



L'officier de pont à bord du NCSM MARGARET BROOKE, travaille sur la passerelle alors que le navire se dirige vers la station de recherche Rothera sur l'île Adelaïde, en Antarctique, au cours de l'opération PROJECTION 25-01, le 15 mars 2025.

Caporal Connor Bennett, Forces armées canadiennes

Le Canada, puissance technologique responsable au XXI^e siècle

CHRISTINA MARCOTTE

Christina Marcotte est directrice adjointe au Secteur de la sécurité internationale et des affaires politiques d'Affaires mondiales Canada. Elle consacre beaucoup trop de temps à la lecture d'ouvrages d'histoire et demeure convaincue que Vespasien est l'empereur romain le plus sous-estimé. Les opinions exprimées dans le présent commentaire n'engagent qu'elle.

À mesure que le Canada progresse dans le XXI^e siècle, je repense aux paroles de Lord Palmerston, premier ministre britannique du XIX^e siècle : « Nous n'avons pas d'alliés éternels, et nous n'avons pas d'ennemis perpétuels. Nos intérêts sont éternels et perpétuels, et c'est notre devoir de les suivre. »¹

Le présent commentaire décrit les mesures prises par le gouvernement du Canada pour protéger et promouvoir les intérêts du pays en matière de sécurité à l'ère de la puissance technologique. Il porte principalement sur le cyberspace et les cyberoutils, y compris l'intelligence artificielle (IA). Aux fins du présent

commentaire, je ne tiendrai pas compte des avantages potentiellement transformateurs de l'IA et des autres technologies pour les processus opérationnels. Je m'intéresserai plutôt à l'adoption des technologies par l'État ainsi qu'à la gouvernance de leur utilisation, selon une approche responsable dans les deux cas. Dans ce

contexte, la responsabilité signifie que les mesures prises renforcent la coopération internationale, dont le Canada tire profit, et qu'elles respectent les principes démocratiques. En agissant ainsi, le Canada consolide les mécanismes de gouvernance qui ont permis au pays et à sa population de prospérer.

Premièrement, pour assurer la sécurité au XXI^e siècle, l'État doit s'adapter à l'évolution des technologies, sans quoi la population canadienne risque d'être exposée à des menaces pesant sur ses renseignements personnels et financiers, et le Canada se retrouverait désavantagé face aux menaces provenant d'États adverses et d'acteurs non étatiques. Les forces armées étrangères, les services d'espionnage, les organisations criminelles, les cyber-militants et d'autres acteurs malveillants mènent leurs activités dans le cyberspace.

Compte tenu du grand nombre de menaces auxquelles la population est confrontée dans le cyberspace, le Canada manquerait à ses obligations, découlant du contrat social, s'il ne développait pas et n'utilisait pas les outils nécessaires pour les contrer. Ce contrat social prévoit notamment que le gouvernement utilise les ressources financières fournies par les citoyens afin d'assurer leur protection. La capacité d'agir dans le cyberspace pour perturber les activités des cyberacteurs malveillants, les affaiblir et neutraliser les infrastructures cybernétiques qu'ils utilisent, y compris les organisations criminelles, fait partie intégrante de cette protection.²

Deuxièmement, en ce qui concerne la gouvernance, celle-ci est liée à l'ordre international qui est fondé sur des règles. Cet ordre international s'est développé depuis la Seconde Guerre mondiale et repose sur le multilatéralisme ainsi que sur ses institutions, notamment l'Organisation des Nations Unies (ONU), le droit international, les traités et les normes.

