



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.

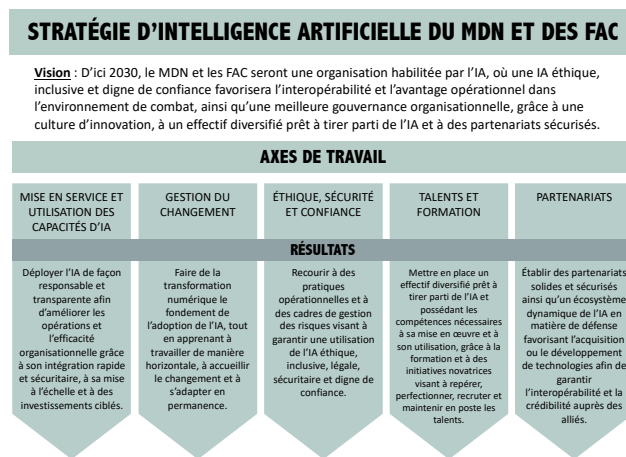
Matthew da Mota est directeur de la recherche, Technologies émergentes et sécurité nationale au Canadian Shield Institute for Public Policy. Son travail explore comment les technologies émergentes et les dynamiques géopolitiques changeantes redéfinissent la sécurité, la gouvernance, la connaissance et 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

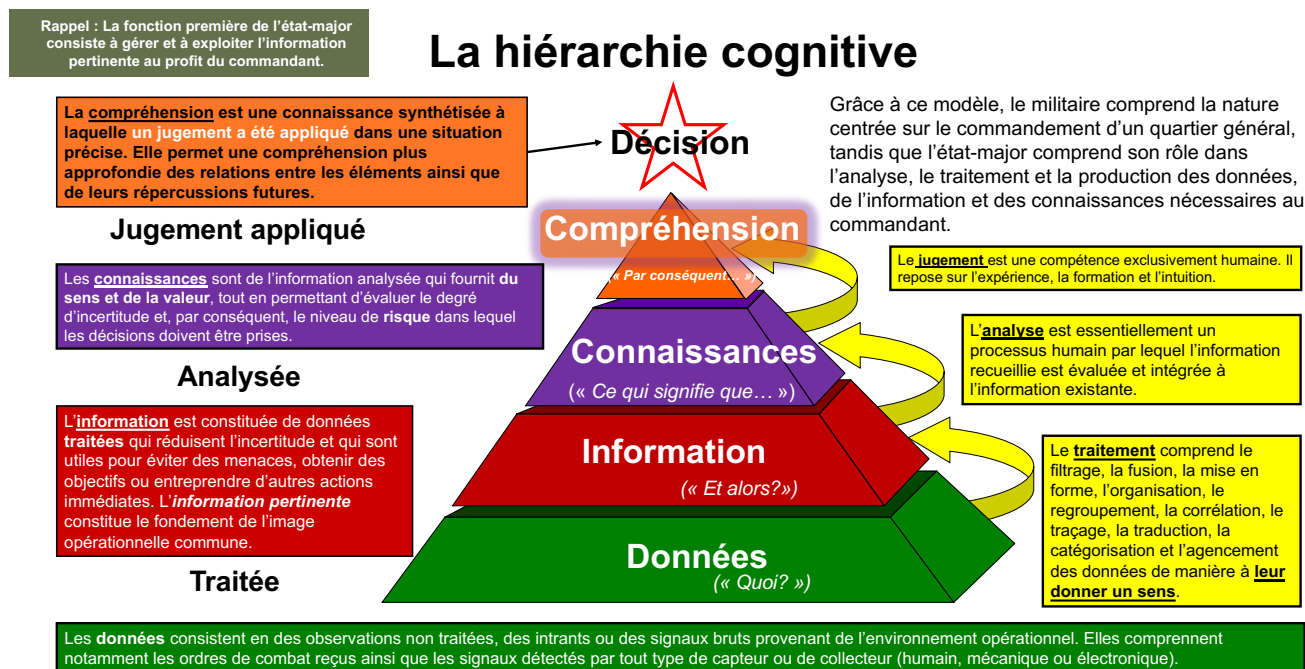
Tout comme la navigation céleste sur l'océan, l'intégration de l'IA au sein du MDN et des FAC nécessite des points de référence fixes pour maintenir le cap et l'azimut. Le sextant mesure les angles entre les corps célestes connus et l'horizon; l'astrocompas aide à déterminer le vrai nord. En ce qui concerne 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_fbab3ad/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-crtesp.gc.ca/fpslreb-crtesp/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>.