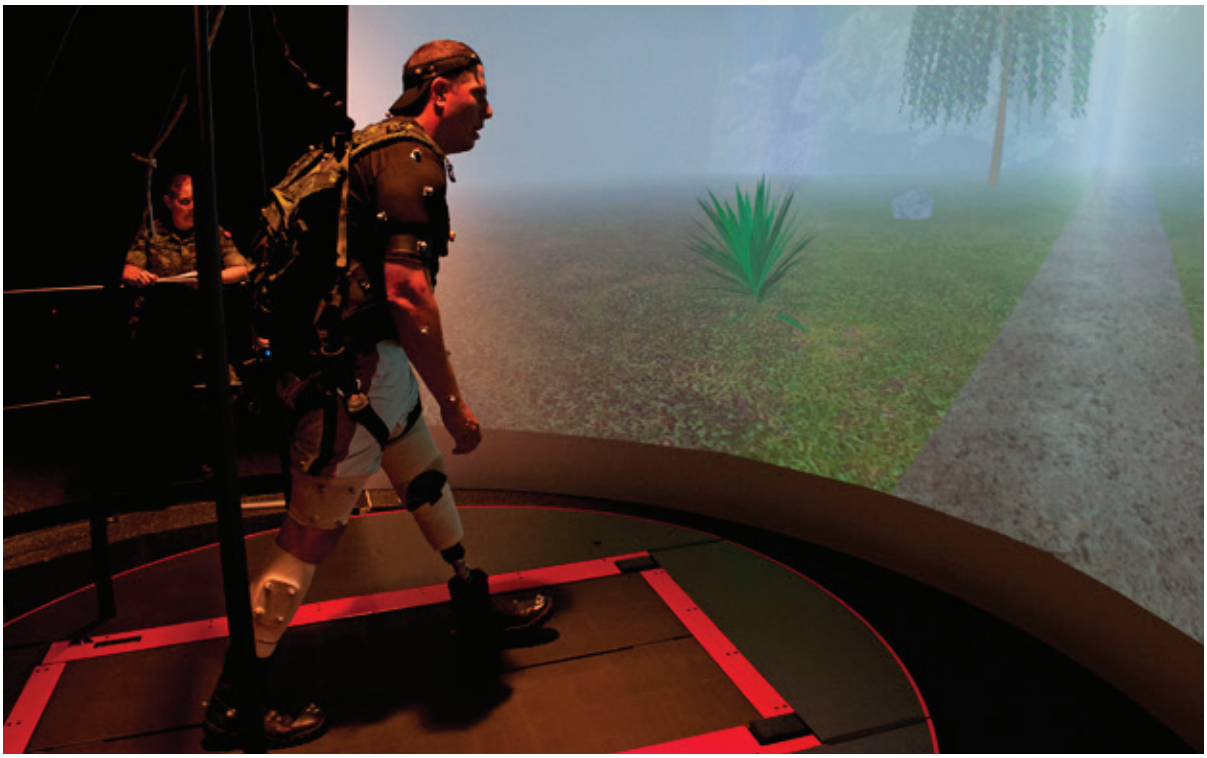
# LIGNE D'EFFORT 1 : MISE EN SERVICE ET UTILISATION DES CAPACITÉS D'IA

## Le défi

***L'IA sera fondamentale pour la modernisation de la Défense.*** La fusion de l'IA, du réseautage, de l'analytique prédictive et prescriptive, de l'AA et de la robotique sera essentielle pour équiper le MDN et les FAC et transformer la défense sur le plan numérique. Cela fournira les capacités nécessaires pour assurer la supériorité opérationnelle sur nos adversaires, de même que la parité technologique et l'interopérabilité avec nos alliés. Le simple volume, la diversité et la complexité des données produites par les capteurs modernes ont déjà dépassé la capacité des analystes humains de les traiter et les interpréter. Ce problème ne fera qu'augmenter à mesure que les systèmes existants seront mis à niveau et remplacés.

***Malgré cela, nous commençons à peine à déterminer les capacités habilitées par l'IA dont nous avons besoin et la manière de les réaliser.*** Bien que le MDN et les FAC possèdent une expertise en matière d'IA, sa maturité, son intégration et sa mise en œuvre sont encore à un stade précoce de développement. Nos efforts actuels sont répartis entre les environnements et les commandements, chaque partie abordant l'habilitation de l'IA et des capacités connexes séparément, et sont entravés par des problèmes de qualité des données. La mise en service et l'utilisation efficaces des capacités d'IA nécessiteront un effort concerté et collaboratif jusqu'à ce que le MDN et les FAC soient plus avancés sur le plan numérique et plus compétents sur le plan technologique.

***L'IA commence à proliférer dans de nombreuses facettes des opérations et des activités de la Défense.*** Le MDN et les FAC doivent être pleinement conscients des avantages et des défis de l'IA afin de favoriser une utilisation responsable et transparente de cet outil puissant, tout en minimisant les risques. Toute IA employée par les FAC dans le cadre d'opérations, y compris l'IA et les renseignements basés sur l'IA obtenus auprès



d'alliés ou de partenaires, fera probablement l'objet d'un examen minutieux, ce qui nécessite une attention supplémentaire de la part des autorités opérationnelles afin de veiller à ce qu'elles soient conformes à la loi et aux politiques canadiennes.

***Les obligations et responsabilités des systèmes d'IA peuvent recouper les structures existantes au sein et à l'extérieur du MDN et des FAC.*** En outre, compte tenu de leur application en matière de défense nationale, certains cas d'usage au sein du MDN et des FAC pourraient relever des directives fournies par le Secrétariat du Conseil du Trésor du Canada et l'écart entre le développement de l'IA et la couverture législative et de politiques continuera de se creuser. Si les lois et les politiques ne s'appliquent pas ou n'ont pas encore été élaborées, les N1 doivent travailler en collaboration à l'élaboration de directives appropriées afin de garantir une utilisation responsable et transparente de l'IA. Nous devons établir un équilibre entre les essais, la validation et l'atténuation des risques et l'agilité nécessaire pour adopter les technologies d'IA à un rythme pertinent.

## Ce que nous devons faire

***Nous devons utiliser l'IA de manière responsable et transparente pour fournir des capacités en matière d'opérations et pour résoudre des problèmes opérationnels importants.*** Nous devons rapidement acquérir l'expertise et l'expérience internes nécessaires pour évaluer, conseiller, mettre en œuvre et gérer les outils et applications d'IA pour les opérations et les activités de défense. Nous devons également fournir des mécanismes de collaboration afin de soutenir l'utilisation de l'IA pendant les opérations, que la technologie provienne du MDN et des FAC ou qu'elle soit partagée avec nous par nos alliés ou partenaires.

