Août 2026 – Numéro 7

# Forum politique

## Quels avantages ou risques en matière de sécurité avec l'IA?

*Policy Forum Politique* est une série de publications visant à stimuler le débat en présentant un large éventail d'avis d'experts sur un sujet d'importance pour la sécurité nationale du Canada. Pour cette septième édition, nous avons demandé à quatre experts de nous faire part de leur point de vue sur la question suivante : *En juin 2026, le Canada a dévoilé sa nouvelle stratégie en matière d'intelligence artificielle (IA). Bien que cette stratégie fasse largement état des avantages économiques liés à l'adoption de l'IA, elle reste muette sur les considérations sécuritaires ou militaires, même si elle préconise certaines capacités souveraines. Quels avantages ou risques en matière de sécurité le gouvernement du Canada devrait-il prendre en compte lorsqu'il réfléchit à l'IA?*

**Matthew da Mota | Canadian Shield Institute**

*Matthew est directeur de recherche en technologies émergentes et sécurité nationale au Canadian Shield Institute. Ses travaux portent sur la manière dont les technologies émergentes et l'évolution de la dynamique géopolitique redéfinissent la gouvernance, le savoir et la souveraineté, en mettant particulièrement l'accent sur les répercussions de l'intelligence artificielle et des infrastructures numériques sur la sécurité nationale.*

La nouvelle stratégie canadienne en matière d'IA promet des possibilités et préconise le développement de capacités souveraines, mais elle traite la souveraineté comme une question industrielle axée sur la puissance de calcul, les micropuces, les modèles et les centres de données. Cette perspective confond propriété et contrôle. La souveraineté qui importe est d'ordre épistémique, et elle repose sur la gouvernance : la capacité de définir les conditions selon lesquelles l'IA s'intègre aux institutions qui détiennent le savoir du Canada, et de préserver le jugement humain qui vérifie la qualité de ce savoir.

L'IA générative sape ces deux aspects. La désinformation et les « deepfakes » sont peu coûteux à produire; les individus peuvent se replier sur des machines privées de rétroaction flagorneuses; et il suffit d'un nombre étonnamment faible d'entrées malveillantes pour corrompre un modèle d'IA largement utilisé. C'est la confiance dans l'information elle-même qui est en jeu. Un adversaire n'a pas besoin de vaincre le Canada sur un champ de bataille où l'IA est mise à contribution; il lui suffit de pousser les Canadiens à se méfier de leurs propres connaissances. Or, les modèles sur lesquels repose cet environnement dépendent de quelques entreprises privées étrangères, qui échappent à la gouvernance canadienne. Une plus grande souveraineté informatique n'y changerait rien.

L'armée n'est pas épargnée. À mesure que l'IA s'intègre dans la boucle décisionnelle, elle risque de nuire au jugement qu'elle est censée soutenir, par le biais de biais, d'une atrophie des compétences et d'une responsabilité floue lorsque les décisions sont éclairées, ou prises, par des acteurs non humains.

Un danger encore plus profond réside dans le fait de succomber à la tentation de remplacer des systèmes de connaissances durement acquis et éprouvés par des systèmes automatisés avant même de saisir ce que nous sommes en train de céder. Ce problème est aggravé par le fait que nous ne comprenons pas comment l'IA va remodeler l'espace de combat. Nous ne pouvons donc pas juger dans quelle mesure nous pouvons nous y fier. En s'y engageant trop, le Canada s'expose à ces risques; en s'y engageant trop peu, il cède du terrain stratégique.

