Équilibrer la sécurité de la recherche et la science ouverte

Comité d'experts sur la recherche sensible préoccupante

CCA | CAC

Équilibrer la sécurité de la recherche et la science ouverte

Comité d'experts sur la recherche sensible préoccupante

CCA | CAC

CONSEIL DES ACADÉMIES CANADIENNES
180, rue Elgin, bureau 1401, Ottawa (Ontario) Canada K2P 2K3

Le projet sur lequel porte ce rapport a été réalisé avec l'approbation du conseil d'administration du Conseil des académies canadiennes (CAC). Il répond à une demande des commanditaires, Recherche et développement pour la défense Canada (RDDC) et l'Agence de la santé publique du Canada (ASPC), qui souhaitaient obtenir une évaluation indépendante. Les commanditaires n'ont participé ni à la sélection des membres du comité d'experts ni à l'élaboration du rapport. Les opinions, constatations et conclusions exprimées dans cette publication sont celles des auteurs, les membres du comité d'experts sur la recherche sensible préoccupante, et ne reflètent pas nécessairement les points de vue de leurs organisations d'affiliation ou d'emploi.

Ce rapport devrait être cité comme suit :

CAC — Conseil des académies canadiennes, 2025. *Équilibrer la sécurité de la recherche et la science ouverte.* Ottawa, ON : Comité d'experts sur la recherche sensible préoccupante, CAC. https://doi.org/10.60870/9yzn-0018. .

ISBN : 978-1-990592-61-4 (livre électronique)
DOI : 10.60870/9yzn-0018

Merci à :

Conception de la couverture	Ryan Hook, Atiigo Media
Révision	Jody Cooper
Mise en page et conception	Atiigo Media
Traduction, en-fr	Dany Gagnon et Anne-Marie Mesa

Avis de non-responsabilité :

Les mentions faites dans le présent rapport à une entreprise, un produit commercial, un processus ou un service donné par le biais d'un nom commercial, d'une marque de commerce, d'un fabricant ou autre ne constituent pas l'approbation ou la recommandation de celui-ci ou une marque de favoritisme à son égard.

Sauf indication contraire, ce travail est soumis à une licence Creative Commons : Attribution - Utilisation non commerciale - Pas d'œuvre dérivée 4.0 International.

Canada

Ce projet a été rendu possible grâce au soutien du gouvernement du Canada par l'intermédiaire du Fonds stratégique des sciences.

Les bureaux du Conseil des académies canadiennes (CAC) à Ottawa sont situés sur le territoire traditionnel non cédé du peuple algonquin Anishinaabe, qui s'occupe de ces terres depuis des millénaires.

Le CAC participe à la réconciliation et s'engage à honorer la souveraineté autochtone. Dans le cadre de ses activités visant à fournir des données probantes pour la prise de décision, le CAC reconnaît qu'un large éventail de connaissances et d'expériences contribue à l'édification d'une société plus équitable et plus juste. Nous encourageons tous ceux qui participent à notre travail à mieux connaître et reconnaître le contexte passé et présent du territoire aujourd'hui appelé Canada et des nations et peuples autochtones qui en sont les gardiens.

Comité d'experts sur la recherche sensible préoccupante

Les membres du comité d'experts agissent à titre personnel et ne représentent pas leur organisation d'affiliation ou leur employeur. Chaque membre a été sélectionné pour son expertise, son expérience et son leadership démontré dans des domaines pertinents pour ce projet.

Martha Crago, C.M., Ph. D., D. Sc., BVO, (présidente), professeure et ancienne vice-présidente à la recherche et à l'innovation, Université McGill (Montréal, Qc)

Kelly Cobey, Ph. D., directrice, Programme de métarecherche et de science ouverte, Institut de cardiologie de l'Université d'Ottawa (Ottawa, Ont.)

Jim Ghadbane, ancien président-directeur général, CANARIE Inc. (Ottawa, Ont.)

Garfield Giff, Ph. D., chaire de recherche, Adaptation aux changements climatiques, Institut de recherche Aurora (Inuvik, T.N.-O.)

Jacqueline Littlewood, M.A., directrice, Sécurité de la recherche, Université de l'Alberta (Edmonton, Alb.)

Allison M. Macfarlane, Ph. D., professeure et directrice, École des politiques publiques et des affaires mondiales, Université de la Colombie-Britannique (Vancouver, C.-B.)

