THEBUSINESSCOUNCIL.CA/FR

Conseil canadien des affaires

# LA SÉCURITÉ ÉCONOMIQUE EST LA SÉCURITÉ NATIONALE

*les arguments en faveur d'une stratégie canadienne*

Rapport

## Table des matiéres



## Principaux points à retenir

1. Les entreprises canadiennes sont dans la ligne de mire d'acteurs soutenus par l'État qui cherchent à promouvoir leurs intérêts d'une manière qui porte atteinte à la sécurité nationale et économique du Canada.
2. Les gouvernements successifs ont tardé à réagir à une nouvelle réalité géopolitique qui fait peser une menace sans précédent sur la sécurité nationale et le bien-être économique de tous les Canadiens.
3. Le Canada devrait suivre la voie tracée par nombre de ses alliés les plus proches en intégrant les considérations de sécurité économique dans une stratégie de sécurité nationale qui aide à identifier et à atténuer les menaces stratégiques.
4. Une stratégie de sécurité canadienne devrait renforcer l'architecture de sécurité économique, renforcer les capacités d'innovation et élargir les partenariats internationaux en matière de sécurité.


99 Bank, Suite / bureau 1001, Ottawa, Canada K1P 6B9 THEBUSINESSCOUNCIL.CA

## Le Canada a besoin d'une stratégie de sécurité nationale

La sécurité nationale du Canada dépend de la vitalité économique et de la résilience de notre pays. Ce n'est que grâce à notre prospérité économique durable que nous trouvons les talents, les ressources et l'innovation nécessaires pour réaliser nos ambitions nationales, protéger la vie et les moyens de subsistance des Canadiens, et jouer un rôle positif et influent sur la scène mondiale.

L'inverse est également vrai. Sans un environnement de sécurité nationale solide, il est impossible d'avoir une économie saine et productive.

Bon nombre des alliés les plus proches du Canada reconnaissent ce « lien qui se renforce mutuellement »[1] et ont élaboré des approches intégrées de la sécurité économique et nationale qui visent à renforcer leur prospérité, leur sécurité et leur souveraineté en période de risques géopolitiques accrus.

Ce n'est pas le cas du Canada. Depuis des décennies, les gouvernements canadiens successifs ont négligé, tenu pour acquis ou simplement ignoré le principe que *la sécurité économique est la sécurité nationale*.

Cette négligence nous a rendus vulnérables. À une époque de rivalité géopolitique renouvelée, où la capacité des pays à favoriser la croissance économique constitue le fondement de la puissance militaire, économique et culturelle, les entreprises canadiennes de toutes tailles se retrouvent de plus en plus dans la ligne de mire d'auteurs de menace stratégique[2] qui cherchent à promouvoir leurs intérêts nationaux d'une manière qui peut nuire, et qui nuit effectivement, à la sécurité nationale et économique du Canada.

Ces menaces sont susceptibles de causer des ravages à grande échelle dans la vie quotidienne des Canadiens. Les conséquences sont notamment des licenciements massifs causés par le vol de la propriété intellectuelle, des perturbations dans la capacité des Canadiens à chauffer et à alimenter leurs maisons en raison de cyberattaques paralysantes, et la montée en flèche du coût des produits ménagers quotidiens en raison de l'armement des chaînes d'approvisionnement.

La défense de la sécurité économique du Canada est une tâche trop importante pour être confiée au secteur public ou au secteur privé qui travaillent seuls. Les deux doivent collaborer sans faille pour détecter, dissuader, et interrompre un large éventail de menaces émergentes et évolutives.

**C'est pourquoi le présent rapport invite le gouvernement du Canada à collaborer avec les entreprises canadiennes pour élaborer et mettre en œuvre une stratégie de sécurité nationale qui, pour la première fois, accorde une place centrale à la sécurité économique.**

Fondé sur des consultations approfondies avec les dirigeants des entreprises les plus innovantes et les plus prospères du Canada, des experts en sécurité, et d'anciens fonctionnaires, ce rapport examine les menaces auxquelles sont confrontés les Canadiens, explore les conséquences de l'inaction, et recommande des mesures pour combler les lacunes les plus flagrantes dans la posture de sécurité économique du Canada.

---

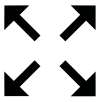
[1] Voir Gouvernement de l'Australie, « Strong and Secure: A Strategy for Australia's National Security », 2013, page 4, lien : https://www.files.ethz.ch/isn/167267/Australia%20A%20Strategy%20for%20National%20Securit.pdf
[2] Dans le présent document, les acteurs soutenus par l'État dont les activités constituent des menaces pour la sécurité économique et nationale du Canada sont collectivement appelés « auteurs de menace stratégique ».


99 Bank, Suite / bureau 1001, Ottawa, Canada K1P 6B9 THEBUSINESSCOUNCIL.CA

Les recommandations du document s'articulent autour de trois thèmes:

**Renforcer l'architecture de la sécurité économique du Canada,** notamment en créant un cadre juridique permettant au gouvernement de partager en temps opportun des renseignements sur les menaces exploitables avec les entreprises ciblées par les attaques;

**Renforcer les capacités économiques et d'innovation du Canada,** notamment en encourageant la recherche à haut risque et à haut rendement dans les domaines perturbateurs et émergents qui sont fondamentaux pour stimuler la croissance économique et qui sont stratégiques du point de vue de la sécurité nationale; et



**Élargir et redynamiser les partenariats internationaux du Canada en matière de sécurité,** inotamment en prenant des mesures pour contrer collectivement l'armement des chaînes d'approvisionnement, telles qu'une « OTAN pour le commerce ».

Dans un contexte où la sécurité est une condition préalable à la prospérité, et la prospérité une condition préalable à la sécurité, le Canada ne pourra pas maintenir une société saine et prospère sans une stratégie de sécurité nationale qui protège notre sécurité économique. Le moment est venu pour les décideurs politiques canadiens de reconnaître cette réalité et de s'unir aux entreprises canadiennes pour protéger la vitalité économique et la résilience de notre nation.


99 Bank, Suite / bureau 1001, Ottawa, Canada K1P 6B9

## Les auteurs de menace stratégique font progresser leurs intérêts nationaux à nos dépens

Le Canada se trouve aujourd'hui au cœur de l'environnement de sécurité le plus important, le plus complexe et le plus imprévisible depuis une génération.

L'ordre unipolaire libre, ouvert et relativement stable qui a prévalu après la fin de la guerre froide — et qui a procuré au Canada des niveaux de sûreté, de sécurité et de prospérité sans précédent — cède la place à une nouvelle réalité multipolaire, plus turbulente et marquée par la rivalité géopolitique.[3]

La fragmentation des biens communs mondiaux en camps rivaux luttant pour la supériorité stratégique a intensifié la concurrence et la confrontation entre les États dans des domaines très variés. Cela est particulièrement vrai dans les domaines des affaires, de l'économie et de la technologie.

Comme d'autres époques définies par une concurrence géopolitique exacerbée,[4] la capacité des pays à favoriser la croissance économique — en particulier par l'invention, la diffusion et l'adoption de technologies émergentes et perturbatrices — est le fondement sur lequel repose aujourd'hui la puissance militaire, économique et culturelle.[5]

Conscients de cette réalité, les auteurs de menace stratégique ont montré leur capacité et leur volonté de voler, de saboter et de perturber leur ascension économique afin de renforcer leur pouvoir géopolitique et de remodeler unilatéralement l'ordre international actuel pour le rendre plus favorable à leurs intérêts.[6]

---

[3] Voir Groupe de travail sur la sécurité nationale, « Une stratégie de sécurité nationale pour les années 2020 », École supérieure d'affaires publiques et internationales, Université d'Ottawa, mai 2020, pages 4-5, lien : https://www.uottawa.ca/publisher/sites/g/files/bhrskd311/files/2022-12/rapport_secnat_esapi_mai2022.pdf ; Aaron Shull and Wesley Wark, "Reimagining a Canadian National Security Strategy," Centre pour l'innovation dans la gouvernance internationale, 6 décembre 2021, pages 11-12 lien : https://www.cigionline.org/publications/reimagining-a-canadian-national-security-strategy/.

[4] Les plus grandes périodes d'innovation technologique ont souvent coïncidé avec d'intenses rivalités géopolitiques. Les fondements de la révolution informatique et des télécommunications, pour donner l'exemple le plus récent d'une innovation axée sur la sécurité, trouvent leur origine dans la concurrence de la guerre froide.

[5] La puissance économique renforce la capacité d'un pays à faire la guerre. Elle donne aux États un pouvoir sur les chaînes d'approvisionnement mondiales. Elle accroît la puissance douce d'un pays par l'exportation de ses valeurs. En bref, la capacité d'un pays à projeter sa puissance sur la scène internationale dépend maintenant largement de sa capacité à rivaliser dans les industries de pointe où la concurrence est la plus féroce. Voir Groupe de travail sur la sécurité nationale, « Une stratégie de sécurité nationale pour les années 2020 », École supérieure d'affaires publiques et internationales, Université d'Ottawa, mai 2020, pages 9-10, lien : https://www.uottawa.ca/publisher/sites/g/files/bhrskd311/files/2022-12/rapport_secnat_esapi_mai2022.pdf; Aaron Shull et Wesley Wark, « Reimagining a Canadian National Security Strategy, » Centre pour l'innovation dans la gouvernance internationale, 6 décembre 2021, pages 14-18 lien : https://www.cigionline.org/publications/reimagining-a-canadian-national-security-strategy/.

[6] Voir Bureau du Conseil privé, « Allocution du conseiller à la sécurité nationale et au renseignement auprès du premier ministre au Centre pour l'innovation dans la gouvernance internationale », Gouvernement du Canada, 8 juin 2021, lien : https://www.canada.ca/fr/conseil-prive/services/conseiller-securite-nationale-renseignement-defis.html; Intelligence and Security Committee of Parliament, « China », Parlement du Royaume-Uni, 13 juillet 2023, paragraphes 9 et 49, lien : https://isc.independent.gov.uk/wp-content/uploads/2023/07/ISC-China.pdf.

Les nouvelles avancées technologiques, notamment dans le cyberespace, ont permis à ces acteurs d'élargir et d'adapter leurs tactiques afin de mieux pénétrer nos défenses et d'atteindre leurs objectifs révisionnistes.

Le résultat : Les entreprises canadiennes, dans presque toutes les régions et tous les secteurs de notre économie, sont aujourd'hui confrontées à des dangers sans précédent. Elles exercent leurs activités dans un environnement de plus en plus déséquilibré, une situation qui désavantage toujours le commerce privé traditionnel.

La piètre performance économique du Canada ne fait qu'ajouter à cette menace.[7] Le Canada est moins performant que ses rivaux mondiaux dans une variété de domaines essentiels pour stimuler l'innovation, faire croître les entreprises et s'approprier une part du marché mondial dans des secteurs de pointe essentiels à notre prospérité et à notre sécurité.[8] En effet, le Canada n'est en tête dans aucune des 44 catégories de technologies de pointe — telles que l'intelligence artificielle, les technologies quantiques ou la cybersécurité avancée — identifiées par un groupe de réflexion comme étant essentielles à la sécurité économique et nationale d'un pays.[9]

[7] Selon les prévisions, le Canada aura l'économie la moins performante des pays industrialisés entre 2020 et 2030. Voir Organisation de coopération et de développement économiques, « The Long Game: Fiscal Outlooks to 2060 Underline Need for Structural Reform », 19 octobre 2021, page 13, lien : .

[8] Ceci est notamment les dépenses des entreprises en recherche et développement, la commercialisation de la propriété intellectuelle et la rétention des talents. Le Canada s'est classé 22e sur 44 nations suivies par l'Organisation de coopération et de développement économiques en ce qui concerne les dépenses intérieures en recherche et développement en proportion du produit intérieur brut en 2020. Voir Organisation de coopération et de développement économiques, « OECD Main Science and Technology Indicators Highlights », mars 2022, page 2,lien : https://www.oecd.org/sti/msti-highlights-march-2022.pdf. Le Canada s'est classé 17e dans l'Indice mondial de l'innovation 2020 de l'Organisation mondiale de la propriété intellectuelle. Les importations d'innovation du Canada (9e) ont largement dépassé ses exportations d'innovation (22e). Voir Office de la propriété intellectuelle du Canada, « Rapport sur la PI au Canada 2019 », Gouvernement du Canada, septembre 2019, page 6, lien : https://ised-isde.canada.ca/site/office-propriete-intellectuelle-canada/sites/default/files/attachments/2022/IP_Canada_Report_2019_fra.pdf. Dans le Global Talent Competitiveness Index 2022, un indice de compétitivité mondiale relatif aux talents, le Canada est tombé à la 15e place, alors qu'il était 9e en 2015, avec ses notes les plus faibles en matière de rétention des immigrants (19e). Voir INSEAD, « The Global Talent Competitiveness Index 2022 », novembre 2022, page 32, lien : https://www.insead.edu/sites/default/files/assets/dept/fr/gtci/GTCI-2022-report.pdf.

