

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

**JENNIFER GEAREY ET MAJOR TYLER CURRIE**

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

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

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

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

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

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

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

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

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

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



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

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

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

## L'IA en tant que défi stratégique

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

## Approvisionnement, volatilité du marché et économie de la rapidité

Le MDN et les FAC avec leurs alliés peuvent avoir un avantage en ce qui concerne les puces avancées et les plateformes info-nuagiques, mais cet avantage ne vaut pas grand-chose si les gouvernements ne peuvent pas acheter et déployer rapidement de nouveaux outils. Aujourd'hui, l'approvisionnement est souvent le goulot d'étranglement. Les processus concurrentiels lents pour l'achat des grands systèmes universels peuvent prendre tellement de temps que la technologie devient obsolète avant même d'être obtenue. Au Canada, les grands cycles d'approvisionnement dans le domaine de la défense peuvent durer sept ou huit ans.<sup>30</sup> Les méthodes d'évaluation ont tendance à récompenser les fournisseurs familiers plutôt que ceux qui innovent<sup>31</sup>. Les contestations juridiques peuvent retarder les progrès pendant des mois, voire des années. Pendant ce temps, la technologie de l'IA évolue tous les trois à six mois, et non chaque décennie.<sup>32</sup>

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

## Conclusion

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

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

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

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

## Notes

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

- AI: Buy What Works, Skip the Build », Government Technology Insider, 8 juillet 2025. Tiré de <https://governmenttechnologyinsider.com/the-fast-track-to-mission-ready-ai-buy-what-works-skip-the-build/>.
- 15 Margarida Silva, Jasper van Teeffelen et Çağrı Çavuş, « Big Tech Acquires a New Company Every 11 Days », SOMO, 15 avril 2025, <https://www.somo.nl/big-tech-acquires-a-new-company-every-11-days/>.
  - 16 Didi Tang et Collin Binkley, « Pentagon-Funded Research at Colleges Has Aided the Chinese Military, a House GOP Report Says », AP News, 5 septembre 2025. Tiré de <https://apnews.com/article/china-pentagon-funding-research-military-bf8640d0e04c0164af513350078d58c>.
  - 17 U.S. National Security Agency et Cybersecurity and Infrastructure Security Agency, Use Secure Cloud Key Management Practices, mars 2024. Tiré de <https://media.defense.gov/2024/Mar/07/203407858/-1/-1/0/CSI-CloudTop10-Key-Management.PDF>.
  - 18 Office of the Under Secretary of Defense for Research and Engineering, Software Engineering for Continuous Delivery of Warfighting Capability, U.S. Department of Defense, avril 2023. Tiré de <https://www.cto.mil/wp-content/uploads/2023/07/SWE-Guide-April2023.pdf>.
  - 19 James Kavanagh, « AI Model Lifecycle Governance », Ethos AI, 23 juin 2025. Tiré de <https://www.ethos-ai.org/p/ai-model-lifecycle-governance?>
  - 20 Cybersecurity and Infrastructure Security Agency, Securing the Software Supply Chain: Recommended Practices for Suppliers, Department of Homeland Security, septembre 2022. Tiré de [https://www.cisa.gov/sites/default/files/2024-08/SECURING\\_THE\\_SOFTWARE\\_SUPPLY\\_CHAIN\\_SUPPLIERS\\_508.pdf](https://www.cisa.gov/sites/default/files/2024-08/SECURING_THE_SOFTWARE_SUPPLY_CHAIN_SUPPLIERS_508.pdf).
  - 21 Par exemple, la loi américaine CLOUD Act impose aux prestataires relevant de la juridiction des États-Unis de conserver et de communiquer les données, dont ils ont la possession, la garde ou le contrôle, que ces données se trouvent ou non sur le territoire américain.