***Nous devons harmoniser nos investissements dans l'IA avec les priorités existantes.*** La mise en service et l'utilisation des capacités d'IA ne se produiront pas d'un seul coup. Le MDN et les FAC accorderont donc la priorité à la mise en service de systèmes d'IA qui appuient les engagements prévus dans le cadre du plan ministériel, afin d'améliorer la prise de décisions et les processus et de renforcer les capacités et le rendement de notre personnel en le libérant de l'exécution de tâches répétitives ou dangereuses. Dans un premier temps, les efforts seront axés sur l'activation des capacités opérationnelles des FAC, ainsi que sur les efforts qui soutiennent les activités de la défense, en particulier ceux qui soutiennent la reconstitution et la disponibilité opérationnelle des FAC. Ces domaines d'intervention opérationnelle peuvent être directement liés aux priorités du plan ministériel pour surmonter les défis existants du MDN et des FAC. Bien que ces efforts doivent être collaboratifs et exécutés horizontalement au niveau le plus bas, une gouvernance efficace sera nécessaire pour s'assurer qu'ils soient coordonnés, hiérarchisés et mis en œuvre conformément aux plans et priorités du MDN et des FAC. Des évaluations régulières seront nécessaires pour suivre les progrès et en rendre compte.

***Nous déterminerons ou développerons des outils pour soutenir la conception, l'acquisition, l'intégration et l'évolution rapides et sûres de l'IA.*** On accordera d'abord la priorité aux outils visant à soutenir l'évaluation de l'IA pour les opérations, mais on utilisera également des outils de définition de problèmes qui permettront de déterminer les problèmes qui nécessiteront une solution basée sur l'IA, des lignes directrices pour aider les équipes de projets et le personnel de soutien à se procurer ces solutions, ainsi que des outils d'évaluation quantitative et qualitative des risques pour déterminer et atténuer les risques liés à des considérations en matière de protection des renseignements personnels, de sûreté, de sécurité, de droits de la personne et d'ACS Plus.

## COMMENT NOUS NOUS Y PRENDRONS

1. ***Mettre en place un Centre d'IA du MDN et des FAC (CIAMF) à l'interne.*** Un CIAMF, comme ceux de certains de nos partenaires de défense (ci-dessous), servira de pôle d'expertise en matière d'IA et accélérera l'expérimentation, la mise à l'essai, l'évaluation et le déploiement de l'IA. Ce centre établira des processus d'adoption de l'IA pour développer et intégrer les technologies d'IA en collaboration avec ses principaux partenaires et fournira un soutien et des conseils à tous afin de permettre une adoption et une utilisation sûres et responsables de l'IA.

2. ***Effectuer une évaluation de la maturité de l'IA et élaborer des paramètres pour mesurer nos progrès et notre rendement.*** Une évaluation des niveaux actuels de la mise en œuvre et des capacités en matière d'IA établira une base de référence par rapport à laquelle le succès de la Stratégie d'IA et notre propre développement de l'IA pourront être mesurés à l'aide d'indicateurs de rendement clés (IRC).

3. ***Élaborer des mécanismes et des outils pour soutenir la croissance de l'IA.*** Le MDN et les FAC auront besoin de normes, de mesures de protection, de listes de vérification et de processus internes pour permettre l'utilisation, la conception, l'approvisionnement, l'intégration, la gestion des risques et la mise à l'échelle rapides et sécuritaires de l'IA. Le CIAMF dirigera ces efforts en collaboration avec toutes les parties prenantes.

4. ***Développer la gouvernance pour l'IA afin d'harmoniser les ressources avec les objectifs.*** Des options pour une gouvernance efficace de l'IA seront élaborées et considérées dans le cadre de la structure de gouvernance globale au sein du MDN et des FAC. Cette gouvernance veillera à ce que les efforts demeurent harmonisés avec les priorités, les politiques et les capacités existantes.

# UN CENTRE D'IA DU MDN ET DES FAC

Au cours des cinq dernières années, trois des plus proches partenaires de défense du Canada ont établi des centres d'excellence afin d'accélérer la mise à l'essai et l'évolution de l'IA à l'échelle de l'organisation de la défense. En 2018, le département de la Défense des États-Unis (DoD) a établi le Joint AI Centre (Centre conjoint d'IA) pour accélérer le développement et le déploiement de l'IA et pour soutenir la mise en œuvre de la stratégie d'IA du DoD. Le centre d'IA de la défense de l'Australie a été créé la même année et le ministère de la Défense du Royaume-Uni a inauguré son propre centre d'IA de la défense en avril 2022 pour qu'il accélère l'implémentation de concepts d'opérationnalisation et d'évolution à l'échelle de la défense selon des piliers clés axés sur la robotique, le numérique et l'IA responsable. De plus, des accélérateurs de l'IA pour la défense ont été approuvés comme pratique exemplaire par la Commission de la sécurité nationale sur l'intelligence artificielle américaine dans son rapport final de 2021.

***Pour atteindre ses objectifs en matière d'IA, le MDN et les FAC ont besoin de leur propre Centre d'IA.*** Le centre travaillerait de manière interfonctionnelle avec des équipes qui exploitent ou mettent à l'essai l'IA à l'heure actuelle et servirait de pôle d'expertise en matière d'IA pour l'Équipe de la Défense. Il identifierait des capacités développées par l'industrie, le milieu universitaire ou les alliés du Canada et soutiendrait leur intégration, faciliterait la création d'un inventaire commun d'applications, de techniques et de données liées à l'IA, élaborerait des applications d'IA communes pour relever des défis collectifs dans l'ensemble de l'organisation et appuierait le développement de l'IA à l'échelle locale au sein des commandements et des environnements. Il offrirait également des conseils relatifs à des questions connexes nécessaires à la réussite de la mise en œuvre de l'IA, notamment en matière de politiques, d'éthique, d'ACS Plus, d'approvisionnement et de formation. Le Centre d'IA du MDN et des FAC collaborerait avec des intervenants des centres de guerre, des centres de recherche de Recherche et développement pour la défense Canada (RDDC), du Laboratoire de fusion des opérations interarmées, d'Innovation pour la défense, l'excellence et la sécurité (IDEeS) et d'autres branches de l'Équipe de la Défense pour coordonner l'établissement des priorités organisationnelles en matière d'IA, assurer l'interopérabilité interne et effectuer des économies d'effort et d'échelle ainsi que veiller à ce que les initiatives réussies puissent évoluer convenablement. Le centre collaborerait également avec les partenaires du Groupe des cinq et les alliés de l'Organisation du Traité de l'Amérique du Nord (OTAN) au sujet de normes et de lignes directrices en matière d'interopérabilité et d'utilisation responsable. En outre, il assumerait un rôle de diffusion et de rayonnement auprès du milieu universitaire, de l'industrie et de la société civile ainsi qu'auprès d'autres ministères et des organes d'examen. Dans l'exercice de ce rôle, il aiderait à favoriser le développement de l'écosystème de l'IA de la défense canadienne, à déterminer des solutions prometteuses et à promouvoir leur adoption au sein du MDN et des FAC et à fournir un environnement qui permettrait de discuter des défis en matière de défense et de sécurité.