[9]Voir Australian Strategic Policy Institute, « Critical Technology Tracker, Appendix 1.1 : Top 5 country visual snapshot », avril 2023, lien : https://ad-aspi.s3.ap-southeast-2.amazonaws.com/2023-03/PB69-CriticalTechTracker-Appendix-1.1_0.pdf?VersionId=A_QAiK_ps0.4cYJ.qfJB1eoEk15SlqYq.

## Les menaces pour la sécurité économique représentent des risques sérieux de dommages importants pour notre société

Soyons clairs : toutes les attaques dirigées contre des entreprises canadiennes ne constituent pas des menaces pour la sécurité économique nécessitant une réponse en matière de sécurité nationale. La plupart des menaces actuelles peuvent être contrées par des outils conventionnels, tels que les procédures civiles.

Les menaces pour la sécurité économique sont différentes. Elles représentent des risques sérieux de dommages importants pour notre pays dans son ensemble — pour notre souveraineté, nos valeurs, notre économie et notre population. En tant que telles, elles dépassent largement la capacité des outils conventionnels à y faire face seuls et nécessitent une réponse nationale coordonnée.

Le Canada est confronté à une série de menaces liées à la sécurité économique qui érodent la compétitivité économique du pays en faisant pencher la balance à l'avantage d'autres pays. La liste est longue. Elle est constituée de mercantilisme, de l'armement du commerce, d'espionnage, de cyberattaques, d'influence étrangère malveillante et de recherche universitaire cooptée.

Les acteurs soutenus par des États en sont les principaux auteurs.[10] Le gouvernement du Canada identifie régulièrement les activités perturbatrices de pays tels que la Chine, la Russie, l'Iran et la Corée du Nord comme posant les « plus graves menaces stratégiques » pour la sécurité du Canada.[11]

---

[10] Les activités des acteurs non étatiques présentent également des risques pour la sécurité du Canada. Par exemple, la plupart des activités criminelles n'atteignent pas le niveau d'une menace à la sécurité économique. Mais lorsque la criminalité est susceptible de nuire aux Canadiens à une échelle potentiellement illimitée ou sans discernement, elle sera considérée comme une menace nécessitant une réponse en matière de sécurité nationale. Les rançongiciels ciblant les infrastructures essentielles en est un excellent exemple. Cependant, il est également important de souligner que la distinction entre les acteurs étatiques et non étatiques est devenue de plus en plus floue. Le Centre canadien pour la cybersécurité, par exemple, note qu'il est « presque assuré » que les services de renseignement de plusieurs pays « collaborent avec des cybercriminels qui se livrent à des stratagèmes par rançongiciel ». Dans cette collaboration avec bénéfices mutuels, « les cybercriminels échangent des données avec les services de renseignement et ces derniers leur permettent de poursuivre leurs opérations sans avoir à respecter les lois ». Voir Centre canadien pour la cybersécurité, « Évaluation des cybermenaces nationales: 2020 » Gouvernement du Canada, 16 novembre 2020, page 22, lien : https://www.cyber.gc.ca/sites/default/files/cyber/publications/ncta-2020-f-web.pdf.

[11] Voir Centre canadien pour la cybersécurité, « Évaluation des cybermenaces nationales 2020 » Gouvernement du Canada, 16 novembre 2020, page 5, lien : ; Centre canadien pour la cybersécurité, « Évaluation des cybermenaces nationales 2023-2024 », Gouvernement du Canada, 28 octobre 2022, page 13, lien : https://publications.gc.ca/collections/collection_2022/cstc-csec/D98-4-2023-fra.pdf; Comité permanent de la sécurité publique et nationale, « Témoignage de Caroline Xavier », Évaluation de la posture de sécurité du Canada par rapport à la Russie, numéro 037, 44elégislature, 1re session, 6 octobre 2022, lien : https://www.noscommunes.ca/DocumentViewer/fr/44-1/SECU/reunion-37/temoignages ; Bureau du Conseil privé, « Allocution du conseiller à la sécurité nationale et au renseignement auprès du premier ministre au Centre pour l'innovation dans la gouvernance internationale », Gouvernement du Canada, 8 juin 2021, lien : ; Service canadien du renseignement de sécurité, « Allocution de M. David Vigneault, directeur du SCRS, au Centre pour l'innovation dans la gouvernance internationale », Gouvernement du Canada, 9 février 2021, lien : https://www.securitepublique.gc.ca/cnt/trnsprnc/brfng-mtrls/prlmntry-bndrs/20210625/28-fr.aspx ; Service canadien du renseignement de sécurité, « Matériel de transition pour le ministre de la Sécurité publique et de la Protection civile », Gouvernement du Canada, 25 février 2022, lien : https://www.canada.ca/fr/service-renseignement-securite/organisation/transparence/document-dinformation/2021-materiel-de-transition/contexte-de-la-menace.html.


99 Bank, Suite / bureau 1001, Ottawa, Canada K1P 6B9

## Mercantilisme : en concurrence avec l'« État, inc. »

Le Canada et ses alliés adhèrent à un ensemble commun de valeurs de marché — telles que la primauté du droit — qui garantissent que la concurrence économique se déroule sur un pied d'égalité.[12]

Les auteurs de menace stratégique rejettent ces règles reconnues mondialement. Ils adoptent de plus en plus de pratiques mercantilistes visant à donner à leurs champions nationaux les avantages nécessaires pour remplacer les importations par la production nationale, avancer dans les chaînes de valeur mondiales et gagner des parts de marché mondiales dominantes dans des secteurs stratégiques.[13]

La liste des pratiques prédatrices est longue. Il s'étend bien au-delà du soutien généralement admis aux industries nationales, et est constitué de la manipulation des devises locales pour donner à leurs champions nationaux un avantage de prix injuste sur les marchés étrangers, de l'obligation pour les entreprises étrangères de transférer des technologies de pointe aux champions nationaux comme condition préalable à l'accès à leurs marchés, et de l'octroi de subventions industrielles massives aux champions nationaux pour leur permettre de mener des activités non rentables qui anéantissent la concurrence étrangère.[14]

Ces interventions mercantilistes signifient que les entreprises canadiennes ne sont pas en concurrence avec une société commerciale typique. Au contraire, elles opèrent sur des règles du jeu inégales, en rivalisant avec la force et les ressources d'un État étranger.[15] Autrement dit : « État, inc. »

Le mercantilisme mine la société canadienne en introduisant dans notre économie des entreprises non compétitives et inefficaces qui sont en mesure d'accepter des pertes financières importantes pour surenchérir sur les entreprises canadiennes et leur faire concurrence, parce qu'elles sont gouvernées par les intérêts de l'État et non par ceux des actionnaires.[16] Ceci, à son tour, détruit les industries nationales et ne donne au Canada d'autre choix que de compter sur les champions nationaux pour les intrants économiques essentiels.[17]

---

[12] Stephanie Carvin souligne que « les systèmes de marché libre/capitaliste ont besoin de règles du jeu équitables et de la primauté du droit pour fonctionner efficacement ». Voir Stephanie Carvin, « Stand on Guard: Reassessing Threats to Canada's National Security » , Toronto University Press, mai 2021, page 144.
[13] Voir Stephanie Carvin, « Stand on Guard:Reassessing Threats to Canada's National Security », Toronto University Press, mai 2021, page 144 ; Robert D. Atkinson, « What is Chinese 'Innovation Mercantilism' and How Should the UK and Allies Respond? », Information Technology and Innovation Foundation, juin 2021, pages 1-3, lien : https://static1.squarespace.com/static/5f75a6c74b43624d99382ab6/t/60d9958153ee2b4b30210fc0/1624872326116/China+Research+Group+-+NATO+for+Trade+-+June.pdf.
[14] Voir Robert D. Atkinson, « What is Chinese 'Innovation Mercantilism' and How Should the UK and Allies Respond? », Information Technology and Innovation Foundation, juin 2021, pages 1-3, lien : https://static1.squarespace.com/static/5f75a6c74b43624d99382ab6/t/60d9958153ee2b4b30210fc0/1624872326116/China+Research+Group+-+NATO+for+Trade+-+June.pdf ; Voir Robert D. Atkinson, « Innovation Drag: China's Economic Impact on Developed Nations », Information Technology and Innovation Foundation, 6 janvier 2020, lien : https://itif.org/publications/2020/01/06/innovation-drag-chinas-economic-impact-developed-nations/.
[15] Stephanie Carvin note que « l'ensemble des stratégies et tactiques des auteurs de menace stratégique visent à biaiser le paysage économique canadien ». Voir Stephanie Carvin, « Stand on Guard: Reassessing Threats to Canada's National Security » , Toronto University Press, mai 2021, page 144.
[16] Voir Sephanie Carvin, « Stand on Guard: Reassessing Threats to Canada's National Security », Toronto University Press, mai 2021, pages 144-145.
[17] Voir Stephanie Carvin, « Stand on Guard:Reassessing Threats to Canada's National Security », Toronto University Press, mai 2021, page 144.


99 Bank, Suite / bureau 1001, Ottawa, Canada K1P 6B9 THEBUSINESSCOUNCIL.CA

Cette dépendance est problématique. Les limites floues entre la politique de l'État et les activités privées signifient que même les entreprises ostensiblement privées n'ont souvent pas d'autre choix que de soutenir les objectifs de leur gouvernement en matière de sécurité nationale. Cela inclut le soutien, l'assistance et la coopération avec leurs agences de renseignement.[18]

## L'armement du commerce : transformer une activité à somme positive en un jeu à somme nulle

La prospérité des Canadiens repose sur un système commercial international équitable, prévisible et ouvert. Ce système crée de bons emplois bien rémunérés pour les Canadiens, favorise la concurrence et le choix des produits et fait baisser les prix à la consommation.

Notre dépendance à l'égard du commerce international nous rend également vulnérables. Les auteurs de menace stratégique cherchent à étendre leur influence mondiale en utilisant la dépendance du Canada à l'égard du commerce pour faire pression sur le gouvernement du Canada, l'inciter ou l'influencer afin qu'il prenne des mesures conformes à leurs priorités nationales.[19]

Ces acteurs emploient diverses tactiques pour contraindre le gouvernement du Canada. Ils peuvent limiter la circulation de biens essentiels pour lesquels il n'existe pas de substituts, refuser l'accès réciproque aux marchés nationaux et soumettre les biens canadiens à des inspections et des conditions d'importation onéreuses.[20]

Alors que les exportations canadiennes soutiennent plus d'un emploi sur six dans le pays,[21]

l'armement du commerce peut directement menacer les moyens de subsistance des Canadiens. En effet, entre 2019 et 2020, le ciblage du secteur du canola par la Chine a coûté aux agriculteurs canadiens plus de 2,35 milliards de dollars en pertes d'exportations et en baisse des prix.[22]

---

[18] Voir Murray Scot Tanner, « Beijing's New National Intelligence Law: From Defense to Offense », Lawfare, 20 juillet 2017, lien: https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense ; Intelligence and Security Committee of Parliament, « China », Parlement du Royaume-Uni, 13 juillet 2023, paragraphe 8, lien: https://isc.independent.gov.uk/wp-content/uploads/2023/07/ISC-China.pdf.
[19] Voir Matthew Reynolds et Matthew P Goodman, « Deny, Deflect, Deter: Countering China's Economic Coercion », Centre for Strategic and International Studies, mars 2023, https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-03/230321_Goodman_CounteringChina%27s_EconomicCoercion.pdf?VersionId=UnF29IRogQV4vH6dy6ixTpfTnWvftd6v.
[20] Voir Matthew Reynolds et Matthew P Goodman, « Deny, Deflect, Deter: Countering China's Economic Coercion », Centre for Strategic and International Studies, mars 2023, https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-03/230321_Goodman_CounteringChina%27s_EconomicCoercion.pdf?VersionId=UnF29IRogQV4vH6dy6ixTpfTnWvftd6v.
[21] Voir Affaires mondiales Canada, « Le point sur le commerce 2022 : Les avantages des accords de libre-échange », Gouvernement du Canada, 1er août 2022, page 14, lien : https://www.international.gc.ca/transparency-transparence/state-trade-commerce-international/2022.aspx?lang=fra.
[22] Voir Left Field Commodity Research, « Case Study - Impacts of the Chinese Trade Restrictions on the Canadian Canola Industry, Final Report », février 2021, page 22, lien : https://www.canolacouncil.org/wp-content/uploads/2021/03/CCC-Market-Access-Impact-Report-China-Final.pdf.
[23] Bien qu'il soit la neuvième économie mondiale, le Canada se classe troisième sur 164 membres de l'Organisation mondiale du commerce en ce qui concerne la fréquence des différends soumis pour résolution, et sixième pour le nombre de différends défendus. Voir Valerie Hughes, « Canada: A Key Player in WTO Dispute Settlement », Centre pour l'innovation dans la gouvernance internationale, février 2018, page 2, lien : https://www.cigionline.org/static/documents/documents/Reflections%20Series%20Paper%20no.11%20HughesWEB.pdf.