La prospérité économique du Canada découle en grande partie du fait que l'ordre international fondé sur des règles offre un cadre stable et prévisible pour le commerce mondial et les relations économiques internationales. Parallèlement, il contribue à la sécurité du Canada, en fournissant un cadre stable de coopération face aux défis internationaux ainsi qu'un mécanisme permettant d'élaborer des règles de conduite et des normes de comportement reconnues par tous. En tant que l'un des 193 États membres de l'ONU et puissance moyenne dans un monde qui compte un nombre croissant de puissances moyennes aux côtés de plusieurs superpuissances, le Canada ne peut pas façonner le monde à son image. Il est donc dans son intérêt de travailler avec des pays aux vues similaires. L'ordre international fondé sur des règles offre un cadre de coopération connu et fiable. Il n'est pas parfait, mais les principes d'égalité et de prévisibilité sur lesquels il repose servent beaucoup mieux les intérêts du Canada qu'un système où seule la force détermine l'issue des rapports entre les États.

Dans cet ordre international, la responsabilité constitue un pilier fondamental des principes et des processus du Canada. Cette responsabilité comporte deux dimensions : celle d'agir et celle de le faire de façon responsable. D'abord, les États qui disposent des

moyens d'action devraient le faire. Un État responsable intervient lorsqu'il en a la capacité. Il conteste l'espace dans lequel évoluent les acteurs malveillants. Laisser cet espace sans opposition expose inutilement les citoyens à des risques. Cette responsabilité vaut autant envers la population canadienne qu'envers les citoyens des États qui ne disposent ni des ressources ni des moyens permettant de prendre les mêmes mesures que le Canada.

Ces interventions doivent également être menées de manière responsable. Le Canada doit utiliser ces outils dans le respect de l'ordre international et de ses règles. Plus précisément, il doit agir conformément au *Cadre des Nations Unies pour le comportement responsable des États dans le cyberspace* auquel il a publiquement souscrit.³ Ce cadre reconnaît notamment que le droit international s'applique au cyberspace, prévoit la mise en œuvre des normes convenues, en particulier les onze normes des Nations Unies, l'application de mesures de confiance liées au cyberspace et le renforcement des capacités des États en développement.⁴

L'utilisation responsable de ces outils soutient et renforce l'ordre international fondé sur des règles, le système même qui a contribué à la prospérité du Canada. Cet enjeu revêt une importance particulière à un moment où cet ordre est confronté à des défis considérables. Certains États cherchent activement à remodeler l'ordre international afin de servir leurs propres intérêts, sans égard aux conséquences pour les autres États, ou encore à tirer parti des faiblesses de pays moins puissants dans un système où la loi du plus fort prévaut.

En tant que démocratie, le comportement responsable du Canada comprend également la reddition de comptes et la transparence. La reddition de comptes signifie que le Canada respecte les obligations qui lui incombent en vertu du droit international et du droit interne applicables, les engagements qu'il a pris relativement aux normes volontaires et aux autres engagements publics, ainsi que les mécanismes de gouvernance qui lui sont propres, notamment la chaîne de commandement militaire. La transparence signifie que le Canada informe le public de ses capacités et de la manière dont il les utilise, sans divulguer les détails opérationnels, et qu'il se soumet aux mécanismes de surveillance appropriés. Ces deux principes sont essentiels pour prévenir les abus de pouvoir et maintenir la confiance de la population envers son gouvernement.

Commençons par la question de la responsabilité. La technologie est utilisée comme un outil du pouvoir étatique, y compris l'IA, que ce soit à des fins d'espionnage ou d'armement ou pour d'autres usages encore imprévisibles. Toutefois, la technologie et l'IA ne peuvent être dissociées des infrastructures qui les soutiennent. Lorsque j'écris que « l'IA sera utilisée comme un outil du pouvoir étatique », cela signifie également que « l'IA sera utilisée dans le cyberspace et en tant que cyberoutil du pouvoir étatique ». Le cyberspace constitue à la fois un domaine et un outil. À l'instar des domaines terrestre, maritime, aérien et spatial, le cyberspace est un domaine d'activités civiles et militaires, un espace doté de dimensions dans lequel se déroulent des opérations. C'est

« Le Canada dispose déjà de règles et de normes claires concernant le cyberspace et l'utilisation des cyberoutils, notamment le cadre des Nations Unies pour le comportement responsable des États. »

d'ailleurs dans le cadre international basé sur des règles que les États ont établi les principes qui régissent le cyberspace. Le Canada dispose déjà de règles et de normes claires concernant le cyberspace et l'utilisation des cyberoutils, notamment le cadre des Nations Unies pour le comportement responsable des États mentionné précédemment. De plus, à mesure que l'IA est intégrée aux systèmes d'armes, leur emploi continue d'être régi par les règles d'engagement et le droit applicable.