  - 22 Forum économique Mondial et Accenture, Blueprint to Action: China's Path to AI-Powered Industry Transformation, janvier 2025. Tiré de [https://reports.weforum.org/docs/WEF\\_Blueprint\\_to\\_Action\\_Chinas\\_Path\\_to\\_AI-Powered\\_Industry\\_Transformation\\_2025.pdf](https://reports.weforum.org/docs/WEF_Blueprint_to_Action_Chinas_Path_to_AI-Powered_Industry_Transformation_2025.pdf).
  - 23 Robert O. Work et Tara Murphy Dougherty, « It's Time for the Pentagon to Take Data Principles More Seriously », War on the Rocks, 6 octobre 2020. Tiré de <https://warontherocks.com/2020/10/its-time-for-the-pentagon-to-take-data-principles-more-seriously/>.
  - 24 Harry Davies et Yuval Abraham, « Revealed: Microsoft Deepened Ties with Israeli Military to Provide Tech Support During Gaza War », The Guardian, 23 janvier 2025. Tiré de <https://www.theguardian.com/world/2025/jan/23/israeli-military-gaza-war-microsoft>.
  - 25 Brodi Kotila et al., Strengthening the Defense Innovation Ecosystem, RAND Corporation, 7 mars 2023. Tiré de [https://www.rand.org/content/dam/rand/pubs/research\\_reports/RR1300/RR1352-1/RAND\\_RRA1352-1.pdf](https://www.rand.org/content/dam/rand/pubs/research_reports/RR1300/RR1352-1/RAND_RRA1352-1.pdf).
  - 26 Stefan Vladislavjev, « Surveying China's Digital Silk Road in the Western Balkans », War on the Rocks, 3 août 2021. Tiré de <https://warontherocks.com/2021/08/surveying-chinas-digital-silk-road-in-the-western-balkans/>.
  - 27 Thomas Morley et Matthew Schrader, « Huawei Espionage Arrests in Poland: A Wake-Up Call to Europe », German Marshall Fund of the United States, consulté le 25 septembre 2025. Tiré de <https://www.gmfus.org/news/huawei-espionage-arrests-poland-wake-call-europe>.
  - 28 Innovation, Sciences et Développement économique Canada, « Énoncé de politique - Sécuriser le système de télécommunications au Canada », Gouvernement du Canada, 19 mai 2022. Tiré de <https://www.canada.ca/fr/innovation-sciences-developpement-economique/nouvelles/2022/05/enonce-de-politique--securiser-le-systeme-de-telecommunications-au-canada.html>.
  - 29 Darren Death, « Understanding and Addressing Supply Chain Risks in AI Systems », LinkedIn, 8 janvier 2025, <https://www.linkedin.com/pulse/understanding-addressing-supply-chain-risks-ai-systems-death-kz2jc>.
  - 30 Chambre des communes du Canada, Comité permanent de la défense nationale, Témoignages, 45<sup>e</sup> législature, 1<sup>re</sup> session, réunion n° 9, 23 octobre 2025. Tiré de <https://www.noscommunes.ca/documentviewer/fr/45-1/NDDN/reunion-9/temoignages>.
  - 31 Chloe Autio, Kate Cummings, Brinson S. Elliott et Beth Simone Noveck, A Snapshot of Artificial Intelligence Procurement Challenges: Diagnosing Perceived and Actual Risks Impeding Responsible AI Acquisition, The GovLab, 2023. Tiré de <https://files.thegovlab.org/a-snapshot-of-ai-procurement-challenges-june2023.pdf>.
  - 32 Akhil Gupta, « Government AI Adoption: Unique Challenges in Pricing and Procurement », Agentic AI Pricing, 6 janvier 2025. Tiré de <https://www.agenticai-pricing.com/government-ai-adoption-unique-challenges-in-pricing-and-procurement/>.
  - 33 Recherche et développement pour la défense Canada (RDDC) mène depuis longtemps des travaux sur l'IA, notamment dans les domaines de la connaissance de la situation, de la surveillance, de la cyberdéfense et de la détection des menaces. Parmi les initiatives susceptibles de soutenir le développement et la commercialisation de solutions canadiennes d'IA pour la défense figurent le programme Innovation pour la défense, l'excellence et la sécurité (IDEES) et le Bureau de recherche, d'ingénierie et de leadership avancés en matière d'innovation et de science (BOREALIS). Le programme Mobilisation des idées nouvelles en matière de défense et de sécurité (MINDS) joue un rôle distinct, axé sur la recherche, l'expertise externe et l'élaboration des politiques.
  - 34 Par l'intermédiaire du service d'adoption rapide du DIANA de l'OTAN, le MDN et les FAC sont en voie d'acquiescer un véhicule autonome sans équipage auprès d'une entreprise appelée HonuWorx. Ce véhicule sera contrôlé au moyen d'une plateforme de mission infonuagique et contribuera à la capacité du MDN et des FAC d'entretenir, d'exploiter et de manipuler des infrastructures en eaux profondes ainsi que d'autres objets sous-marins.
  - 35 Alex McPhail, Alexander Rudolph et Philippe Lagassé, rapport final du projet « Aperçu et analyse de l'approvisionnement agile de la Défense (AAAAD) », EXA Consulting Group, 10 juillet 2025. Tiré de <https://static1.squarespace.com/static/5cd08376797f7421f5ea7c-c/t/68af61b380a0f3571c695ae9/1756324275338/Final+Report++Defence+Agile+Procurement+Insights+and+Analysis.pdf>.