L'armement du commerce a également des répercussions économiques plus vastes. En tant que puissance moyenne dont l'économie est dépendante du commerce, le Canada est tributaire d'un système commercial international fondé sur des règles pour promouvoir ses intérêts économiques nationaux[23]. L'armement du commerce met en péril ce système en remettant en question des normes et des lois internationales largement acceptées.

Comme l'invasion non provoquée de l'Ukraine par la Russie l'a également mis en évidence pour nos alliés européens, une dépendance excessive à l'égard d'un acteur de la menace stratégique pour des apports économiques essentiels, en particulier un acteur dont les valeurs et les intérêts divergent de manière systémique, peut s'avérer à la fois coûteuse[24] et mortelle[25] pour la société.

Le Canada dépend d'auteurs de menace stratégique pour un large éventail de produits de base essentiels à la sécurité et à la prospérité des Canadiens. Sur la base de données compilées par les Nations Unies, une étude récente a révélé que le Canada est stratégiquement dépendant de la Chine, un pays qui a l'habitude d'armer le commerce, pour au moins 367 catégories de marchandises.[26] Quatre-vingt-trois de ces catégories desservent les infrastructures essentielles dont les Canadiens dépendent quotidiennement pour chauffer et alimenter leurs maisons, transporter leurs produits à destination et en provenance des marchés internationaux, et communiquer avec leurs proches à travers notre vaste pays.[27]

## Espionnage : utiliser l'ingéniosité canadienne contre les Canadiens

En tant qu'économie de marché avancée abritant un grand nombre des entreprises les plus prospères et les plus innovantes du monde, le Canada est devenu une cible attrayante pour les États qui cherchent à faire progresser leurs industries nationales par l'espionnage.[28]

Les auteurs de menace stratégique utilisent un large éventail de méthodes pour voler secrètement des informations commercialement précieuses, telles que des plans d'affaires confidentiels, des processus de fabrication exclusifs et de la propriété intellectuelle.

---

[24] Sans accès à l'importation d'énergie russe à bas prix, l'Allemagne, moteur économique de l'Europe, a perdu une source essentielle de sa puissance industrielle. Cela pourrait menacer la prospérité de tout le continent. Voir Constanze Stelzenmüller, « A German has crisis will cause jitters across Europe », The Brookings Institution, 18 juillet 2022, lien : https://www.brookings.edu/articles/a-german-gas-crisis-will-cause-jitters-across-europe/ ; Matthew Karnitschnig, « Rust Belt on the Rhine », POLITICO, 13 juillet 2023, lien : https://www.politico.eu/article/rust-belt-on-the-rhine-the-deindustrialization-of-germany/.

[25] La modélisation montre que les prix élevés de l'énergie, résultant de la perte des importations d'énergie russe bon marché, ont coûté la vie à 68 000 Européens au cours de l'hiver 2022-2023. Voir The Economist, « Expensive energy may have killed more Europeans than covid-19 last winter », 10 mai 2023, lien : https://www.economist.com/graphic-detail/2023/05/10/expensive-energy-may-have-killed-more-europeans-than-covid-19-last-winter.

[26] Voir James Rogers, Dr Andrew Foxall, Matthew Henderson et Sam Armstrong, « Breaking the China Supply Chain : How the 'Five Eyes' can Decouple from Strategic Dependency », Henry Jackson Society, 14 mai 2020, page 5, lien : https://henryjacksonsociety.org/publications/breaking-the-china-supply-chain-how-the-five-eyes-can-decouple-from-strategic-dependency/.

[27] Voir James Rogers, Dr Andrew Foxall, Matthew Henderson et Sam Armstrong, « Breaking the China Supply Chain : How the 'Five Eyes' can Decouple from Strategic Dependency », Henry Jackson Society, 14 mai 2020, page 5, lien : https://henryjacksonsociety.org/publications/breaking-the-china-supply-chain-how-the-five-eyes-can-decouple-from-strategic-dependency/.

[28] Voir Stephanie Carvin, « Stand on Guard:Reassessing Threats to Canada's National Security », Toronto University Press, mai 2021, page 119 ; Service canadien du renseignement de sécurité, « Allocution de M. David Vigneault, directeur du SCRS, au Centre pour l'innovation dans la gouvernance internationale », Gouvernement du Canada, 9 février 2021, lien : https://www.securitepublique.gc.ca/cnt/trnsprnc/brfng-mtrls/prlmntry-bndrs/20210625/28-fr.aspx.


99 Bank, Suite / bureau 1001, Ottawa, Canada K1P 6B9 THEBUSINESSCOUNCIL.CA

Ces méthodes sont notamment le recours à des agents du renseignement et à des pirates informatiques affiliés à l'État, à des personnes internes à l'entreprise disposant d'un accès légitime, ainsi qu'à des coentreprises et à des partenariats de recherche universitaire apparemment inoffensifs.[29]

Les entreprises sont généralement ciblées directement. L'arrestation en 2022 d'un employé d'une compagnie d'électricité accusé d'avoir volé des secrets industriels au profit de la Chine en est un exemple.[30]

Cependant, les informations des entreprises seront ciblées, quel que soit l'endroit où elles se trouvent.[31] En 2014, on a découvert qu'un cyberacteur soutenu par l'État chinois avait mis en péril les systèmes numériques du Conseil national de recherches.[32] L'acteur a volé plus de 40 000 fichiers, qui étaient notamment « des éléments de propriété intellectuelle, de l'information sur la recherche de pointe et des renseignements confidentiels d'entreprises » partenaires du secteur privé de l'agence gouvernementale.[33]

Le vol de l'ingéniosité canadienne est exploité pour construire ou améliorer les produits des champions nationaux. Sans avoir à faire des dizaines d'années d'investissements coûteux, par exemple dans la recherche et le développement, le vol par l'État donne à ces entreprises une longueur d'avance sur les entreprises canadiennes.[34]

Les informations volées sont également utilisées pour donner aux champions nationaux un aperçu des transactions commerciales des entreprises canadiennes, par exemple dans le cadre d'appels d'offres importants pour des marchés publics à l'étranger.[35] Comme le fait remarquer

---

[29] Voir Service canadien du renseignement de sécurité, « Allocution de M. David Vigneault, directeur du SCRS, au Centre pour l'innovation dans la gouvernance internationale », Gouvernement du Canada, 9 février 2021, lien : https://www.securitepublique.gc.ca/cnt/trnsprnc/brfng-mtrls/prlmntry-bndrs/20210625/28-fr.aspx.
[30] Voir Gendarmerie royale du Canada, « Accusations d'espionnage contre un employé d'Hydro-Québec », Gouvernement du Canada, 14 novembre 2022, lien : https://www.rcmp-grc.gc.ca/fr/nouvelles/2022/accusations-despionnage-employe-dhydro-quebec.
[31] Selon le Comité des parlementaires sur la sécurité nationale et le renseignement, le gouvernement « détient une quantité énorme de données sur [...] les entreprises et les secteurs de l'innovation du Canada ». Les auteurs de menace stratégique sont conscients de ce fait. Le Comité affirme que les auteurs de menace stratégique cherchent à compromettre les systèmes gouvernementaux afin de « miner la vitalité d'entreprises précises et de l'économie ». Voir Comité des parlementaires sur la sécurité nationale et le renseignement, « Rapport spécial sur le cadre et les activités du gouvernement pour défendre ses systèmes et ses réseaux contre les cyberattaques », Gouvernement du Canada, 14 février 2022, paragraphe 1, lien : https://www.nsicop-cpsnr.ca/reports/rp-2022-02-14/2022-cyber-attack-framework-report-fr.pdf. La même logique s'applique aux institutions universitaires. Le Comité souligne que les auteurs de menace stratégique « tentent d'utiliser les aspects ouverts ou innovateurs de ces établissements [d'enseignement postsecondaire canadiens] pour faire avancer leurs propres objectifs, [notamment] [...] l'espionnage et le vol de propriété intellectuelle ». Voir Comité des parlementaires sur la sécurité nationale et le renseignement, « Rapport annuel 2019 », Gouvernement du Canada, 12 mars 2020, paragraphe 171, lien : https://www.nsicop-cpsnr.ca/reports/rp-2020-03-12-ar/annual_report_2019_public_fr.pdf;
[32] Voir Comité des parlementaires sur la sécurité nationale et le renseignement, « Rapport spécial sur le cadre et les activités du gouvernement pour défendre ses systèmes et ses réseaux contre les cyberattaques », Gouvernement du Canada, 14 février 2022, page 107, lien : https://www.nsicop-cpsnr.ca/reports/rp-2022-02-14/2022-cyber-attack-framework-report-fr.pdf.
[33] Voir Comité des parlementaires sur la sécurité nationale et le renseignement, « Rapport spécial sur le cadre et les activités du gouvernement pour défendre ses systèmes et ses réseaux contre les cyberattaques », Gouvernement du Canada, 14 février 2022, page 107, lien : https://www.nsicop-cpsnr.ca/reports/rp-2022-02-14/2022-cyber-attack-framework-report-fr.pdf.
[34] Voir Stephanie Carvin, « Stand on Guard:Reassessing Threats to Canada's National Security », Toronto University Press, mai 2021, page 119.
[35] Voir Stephanie Carvin, « Stand on Guard:Reassessing Threats to Canada's National Security », Toronto University Press, mai 2021, page 119.

un expert, « si le résultat net d'une entreprise canadienne est déjà connu, il sera facile pour l'autre partie de surenchérir ou de négocier autour d'elle ». [36]

Ces tactiques détruisent collectivement l'incitation des entreprises canadiennes à innover et à se développer.[37] Avec le temps, elles risquent d'exclure définitivement les entreprises canadiennes des marchés mondiaux.[38]

Bien qu'il n'existe actuellement aucune estimation précise du coût de l'espionnage économique dans notre pays, des études réalisées aux États-Unis[39] montrent que le coût pour les Canadiens s'élève probablement à des dizaines de milliards de dollars par an.

## Les cyberattaques : une perturbation de l'épine dorsale de la société canadienne

Tout comme la révolution industrielle a apporté d'énormes avantages à la société, la révolution numérique en cours[40] a le potentiel de faire de même. Elle peut aider les entreprises à atteindre de nouveaux acheteurs et marchés, à fabriquer des produits plus rapidement et plus efficacement, et à améliorer la commodité, le choix et la valeur pour le consommateur.

Cependant, à mesure que les interactions internationales se déplacent dans le cyberespace, nous avons constaté une montée en flèche des cyberattaques ciblant les entreprises canadiennes.

Les entreprises canadiennes représentent plus de la moitié de toutes les cybervictimes connues dans ce pays et sont la cible la plus fréquente des cyberattaques d'inspiration géopolitique menées contre le Canada[41]. Pour donner une idée de l'ampleur du problème, deux entreprises canadiennes sur cinq ont été victimes d'une cyberattaque au cours des deux dernières années.[42]

---

[36] Voir Stephanie Carvin, « Stand on Guard:Reassessing Threats to Canada's National Security », Toronto University Press, mai 2021, page 119.
[37] Voir Robert D. Atkinson, « Innovation Drag: China's Economic Impact on Developed Nations », Information Technology and Innovation Foundation, 6 janvier 2020, lien : https://itif.org/publications/2020/01/06/innovation-drag-chinas-economic-impact-developed-nations/.
[38] Voir Robert D. Atkinson, « Innovation Drag: China's Economic Impact on Developed Nations », Information Technology and Innovation Foundation, 6 janvier 2020, lien : https://itif.org/publications/2020/01/06/innovation-drag-chinas-economic-impact-developed-nations/.
[39] Aux États-Unis, une commission indépendante a estimé que l'espionnage économique et le vol de propriété intellectuelle pratiqués par des auteurs de menace stratégique coûtaient à l'économie américaine jusqu'à 600 milliards de dollars par an, en décourageant les investissements en capital nécessaires à l'innovation et en sapant la compétitivité des employeurs américains à l'étranger. Voir The Commission on the Theft of American Intellectual Property, « Written Comments on Behalf of the Commission on the Theft of American Intellectual Property to the United States Trade Representative », Gouvernement des États-Unis, 11 mai 2018, page 3, lien : https://www.nbr.org/wp-content/uploads/pdfs/publications/ustr_written_comments_301_tariffs-may2018.pdf.
[40] L'économie canadienne se numérise à une vitesse fulgurante. Au cours de la dernière décennie, l'économie numérique du Canada a connu une croissance d'environ 40 % plus rapide que l'économie globale et a généré près de quatre fois plus d'emplois que cette dernière. Voir Statistique Canada, « Mesurer les activités économiques numériques au Canada, 2010 à 2017 », Gouvernement du Canada, 3 mai 2019, lien : https://www150.statcan.gc.ca/n1/daily-quotidien/190503/dq190503a-fra.htm.
[41] Voir Center on Multidimensional Conflicts, « Geopolitical Cyber Incidents in Canada: 2023 Assessment », Université du Québec à Montréal, juillet 2023, page 5, lien : https://dandurand.uqam.ca/wp-content/uploads/2023/06/2023-06-05-rapport-OCM-ENG.pdf.
[42] Voir Statistique Canada, « Incidents de cybersécurité en 2020 par rapport à 2019, selon les caractéristiques de l'entreprise », Gouvernement du Canada, 28 mai 2021, lien : ;

L'impact est énorme. Les attaques entraînent souvent une atteinte à la réputation, une perte de revenus et de possibilités commerciales, des répercussions juridiques, ainsi que des dommages durables à l'infrastructure et aux opérations de l'entreprise. Selon une estimation, les rançongiciels[43] ont à eux seuls coûté à l'économie canadienne 4,3 milliards de dollars américains en rançons payées et en perte de productivité en 2021.[44]

Les cyberattaques contre les infrastructures essentielles — telles que les réseaux électriques, les réseaux de télécommunication et les gazoducs — sont particulièrement inquiétantes, compte tenu de leur fréquence accrue et de leur capacité à causer des ravages à grande échelle dans la vie quotidienne des Canadiens.