L'IA représente également bien davantage qu'une simple évolution du cyberspace, et il demeure difficile d'anticiper l'ensemble de ses applications possibles. Les États en sont conscients et travaillent actuellement, selon les normes sur lequel repose l'ordre international, à l'élaboration de règles encadrant l'utilisation de l'IA comme outil du pouvoir étatique. Dans le domaine militaire, plusieurs initiatives plurilatérales portent expressément sur l'IA et son utilisation. Parmi celles-ci figure la *Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy*,⁵ lancée en 2023 sous la direction des États-Unis à l'occasion du Sommet sur l'intelligence artificielle responsable dans le domaine militaire (REAIM), organisé par les Pays-Bas. Par ailleurs, la version révisée en 2024 de la *Stratégie OTAN pour l'intelligence artificielle* comprend un objectif consacré au comportement responsable, précisant de « jeter les bases qui permettront à l'OTAN et aux alliés de montrer l'exemple et de piloter le développement et l'utilisation responsables de l'IA pour les besoins de la défense et de la sécurité des alliés ».⁶ Sur le plan multilatéral, il convient également de mentionner la résolution 79/239 de l'Assemblée générale des Nations Unies sur l'intelligence artificielle dans le domaine militaire.⁷

À l'échelle nationale, le gouvernement du Canada doit rendre compte de ses actes à ses citoyens. Les mesures qu'il a prises au cours des dernières années témoignent également de sa crédibilité comme acteur responsable et de son engagement à respecter les obligations qu'il a envers la population canadienne en matière de sécurité. Ces mesures comprennent notamment la publication de la *Stratégie nationale de cybersécurité* en 2018 et en 2024,⁸

en 2018 la création du Centre canadien pour la cybersécurité et l'établissement du Centre national de coordination en cybercriminalité de la Gendarmerie royale du Canada (GRC), la place importante accordée aux technologies dans les politiques de défense *Protection, Sécurité, Engagement* (2017)⁹ et *Notre Nord, fort et libre* (2024),¹⁰ ainsi que la mise à jour en 2019 de la *Loi sur le Centre de la sécurité des télécommunications*.¹¹

Moins visible pour le public, mais tout aussi importante, la création, en 2018, d'une unité au sein d'Affaires mondiales Canada chargée des politiques internationales en matière de cybersécurité, dont le mandat englobe maintenant également la gouvernance de l'IA, mérite aussi d'être soulignée. Cette unité possède l'expertise nécessaire pour représenter le Canada et défendre les intérêts du pays en matière de sécurité aux Nations Unies et dans d'autres forums multilatéraux. Elle coordonne également la contribution du Canada à des initiatives internationales, notamment le Processus de Pall Mall,¹² dirigé par le Royaume-Uni et la France afin de lutter contre la prolifération des outils de cyberintrusion. En parallèle, la Direction générale du droit international d'Affaires mondiales Canada compte des juristes, spécialisés dans le cyberspace. Cette direction a contribué de façon importante à l'ordre international fondé sur des règles et à la transparence du gouvernement du Canada, en élaborant et en publiant la position officielle du Canada sur l'application du droit international dans le cyberspace.¹³

Parmi les autres mesures, favorisant la transparence, figure l'initiative 88 de la politique de défense *Protection, Sécurité, Engagement* (2017), qui prévoit expressément ce qui suit : « nous nous doterons de la capacité de mener des cyberopérations actives axées sur les menaces externes au Canada dans le contexte de missions militaires autorisées par le gouvernement. L'emploi de cette capacité [...] sera assujéti à la même rigueur que d'autres formes de recours à la force militaire. Les cyberopérations seront assujetties à toutes les lois nationales et internationales applicables ainsi qu'aux garde-fous éprouvés comme les règles d'engagement et les évaluations de ciblage et de dommages collatéraux. »¹⁴ Que ces cyberoutils soient ou non renforcés par l'IA, ils demeureront assujettis aux mécanismes de reddition de comptes. En informant publiquement la population de la capacité des forces armées à mener des cyberopérations actives, également appelées cyberopérations offensives, ainsi que du cadre qui en régit l'emploi, le Canada contribue à renforcer l'ordre international.