# LIGNE D'EFFORT 2 : GESTION DU CHANGEMENT

## Le défi

***Tirer largement parti de l'IA à l'échelle de l'entreprise nécessitera un changement et ce changement devra être pris en charge, surveillé et géré.*** La nature transformatrice et en évolution rapide de l'IA exige que le MDN et les FAC favorisent activement le développement de l'IA à l'échelle de l'organisation en adoptant une culture étant plus agile, novatrice, inclusive, axée sur les solutions et tolérante aux risques. Non seulement ces changements sont-ils nécessaires pour exploiter pleinement l'IA, mais ils sont aussi exigés de la part de l'organisation compte tenu de son engagement à l'égard de la transformation numérique et par des changements sécuritaires, techniques, industriels et sociaux rapides et souvent perturbateurs qui se produisent actuellement dans le monde.

***Notre structure, nos processus et nos mesures incitatives actuels n'appuient pas entièrement ce changement nécessaire.*** Notre attention et nos dépenses ont été orientées vers le matériel militaire et nos structures et processus reflètent cette orientation. Nos processus limitent notre capacité à nous procurer l'IA ou à collaborer avec d'autres intervenants pour la développer, ce qui entrave l'expérimentation et l'innovation. Les données et les renseignements sont souvent disparates ou non disponibles et les responsables fonctionnels ne sont pas disposés à les partager en raison de problèmes de sécurité. Les styles traditionnels de leadership ont eu tendance à confier le pouvoir aux échelons supérieurs et à récompenser la conformité plutôt que l'innovation. Cela doit changer si nous voulons réussir la mise en œuvre de l'IA.

## Ce que nous devons faire

***Nous devons accepter la transformation numérique comme fondement de l'adoption de l'IA.*** La transformation numérique et l'adoption de l'IA exigeront de notre organisation qu'elle accepte une plus grande tolérance aux risques et aux échecs. La recherche et le développement en matière d'IA présentent un risque élevé et supposent souvent un tâtonnement avant que le succès ne soit atteint. Nous devrons accueillir l'expérimentation et une prise de risques appropriée et fournir des environnements protégés dans lesquels cela pourra être fait en toute sécurité. Nous devrons faire preuve de tolérance à l'idée d'échouer, tôt ou tard, en avançant dans le cadre de l'expérimentation et de la découverte des possibilités.

***Nous devons apprendre à travailler horizontalement.*** Le travail au sein de commandements ou de structures organisationnelles verticales ne donnera pas les résultats que nous recherchons. Nous devons plutôt apprendre à travailler en collaboration dans l'ensemble de l'organisation. Dans la mesure du possible, nous devrions rechercher une capacité conjointe à réduire le cloisonnement propre à un domaine. Étant donné la complexité de la technologie, nous devons adopter une approche intersectionnelle, multidisciplinaire et interfonctionnelle en matière de conception de projets et de résolution de problèmes. Cette approche horizontale et interfonctionnelle permettra à la haute direction de doter les décideurs, à tous les échelons, du pouvoir nécessaire pour déterminer et mettre en œuvre des initiatives d'IA, tout en adoptant une diversité de perspectives qui serait perçue comme une force plutôt qu'une faiblesse.

***Nous devons accepter la perturbation.*** L'IA est perturbatrice et nous devons être préparés au fait que son adoption entraînera des changements — parfois de profonds changements — à nos structures et à nos méthodes de travail. Nous devons accepter ce fait. Nous devons être disposés à remettre en question les méthodes orthodoxes et adopter de nouvelles méthodes pour atteindre nos objectifs, en utilisant l'innovation, la diversité, l'agilité et l'excellence qui existent au sein de l'Équipe de la Défense.

***Nous devons nous adapter en permanence.*** Dans le passé, les changements technologiques ont entraîné des perturbations épisodiques de la culture, des processus et des rôles, suivies de périodes de stabilité. Avec l'apparition de l'IA et des technologies connexes, les cycles d'innovation ont été considérablement comprimés. Nous devrons être préparés à passer à un état d'adaptation continue, en étant attentifs aux nouvelles réalités et prêts à les intégrer à notre espace organisationnel et de combat. Plus particulièrement, le coût de l'expérimentation, du développement, de la mise en service et du maintien de l'IA devra être intégré dans les plans de développement des capacités de défense. Le MDN et les FAC exigeront plus de souplesse et d'agilité sur le plan de leurs processus de soutien dans leurs branches militaires et civiles, y compris la nécessité d'un examen et d'une mise à jour continus de la formation et des pouvoirs délégués pour maximiser l'action horizontale quant à la pensée et au but. Enfin, notre système de formation doit intégrer pleinement l'IA dans la mesure du possible pour permettre des systèmes générateurs de force individuels et collectifs, plus rapides et adaptatifs.

## COMMENT NOUS NOUS Y PRENDRONS

1. ***Attribuer des pouvoirs décisionnels en matière d'IA à l'échelon approprié le plus bas afin de favoriser l'innovation.*** Bien que des centres d'excellence soient essentiels à la réussite de la mise en œuvre de l'IA, le développement local est tout aussi indispensable pour favoriser l'élaboration de solutions visant à répondre à des besoins précis. Les dirigeants doivent donc être dotés de pouvoirs en matière d'expérimentation et d'innovation, dans un environnement horizontal et interfonctionnel, tout en identifiant et respectant les processus d'adoption de l'IA développés par le CIAMF et qui sont le mieux adaptées aux circonstances spécifiques.
2. ***Déterminer et modifier les mesures incitatives.*** Nous devons déterminer les manières dont nous pouvons utiliser efficacement des mesures incitatives, telles que les promotions, la reconnaissance ou les structures de développement de carrière, afin d'encourager les types de comportements nécessaires à l'adoption de l'IA à grande échelle. Nous devrons accroître les mesures incitatives visant à innover et à réduire les coûts et les risques d'échec en fournissant des environnements protégés en cas de défaillances précoces et en adoptant une approche sans reproche.
3. ***Inclure l'IA comme un catalyseur de la capacité de défense qui nécessite un financement.*** Si le MDN et les FAC doivent réaliser leurs aspirations en matière d'IA, ils doivent s'engager à financer les catalyseurs techniques, numériques et de données ainsi que la recherche, l'engagement et le personnel que l'IA exige. Il faut établir les coûts de ces catalyseurs et ces coûts doivent être intégrés à la planification et au développement de programmes et de projets dès le début. De nouveaux programmes, projets et initiatives seront nécessaires pour évaluer la mise en œuvre potentielle de l'IA et les capacités existantes seront évaluées pour déterminer la nécessité d'intégrer les améliorations rendues possibles grâce à l'IA dans les systèmes existants.
4. ***Identifier, hiérarchiser et surmonter les principaux obstacles à l'acquisition, au développement, à la mise à l'essai, à la validation, à la certification, à la mise en service et à la mise hors service responsables de l'IA.*** En plus du financement et du soutien des catalyseurs de l'IA, nous devons veiller à ce que les principaux organes de gouvernance de l'IA disposent du pouvoir et des ressources nécessaires pour réduire au minimum les obstacles liés aux politiques et aux processus touchant le développement, la mise en œuvre et l'adoption.