Les opérateurs d'infrastructures essentielles continueront d'être confrontés à un risque élevé de la part des cybercriminels, y compris ceux qui sont affiliés à des États-nations, en raison des « poches pleines » des opérateurs et de « l'impact des temps d'arrêt opérationnel sur les clients [des opérateurs] ».[45] On s'attend à ce que les acteurs étatiques continuent à cibler les infrastructures essentielles pour « se prépositionner en cas d'éventuelles hostilités et de faire acte de force et d'intimidation ».[46]

Parmi les incidents récents survenus au Canada touchant des infrastructures essentielles, on peut citer les suivants :

- En mai 2022, un « groupe de cybercriminels russophones » a perturbé les opérations d'une entreprise aérospatiale canadienne fournissant des services d'ingénierie et de recherche et développement aux Forces armées canadiennes. L'entreprise avait récemment été sélectionnée pour participer à la modernisation de la flotte d'hélicoptères CH-146 Griffon.[47]

- En avril 2023, un groupe de pirates informatiques « prorusses » a lancé une série d'attaques par déni de service pendant la visite du premier ministre de l'Ukraine au Canada. Ces attaques ont provoqué la panne des sites Web de nombreuses grandes entreprises canadiennes dans les secteurs des services publics, des transports et du secteur bancaire.[48]

---

[43] Le rançongiciel est un type de logiciel malveillant conçu pour bloquer l'accès à un système informatique jusqu'à ce qu'une somme d'argent soit versée.
[44] Voir Emisoft Malware Lab, « The Cost of Ransomware in 2021. A Country-by-Country Analysis », 27 avril 2021, lien : https://www.emsisoft.com/en/blog/38426/the-cost-of-ransomware-in-2021-a-country-by-country-analysis/.
[45] Voir Centre canadien pour la cybersécurité, « Évaluation des cybermenaces nationales 2023-2024 », Gouvernement du Canada, 28 octobre 2022, page 13, lien : https://publications.gc.ca/collections/collection_2022/cstc-csec/D98-4-2023-fra.pdf.
[46] Voir Centre canadien pour la cybersécurité, « Évaluation des cybermenaces nationales 2023-2024 », Gouvernement du Canada, 28 octobre 2022, page 12, lien : https://publications.gc.ca/collections/collection_/cstc-csec/D98-4-2023-fra.pdf.
[47] Voir Center on Multidimensional Conflicts, « Geopolitical Cyber Incidents in Canada: 2023 Assessment », Université du Québec à Montréal, juillet 2023, page 4, lien : https://dandurand.uqam.ca/wp-content/uploads/2023/06/2023-06-05-rapport-OCM-ENG.pdf ; Lyle Adriano, « National defence contractor suffers cyberattack », Insurance Business, 10 juin 2022, lien : https://www.insurancebusinessmag.com/ca/news/cyber/national-defence-contractor-suffers-cyberattack-409136.aspx.
[48] Voir Lillian Roy, « Pro-Russia hackers say they were behind Hydro-Quebec cyberattack » CTV News, 13 avril 2023, lien : https://montreal.ctvnews.ca/pro-russia-hackers-say-they-were-behind-hydro-quebec-cyberattack-1.6353627 ; Tom Blackwell, « 'Trudeau's being cocky': Russian hackers claim attacks on PM, Pearson airport and others », 14 avril 2023, lien : }https://nationalpost.com/news/canada/russian-cyber-attacks-canada; Sidhartha Banerjee, « Cyberattack knocks out Hydro-Québec's website, mobile app », La Presse Canadienne, 13 avril 2023, link: https://globalnews.ca/news/9620864/hydro-quebec-cyber-attack/.

- En avril 2023, une fuite de renseignements a révélé que des « pirates informatiques soutenus par la Russie » avaient accédé aux systèmes numériques d'un distributeur canadien de gaz naturel et en avaient pris le contrôle.[49] Le chef du Centre canadien pour la cybersécurité a affirmé que les pirates « avaient le potentiel de causer des dommages physiques » aux réseaux des distributeurs.[50]

Il est difficile d'exagérer l'importance des infrastructures essentielles pour la sûreté, la sécurité et la prospérité des Canadiens. Bien qu'elle ne résulte pas d'une cyberattaque, une panne d'électricité survenue en août 2003 et qui a duré moins d'une semaine a entraîné une perte estimée à 2,3 milliards de dollars pour l'économie de l'Ontario, a contribué à une baisse de 0,7 % du PIB du Canada en août et a très probablement causé des pertes de vies humaines.[51] Compte tenu de la croissance de l'économie canadienne au cours des 20 années qui se sont écoulées depuis, l'impact d'une panne similaire provoquée par la cybernétique serait de plusieurs ordres de grandeur supérieurs.

## Influence étrangère malveillante : érosion de la confiance des Canadiens

Les États étrangers cherchent à influencer la société canadienne. La plupart de ces activités sont parfaitement légitimes. Il est à la fois légal et approprié pour les États étrangers d'afficher des opinions sur les affaires intérieures du Canada et d'exprimer ces opinions avec les Canadiens.[52]

Cependant, les États étrangers s'écartent de la diplomatie pour exercer une influence étrangère malveillante inacceptable lorsque leurs activités sont secrètes, trompeuses ou menaçantes.[53]

Le discours actuel sur l'influence étrangère malveillante se concentre à juste titre sur l'intégrité des processus démocratiques et sur la sûreté et la sécurité des groupes ethniques ou culturels ciblés.

Cependant, les auteurs de menace stratégique ciblent activement tous les aspects de la société canadienne pour faire avancer leurs intérêts stratégiques à notre détriment.[54] Cela inclut le recours à des tiers qui utilisent des tactiques trompeuses en ligne pour nuire à des secteurs stratégiquement importants de l'économie canadienne.

---

[49] Voir Amanda Stephenson, « Apparent leaked U.S. docs suggest pro-Russian hackers accessed Canada's gas network. Should we be concerned? », La Presse canadienne, 10 avril 2023, lien : https://www.cbc.ca/news/politics/energy-sector-target-cyberattacks-experts-1.6806300.
[50] Catherine Tunney, « Intelligence agency says cyber threat actor 'had the potential' to damage critical infrastructure », Canadian Broadcasting Corporation, 13 avril 2023, lien : https://www.cbc.ca/news/politics/cse-critical-infrastructure-1.6809645.
[51] Voir Centre canadien pour la cybersécurité, « Bulletin sur les cybermenaces : Les cyberattaques visant le secteur canadien de l'électricité », Gouvernement du Canada, 30 novembre 2020, lien : https://www.cyber.gc.ca/fr/orientation/bulletin-sur-les-cybermenaces-les-cyberattaques-visant-le-secteur-canadien-de.
[52] Voir Le très honorable David Johnston, Rapporteur spécial indépendant sur l'ingérence étrangère, « Premier rapport », Gouvernement du Canada, 23 mai 2023, page 12, lien : https://www.canada.ca/content/dam/di-id/documents/rpt/rapporteur/Independent-Special-Rapporteur%20-Report-fra.pdf; Stephanie Carvin, « Stand on Guard: Reassessing Threats to Canada's National Security », Toronto University Press, mai 2021, page 186.
[53] Voir Le très honorable David Johnston, Rapporteur spécial indépendant sur l'ingérence étrangère, « Premier rapport », Gouvernement du Canada, 23 mai 2023, page 12, lien : https://www.canada.ca/content/dam/di-id/documents/rpt/rapporteur/Independent-Special-Rapporteur%20-Report-fra.pdf.
[54] Voir Sécurité publique Canada, « Accroître la transparence en matière d'influence étrangère : Examiner les mesures pour renforcer l'approche du Canada », Gouvernement du Canada, 10 mars 2023, lien : https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2023-nhncng-frgn-nfluence/index-fr.aspx.

En juin 2022, un acteur malveillant ayant des liens possibles avec la Chine a déployé des milliers de comptes de médias sociaux inauthentiques pour mener une campagne de désinformation coordonnée contre une entreprise canadienne développant une mine de terres rares dans le nord de la Saskatchewan.[55]

Peu après l'annonce du projet par la société minière, des messages inauthentiques sur les médias sociaux ont commencé à cibler les habitants de la région avec de fausses affirmations concernant le bilan environnemental et social du projet.[56]

Une publication d'« Ashely Wilson » affirme que « [l] a protection du lac, la responsabilité de chacun, si une fois l'exploitation minière, comment assurer la santé des travailleurs, résister fermement. »[57] Un autre utilisateur, « Farrah », a déclaré : « [c] e n'est pas excitant, nos lacs seront détruits ». [58] « Brown Emily » et « Gonzales Bonnie » se sont montrées tout aussi consternées, qualifiant respectivement la découverte de « terrible » et de « terrifiante »[59].

Le plan d'attaque était clair : attiser l'opposition locale contre le projet, forcer l'arrêt des activités des mineurs et saper un secteur essentiel à la sécurité et à la prospérité du Canada.[60]

À une époque où les rivalités géopolitiques s'exacerbent, ces attaques deviennent de plus en plus la norme. Parmi les autres attaques récentes ciblant l'économie canadienne, on peut citer les campagnes de désinformation russes et iraniennes qui critiquent les pipelines d'énergie et les politiques d'immigration du gouvernement du Canada.[61]

## Recherche universitaire en cooptation : exploiter l'ouverture et la collaboration du Canada

La recherche universitaire ouverte et collaborative est indispensable pour repousser les limites de la science et de la technologie canadiennes. Cependant, les auteurs de menace stratégique exploitent cette caractéristique de nos établissements universitaires pour faire avancer leurs priorités à nos dépens.[62]

---

[55] Voir Mandiant, « Pro-PRC DRAGONBRIDGE Influence Campaign Targets Rare Earths Mining Companies in Attempt to Thwart Rivalry to PRC Market Dominance », 28 juin 2022, lien : https://www.mandiant.com/resources/blog/dragonbridge-targets-rare-earths-mining-companies.
[56] Voir Mandiant, « Pro-PRC DRAGONBRIDGE Influence Campaign Targets Rare Earths Mining Companies in Attempt to Thwart Rivalry to PRC Market Dominance », 28 juin 2022, lien : https://www.mandiant.com/resources/blog/dragonbridge-targets-rare-earths-mining-companies.
[57] Voir Mandiant, « Pro-PRC DRAGONBRIDGE Influence Campaign Targets Rare Earths Mining Companies in Attempt to Thwart Rivalry to PRC Market Dominance », 28 juin 2022, lien : https://www.mandiant.com/resources/blog/dragonbridge-targets-rare-earths-mining-companies.
[58] Voir Mandiant, « Pro-PRC DRAGONBRIDGE Influence Campaign Targets Rare Earths Mining Companies in Attempt to Thwart Rivalry to PRC Market Dominance », 28 juin 2022, lien : https://www.mandiant.com/resources/blog/dragonbridge-targets-rare-earths-mining-companies.
[59] Voir Mandiant, « Pro-PRC DRAGONBRIDGE Influence Campaign Targets Rare Earths Mining Companies in Attempt to Thwart Rivalry to PRC Market Dominance », 28 juin 2022, lien : https://www.mandiant.com/resources/blog/dragonbridge-targets-rare-earths-mining-companies.
[60] Voir Mandiant, « Pro-PRC DRAGONBRIDGE Influence Campaign Targets Rare Earths Mining Companies in Attempt to Thwart Rivalry to PRC Market Dominance », 28 juin 2022, lien : https://www.mandiant.com/resources/blog/dragonbridge-targets-rare-earths-mining-companies ; Heureusement, la campagne de désinformation a échoué. Selon la société de sécurité qui a découvert les attaques, la mauvaise exécution de l'acteur malveillant - mise en évidence par le « tweet » presque incompréhensible d'Ashley Wilson - a été le facteur limitant de la campagne ayant obtenu suffisamment de traction pour faire échouer le projet d'exploitation minière.
[61] Voir Roberto Rocha et Jeff Yates, « Twitter trolls stoked debates about immigrants and pipelines in Canada, data show », Canadian Broadcasting Corporation, 12 février 2019, lien : https://www.cbc.ca/news/canada/twitter-troll-pipeline-immigrant-russia-iran-1.5014750.