  - 36 Carlo Munoz, « Le Pentagone lance l'initiative d'accélération de l'infonuagique de la JWCC », Janes, 31 octobre 2024. Tiré de <https://www.janes.com/osint-insights/defence-news/defence/pentagon-rolls-out-jwcc-cloud-accelerator-initiative>.
  - 37 U.S. Defense Innovation Board, Scaling Nontraditional Defense Innovation, U.S. Department of Defense, 8 janvier 2025. Tiré de <https://innovation.defense.gov/Portals/63/DIB%20Scaling%20Nontraditional%20Defense%20Innovation%20250113%20PUBLISHED.pdf>.
  - 38 MITRE Corporation, AI Red Teaming: Advancing Safe and Secure AI Systems, juillet 2024. Tiré de <https://www.mitre.org/sites/default/files/2024-07/PR-24-01820-4-AI-Red-Teaming-Advancing-Safe-Secure-AI-Systems.pdf>.
  - 39 Pour obtenir d'autres lignes directrices sur ces pratiques d'évaluation, voir le *Responsible AI Toolkit* du département de la Défense des É.-U., qui propose des outils d'évaluation du cycle de vie et d'assurance pour les systèmes d'IA; voir aussi le JSP 936 du ministère de la Défense du R.-U., qui établit les exigences pour des capacités d'AI de défense fiables, sécuritaires et robustes. Voir : Department of Defense, *Responsible Artificial Intelligence (RAI) Toolkit*, Chief Digital and Artificial Intelligence Office, 14 novembre 2023, <https://rai.tradewindai.com/>; Ministry of Defence, JSP 936: *Dependable Artificial Intelligence (AI) in Defence (Part 1: Directive)*, 13 novembre 2024. Tiré de <https://www.gov.uk/government/publications/jsp-936-dependable-artificial-intelligence-ai-in-defence-part-1-directive>.
  - 40 U.S. Congress, Senate Committee on Small Business and Entrepreneurship, Golden Age of American Innovation: Reforming SBIR-STTR for the 21<sup>st</sup> Century, S. Hrg. 119-20, 119<sup>th</sup> Cong., 1<sup>st</sup> sess., 5 mars 2025. Tiré de <https://www.digitaljournal.com/business/canadas-innovation-pipeline-is-stalling-sir-michael-houghton-calls-for-a-vc-mind-set-shift/article>.
  - 41 U.S. Congress, Senate Committee on Small Business and Entrepreneurship, Golden Age of American Innovation: Reforming SBIR-STTR for the 21<sup>st</sup> Century, S. Hrg. 119-20, 119<sup>th</sup> Cong., 1<sup>st</sup> sess., 5 mars 2025. Tiré de <https://www.congress.gov/event/119th-congress/senate-event/LC74425/text>.
  - 42 IBM, « Qu'est-ce que la gestion des coûts liés au cloud? », 5 octobre 2023. Tiré de <https://www.ibm.com/fr-fr/think/topics/cloud-cost-management>.
  - 43 Secrétariat du Conseil du Trésor du Canada, *Livre blanc du gouvernement du Canada sur la souveraineté des données et le nuage public*, Gouvernement du Canada, 2018. Tiré de <https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/innovations-gouvernementales-numeriques/services-informatique-nuage/souverainete-numerique/qc-livre-blanc-souverainete-donnees-nuage-public.html>.
  - 44 Organisation du Traité de l'Atlantique Nord, « Approche de l'OTAN pour la lutte contre les menaces informationnelles », 3 février 2025. Tiré de <https://www.nato.int/fr/what-we-do/wider-activities/natos-approach-to-counter-information-threats>.
  - 45 Ann M. Fitz-Gerald, Carsten Maple et Halyna Padalko, « Collaborative AI Governance: A Policy Roadmap for Canada and the UK », Royal United Services Institute, 13 novembre 2024. Tiré de <https://www.rusi.org/explore-our-research/publications/commentary/collaborative-ai-governance-policy-roadmap-canada-and-uk>.
  - 46 Steve Feldstein, « The Global Expansion of AI Surveillance », Carnegie Endowment for International Peace, 17 septembre 2019. Tiré de <https://carnegieendowment.org/research/2019/09/the-global-expansion-of-ai-surveillance?lang=en>.
  - 47 Centre canadien pour la cybersécurité, Évaluation des cybermenaces nationales 2025-2026, Gouvernement du Canada, 2024. Tiré de <https://www.cyber.gc.ca/sites/default/files/evaluation-cybermenaces-nationales-2025-2026-f.pdf>.
  - 48 Service canadien du renseignement de sécurité, « Protection des jeunes pousses technologiques : exploitation des concours de pitch internationaux », 8 septembre 2025.
  - 49 Pew Research Center, Representative Democracy Remains a Popular Ideal, but People Around the World Are Critical of How It's Working, Washington, DC : Pew Research Center, 28 février 2024. Tiré de [https://www.pewresearch.org/global/wp-content/uploads/sites/2/2024/02/gap\\_2024.02.28\\_democracy-closed-end-report.pdf](https://www.pewresearch.org/global/wp-content/uploads/sites/2/2024/02/gap_2024.02.28_democracy-closed-end-report.pdf).