## AGENT CONVERSATIONNEL RELATIF AUX POLITIQUES ET AUX NORMES

**Capacité d'IA requise :** robot conversationnel issu de l'IA qui peut donner des réponses aux questions sur la politique relative à la tenue militaire.

**Techniques d'IA utilisées :** traitement du langage naturel

**Proposition de valeur :** amélioration de la compréhension et du respect des politiques parmi les membres des FAC

Les documents de politiques contiennent des renseignements essentiels, mais ils peuvent être longs et difficiles à parcourir pour les membres du personnel qui cherchent des réponses à des questions précises. En réponse à ce défi, l'équipe de science des données du Bureau de la transformation numérique a produit un prototype fonctionnel qui pourrait aider les membres des FAC à trouver des réponses à leurs questions sur la politique relative à la tenue militaire.

Élaboré à partir de rien par l'équipe de science des données à l'aide de technologies à « source ouverte » (« open source ») types de l'industrie, l'agent conversationnel permet aux utilisateurs de saisir des questions dans un langage naturel et de recevoir des renvois au passage qui, selon le système, comporte une réponse à la question de l'utilisateur, avec en plus des liens vers les politiques pertinentes. Le prototype contient également des fonctionnalités permettant aux utilisateurs de donner leur avis au sujet de la pertinence de la réponse aux fins d'amélioration de la précision de l'outil et d'envoyer à l'équipe des commentaires concernant leur expérience. Selon les développeurs de l'agent conversationnel, celui-ci est précis à plus de 90 p. dans ses réponses aux questions. Ce robot conversationnel n'a été déployé que dans des environnements d'essai afin de valider le principe du concept. Cette classe d'outils d'IA promet de pouvoir répondre à des questions sur d'autres types de politiques.

# LIGNE D'EFFORT 3 : ÉTHIQUE, SÉCURITÉ ET CONFIANCE

## Le défi

***Les Canadiens s'attendent à ce que nous acquérions, développions et mettions en œuvre une IA légale, inclusive, éthique et sûre.*** L'utilisation de l'IA dans le cadre de la défense, en particulier celle avec des applications liées au recours à la force, sera examinée de près pour veiller à ce qu'elle soit conforme à nos valeurs communes et aux lois canadiennes ainsi qu'au droit international. Notre légitimité en ce qui concerne l'utilisation de la force militaire découle du consentement des personnes que nous servons et nous devons nous assurer de préserver cette légitimité en utilisant l'IA. Faute de quoi, nous pourrions perdre la confiance du public, courir le risque d'une atteinte à notre réputation, perpétuer de la discrimination et des préjugés et contribuer à un faible moral parmi notre personnel.

***L'IA pourrait comporter des risques pour les droits de la personne, la vie privée et la sécurité.*** Alors que le MDN et les FAC font face à des risques réels s'ils ne suivent pas le rythme de leurs adversaires en matière d'IA, ils doivent rester conscients des risques possibles pour les droits de la personne liés à cette technologie. L'IA est un produit provenant de l'humain et des préjugés et des défauts propres aux humains sont intégrés dans ses données, ses algorithmes, ses modèles et les processus qui les accompagnent. Un nombre croissant d'incidents démontrent que l'IA peut échouer ou causer des dommages et des préjudices en raison de ces défauts et ainsi entraîner des décisions discriminatoires qui ne peuvent pas être expliquées ou vérifiées. L'IA peut également causer des dommages en raison d'un manque d'essai, d'expérimentation, d'évaluation et de surveillance et peut créer de nouveaux risques liés à la protection des données et des renseignements personnels et au droit à la vie privée. Dans un contexte de défense nationale comportant des renseignements hautement classifiés, les risques liés à l'IA comprennent également la possibilité de fuites, de cyberattaques, d'exposition d'actions de renseignement par inadvertance, de manipulation et de biais.

***Une IA éthique et sûre sera essentielle afin de s'assurer que les membres de notre personnel s'y fient et l'utilisent.*** La volonté des membres et des employés d'utiliser les applications d'IA, en particulier dans un environnement de combat, dépendra de leur confiance à l'égard de la sécurité et du caractère éthique de ces technologies ainsi que de leurs effets et des décisions qui en découleront. Une adoption généralisée de l'IA exigera donc que nous démontrions cette sécurité à nos membres et à notre personnel. Les décisions, les comportements et les performances fondés sur l'IA doivent être cohérents, fiables et dignes de confiance autant que possible.

## Ce que nous devons faire

***Nous devons accorder une importance égale aux préoccupations éthiques, liées à la sécurité et techniques.*** L'identification, l'atténuation et le traitement des sources de préjudices involontaires et d'activités malveillantes intentionnelles doivent faire partie du cycle de vie des systèmes d'IA et devraient se voir accorder la même importance que la résolution de problèmes techniques.

***Nous devons intégrer des exigences en matière d'éthique, d'équité et de sécurité à toutes les étapes du cycle de vie des projets et des systèmes,*** notamment la conception, le développement, la validation et la certification, l'acquisition et le déploiement de systèmes d'IA et leur éventuelle mise hors service. Les décisions visant à accroître les capacités liées à des tâches fondées sur la prise de décision humaine ou le jugement humain doivent être justifiées et documentées et des mécanismes doivent être mis en place pour veiller à ce que les décisions finales soient traçables et explicables par des mesures de responsabilisation appropriées. Tous les membres du personnel qui participent au développement, à l'acquisition et à l'utilisation de l'IA doivent bien comprendre leur rôle et leur niveau de responsabilité et de pouvoir à l'égard de ces projets et de ces systèmes. En outre, les projets doivent incorporer ACS Plus tout au long du cycle de vie de l'IA afin de garantir que les solutions répondent aux besoins de groupes divers et aux différentes expériences, qu'elles contribuent à des résultats positifs et qu'elles n'entraînent pas de préjudices découlant de préjugés ou biais algorithmiques ou liés aux données.

***Nous devons rendre l'éthique relative à l'IA claire, cohérente et réalisable.*** De nombreuses organisations ont créé des principes d'éthique en matière d'IA, mais la plupart d'entre elles n'ont pas communiqué la manière de les mettre en pratique. Les personnes qui interviennent dans la conception, le développement et l'exécution de systèmes d'IA ont besoin d'étapes claires à suivre pour intégrer des approches éthiques à leur processus. Nous devons créer des outils pour permettre aux équipes de projets d'IA d'identifier les risques, de définir des stratégies d'atténuation et d'adopter de saines pratiques de fonctionnement éthiques à chaque étape du cycle de vie du projet.