La *Loi sur le Centre de la sécurité des télécommunications* traite également publiquement des cyberopérations actives du Canada. L'article 30 de cette loi prévoit que les ministres de la Défense nationale et des Affaires étrangères autorisent les cyberopérations actives. Les articles suivants précisent les types d'activités autorisées et interdites ainsi que les procédures applicables à leur autorisation.¹⁵

Par ailleurs, tant du point de vue des principes démocratiques que de la transparence, l'Office de surveillance des activités en

matière de sécurité nationale et de renseignement (OSSNR) et le Comité des parlementaires sur la sécurité nationale et le renseignement (CPSNR) jouent un rôle essentiel. Le mandat de l'OSSNR comprend l'examen et l'enquête sur les activités du gouvernement du Canada en matière de sécurité nationale et de renseignement afin de vérifier qu'elles sont légales, raisonnables et nécessaires.¹⁶ De façon plus générale, le CPSNR examine le cadre législatif, réglementaire, stratégique, administratif et financier applicable à la sécurité nationale et au renseignement, ainsi que toute activité menée par un ministère en lien avec ces domaines.¹⁷ L'OSSNR et le CPSNR doivent chacun présenter un rapport annuel au premier ministre, qui dépose ensuite les rapports du Comité devant les deux chambres du Parlement.

Enfin, le fait d'agir comme une puissance technologique responsable renforce également la crédibilité du Canada lorsqu'il approfondit sa coopération avec ses partenaires et ses alliés. L'ampleur et la diversité des menaces font en sorte que le Canada ne peut assurer seul sa sécurité, d'où l'importance essentielle de ces partenariats. Ils permettent de mieux comprendre les menaces, d'élaborer les moyens les plus efficaces pour les atténuer et les gérer, puis de les contrer. Travailler ensemble exige de la confiance; travailler efficacement ensemble en exige davantage

encore. La cohérence entre les actions du Canada et les principes qu'il défend contribue à établir sa réputation de partenaire digne de confiance. Cela vaut autant pour des partenariats de longue date, comme l'OTAN, que pour ceux établis et approfondis dans le cadre de la *Stratégie du Canada pour l'Indo-Pacifique*.

En se tournant vers l'avenir et en répondant à ses besoins de sécurité dans les années à venir, le Canada continuera d'agir comme un acteur étatique responsable dans le cyberspace, y compris à mesure que de nouvelles technologies feront leur apparition. Cela concerne notamment la manière dont le Canada utilisera l'IA et toute autre technologie comme outil du pouvoir étatique. Les progrès technologiques et les changements qui les accompagnent ne modifieront ni le contrat social qui unit la population canadienne à son gouvernement ni l'engagement constant de celui-ci à protéger ses citoyens. Les mesures déjà prises par le gouvernement du Canada témoignent de cet engagement. En continuant d'agir comme un acteur étatique responsable, le Canada réaffirme son attachement aux mécanismes de gouvernance, tant sur le plan international qu'à l'échelle nationale, qui ont permis à la population canadienne de prospérer.