99 Bank, Suite / bureau 1001, Ottawa, Canada K1P 6B9 THEBUSINESSCOUNCIL.CA

Ils peuvent déployer des professeurs invités, des collaborateurs du secteur privé ou des organisations à but non lucratif pour obtenir un accès non autorisé à des informations, des compétences ou des technologies précieuses.[63]

Dans certains cas, la cooptation de recherches menées par le Canada peut conduire à des avancées dans les capacités stratégiques, militaires ou de renseignement d'États étrangers.[64]

Par exemple, au lieu de renforcer les capacités défensives du Canada par le développement national et la commercialisation de technologies de pointe, nous avons vu à plusieurs reprises des institutions universitaires canadiennes conclure des partenariats qui soutiennent les ambitions militaires d'États étrangers.

De 2018 à 2023, des universitaires de dix grandes universités canadiennes ont publié plus de 240 articles conjoints sur des sujets de recherche avancés, notamment la cryptographie quantique, la photonique et les sciences spatiales, avec des scientifiques militaires travaillant au sein de la plus grande institution militaire chinoise.[65]

## L'incapacité à faire face aux menaces croissantes met notre pays en danger

La nouvelle réalité géopolitique du Canada signifie que la sécurité économique — souvent considérée comme acquise, négligée ou carrément ignorée — est désormais au cœur de la préservation de notre sécurité nationale.

C'est là que réside le défi pour le pays.

Le fait d'avoir négligé pendant des décennies les questions de sécurité économique nous a rendus vulnérables. Pour reprendre les termes mêmes du Service canadien du renseignement de sécurité, le Canada est devenu une « cible attrayante et permissive »[66].

Le fait de ne pas relever ce défi avec urgence et ambition aura des conséquences graves et à long terme pour les Canadiens. Le chef du Centre de la sécurité des télécommunications l'a expliqué de la manière suivante : « La cybersécurité n'est pas quelque chose d'abstrait. Les systèmes numériques n'existent pas en vase clos. Ils existent en relation avec les personnes et ont des conséquences réelles sur leur vie privée, leur prospérité et leur bien-être. »[67]

---

[62] Voir Service canadien du renseignement de sécurité, « Protégez vos recherches », Gouvernement du Canada, 31 janvier 2022, lien : ; Comité des parlementaires sur la sécurité nationale et le renseignement, « Rapport annuel 2019 », Gouvernement du Canada, 12 mars 2020, paragraphe 171, lien : https://www.nsicop-cpsnr.ca/reports/rp-2020-03-12-ar/annual_report_2019_public_fr.pdf.
[63] Voir Intelligence and Security Committee of Parliament, « China », Parlement du Royaume-Uni, 13 juillet 2023, paragraphe 8, lien: https://isc.independent.gov.uk/wp-content/uploads/2023/07/ISC-China.pdf.
[64] Voir Groupe de travail sur la sécurité nationale, « Une stratégie de sécurité nationale pour les années 2020 », École supérieure d'affaires publiques et internationales, Université d'Ottawa, mai 2020, pages 9-10, lien : https://www.uottawa.ca/publisher/sites/g/files/bhrskd311/files/2022-12/rapport_secnat_esapi_mai2022.pdf.
[65] {Voir Steven Chase et Robert Fife, « Canadian universities conducting joint research with Chinese military scientists », The Globe and Mail, 30 janvier 2023, lien : https://www.theglobeandmail.com/politics/article-chinese-military-scientists-canadian-universities/.
[66] Voir Comité des parlementaires sur la sécurité nationale et le renseignement, « Rapport annuel 2019 », Gouvernement du Canada, 12 mars 2020, paragraphe 294, lien : https://www.nsicop-cpsnr.ca/reports/rp-2020-03-12-ar/annual_report_2019_public_fr.pdf ; Stephanie Carvin a noté que « l'espionnage contre les entreprises canadiennes est bien réel ». Voir Stephanie Carvin, « Stand on Guard:Reassessing Threats to Canada's National Security », Toronto University Press, mai 2021, page 116.

Si rien n'est fait, les tentatives d'affaiblissement de notre capacité économique entraîneront la perte d'emplois sûrs et bien rémunérés pour les travailleurs canadiens, la perte de recettes fiscales pour financer des services publics essentiels, tels que les soins de santé et les transports publics, ainsi que la perte de leadership dans des industries de pointe essentielles à la force nationale et à la santé économique à long terme du pays.[68]

Ce point revêt une importance accrue puisque le gouvernement du Canada dépense des dizaines de milliards de dollars par an pour promouvoir la transition du Canada vers une économie carboneutre[69]. Si les considérations de sécurité économique — telles que les mesures de lutte contre l'espionnage — ne sont pas intégrées dans les investissements du gouvernement du Canada dans la capacité industrielle, l'argent durement gagné par les contribuables finira probablement par subventionner les industries et la main-d'œuvre carboneutres d'autres pays.

Les attaques visant les entreprises canadiennes portent également atteinte aux valeurs qui nous sont les plus chères en tant que Canadiens. Cela comprend les droits et les libertés que nos lois promettent, tels que le droit des Canadiens à la vie privée, la primauté du droit, ainsi que le principe de la libre entreprise et une concurrence saine.[70]

La menace de cyberattaques punitives contre des infrastructures essentielles illustre bien cette situation. Des cyberacteurs dont les intérêts correspondent à ceux de la Russie ont ciblé des entreprises énergétiques canadiennes pour leur « impact psychologique », notamment pour « affaiblir le soutien [militaire et humanitaire] canadien à l'Ukraine »[71]. En créant des conséquences pour la contestation des comportements illibéraux sur la scène internationale, les cyberattaques punitives sapent la capacité du Canada à affirmer ses valeurs de manière indépendante.

---

[67]Centre de la sécurité des télécommunications, « Discours de la chef Shelly Bruce présenté au Centre pour l'innovation dans la gouvernance internationale », Gouvernement du Canada, mai 18 2021, lien : https://www.cse-cst.gc.ca/fr/ressources-et-information/discours-de-la-chef-shelly-bruce-presente-au-centre-pour-linnovation-dans.
[68] L'examen de la littérature scientifique a montré qu'en réduisant les possibilités commerciales et les profits dont les innovateurs doivent investir, les pratiques des auteurs de menace stratégique ont ralenti le processus d'innovation dans les pays occidentaux. L'innovation est le principal moteur durable de la croissance économique pour les économies avancées comme le Canada. Ainsi, laisser les pratiques des auteurs de menace stratégique se poursuivre sans relâche entravera la capacité de notre économie à générer des possibilités et de la prospérité pour les Canadiens. Voir Robert D. Atkinson, « Innovation Drag: China's Economic Impact on Developed Nations », Information Technology and Innovation Foundation, 6 janvier 2020, lien : https://itif.org/publications/2020/01/06/innovation-drag-chinas-economic-impact-developed-nations/ ; Le directeur du Service canadien du renseignement de sécurité a fait remarquer qu' « [e]n compromettant notre capacité à innover et à commercialiser le produit de nos recherches, l'espionnage cause la perte d'emplois et freine la croissance économique. » Voir Service canadien du renseignement de sécurité, « Allocution de M. David Vigneault, directeur du SCRS, au Centre pour l'innovation dans la gouvernance internationale », Gouvernement du Canada, 9 février 2021, lien : https://www.securitepublique.gc.ca/cnt/trnsprnc/brfng-mtrls/prlmntry-bndrs/20210625/28-fr.aspx.
[69] Voir Ministère des Finances Canada, « Budget 2023, chapitre 3 : Le plan canadien : une énergie abordable, de bons emplois et une économie propre en croissance », Gouvernement du Canada, 28 mars 2023, lien : https://www.budget.canada.ca/2023/home-accueil-fr.html.
[70] Voir Centre de la sécurité des télécommunications, « Discours de la chef Shelly Bruce présenté au Centre pour l'innovation dans la gouvernance internationale », Gouvernement du Canada, mai 18 2021, lien : https://www.cse-cst.gc.ca/fr/ressources-et-information/discours-de-la-chef-shelly-bruce-presente-au-centre-pour-linnovation-dans.
[71] Voir Centre canadien pour la cybersécurité, « Cybermenaces contre le secteur pétrolier et gazier du Canada », Gouvernement du Canada, 22 juin 2023, page 8, lien : .

Nous devons également garder à l'esprit que les alliés les plus proches du Canada agissent rapidement en cette période de risques géopolitiques accrus afin d'améliorer leurs capacités à identifier et à atténuer les menaces à la sécurité économique.[72]

Si le Canada n'avance pas au même rythme que ses alliés les plus proches dans le renforcement de sa capacité de sécurité économique, il risque d'être perçu comme un « maillon faible ». Cela mettrait en péril les relations du pays avec ses alliés les plus proches à un moment charnière où l'ordre mondial se transforme et où les partenariats sont les plus importants.

Des indices inquiétants montrent déjà que les plus proches alliés du Canada remarquent sa réticence à affronter sérieusement les menaces croissantes qui pèsent sur la sécurité, ce qui fait que le pays reste de plus en plus à l'écart lorsqu'il s'agit de conversations vitales sur la sécurité.[73]

L'ancien conseiller à la sécurité nationale et au renseignement du premier ministre a écrit que « le rythme glacial auquel le Canada semble s'adapter aux réalités de la concurrence moderne des grandes puissances l'a laissé largement à la traîne, avec des conséquences pour la réputation d'Ottawa auprès de ses alliés »[74].

Cela a probablement contribué à l'exclusion du Canada d'AUKUS, un partenariat de sécurité entre trois des plus proches alliés du Canada visant à aligner les secteurs de la défense et de la technologie des États membres afin de développer la prochaine génération de capacités militaires.[75]

---

[72] Il s'agit notamment de remanier les politiques, de légiférer sur de nouveaux outils et pouvoirs et d'établir de nouveaux partenariats. Voir Groupe de travail sur la sécurité nationale, « Une stratégie de sécurité nationale pour les années 2020 », École supérieure d'affaires publiques et internationales, Université d'Ottawa, mai 2020, page 2, lien : https://www.uottawa.ca/publisher/sites/g/files/bhrskd311/files/2022-12/rapport_secnat_esapi_mai2022.pdf. Selon le Comité des parlementaires sur la sécurité nationale et le renseignement, l'Australie est « à l'avant-garde des nations occidentales pour ce qui est de s'attaquer à la menace que représente l'ingérence étrangère ». Le Comité souligne que « l'Australie a adopté une série d'outils législatifs pour [...] résoudre le problème. Notamment, le pays a ajouté à son code criminel de nouvelles infractions relatives à l'espionnage et a l'ingérence étrangère et a apporté des modifications des infractions comme la trahison et la traîtrise ». Le Comité poursuit en affirmant que « [l]a loi crée un mécanisme transparent qui prévoit l'inscription des personnes agissant comme mandataire des donneurs d'ordre étrangers et dicte des divulgations publiques régulières » et que « [l]'Australie a aussi mis en place un coordonnateur de la lutte nationale contre l'ingérence étrangère mandaté de donner une réponse nationale efficace, efficiente et uniforme a l'ingérence étrangère en fournissant un point central pour la coordination des stratégies et de l'élaboration de programme et dirigeant la collaboration avec les secteurs privés > ». Voir Comité des parlementaires sur la sécurité nationale et le renseignement, « Rapport annuel 2019 », Gouvernement du Canada, 12 mars 2020, paragraphe 177, lien : https://www.nsicop-cpsnr.ca/reports/rp-2020-03-12-ar/annual_report_2019_public_fr.pdf.
[73] Selon un groupe d'universitaires et de praticiens de premier plan dans le domaine de la sécurité, « nos alliés nous surclassent en prenant des mesures pratiques et concrètes pour contrer les menaces à leur sécurité nationale ». Le groupe affirme qu' « [à] défaut de réagir avec fermeté, nous mettons [...] en péril nos alliés et, conséquemment, nos relations avec eux sur les plans de la sécurité et du renseignement ». Voir Groupe de travail sur la sécurité nationale, « Une stratégie de sécurité nationale pour les années 2020 », École supérieure d'affaires publiques et internationales, Université d'Ottawa, mai 2020, pages 2 et 5, lien : https://www.uottawa.ca/publisher/sites/g/files/bhrskd311/files/2022-12/rapport_secnat_esapi_mai2022.pdf. Des documents classifiés américains ayant fait l'objet d'une fuite indiquent que la résistance de longue date du Canada à atteindre les objectifs de dépenses de l'OTAN a entraîné une frustration croissante chez les alliés. Selon un document, « [l]es insuffisances généralisées en matière de défense entravent les capacités canadiennes, tout en mettant à rude épreuve les relations avec les partenaires et les contributions de l'alliance ». Voir Lili Bayer et Zi-Ann Lum, « NATO vs. Canada, its nicest truant », POLITICO, 15 juin 2023, lien : 4>https://www.politico.eu/article/nato-vs-canada-its-nicest-truant/ ; Christopher Hernandez-Roy, Vincent Rigby et Henry Ziemer, « Canadian Membership in AUKUS : A Time for Action », Center for Strategic and International Studies, 9 mai 2023, lien : https://www.csis.org/analysis/canadian-membership-aukus-time-action.
[74] Voir Christopher Hernandez-Roy, Vincent Rigby et Henry Ziemer, « Canadian Membership in AUKUS : A Time for Action », Center for Strategic and International Studies, 9 mai 2023, lien : https://www.csis.org/analysis/canadian-membership-aukus-time-action.
[75] Voir Christopher Hernandez-Roy, Vincent Rigby et Henry Ziemer, « Canadian Membership in AUKUS : A Time for Action », Center for Strategic and International Studies, 9 mai 2023, lien : https://www.csis.org/analysis/canadian-membership-aukus-time-action.