Le plus grand risque pour la sécurité, mais aussi la plus grande occasion, que présente l'IA réside dans son potentiel à transformer de façon irréversible l'environnement du savoir. La capacité souveraine doit impliquer la gestion du flux de connaissances et la préservation délibérée du jugement humain indépendant — une infrastructure du savoir suffisamment résiliente pour soutenir l'IA et qui ne serait donc pas compromise par celle-ci. Concrètement, Ottawa devrait investir dans une infrastructure publique de recherche et de données digne de confiance — des dépôts sécurisés dont la provenance est vérifiable et dont l'intégrité est protégée — et établir des modalités de gouvernance régissant la manière dont l'IA est acquise et intégrée dans les institutions publiques, en trouvant un équilibre entre la sécurité de la recherche et la science ouverte. Poser d'abord ces fondements permet d'intégrer l'IA à une base de connaissances à laquelle les Canadiens peuvent faire confiance, plutôt que d'adopter l'IA pour ensuite seulement tenter de donner un sens aux systèmes hybrides homme-IA qu'elle crée. »

**Balkan Devlen | Institut de Montréal pour la sécurité mondiale**

*Balkan Devlen est chercheur principal en prospective stratégique à l'Institut de Montréal pour la sécurité mondiale (MIGS), chercheur principal à l'Institut Macdonald-Laurier (MLI) et professeur de recherche associé à l'Université Carleton.*

La nouvelle stratégie d'Ottawa en matière d'IA est un document bien conçu qui aborde un problème bien précis. Elle vise à inciter davantage d'entreprises à adopter l'IA, à accroître la puissance de calcul sur le sol canadien et à réduire la dépendance vis-à-vis des nuages étrangers. Cependant, sa conception de l'exposition se limite aux centres de données et aux chaînes d'approvisionnement, et sa conception de la protection des Canadiens se limite à la vie privée et aux préjudices en ligne. Certes, ce sont là des préoccupations réelles, mais ce ne sont pas celles qui empêchent de dormir les milieux de la sécurité et du renseignement, tant au Canada que chez nos alliés.

Les risques qui font de l'IA avancée un enjeu de sécurité nationale plutôt qu'un dossier de politique industrielle sont ceux qui pourraient s'avérer irréversibles. L'Institut pour la politique et la stratégie en matière d'IA les regroupe en trois catégories : la perte de contrôle, où des systèmes performants échappent à la surveillance humaine; la concentration extrême du pouvoir, où celui qui maîtrise en premier ces systèmes s'assure un avantage qu'aucun rival ni aucun électorat ne pourra contester par la suite; et la guerre entre grandes puissances, où la course elle-même — par erreur d'appréciation, action préventive ou instabilité liée à la course aux armements — prend une

tournure cinétique. D'autres ajoutent une quatrième préoccupation : l'utilisation abusive catastrophique ou malveillante — pensez aux armes biologiques basées sur l'IA ou à la subversion de masse par le biais d'une guerre politique hyper-individualisée à grande échelle.

Il ne s'agit pas là d'histoires de science-fiction transposées dans le domaine politique. Trois de ces risques sur quatre (à l'exception de la perte de contrôle) peuvent devenir réalité avant même que les systèmes d'IA ne surpassent l'intelligence humaine. Le Bureau du Conseil privé a coorganisé avec le CIGI un exercice de simulation qui a permis aux responsables de se familiariser avec ces risques et qui a conclu que les gouvernements doivent se préparer dès maintenant à l'arrivée, d'ici cinq ans, de systèmes dotés d'une intelligence équivalente à celle des humains ou surhumaine. Plus de trente députés et sénateurs de tous les partis ont qualifié la superintelligence de priorité en matière de sécurité nationale.

L'objection évidente — le Canada ne développera pas d'intelligence artificielle générale (AGI), alors pourquoi s'y préparer? — repose sur un raisonnement erroné. C'est précisément parce que nous ne la développerons pas que nous avons toutes les raisons de façonner les règles et les résultats tant que nous le pouvons encore. Une stratégie à 360 degrés aurait identifié ces quatre risques comme des enjeux de sécurité pour le Canada et leur aurait attribué un mandat et un budget. Les États qui traitent l'IA avancée uniquement comme un dossier d'adoption seront régis par des décisions prises ailleurs. Espérons que la Stratégie de sécurité nationale tant attendue abordera ces questions.