Notes

- 1 Le vicomte Palmerston, « Treaty of Adrianople—Charges Against Viscount Palmerston », *House of Commons Debates*, 1^{er} mars 1848, Hansard, vol. 97, col. 122. Source originale : <https://api.parliament.uk/historic-hansard/commons/1848/mar/01/treaty-of-adrianople-charges-against>
- 2 Jacques J. M. Shore, « An Obligation to Act: Holding Government Accountable for Critical Infrastructure Cyber Security », *International Journal of Intelligence and Counterintelligence* 28, no 2 (2015) : 238. Source originale : <https://doi.org/10.1080/08850607.2014.96235>
- 3 Affaires mondiales Canada, « Politique internationale en matière de cybersécurité », consulté le 11 août 2026. Source originale : https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_scurite/cyber_policy-politique_cyberspace.aspx?lang=eng, citant Assemblée générale des Nations Unies, source originale : *Progrès de l'informatique et des télécommunications et sécurité internationale*, A/RES/70/237 (23 décembre 2015).
- 4 Assemblée générale des Nations Unies, Groupe d'experts gouvernementaux, A/RES/70/237.
- 5 Département d'État des États-Unis, Bureau du contrôle des armements, de la dissuasion et de la stabilité, *Déclaration politique sur l'utilisation militaire responsable de l'intelligence artificielle et de l'autonomie*, 9 novembre 2023, source originale : <https://www.state.gov/political-declaration-on-responsible-military-use-of-artificial-intelligence-and-autonomy-2/>
- 6 *Résumé de la stratégie révisée de l'OTAN en matière d'intelligence artificielle* (IA), 5, 1.1, 10 juillet 2024. Source originale : <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/07/10/summary-of-natos-revised-artificial-intelligence-ai-strategy>
- 7 Assemblée générale des Nations Unies, *L'intelligence artificielle dans le domaine militaire et ses incidences sur la paix et la sécurité internationales*, A/RES/79/239 (24 décembre 2024).
- 8 Sécurité publique Canada, *Stratégie nationale de cybersécurité : Vision du Canada pour la sécurité et la prospérité dans l'ère numérique* (gouvernement du Canada, juin 2018). Source originale : <https://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/ntnl-cbr-scrst-strtg/ntnl-cbr-scrst-strtg-en.pdf>; Sécurité publique Canada, *Stratégie nationale de cybersécurité : Sécuriser l'avenir numérique du Canada* (gouvernement du Canada, 2025), source originale : <https://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/ntnl-cbr-scrst-strtg-2025/ntnl-cbr-scrst-strtg-2025-en.pdf>.
- 9 Ministère de la Défense nationale, *Protection, Sécurité, Engagement : La politique de défense du Canada* (gouvernement du Canada, juin 2017). Source originale : <https://www.canada.ca/en/departement-national-defence/corporate/reports-publications/canada-defence-policy.html>.
- 10 Ministère de la Défense nationale, *Notre Nord, fort et libre : Une vision renouvelée pour la défense du Canada* (gouvernement du Canada, avril 2024). Source originale : <https://www.canada.ca/en/departement-national-defence/corporate/reports-publications/north-strong-free-2024.html>.
- 11 *Loi sur le Centre de la sécurité des télécommunications*, LC 2019, ch. 13, art. 76. Source originale : <https://laws-lois.justice.gc.ca/eng/acts/C-35.3/page-1.html>.
- 12 Royaume-Uni, Foreign, Commonwealth & Development Office, *Code de pratique du Processus de Pall Mall à l'intention des États* (gouvernement du Royaume-Uni, 4 avril 2025). Source originale : <https://www.gov.uk/government/publications/the-pall-mall-process-code-of-practice-for-states>.
- 13 *Le droit international applicable dans le cyberspace*. Source originale : https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_scurite/cyberspace_law-cyberespace_droit.aspx?lang=eng
- 14 Ministère de la Défense nationale, *Protection, Sécurité, Engagement*, p. 73.
- 15 *Loi sur le Centre de la sécurité des télécommunications*, art. 30.
- 16 *Loi sur l'Office de surveillance des activités en matière de sécurité nationale et de renseignement*, LC 2019. Source originale : <https://laws-lois.justice.gc.ca/eng/acts/N-16.62/page-1.html>.
- 17 *Loi sur le Comité des parlementaires sur la sécurité nationale et le renseignement*. Source originale : <https://laws-lois.justice.gc.ca/eng/acts/N-16.61/page-1.html>.