99 Bank, Suite / bureau 1001, Ottawa, Canada K1P 6B9 THEBUSINESSCOUNCIL.CA

## L'ère des correctifs après coup est révolue

Le gouvernement du Canada a réagi à notre nouvelle réalité géopolitique. Mais ses actions ont été lentes, modestes et fragmentaires.

Cette approche découle en grande partie d'un mode de gouvernance qui répond aux questions immédiates et urgentes qui se posent sans planification à long terme suffisante pour faire face aux auteurs de menace stratégique qui pensent bien au-delà de la durée d'un cycle politique canadien moyen.

Les efforts déployés par le Canada pour lutter contre l'ingérence étrangère démontrent la faiblesse de cette approche. Selon le Comité des parlementaires sur la sécurité nationale et le renseignement, « [l]'absence d'une approche globale [...] limite la capacité du Canada à agir sur l'ingérence étrangère ». [76] Le Comité affiche que les « réactions à l'ingérence étrangère demeurent ponctuelles et selon le cas, et ne sont que rarement envisagées dans un contexte élargi ».[77]

L'absence de pouvoirs de partage d'informations accordés au Service canadien du renseignement de sécurité offre un autre exemple des écueils de l'approche. Alors que le ministre de la Sécurité publique a chargé le directeur du Service canadien du renseignement de sécurité, en mai 2022, de veiller à ce que « les organisations qui travaillent dans des domaines délicats sont conscientes des menaces économiques et de sécurité actuelles et émergentes »[78], l'agence ne dispose toujours pas des pouvoirs législatifs nécessaires pour partager de manière proactive des renseignements et des conseils sur les menaces avec ces organisations.[79] Il ne s'agit en aucun cas d'une approche cohérente pour lutter contre les auteurs de menace stratégique qui pensent à long terme et opèrent de manière sophistiquée et généralisée. L'ère des correctifs politiques après coup est révolue.

[76]Voir Comité des parlementaires sur la sécurité nationale et le renseignement, « Rapport annuel 2019 », Gouvernement du Canada, 12 mars 2020, paragraphe 296, lien : https://www.nsicop-cpsnr.ca/reports/rp-2020-03-12-ar/annual_report_2019_public_fr.pdf

[77] Voir Comité des parlementaires sur la sécurité nationale et le renseignement, « Rapport annuel 2019 », Gouvernement du Canada, 12 mars 2020, paragraphe 294, lien : https://www.nsicop-cpsnr.ca/reports/rp-2020-03-12-ar/annual_report_2019_public_fr.pdf

[78] Voir Ministre de la Sécurité publique Canada, « Lettre de mandat du directeur 2022 », Gouvernement du Canada, 27 mai 2023, lien : https://www.canada.ca/fr/service-renseignement-securite/organisation/transparence/mandate-dir-mandat-fra.html.

[79] S'adressant à une foule de chercheurs à l'Université de Waterloo en 2021, le directeur du Service canadien du renseignement de sécurité a noté que « [l]a Loi permet au Service de prodiguer des conseils au gouvernement, mais limite sa capacité de fournir des conseils utiles à des partenaires clés, dont bon nombre d'entre vous sont à l'écoute en ce moment ». Voir Service canadien du renseignement de sécurité, « Allocution de M. David Vigneault, directeur du SCRS, au Centre pour l'innovation dans la gouvernance internationale », Gouvernement du Canada, 9 février 2021, lien : https://www.securitepublique.gc.ca/cnt/trnsprnc/brfng-mtrls/prlmntry-bndrs/20210625/28-fr.aspx.


99 Bank, Suite / bureau 1001, Ottawa, Canada K1P 6B9

## Le Canada doit rattraper ses alliés

Le Canada doit modifier radicalement sa façon d'aborder la sécurité nationale. Pour ce faire, il devra se doter d'une stratégie globale de sécurité nationale qui tienne compte de la complexité des moyens utilisés par les auteurs de menace stratégique pour miner le Canada[80], tout en reconnaissant explicitement que la sécurité économique est au cœur d'une vision nationale plus large, celle d'un pays plus sûr.

Ce n'est qu'ainsi que le gouvernement du Canada pourra tirer pleinement parti de toutes les facettes de sa puissance nationale — y compris ses capacités diplomatiques, de défense, financières, économiques, technologiques et de renseignement — pour préserver de manière efficace notre sécurité économique et garantir notre prospérité, notre sécurité et notre souveraineté communes en cette période de risques géopolitiques accrus.

La seule et unique politique de sécurité nationale du Canada — *protéger une société ouverte[81]* — n'est pas à la hauteur de la tâche. Publiée il y a près de vingt ans, alors que les attaques terroristes, les armes de destruction massive et l'épidémie de SRAS étaient les préoccupations du moment, cette politique ne mentionne pratiquement pas les menaces qui pèsent aujourd'hui sur la sécurité économique du pays.

*Protéger une société ouverte* ne correspond donc pas du tout aux stratégies modernes de sécurité nationale des alliés les plus proches du Canada :

La stratégie de sécurité nationale 2022 des États-Unis énonce clairement le principe selon lequel *la sécurité économique est la sécurité nationale.* La stratégie américaine envisage la sécurité économique d'un point de vue global et multidimensionnel, y compris les échanges et le commerce, la stratégie industrielle et les règles gouvernant le cyberespace. La stratégie souligne que « si les États-Unis veulent réussir [...], nous devons investir dans notre innovation et notre force industrielles, et renforcer notre résilience, chez nous ».[82]

Réfléchissant aux « changements dans l'équilibre des pouvoirs [mondiaux] et à l'intensification des compétitions géopolitiques », la stratégie de sécurité nationale 2022 du Japon affirme que « des questions qui n'étaient pas nécessairement considérées comme des cibles de sécurité par le passé, telles que les vulnérabilités de la chaîne d'approvisionnement, les menaces croissantes pesant sur les infrastructures essentielles et les luttes de pouvoir sur les technologies de pointe, sont [...] devenues un défi majeur en matière de sécurité ». La stratégie de sécurité du Japon affirme ainsi que « la portée de la sécurité s'est élargie pour inclure le secteur économique, ce qui rend les mesures économiques encore plus nécessaires pour garantir la sécurité ».[83]

[80] Voir Aaron Shull et Wesley Wark, « Reimagining a Canadian National Security Strategy », Centre pour l'innovation dans la gouvernance internationale, 6 décembre 2021, lien : https://www.cigionline.org/publications/reimagining-a-canadian-national-security-strategy/ ; Groupe de travail sur la sécurité nationale, « Une stratégie de sécurité nationale pour les années 2020 », École supérieure d'affaires publiques et internationales, Université d'Ottawa, mai 2020, lien : https://www.uottawa.ca/publisher/sites/g/files/bhrskd311/files/2022-12/rapport_secnat_esapi_mai2022.pdf.
[81] Voir Bureau du Conseil privé, « Protéger une société ouverte : la politique canadienne de sécurité nationale », Gouvernement du Canada, avril 2004, lien : https://publications.gc.ca/collections/Collection/CP22-77-2004F.pdf.
[82] Voir Gouvernement des États-Unis, « National Security Strategy », octobre 2022, page 11, lien : https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf.
[83] Voir Gouvernement du Japon, « National Security Strategy of Japan », décembre 2022, pages 1 et 6, lien : https://www.cas.go.jp/jp/siryou/221216anzenhoshou/nss-e.pdf.


99 Bank, Suite / bureau 1001, Ottawa, Canada K1P 6B9

La stratégie de sécurité nationale de l'Allemagne pour 2023, intitulée à juste titre *Integrated Security for Germany* [Sécurité intégrée pour l'Allemagne], suit la même logique. On y lit ce qui suit : « Au XXIe siècle, la sécurité signifie s'assurer que notre chauffage fonctionne en hiver, [...] avoir des téléphones intelligents qui fonctionnent parce que l'approvisionnement en puces nécessaires est fiable, [...] se rendre au travail en toute sécurité parce que nos trains ne sont pas paralysés par des cyberattaques ».[84]

Même la stratégie de sécurité nationale de l'Australie de 2013 identifie des impératifs économiques clés, tels que la protection de la propriété intellectuelle, des infrastructures essentielles et des chaînes d'approvisionnement, comme étant essentiels à sa sécurité nationale. La stratégie australienne souligne qu'« il existe un lien de renforcement mutuel entre notre sécurité nationale et notre bien-être économique, [...] une économie saine soutient notre stabilité et notre sécurité, qui à son tour est propice à la poursuite de nos objectifs économiques personnels et nationaux ».[85]

Le Canada a besoin d'une stratégie de sécurité nationale qui accorde une place centrale à la sécurité économique. Cette stratégie doit décrire les défis actuels et anticipés en matière de sécurité économique, le rôle de la sécurité économique dans la promotion de la sécurité nationale du Canada, les objectifs de la politique de sécurité économique et les moyens par lesquels le Canada peut atteindre ces objectifs.

La stratégie doit également être équilibrée. Tout en étant capable de faire face aux menaces auxquelles les Canadiens sont confrontés au pays et à l'étranger, elle doit également rester conforme aux valeurs démocratiques du Canada et veiller à ce que l'environnement national et international reste propice aux activités transfrontalières bénéfiques, telles que le commerce et l'immigration économique, qui sont au cœur de nos intérêts nationaux.

Autrement dit, la protection de la sécurité économique du Canada ne doit pas servir de prétexte au gouvernement du Canada pour porter atteinte aux droits des Canadiens, adopter des règles protectionnistes en matière de commerce et d'investissement ou découpler complètement ses relations avec les auteurs de menace stratégique.

Ce point ne peut être négligé. Certains des plus proches alliés du Canada ont réagi à notre nouvelle réalité géopolitique d'une manière qui n'est pas toujours à la hauteur de leur engagement à l'égard de l'ordre international fondé sur des règles[86]. Dans de rares cas, ces actions pourraient s'avérer tout aussi néfastes pour la prospérité économique du Canada que la menace posée par les auteurs de menace stratégique.

---

[84] Voir Gouvernement allemand, « Robust, Resilient, Sustain : Integrated Security for Germany », juin 2023, page 6, lien : https://www.nationalesicherheitsstrategie.de/National-Security-Strategy-EN.pdf.
[85] Voir Gouvernement allemand, « Strong and Secure: A Strategy for Australia's National Security », 2013, page 4, lien : https://www.files.ethz.ch/isn/167267/Australia%20A%20Strategy%20for%20National%20Securit.pdf.
[86] Il s'agit notamment des efforts visant à miner la capacité des pays à faire respecter efficacement leurs droits conformément aux règles commerciales reconnues à l'échelle mondiale. Voir Keith Johnson, « How Trump May Finally Kill the WTO », Foreign Policy, 9 décembre 2019, lien : https://foreignpolicy.com/2019/12/09/trump-may-kill-wto-finally-appellate-body-world-trade-organization/. Il comprend également l'adoption de mesures économiques protectionnistes, telles que la volonté d'utiliser la réglementation et le pouvoir de marché, pour faire pencher les règles du jeu économique en leur faveur. Voir Rapport du Comité permanent du commerce international, « Répercussions commerciales sur certains secteurs canadiens de la loi américaine de 2022 sur la réduction de l'inflation », Chambre des communes, mai 2023, pages 10-12, lien : https://www.ourcommons.ca/content/Committee/441/CIIT/Reports/RP12414355/441_CIIT_Rpt9_PDF/441_CIIT_Rpt9-f.pdf.

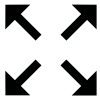

99 Bank, Suite / bureau 1001, Ottawa, Canada K1P 6B9 THEBUSINESSCOUNCIL.CA

## Recommandations pour une stratégie de sécurité nationale

Pour remédier aux vulnérabilités les plus flagrantes de la posture de sécurité économique du Canada, nous exhortons le gouvernement du Canada à adopter, dans le cadre de sa nouvelle stratégie de sécurité nationale, des mesures visant à :

renforcer l'architecture de la sécurité économique du Canada,

renforcer les capacités économiques et d'innovation du Canada, et



élargir et redynamiser les partenariats internationaux du Canada en matière de sécurité.