## COMMENT NOUS NOUS Y PRENDRONS

1. ***Veiller à ce que toute nouvelle IA ou technologie basée sur l'IA soit élaborée et mise en œuvre conformément aux lois, aux politiques et aux lignes directrices applicables.*** Il s'agit notamment du droit canadien et international, de la réglementation applicable et des politiques du gouvernement du Canada telles que le ***Code de conduite volontaire visant un développement et une gestion responsables des systèmes d'IA générative avancés***, le ***Guide sur l'utilisation de l'intelligence artificielle générative*** et la ***Directive sur la prise de décisions automatisée***. Cela inclut l'engagement du MDN et des FAC à intégrer l'ACS Plus aux opérations, aux politiques et aux programmes et aux instruments connexes du MDN et des FAC, comme le cycle de ciblage, les règles d'engagement, la gestion des risques et les politiques et lignes directrices en matière de sécurité et de gestion de l'information. Le MDN et les FAC répondront également aux directives d'organes d'examen externes, comme le Secrétariat du Comité des parlementaires sur la sécurité nationale et le renseignement (CPSNR), l'Office de surveillance des activités en matière de sécurité nationale et de renseignement (OSSNR) et le Commissariat à la protection de la vie privée du Canada (CPVP).

2. ***Élaborer des principes d'éthique en matière d'IA, des cadres de risques et des pratiques opérationnelles pour le cycle de vie de l'IA.*** En s'appuyant sur les pratiques exemplaires fédérales et internationales, le MDN et les FAC, à l'initiative du CIAMF, élaboreront un ensemble de principes d'éthique, des pratiques opérationnelles et un cadre de prévention des risques en matière d'IA pour intégrer ces pratiques exemplaires à l'ensemble du cycle de vie de l'IA. Ce cadre identifiera les risques et leurs répercussions afin qu'ils puissent être atténués et pour assurer un niveau de transparence, de compréhension et d'intervention humaine adapté aux risques et aux répercussions en cause. Conformément à la Directive sur la prise de décisions automatisée et aux évaluations de l'incidence algorithmique, le cadre tiendra compte des risques pour les droits, la santé et le bien-être ainsi que les intérêts économiques des personnes et des collectivités touchées par le système, y compris les conséquences discriminatoires découlant de préjugés algorithmiques ou liés aux données et des risques pour la durabilité continue d'un écosystème. Au fil de l'évolution de la technologie et des pratiques exemplaires, nous mettrons à jour ce cadre et ces pratiques afin de veiller à ce qu'ils restent évolutifs.

3. ***Intégrer des normes et élaborer des exigences relatives à des systèmes d'IA éthiques, sûrs, inclusifs et fiables en matière de défense et de sécurité.*** Cela inclut les normes éthiques canadiennes et internationales existantes, ainsi que les normes en matière de données, de confiance du numérique et de gestion de l'identité. Nous devons également favoriser l'adoption et l'opérationnalisation des principes de l'IA chez les fournisseurs tiers et collaborer avec nos principaux alliés et partenaires pour poursuivre l'élaboration et l'intégration de normes nationales et internationales en matière d'éthique de données et d'IA, par exemple les principes de l'OTAN relatifs à l'utilisation responsable de l'intelligence artificielle dans la défense.

4. ***Collaborer avec des partenaires internes et externes pour une IA éthique, sûre et fiable.*** Le MDN et les FAC tireront parti du leadership du secteur public et de la société civile du Canada en matière d'éthique relative à l'IA et de l'expertise du Programme d'éthique de la Défense, du directeur – Égalité des genres et analyse intersectionnelle (DEGAI) et d'autres intervenants pour favoriser l'utilisation responsable, sûre et inclusive des technologies d'IA. Nous collaborerons avec d'autres organismes et ministères du gouvernement du Canada et nos partenaires en matière de sécurité pour continuer de promouvoir l'équité, la sécurité et la confiance relatives à l'IA ainsi qu'avec d'autres pays pour élaborer des normes et des mesures de renforcement de la confiance en matière d'IA et pour ouvrir des voies de communication concernant les accidents, le comportement imprévu de systèmes, les cyberattaques et les effets émergents à la suite de l'interaction de systèmes. Nous encouragerons le développement et l'utilisation responsables de l'IA par les autres pays.

# LIGNE D'EFFORT 4 : TALENTS ET FORMATION

## Le défi

***La mise en œuvre efficace de l'IA exigera que les bonnes personnes ayant reçu la bonne formation soient affectées au bon endroit au bon moment.*** Les effectifs futurs du MDN et des FAC devront être composés d'un personnel diversifié doté d'un large éventail de compétences techniques et non techniques. Il s'agira notamment de spécialistes multidisciplinaires possédant des compétences avancées, dont des ingénieurs en apprentissage automatique, des ingénieurs de données, des scientifiques de données, des spécialistes de la cybersécurité et des gestionnaires de produits d'IA. Les effectifs devront également compter des personnes dotées des compétences personnelles générales, notamment le raisonnement éthique, la pensée systémique, la créativité, la résolution de problèmes, les communications et la conception axée sur la personne. De plus, ils devront compter sur du personnel dans les domaines des technologies de l'information (TI), du droit, des politiques, des ressources humaines, de l'approvisionnement et des finances doté des compétences et des connaissances nécessaires pour appuyer les initiatives en matière d'IA et ayant une diversité d'identités, de formation et de perspectives. Ces talents devront être identifiés, cultivés et utilisés à leur plein potentiel au moment et aux endroits où ils seront nécessaires.

***Le recrutement, le maintien en poste, la formation et le déploiement au sein du MDN et des FAC ne sont pas encore à la hauteur de ce défi.*** Les niveaux globaux de littératie des données sont faibles, les compétences en IA sont rares et le personnel doté de connaissances en IA se fait aussi rare. Même si les FAC reconnaissent leur propre besoin en matière de compétences en IA, elles ont souvent de la difficulté à utiliser le personnel spécialisé dont elles disposent déjà. Les membres estiment que leur spécialisation en IA et dans des domaines connexes limite leur carrière et affirment devoir choisir entre rester dans leur domaine technique et préférer un parcours de carrière qui les mènerait à une promotion. Il n'est pas étonnant que cette frustration amène les membres à demander une libération ou une mutation dans les réserves.

