



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

Caporale Connie Valin, photo des Forces armées canadiennes

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

SAMUEL PAQUETTE ET MAJOR TYLER CURRIE

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

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

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

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

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

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

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

La volatilité des marchés et la disponibilité opérationnelle

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

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

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

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

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

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

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

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

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

Les frictions liées à l'approvisionnement

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

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

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

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

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

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

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

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

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

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

Les normes de l'OTAN et la cohésion

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

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

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

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

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

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

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

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

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

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

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

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

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

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

La gouvernance comme catalyseur

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Conclusion

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

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

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

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

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

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

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

Notes

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

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

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

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

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

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

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

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