### Renforcer l'architecture de la sécurité économique du Canada :

Les auteurs de menace stratégique n'ont pas l'intention d'entreprendre les réformes structurelles nécessaires pour mettre les entreprises canadiennes sur un pied d'égalité. Par conséquent, un treillis de lois, de politiques et de programmes nouveaux et interconnectés sera nécessaire pour améliorer la capacité des entreprises canadiennes à dissuader, détecter et interrompre les menaces auxquelles notre pays est confronté.

Recommandations :

1. Le gouvernement du Canada devrait revoir et modifier en profondeur la *Loi sur le Service canadien du renseignement de sécurité* afin d'aligner le mandat législatif et les pouvoirs de l'agence sur les attentes croissantes en matière d'identification, d'analyse et d'interruption des menaces pesant sur la sécurité économique du Canada. La *Loi modifiée sur le Service canadien du renseignement de sécurité* devrait notamment permettre à l'agence de partager de manière proactive des renseignements opportuns et exploitables sur les menaces avec des parties prenantes extérieures au gouvernement fédéral, y compris des entreprises, lorsque cela est dans l'intérêt public et sous réserve de toutes les garanties et de tous les contrôles nécessaires.

2. Le gouvernement du Canada devrait fournir au Service canadien du renseignement de sécurité les ressources nécessaires pour lancer une nouvelle division ayant pour mandat exprès de former et de conseiller un large éventail d'entités du secteur privé sur la manière de se défendre contre les menaces économiques. L'agence devrait s'inspirer des modèles établis dans les pays alliés, tels que la National Protective Security Authority du MI5.

3. Afin de réduire les risques pour la sécurité de l'approvisionnement, de prévenir les dépendances à l'égard des infrastructures essentielles et de contrer le transfert problématique de technologies sensibles, le gouvernement du Canada devrait modifier

les dispositions relatives à la sécurité nationale de la *Loi sur Investissement Canada* afin de cibler et de filtrer plus précisément les investissements étrangers malveillants. La modification de la *Loi sur Investissement Canada* devrait inclure l'obligation pour le gouvernement du Canada d'intégrer de manière formelle les perspectives uniques des entreprises canadiennes sur les menaces nouvelles et émergentes pour la sécurité nationale dans le cadre du processus d'examen des investissements.

4. Afin d'améliorer la capacité des organismes d'application de la loi à lutter contre les menaces à la sécurité économique, le gouvernement du Canada devrait renforcer l'infraction d'espionnage économique prévue par la *Loi sur la protection de l'information*. Parallèlement à cette initiative, le gouvernement du Canada devrait élaborer un nouveau régime juridique qui permette l'utilisation de renseignements comme éléments de preuve dans le cadre de poursuites pénales, tout en respectant le principe constitutionnel d'un procès équitable pour l'accusé.

5. Pour renforcer la cybersécurité et la résilience des infrastructures essentielles, le gouvernement du Canada devrait :

    - suivre l'exemple des États-Unis et légiférer sur les protections de la sphère de sécurité[87] afin d'éliminer les obstacles juridiques inutiles qui empêchent les entreprises de collaborer volontairement entre elles et avec les gouvernements pour relever les défis cybernétiques,

    - explorer de nouveaux mécanismes juridiques pour encourager les concepteurs de produits et services numériques utilisés par les opérateurs d'infrastructures essentielles à prendre toutes les précautions raisonnables pour sécuriser leurs produits, et

    - créer un centre d'excellence au sein du Centre canadien pour la cybersécurité afin de

        › rassembler les partenaires des secteurs public et privé afin d'unifier leurs actions défensives par le biais d'une planification, d'une préparation et d'une réponse synchronisées en matière de cybersécurité, à l'instar de ce que fait le Joint Cyber Defense Collaborative de la Cybersecurity and Infrastructure Security Agency des États-Unis ;

        › encourager un échange d'informations plus significatif et réciproque au sein du gouvernement et des fournisseurs d'infrastructures essentielles et entre eux, notamment en ce qui concerne les nouvelles menaces qui pèsent sur les cybersystèmes essentiels, le bilan de sécurité des technologies actuelles et les avantages relatifs des différentes mesures de sécurité ;

        › organiser et soutenir des exercices réguliers de simulation et de chasse aux menaces au cours desquels les fournisseurs d'infrastructures essentielles et les parties prenantes gouvernementales interviennent lors d'incidents simulés afin d'améliorer leurs réponses collectives aux incidents cybernétiques graves ;

[87] Par exemple, le gouvernement du Canada devrait expliciter dans la Loi sur la concurrence que les collaborations entre concurrents qui n'ont pas de répercussions anticoncurrentielles sont autorisées.


99 Bank, Suite / bureau 1001, Ottawa, Canada K1P 6B9 THEBUSINESSCOUNCIL.CA

- mettre en place un processus systématisé d'examen des cyberintrusions importantes afin de recueillir et de partager les enseignements tirés et de formuler des recommandations concrètes pour améliorer la cybersécurité et la résilience ; et

- offrir des services d'intervention en cas d'incident sur place aux fournisseurs d'infrastructures essentielles qui ont besoin d'une assistance immédiate.

**6.** Afin de préserver notre accès continu aux intrants économiques essentiels, tout en renforçant la capacité du gouvernement du Canada à agir de manière indépendante sur la scène mondiale, le gouvernement du Canada devrait collaborer avec les secteurs vulnérables à la coercition économique pour renforcer la profondeur et la résilience des chaînes d'approvisionnement essentielles. Il s'agit notamment de procéder à des examens de la vulnérabilité, de partager les informations sur les menaces, d'élaborer des stratégies d'atténuation solides, de réduire la forte dépendance aux auteurs de menace stratégique et d'accroître la disponibilité de possibilités commerciales sur le marché libre.

**7.** Pour atténuer l'impact des pratiques mercantilistes, le gouvernement du Canada devrait créer de nouveaux mécanismes juridiques pour bloquer l'importation de produits et de services étrangers qui ont profité de manière importante de pratiques économiques déloyales. Le gouvernement du Canada devrait d'abord s'attacher à bloquer l'accès au marché des auteurs de menace stratégique dans les secteurs essentiels où ils prennent des moyens illégaux pour rattraper et surpasser le Canada.

**8.** Pour dissuader, dénoncer et sanctionner les acteurs qui menacent l'intégrité des systèmes d'infrastructures essentielles, le gouvernement du Canada devrait suivre l'exemple des États-Unis et modifier le *Code criminel* pour criminaliser expressément les actes volontaires ou de négligence qui entravent de manière importante les infrastructures essentielles, en prévoyant des sanctions financières, des peines d'emprisonnement, ou les deux.

**9.** Pour éviter que la recherche universitaire canadienne ne serve les intérêts des auteurs de menace stratégique à nos dépens, le gouvernement du Canada devrait, dans des circonstances dûment justifiées, interdire aux entités liées à ces États de participer à la recherche universitaire canadienne ou d'en tirer profit.

**10.** Pour permettre une interruption plus rapide et plus efficace de l'influence étrangère malveillante, ainsi que pour sensibiliser davantage le public à la nature, à l'échelle et à la portée des activités étrangères dans les affaires intérieures, le gouvernement du Canada devrait aller de l'avant avec l'adoption d'un régime de transparence en matière d'influence étrangère. À l'instar des régimes existants aux États-Unis, en Australie et au Royaume-Uni, le régime canadien devrait exiger des entités agissant au nom d'un État étranger qu'elles déclarent publiquement leurs activités visant à influencer la prise de décision gouvernementale ou l'opinion publique. L'adoption de tout registre doit tenir compte des valeurs véhiculées dans notre démocratie, notamment notre engagement à être un lieu ouvert, libre et accueillant pour étudier, travailler et investir.

## Renforcer les capacités économiques et d'innovation du Canada :

Nous devons abandonner l'idée qu'il est possible pour les entreprises canadiennes de rivaliser sur un pied d'égalité avec les champions des États dans la conception et la commercialisation de technologies émergentes et perturbatrices. Ces derniers ne respectent tout simplement pas les règles établies.

Pour s'imposer dans ces circonstances, le gouvernement du Canada devra compléter la capacité économique et innovante des entreprises canadiennes par une stratégie industrielle moderne. Cette stratégie doit accroître la capacité de notre pays à transformer systématiquement le capital intellectuel en technologies de pointe et en entreprises compétitives à l'échelle internationale.

Le gouvernement du Canada doit identifier et soutenir les technologies de pointe qui sont essentielles pour stimuler la croissance économique, stratégique du point de vue de la sécurité nationale, et pour lesquelles les entreprises ne sont pas encore en mesure de faire les investissements nécessaires pour les développer et les commercialiser. L'objectif doit être d'aider les entreprises canadiennes à faire ce qu'elles font le mieux : innover, se développer et concurrencer sur le marché global.

Ensemble, ces investissements appuieront des millions d'emplois sûrs et bien rémunérés en encourageant l'activité économique à hauteur de milliards de dollars. Ils renforceront également notre capacité à agir de manière autonome sur la scène internationale en réduisant la vulnérabilité du Canada à la coercition économique, et stimuleront le pouvoir économique du pays, lui donnant ainsi les moyens d'investir dans notre sécurité.

Recommandations :

1. Le gouvernement du Canada devrait moderniser son architecture scientifique et technologique afin de récompenser la recherche à haut risque et à haut rendement dans les domaines technologiques émergents et perturbateurs essentiels à notre sécurité économique et nationale. Lors de la modernisation des programmes, une attention particulière devrait être accordée à la suppression des sources étrangères de financement de la recherche universitaire qui posent problème, ainsi qu'au maintien et à la commercialisation de la recherche plus avancée au Canada.

2. Le gouvernement du Canada devrait stimuler l'innovation canadienne dans les domaines technologiques émergents et perturbateurs essentiels à notre sécurité économique et nationale, tout en intégrant les nouvelles technologies au sein du gouvernement canadien, grâce à un recours stratégique à l'approvisionnement du secteur public. Pour ce faire, le gouvernement du Canada devrait s'inspirer des modèles agiles et axés sur les défis utilisés dans les pays alliés, tels que la Defense Advanced Research Projects Agency (DARPA) des États-Unis, qui connaît un grand succès.

3. Pour renforcer les capacités de renseignement du Canada, soutenir les institutions universitaires et créer de nouvelles possibilités économiques pour les entreprises, le gouvernement du Canada devrait s'associer à des chercheurs universitaires et à des entreprises de confiance pour développer et déployer conjointement des solutions de sécurité avancées au sein de la communauté canadienne du renseignement. Le gouvernement du Canada devrait s'inspirer de l'approche adoptée par l'Intelligence Advanced Research Projects Activity des États-Unis. Cette agence gouvernementale

spécialisée investit dans des recherches à haut risque et à haut rendement qui repoussent les limites de la science et de la technologie afin de permettre à la communauté américaine du renseignement d'accomplir son travail mieux et plus efficacement.

**4.** Le Canada doit investir dans ce qui est au cœur de la croissance économique et de l'innovation : le talent. Le gouvernement du Canada doit :

- réorienter les programmes canadiens d'immigration de la catégorie économique afin que les secteurs essentiels à la sécurité économique et nationale du Canada aient un accès rapide et fiable aux talents internationaux de confiance, spécialisés et hautement qualifiés dont ils ont besoin pour stimuler l'innovation, se développer et concurrencer à l'échelle internationale ;

- renforcer les organisations qui ont fait leurs preuves en matière de recrutement et de formation des groupes sous-représentés dans les domaines de la sécurité, telles que Rogers Cybersecure Catalyst ;

- inciter les établissements d'enseignement postsecondaire proposant des programmes de sécurité de premier plan, tels que l'Université du Nouveau-Brunswick et le Durham College, à accroître les taux d'inscription et à offrir aux étudiants davantage de possibilités d'apprentissage pratique ; et

- accroître la capacité du Canada à attirer, cultiver et retenir des talents de classe mondiale dans le domaine de la sécurité multipliant les possibilités d'échanges de personnel entre les entreprises fiables et les ministères et organismes gouvernementaux, tels que les Forces armées canadiennes, le Centre de la sécurité des télécommunications, la Gendarmerie royale du Canada et le Service canadien du renseignement de sécurité.

## Élargir et redynamiser les partenariats internationaux du Canada en matière de sécurité :

Les partenariats internationaux du Canada en matière de sécurité — y compris la participation au G7, au Groupe des cinq, à NORAD et à l'OTAN — comptent parmi les atouts stratégiques les plus importants du pays. En offrant une plateforme pour la coopération en matière de sécurité, les partenariats internationaux du Canada en matière de sécurité servent de multiplicateur de force, amplifiant la capacité du Canada à répondre aux défis de sécurité économique communs qui affectent les Canadiens au pays et à l'étranger.

Le Canada doit élargir et revigorer son réseau d'alliances et de partenariats en matière de sécurité afin de maintenir et de renforcer les principes, les institutions et l'ordre international fondé sur des règles qui ont permis tant de stabilité, de prospérité et de croissance. L'objectif final du Canada devrait être un monde dans lequel le comportement responsable de l'État est la norme, et où le comportement irresponsable est isolant et coûteux.