## Ce que nous devons faire

***Nous devons déterminer les besoins de nos effectifs et planifier en conséquence.*** Le MDN et les FAC doivent déterminer les habiletés, les perspectives et les compétences dont les membres de leur personnel militaire et civil auront besoin pour veiller à ce qu'ils puissent comprendre les nouvelles technologies, les assimiler dans l'environnement de combat et le milieu organisationnel et élaborer de nouveaux concepts opérationnels ainsi qu'établir de nouvelles organisations et stratégies, pour les utiliser

de manière efficace et éthique. Ce processus exigera que l'on détermine ce qui devra être cultivé au sein de l'organisation et ce qui pourra être sous-traité de manière sûre et efficace. Il faudra également tenir compte du caractère adéquat des compétences reconnues ainsi que des métiers, des classifications et des professions existants et du fait que les métiers, la gestion de carrière et la dotation pourraient devoir être revues pour être adaptées à l'IA. Étant donné le rythme rapide du développement technologique, il ne pourra pas s'agir d'un exercice ponctuel, mais plutôt d'un exercice continu afin d'établir l'équilibre des compétences exigées par ces technologies et pour veiller à ce que notre formation permette aux membres de notre personnel d'acquérir ces compétences, de les maintenir et de les utiliser de manière efficace et sûre. Une fois les besoins déterminés, ils devront éclairer une planification solide du recrutement militaire et des ressources humaines civiles. À cet égard, il faudra tenir compte de l'incidence de tels changements sur l'inclusion et la diversité de l'organisation.

***Nous devons cultiver la préparation à l'IA parmi les membres de notre personnel actuel.*** Nous devons d'abord assurer une littératie des données et numérique adéquate : sans ces compétences, il sera impossible de réaliser la mise en œuvre de l'IA. Nous devons être prêts à investir dans le perfectionnement continu des compétences de nos effectifs actuels et futurs afin de les aider à suivre le rythme du développement de l'IA en dehors de l'organisation, d'accélérer l'acquisition d'une expertise et de permettre aux membres de notre personnel d'évoluer dans leur carrière et de s'adapter à de nouveaux rôles à l'avenir. Une formation complète et de qualité supérieure en matière d'IA est largement disponible, souvent offerte gratuitement ou à un coût minime par des fournisseurs de logiciels; toutefois, le MDN et les FAC devront permettre aux membres de leur personnel de suivre une formation pendant les heures de travail. Ils devront également leur offrir des possibilités d'apprendre par la pratique et d'utiliser les compétences acquises afin de ne pas les perdre. Une formation plus précise relative aux compétences visant à appuyer l'utilisation de l'IA devra peut-être être élaborée à l'interne ou créée conjointement avec l'École de la fonction publique du Canada (EFPC) ou des fournisseurs privés. Il s'agira notamment d'une formation destinée aux dirigeants et aux décideurs relativement aux possibilités, aux risques et aux limites de l'IA et à la manière d'évaluer les décisions touchant les systèmes et de maintenir une participation humaine appropriée à ces décisions. La formation portera également sur les compétences générales nécessaires à la communication, à l'éthique, à l'idéation et à la conception ainsi que sur les compétences administratives nécessaires à l'acquisition, à la dotation et au maintien d'outils d'IA. En outre, ces compétences devront être revues régulièrement et adaptées en fonction de l'évolution des circonstances stratégiques, des capacités et de la technologie. Les programmes existants d'instruction militaire devront être revus et adaptés pour intégrer ces compétences et pour aborder des questions telles que l'éthique et les implications militaires des données et de la technologie avancée. De plus, alors que nous automatiserons les tâches répétitives, nous devrons prévoir le perfectionnement des compétences et la réaffectation des membres du personnel qui effectuaient auparavant ces tâches à des tâches plus complexes et gratifiantes nécessitant un jugement humain.

***Nous devons trouver de nouveaux moyens d'apporter des compétences critiques au sein de l'organisation ainsi que de les conserver et de les utiliser.*** Les compétences en matière d'IA et de données font l'objet d'une forte demande dans le secteur privé et nous devrons faire concurrence au secteur privé pour recruter et maintenir en poste des personnes dotées de ces compétences. Partout dans le monde, les forces armées essaient de nouvelles manières de repérer des personnes compétentes et de les recruter au sein de leurs effectifs réguliers, de réserve et civils ou en tant qu'entrepreneurs intégrés. Nous devrions tirer des enseignements de leurs initiatives. Nous devons aussi explorer des mécanismes flexibles, simplifiés et non traditionnels pour attirer des talents de classe mondiale en matière d'IA au sein de l'organisation et étendre l'accès à une expertise externe, y compris au moyen d'échanges de courte durée avec l'industrie et le milieu universitaire. Les parcours de carrière, le développement et la gestion des membres des FAC devront être revus et adaptés pour soutenir l'attraction et le maintien de talents liés à l'IA et pour permettre un avancement professionnel. Enfin, nous devons examiner des moyens d'utiliser la profondeur des compétences qui existe chez les membres actuels et potentiels de la Force de réserve. À cet égard, nous pourrions créer des réserves techniques et des parcours pour repérer et récompenser les compétences techniques en dehors des rangs traditionnels. Nous devons offrir aux Canadiens des moyens d'apporter leurs compétences au MDN et aux FAC à temps partiel dans des rôles qui leur permettent d'avoir un impact en utilisant des technologies de premier plan en matière d'IA pour résoudre des problèmes importants.

## COMMENT NOUS NOUS Y PRENDRONS

1. ***Examiner les besoins des effectifs du MDN et des FAC en matière d'IA.*** Le MDN et les FAC doivent examiner les besoins de leurs effectifs en matière d'IA afin de déterminer les habiletés, les compétences et le personnel nécessaires à la réussite de la mise en œuvre de l'IA. Ils doivent à cette fin tenir compte non seulement d'experts en matière d'IA, mais aussi des membres du personnel dont les rôles appuient le cycle de vie de l'IA, y compris les dirigeants civils et militaires. Un tel examen doit incorporer l'ACS Plus pour évaluer l'incidence de ces changements sur l'inclusivité et la diversité des effectifs.

2. ***Déterminer les exigences en matière de formation des effectifs qui sont prioritaires en matière d'IA et élaborer ou acquérir des programmes pour répondre à ces exigences***. Le MDN et les FAC doivent déterminer leurs besoins prioritaires et planifier en vue d'y répondre au moyen de l'élaboration de programmes internes, d'acquisitions externes et de partenariats avec le milieu universitaire. Cet examen devrait tenir compte des besoins en matière de formation à tous les échelons et de nouvelles options de formation universitaire et professionnelle afin de maintenir un bassin de talents permettant de répondre aux besoins futurs.

3. ***Examiner et identifier des processus pour recruter et conserver des talents en matière d'IA et pour les utiliser là où ils sont nécessaires.*** Le MDN et les FAC doivent explorer des voies et des processus non traditionnels pour repérer et affecter des personnes compétentes au bon endroit, par exemple au moyen d'échanges de courte durée, de la création de réserves techniques et de parcours de carrière plus souples permettant l'attraction de talents supérieurs au niveau d'entrée.