**Jennifer Irish | Pendulum Geopolitical Advisory**

*Jennifer Irish est professeure auxiliaire à l'Université d'Ottawa (Telfer) et directrice de Pendulum Geopolitical Advisory. Ancienne diplomate canadienne, elle a été directrice fondatrice du Laboratoire de l'intégrité de l'information de l'Université d'Ottawa.*

**Dave McMahon| Clairvoyance Corp**

*Dave McMahon est chef de la direction de Clairvoyance Corp et chef de l'intelligence chez Sapper Labs. Dave a également occupé divers postes de direction au sein des Forces armées canadiennes, du Service canadien du renseignement de sécurité (SCRS) et du Centre de la sécurité des télécommunications (CST).*

Les progrès rapides de l'IA transforment le secteur canadien de la sécurité, du renseignement et de la défense. L'IA est à la fois un catalyseur et un facteur de bouleversement, et la capacité du Canada à maximiser ses avantages tout en réduisant les risques dépendra non seulement de sa stratégie en matière d'IA, mais aussi d'investissements complémentaires dans la sécurité, l'intégrité de l'information, la résilience et des partenariats de confiance.

L'IA offre des possibilités considérables pour progresser davantage dans l'analyse des mégadonnées, la curation et l'évaluation du renseignement, la cybersécurité, les opérations de défense et la prise de décision fondée sur l'évaluation des risques.

Parallèlement, le Canada est confronté à un environnement de menaces de plus en plus complexe, où la technologie est un élément déterminant de la concurrence et des conflits géopolitiques. L'IA générative permet la création de « deepfakes », de médias synthétiques et de campagnes de désinformation à grande échelle qui sapent la confiance du public. Elle peut également faciliter la

répression transnationale, l'exploitation en ligne, la manipulation financière et des cyberattaques de plus en plus sophistiquées. Il existe un potentiel considérable et inexploité pour tirer parti de l'IA afin de détecter les cybermenaces, de contrer la manipulation de l'information et l'ingérence étrangères, de renforcer la résilience des infrastructures essentielles et d'améliorer la capacité du Canada à répondre à ces menaces émergentes. Une stratégie crédible en matière d'IA doit trouver un équilibre entre l'innovation et les mesures visant à contrer la désinformation et la manipulation de l'information rendues possibles par l'IA.

Une première priorité pour le Canada consiste à se doter de capacités d'IA sécurisées et souveraines en développant les données nationales fiables, la capacité de calcul et l'infrastructure numérique, ainsi qu'une capacité souveraine de collecte de renseignements. Ces investissements réduiront la dépendance à l'égard des technologies étrangères pour les applications critiques en matière de sécurité nationale, tout en renforçant la résilience et la compétitivité économique. La collaboration internationale, y compris les approches fédérées avec des partenaires de confiance comme ceux d'Europe, peut être bénéfique pour compléter (et non remplacer) les capacités souveraines canadiennes, pourvu que l'ouverture d'Internet ne soit pas sacrifiée.

Le succès dépend également d'une collaboration étroite entre les gouvernements, l'industrie, le milieu universitaire, la société civile et les alliés pour contrer les cyberattaques et les attaques informationnelles, soutenue par des méthodologies et des normes communes en matière de menaces, des plateformes sécurisées de partage de l'information, ainsi que des stratégies et des guides d'intervention harmonisés. Nous devrions continuer à explorer des options pour réglementer le développement de l'IA sans étouffer l'innovation.

La stratégie canadienne en matière d'IA constitue une bonne base. Le prochain défi consiste à traduire les objectifs stratégiques en capacités opérationnelles grâce à des investissements soutenus, à des initiatives ciblées de lutte contre la désinformation, à un renforcement de la sécurité de la recherche, à une cyberdéfense coordonnée et à des partenariats durables qui garantissent que l'IA renforce à la fois la sécurité et la prospérité à long terme du Canada.