Recommandations :

1. L'armée canadienne reste le garant de la paix, de la stabilité et de la prospérité du pays, ainsi que de notre engagement envers les nations alliées. Le gouvernement du Canada devrait s'engager à nouveau à atteindre l'objectif d'investissement en matière de défense de deux pour cent du PIB fixé lors du *Sommet du Pays de Galles en 2014* de l'OTAN.Compte tenu du dernier sommet de l'OTAN à Vilnius, en Lituanie, cet engagement doit être interprété comme un « plancher » et non comme un « plafond ».

2. Afin de mieux surveiller, atténuer et contrôler les menaces qui pèsent sur les infrastructures transfrontalières fortement intégrées du Canada et des États-Unis, le gouvernement du Canada devrait créer un groupe de travail bilatéral officiel entre les secteurs public et privé. Composé d'un échantillon représentatif de dirigeants des secteurs public et privé, ce groupe aurait pour objectif de faciliter l'échange libre, franc et confidentiel d'informations stratégiques sur l'évolution du contexte de la menace ainsi que sur les moyens par lesquels les gouvernements et les entreprises peuvent collaborer à bâtir une Amérique du Nord plus forte et plus sûre.

3. Compte tenu de l'importance du commerce international pour la sécurité et la prospérité des Canadiens, le gouvernement du Canada, en partenariat avec d'autres alliés aux vues similaires, devrait renforcer l'ordre économique fondé sur des règles en :

    - renforçant le système commercial multilatéral, avec l'Organisation mondiale du commerce au centre ;

    - renforçant ou en adhérant à des cadres internationaux promouvant les échanges et les investissements internationaux libres et équitables entre les pays axés sur le marché, tels que l'Accord de Partenariat transpacifique global et progressiste et le Cadre économique indo-pacifique ; et

    - créant et renforçant des mesures plurilatérales pour prévenir, résister et contrer collectivement la coercition économique et d'autres pratiques commerciales déloyales, par exemple par le biais d'une « OTAN pour le commerce » dans laquelle les nations alliées acceptent de se porter mutuellement secours lorsqu'elles font l'objet d'une menace économique. Dans le cadre de cette initiative, le Canada devrait tirer parti de ses

avantages économiques, notamment dans la production d'énergie, de nourriture et de minéraux, pour aider à réduire les dépendances commerciales de nos alliés à l'égard des auteurs de menace stratégique.

4. Le gouvernement du Canada devrait collaborer plus étroitement avec ses partenaires du Groupe des cinq et d'autres alliés aux vues similaires afin d'affaiblir les cyberacteurs. Les mesures à prendre sont notamment les suivantes :

   - dissuader, attribuer et intervenir conjointement dans les cyberattaques qui enfreignent les règles et les normes mondiales dans le cyberespace ;
   - mettre fin aux marchés en ligne illégaux d'outils et de services cybernétiques, qui réduisent le temps de démarrage et le niveau de sophistication nécessaire aux acteurs malveillants pour cibler et saboter les entreprises canadiennes ;
   - mieux réglementer les cryptoactifs et les échanges, qui sont exploités par les acteurs malveillants pour dissimuler leur identité et masquer leurs activités aux agences de sécurité nationale et d'application de la loi ; et
   - accroître la pression sur les pays dont les lois et l'application de la loi en matière de cybercriminalité et d'autres activités cybernétiques malveillantes sont indulgentes ou inexistantes.

5. Pour renforcer les capacités du Canada en matière de cybersécurité, d'intelligence artificielle et de technologie quantique, le gouvernement du Canada devrait chercher à adhérer à *AUKUS*, le pacte trilatéral de coopération en matière de sécurité et de technologie conclu entre les États-Unis, le Royaume-Uni et l'Australie. Le gouvernement du Canada devrait d'abord se concentrer sur le deuxième pilier institutionnel d'AUKUS, qui vise à faire progresser ces technologies et d'autres technologies importantes.

6. Les normes techniques internationales ont une incidence directe sur la sécurité nationale du Canada, notamment en limitant l'utilisation abusive de technologies émergentes et perturbatrices qui pourraient menacer la sécurité économique du Canada. Le gouvernement du Canada devrait intensifier sa collaboration avec les entreprises canadiennes afin de soutenir l'élaboration et la mise en œuvre de normes techniques internationales pour les technologies de la prochaine génération qui reflètent nos intérêts nationaux ainsi que les valeurs démocratiques et d'économie de marché.

7. Afin de renforcer l'influence diplomatique du Canada, d'encourager une plus grande collaboration avec les nations aux vues similaires et de promouvoir les intérêts économiques du Canada, le gouvernement du Canada devrait poursuivre un programme de « diplomatie économique », dans le cadre duquel la capacité industrielle du pays est mise à profit pour contribuer à relever les défis mondiaux en matière de sécurité.

## L’exécution et l’évaluation seront essentielles

Une nouvelle stratégie de sécurité nationale n’est pas la fin du chemin, mais le début. La stratégie ne pourra atteindre son objectif que si son contenu est pleinement mis en œuvre. Les mesures incluses dans une nouvelle stratégie doivent donc être mises en œuvre en temps voulu et de manière efficace.

En outre, étant donné qu’une grande partie du champ de bataille que le gouvernement du Canada doit disputer échappe à son contrôle direct, un partenariat approfondi et durable avec les entreprises canadiennes, du niveau stratégique au niveau tactique, sera nécessaire pour parvenir au succès. La consultation ne suffira pas.

Enfin, pour rester pertinente dans un contexte de menaces en évolution rapide, une nouvelle stratégie doit être considérée comme un « document dynamique ». Elle doit être évaluée régulièrement et systématiquement, par exemple tous les trois ans, pour s’assurer qu’elle répond à ses objectifs. Le gouvernement du Canada doit apporter les révisions nécessaires à la stratégie s’il s’attend à des changements importants.

Pour que ces mesures soient prises et se voient accorder une priorité adéquate, nous demandons instamment que :

1. le nouveau comité ministériel sur la sécurité nationale et le renseignement — le Conseil de sécurité nationale — soit présidé par le premier ministre et composé de tous les ministres et hauts fonctionnaires compétents ayant un mandat dans le domaine de la sécurité, afin d’assurer une direction et une prise de décision durables et avant-gardistes nécessaires à la mise en œuvre de la nouvelle stratégie de sécurité nationale ;

2. le rôle du conseiller à la sécurité nationale et au renseignement soit défini dans la législation et renforcé pour mieux organiser et coordonner la communauté du renseignement ainsi que pour consulter les entreprises canadiennes, les mobiliser et établir des partenariats avec elles ;

3. le premier ministre modifie les lettres de mandat de tous les ministres concernés, notamment ceux de la Sécurité publique, des Affaires étrangères, de la Défense nationale, de l’Industrie et des Finances, afin de s’assurer que les considérations de sécurité économique sont intégrées dans chacune de leurs priorités ;

4. une division dédiée à la sécurité économique soit créée au sein du Bureau du Conseil privé et que des unités de sécurité économique soient créées ou renforcées au sein de tous les grands ministères, notamment ceux de la Sécurité publique, des Affaires étrangères, de la Défense nationale, de l’Industrie et des Finances, afin de mieux planifier et coordonner les politiques de sécurité économique en partenariat avec les entreprises canadiennes ;

5. le gouvernement du Canada publie des plans de mise en œuvre annuels qui définissent les mesures précises que le gouvernement a l’intention de prendre au cours d’une année civile donnée pour mettre en œuvre la nouvelle stratégie ; et

6. dans les 18 mois suivant le lancement d'une nouvelle stratégie de sécurité nationale, le Comité des parlementaires sur la sécurité nationale et le renseignement lance une étude spéciale sur le cadre du gouvernement du Canada pour faire face aux menaces à la sécurité économique, et que le gouvernement du Canada y réponde, en vue de :

    - identifier les lacunes qui existent dans la législation, les politiques ou les mécanismes de gouvernance ;
    - renforcer la responsabilité ministérielle ; et
    - améliorer la transparence, notamment en aidant les entreprises à mieux comprendre les rôles des organismes gouvernementaux chargés de les servir.

Dans le cadre de cette étude, le Comité devrait lancer une « tournée de présentation » de la sécurité économique, à l'instar des tournées bipartisanes organisées par le Senate Select Committee on Intelligence des États-Unis, afin de tirer des leçons des entreprises qui se trouvent sur la ligne de front de l'attaque.

## Les entreprises les plus innovantes et les plus prospères du Canada sont disposées à faire leur part

Chaque année, les entreprises les plus innovantes et les plus prospères du Canada dépensent des milliards de dollars pour défendre les Canadiens contre une liste croissante de menaces à la sécurité économique. Elles investissent notamment dans des mesures de détection, d'atténuation et de réaction aux attaques, établissent des partenariats avec des établissements d'enseignement supérieur pour former des professionnels de la sécurité et mettre au point des technologies défensives, et partagent des renseignements sur les menaces, de l'expertise et des pratiques exemplaires avec les gouvernements et les pairs de l'industrie.

Par exemple, dans les secteurs des infrastructures essentielles, comme l'énergie, les transports et les télécommunications, la plupart des membres du Conseil canadien des affaires investissent individuellement bien plus de 100 millions de dollars par an au Canada dans des mesures de prévention, de détection et d'intervention en cas d'incidents liés à la cybersécurité. Un nombre appréciable de ces membres investissent individuellement plus de 500 millions de dollars par année.

S'appuyant sur leur expérience et leur expertise approfondies, les entreprises les plus innovantes et les plus prospères du Canada sont prêtes à collaborer avec le gouvernement du Canada pour élaborer et mettre en œuvre une nouvelle stratégie de sécurité nationale. Cela comprend, sans s'y limiter, ce qui suit :

1. renforcer la résilience économique du Canada en augmentant le montant investi chaque année dans des mesures visant à détecter, prévenir et interrompre les menaces à la sécurité économique du Canada ;

2. partager davantage avec le gouvernement les menaces qu'ils observent sur le terrain afin de mieux informer la politique gouvernementale et d'améliorer la capacité des agences de sécurité nationale à examiner, analyser et interrompre les menaces ;

3. accroître leurs investissements dans la recherche universitaire canadienne pour aider à remplacer les sources étrangères de financement problématiques et pour conserver et commercialiser une recherche plus avancée au pays ; et

4. mieux soutenir leurs chaînes d'approvisionnement vastes et diversifiées, notamment par l'éducation, le renforcement des capacités et le courtage en relations, afin d'accroître la sensibilisation aux menaces auxquelles sont confrontées les petites et moyennes entreprises, ainsi qu'aux rôles et responsabilités des organismes gouvernementaux chargés de les servir.

## Conclusion

L'ordre unipolaire libre, ouvert et relativement stable qui a apporté aux Canadiens des niveaux extraordinaires de sûreté, de sécurité et de prospérité appartient désormais à l'histoire.

Dans notre nouvelle réalité géopolitique, les Canadiens sont confrontés à un environnement turbulent et multipolaire qui fait peser sur leur bien-être économique une menace sans précédent en matière de sécurité nationale.

La santé économique des Canadiens étant plus que jamais liée aux questions de sécurité nationale, le moment est venu pour le gouvernement du Canada de prendre des mesures audacieuses pour protéger les Canadiens.

C'est pourquoi ce rapport demande au gouvernement du Canada de créer une stratégie de sécurité nationale, la première du genre, qui accorde une place centrale à la sécurité économique. Les recommandations contenues dans ce rapport offrent une voie pour aider le gouvernement et les entreprises à naviguer ensemble avec succès dans ce monde nouveau et plus turbulent.

**Citation**
Conseil canadien des affaires, « La sécurité économique est la sécurité nationale : les arguments en faveur d'une stratégie canadienne », 7 septembre 2023.

**À propos du Conseil canadien des affaires**
Fondé en 1976, le Conseil canadien des affaires est un organisme sans but lucratif et non partisan représentant des dirigeants d'entreprises de tous les secteurs et toutes les régions du Canada. Les entreprises membres du Conseil emploient quelque 1,7 million de Canadiens et de Canadiennes, versent la plus grande part des impôts fédéraux sur les sociétés et sont les plus grands contributeurs aux secteurs des exportations du Canada, du mécénat d'entreprise et des investissements du secteur privé en recherche et développement. Au moyen de partenariats dans la chaîne d'approvisionnement, de contrats de service et de programmes de mentorat, les membres du Conseil soutiennent des centaines de milliers de petites entreprises et d'entrepreneurs dans les collectivités de toutes tailles, partout au Canada.

**Avis de non-responsabilité :**
Les opinions présentées dans ce rapport sont celles du Conseil canadien des affaires. Les opinions présentées dans ce rapport ne reflètent pas nécessairement le point de vue des membres individuels du Conseil canadien des affaires et ne doivent donc pas être attribuées à un ou plusieurs de ces membres.


99 Bank, Suite / bureau 1001, Ottawa, Canada K1P 6B9 THEBUSINESSCOUNCIL.CA