# LIGNE D'EFFORT 5 : PARTENARIATS

## Le défi

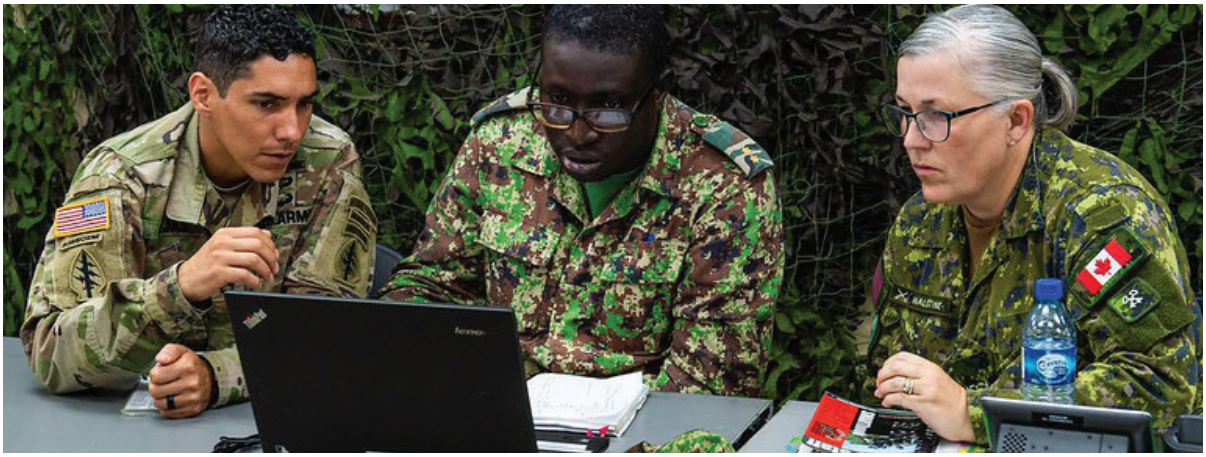
***La nature de la technique en matière d'IA est de nature collaborative — et souvent extérieure à la défense.*** À l'interne, la mise en œuvre et l'exploitation de l'IA nécessiteront la collaboration de nombreux membres de l'Équipe de la Défense, mais ce n'est que le début. À l'échelle mondiale, bien que l'on ait revendiqué que la recherche en matière de défense était à l'avant-garde de la technologie, les techniques et les applications d'IA les plus perfectionnées se trouvent aujourd'hui généralement dans l'industrie privée, le milieu universitaire et la communauté « source ouverte ». Le MDN et les FAC doivent donc être ouverts à l'acquisition, à la co-conception, à la co-élaboration, à la mise à l'essai et à la validation en collaboration avec des partenaires fiables. En outre, l'adoption de technologies basées sur l'IA nécessitera une coopération internationale entre des pays qui partagent les mêmes valeurs pour élaborer des principes, des politiques et des normes et en convenir ainsi pour développer et protéger des infrastructures numériques et une chaîne d'approvisionnement sécurisés avec les bonnes analyses.

***À l'heure actuelle, l'IA au sein du MDN et des FAC nécessite une coordination qui découlerait de partenariats.*** Le MDN et les FAC doivent continuer d'exploiter activement des possibilités de collaboration en matière de défense, de sécurité et de sûreté avec des partenaires d'autres ministères et organismes, de l'industrie, du milieu universitaire et des alliés internationaux afin de maximiser les avantages stratégiques de l'écosystème d'innovation du Canada et de le protéger contre les adversaires et les menaces. Les activités d'engagement, de mobilisation et de sensibilisation doivent couvrir l'ensemble du spectre de l'innovation, y compris l'échange de renseignements scientifiques, techniques et de personnel, le partage de données, des cadres élaborés conjointement, des essais, des expériences, des démonstrations de technologies conceptuelles de pointe et la consultation de communautés de pratique.

## Ce que nous devons faire

***Nous devons veiller à ce que l'innovation soit adaptable et interopérable.*** L'élaboration d'une vision stratégique en matière d'IA harmonisée avec les alliés de la défense du Canada, y compris le partenariat avec le Groupe des cinq, le Programme de coopération technique (TTCP) et nos alliés de l'OTAN, permettra au MDN et aux FAC de prioriser et de poursuivre la recherche en matière d'IA relative aux capacités interopérables, tout en partageant les pratiques exemplaires actuelles concernant l'élaboration d'une capacité militaire en matière d'IA et la formation du personnel quant à son utilisation. Cela offrira également des possibilités d'investissement stratégique dans des technologies qui compléteront celles de nos partenaires de défense.

***Nous devons nous employer à développer et à exploiter un écosystème d'IA en matière de défense et de sécurité.*** Le Canada, ainsi que le MDN et les FAC, bénéficie du développement des talents et de la concurrence dans le domaine de l'IA. Il est dans l'intérêt



du MDN et des FAC de favoriser un écosystème d'innovation en matière de défense dynamique, diversifié, souple et réactif en tirant parti de celui déjà créé en vertu de la Stratégie d'IA pancanadienne et administré par l'Institut canadien de recherches avancées (CIFAR). L'expérience du CIFAR prouve clairement que cela est possible. Toutefois, il faudra des outils novateurs en matière de collaboration avec l'industrie, le milieu universitaire et des partenaires non traditionnels afin de maximiser la détermination et l'exploitation de capacités conjointes, d'accélérer les acquisitions et de faciliter l'accès à des experts en vue d'affectations de courte durée. À cette fin, nous devrons identifier des possibilités en matière de double usage ou spécifiques à la défense et collaborer avec des petites et moyennes entreprises pour mettre en œuvre des capacités à usage limité et évolutives. Cela nécessitera également des efforts pour surmonter les obstacles à la participation efficace de l'industrie, à l'harmonisation de l'infrastructure numérique qui soutient la collaboration externe et à la protection de la propriété intellectuelle. Enfin, il faudra un engagement à long terme en matière d'investissement au-delà d'une expérimentation à grande échelle.

***Nous devons continuer d'innover en partenariat avec des secteurs externes.*** Des partenariats solides avec le secteur privé et des établissements universitaires à la fine pointe des avancées en matière d'IA seront essentiels à toutes les étapes du cycle de vie de l'IA, notamment la recherche, la validation, la certification, la mise en service, le maintien et la mise hors service. Le MDN et les FAC doivent accroître leurs partenariats avec le milieu universitaire et l'industrie pour identifier, définir, financer et permettre des percées dans le domaine de l'IA. Cette collaboration devrait comprendre des modèles de financement traditionnels et des initiatives existantes telles que la Mobilisation des idées nouvelles en matière de défense et de sécurité (MINDS) et Innovation pour la défense, l'excellence et la sécurité (IDEeS); toutefois, elle devrait également comporter une utilisation accrue d'approches novatrices, comme de grands défis, des marathons de programmation et des séances de conception créative avec de jeunes entreprises et des intégrateurs pour concevoir et élaborer conjointement des solutions basées sur l'IA à la fine pointe de la technologie. Nous devons également explorer des partenariats non traditionnels. La défense a beaucoup à apprendre de partenaires non traditionnels tels que la société civile, les secteurs non techniques du milieu universitaire et la communauté « source ouverte ».

***Nous devons approfondir la collaboration avec d'autres ministères pour générer des gains d'efficacité et une approche commune.*** Aux fins d'économie d'effort et d'interopérabilité, le MDN et les FAC doivent s'employer à co-élaborer et à échanger des capacités d'IA avec d'autres ministères, en particulier avec les ministères et les organismes avec lesquels nous partageons des responsabilités en matière de sécurité nationale. Une approche pangouvernementale permettra un transfert de technologie, une amélioration de l'établissement de relations externes et de partenariats, ainsi que l'acquisition d'une technologie d'IA profitable pour tous les domaines.

***Nous devons établir des lignes directrices pour veiller à ce que nos partenariats soient fiables et sûrs.*** Nous savons que nos alliés, l'industrie et le milieu universitaire sont constamment ciblés par des adversaires potentiels, de sorte que notre dépendance à l'égard de partenaires en matière d'IA pourrait constituer une source de vulnérabilité stratégique. Cela s'applique en particulier aux technologies à double usage. Les chercheurs universitaires travaillent souvent au sein de réseaux mondiaux dont les limites et l'adhésion peuvent être difficiles à protéger, alors que des entreprises canadiennes continuent de faire l'objet d'un espionnage industriel et peuvent éprouver des vulnérabilités liées à leur chaîne d'approvisionnement. Nous devons donc investir dans la recherche et le développement de lignes directrices afin de veiller à ce que nos partenariats soient convenablement protégés contre les menaces extérieures.

## COMMENT NOUS NOUS Y PRENDRONS

1. ***Renforcer les partenariats stratégiques et la collaboration avec nos alliés en matière de nouvelles capacités, de pratiques exemplaires et de leçons retenues.*** À cet égard, nous devrions développer notre collaboration stratégique avec le Groupe des cinq, le TTCP et l'OTAN, mais aussi approfondir la coopération bilatérale avec des pays fiables dans des domaines précis d'intérêt commun.

2. ***Contribuer à améliorer le processus d'approvisionnement pour soutenir le développement et l'acquisition d'une IA qui permet d'équilibrer la sûreté, la sécurité, l'éthique et la nécessité de maintenir une souplesse et une agilité.*** Nous devons continuer de collaborer avec Services publics et Approvisionnement Canada (SPAC) pour déterminer les exigences précises et les possibilités visant à simplifier et à accélérer les processus d'approvisionnement. Cela réduira les obstacles administratifs à la participation d'innovateurs canadiens, accroîtra la diversité des fournisseurs et améliorera les perspectives économiques et sociales pour les groupes sous-représentés. Les changements relatifs à l'approvisionnement devraient également encourager les organisations à identifier l'IA et ses bases techniques, telles que les infrastructures de données et numériques, dans les exigences en matière de capacités.

3. ***Contribuer à des activités qui favorisent des infrastructures de données sécurisées et fiables et le partage avec nos partenaires et nos alliés,*** en travaillant à bâtir des ensembles de données communs pour élaborer des solutions interopérables.

4. ***Renforcer les liens avec le milieu universitaire pour favoriser le développement des compétences en appui aux exigences en matière de défense.*** Nous devons favoriser des partenariats novateurs au moyen d'échanges de personnel, comme l'initiative de mobilité, pour permettre l'échange de personnel entre les partenaires d'IDEeS. Nous devons également rechercher des possibilités de nouveaux parcours de formation pour établir un bassin de talents en matière de défense.

5. ***Développer et favoriser davantage l'écosystème d'innovation en matière de défense et de sécurité en partenariat avec l'écosystème d'innovation pancanadien en matière d'IA.*** Nous devons explorer des pistes de partage de compétences et d'affectations pour déployer les talents de manière souple dans tous les secteurs. Nous devrons également accroître les liens et le soutien à l'égard de solutions novatrices face aux défis en matière de défense et favoriser des processus permettant d'étendre ces initiatives à l'ensemble de l'Équipe de la Défense. Cela pourrait comprendre des mécanismes existants, tels que les centres de recherche ainsi que les programmes MINDS et IDEeS, mais aussi de nouvelles lignes de financement à l'appui des capacités et des mécanismes militaires prioritaires pour proposer des défis à l'industrie. Ce faisant, nous devrons adopter une approche stratégique en matière de recherche et développement dans les domaines où nous pourrons prendre appui sur les atouts existants du Canada.

6. ***Collaborer avec des partenaires gouvernementaux pour veiller à ce que les intérêts en matière de défense et de sécurité soient pris en compte dans la conception de l'écosystème d'innovation canadien.*** L'écosystème d'innovation devra être protégé contre les actes d'adversaires et soutenu pour établir des liens avec l'environnement de la défense. À cet égard, nous devrions accorder une attention à la sécurité de la chaîne d'approvisionnement et à la nécessité d'un contrôle des exportations concernant les technologies canadiennes sensibles. Nous devrons également assurer une cohésion et une cohérence dans le domaine de la réglementation afin de réduire les fardeaux administratifs liés à la conformité imposés aux non-spécialistes.

# CONCLUSION

L'IA recèle un énorme potentiel en matière de défense. Des capacités basées sur l'IA peuvent nous permettre d'améliorer la précision de nos renseignements, de notre ciblage, de notre connaissance de la situation et de notre prise de décisions, tout en permettant des gains d'efficacité logistiques et organisationnels et une amélioration des services. Cependant, pour réaliser ces gains, nous devons mettre en place les environnements, les pratiques de gestion des données et les dispositifs de protection nécessaires afin de veiller à ce que l'IA soit sûre, éthique, inclusive, légale et fiable. Nous devons gérer le changement de manière à soutenir l'innovation et nous assurer que les membres de notre personnel, aujourd'hui et à l'avenir, disposeront de la formation et des compétences nécessaires pour mettre en œuvre avec succès des initiatives liées à l'IA. Nous devons également créer des partenariats à l'extérieur de l'organisation afin de tirer profit d'innovations prometteuses et ainsi nous assurer que nos capacités habilitées par l'IA complètent celles de nos partenaires de défense et qu'elles sont interopérables avec ces capacités.

La Stratégie d'IA expose la vision quant à l'adoption et à la mise en œuvre de l'IA et de technologies algorithmiques connexes au sein de l'Équipe de la Défense ainsi que cinq lignes d'effort pour réaliser cette vision. Les objectifs qu'elle comporte sont nécessaires pour établir la voie à suivre, harmoniser les attentes concernant le MDN et les FAC au niveau de l'organisation et intégrer la pensée, l'effort et l'objectif vers ce but commun. Toutefois, ces seuls objectifs ne seront pas suffisants pour nous permettre d'atteindre notre but. Afin de réaliser cette vision et ces lignes d'effort, le Bureau de la transformation numérique élaborera un plan de mise en œuvre par étapes ainsi que des échéanciers, des jalons et des indicateurs de rendement, en s'appuyant sur l'approche interfonctionnelle adoptée pour élaborer la présente Stratégie. On élaborera également un modèle de gouvernance et un cadre de responsabilisation en matière d'IA afin de veiller à ce que la mise en œuvre proprement dite soit réussie et bien gérée.