Rebecca Moritz, M.Sc., CBSP (ABSA), SM (NRCM), directrice, Bureau de la collaboration et de la conformité en matière de recherche, Bureau du vice-président à la recherche, Université d'État du Colorado (Fort Collins, CO)

Delilah Ofosu-Barko, B. Sc. méd. avec distinction, directrice, Institute for Better Health Operations, Trillium Health Partners (Mississauga, Ont.)

Catherine Olivier, Ph. D., professeure adjointe de clinique, Département de médecine sociale et préventive, École de santé publique, Université de Montréal (Montréal, Qc)

Jocelyn Tremblay, ancien directeur général, Sciences et génie, Recherche et développement pour la défense Canada (Québec, Qc)

Andrew Van Kessel, Ph. D., directeur de la recherche, Vaccine and Infectious Disease Organization (VIDO), Université de Saskatchewan (Saskatoon, Sask.)

Anya Waite, Ph. D., directrice générale et scientifique, Ocean Frontier Institute, Université Dalhousie (Halifax, N.-É.)

Matthew S. Wiseman, Ph. D., professeur adjoint, filière d'enseignement, Département d'histoire, Université de Waterloo (Waterloo, Ont.)

Message de la présidente

Le Canada contribue de manière appréciable à la recherche et a un impact important sur l'écosystème scientifique mondial. Tous les aspects de la recherche et de l'innovation peuvent être considérés comme sensibles, c'est-à-dire que, bien qu'ils soient destinés à des fins bénéfiques, ils peuvent également être utilisés par des acteurs malveillants pour nuire au public, à la santé publique, à la sécurité publique et à la sécurité économique et nationale. À une époque où l'innovation s'accélère et où le paysage géopolitique se transforme rapidement, les enjeux liés à la protection de la recherche sensible au Canada se sont accrus de manière très nette.

La recherche sensible est une part intégrante du progrès scientifique et, par extension, des intérêts nationaux du Canada. Elle revêt une valeur inestimable pour la santé publique, le savoir-faire militaire, la souveraineté dans l'Arctique, la biosécurité, la résilience climatique et l'innovation technologique, entre autres domaines. Le défi qui nous attend n'est pas de savoir *si* nous devons mener des recherches sensibles, mais *comment* le faire de manière responsable et sécuritaire. Notre soutien à la science ouverte doit être envisagé parallèlement à la sécurité de la recherche, l'ouverture favorisant la découverte, accélérant l'innovation et permettant la mise en commun des connaissances. À cette fin, la protection de la recherche sensible nécessite des mesures de sécurité réfléchies et adaptatives. Celles-ci doivent être modulées en fonction du risque présenté par la recherche en question; elles seront mises en œuvre tout au long du cycle de vie de la recherche et s'appuieront sur des politiques fondées sur des données probantes. La sécurité de la recherche ne doit pas se faire au détriment du progrès scientifique : elle doit plutôt favoriser la confiance et la viabilité à long terme de l'écosystème lui-même.

La sécurité de la recherche nécessite une responsabilité partagée entre tous les acteurs de l'écosystème de la recherche, des chercheurs individuels et des dirigeants institutionnels aux organismes de financement, en passant par les ministères, les services de renseignement et le secteur privé. Chacun joue un rôle essentiel dans la reconnaissance, l'évaluation et l'atténuation des risques d'utilisation abusive de la recherche. Il est essentiel de clarifier les rôles, les responsabilités et les attentes afin de promouvoir une culture de la sécurité qui soit en phase avec l'engagement pour la science ouverte.

Le Canada est bien placé pour jouer un rôle de premier plan dans l'élaboration et la promotion de modèles de sécurité de la recherche qui protègent les intérêts nationaux comme l'écosystème scientifique mondial, tout en encourageant la mise en commun responsable. En investissant dans

l'éducation, la formation et le renforcement des capacités qui tiennent compte de la diversité de nos environnements de recherche – y compris les droits des Premières Nations, des Inuits et des Métis sur la recherche touchant leurs communautés, – nous pouvons bâtir un écosystème de la recherche dans lequel l'ouverture et la sécurité sont des valeurs qui se renforcent mutuellement.

La recherche sensible se déroule dans un paysage complexe. Je rends hommage à mes collègues pour la finesse avec laquelle ils l'ont exploré. Leur compétence, leurs perspectives et leur dévouement témoignent de leur engagement profond à assurer un avenir solide à la recherche au Canada, où les connaissances progressent de manière responsable, éthique et sécuritaire. Ce fut un plaisir de présider ce comité. Je tiens à remercier mes collègues pour leurs contributions et leurs délibérations réfléchies tout au long du processus, ainsi que l'équipe du CAC pour son soutien. Enfin, je tiens à exprimer ma reconnaissance à Recherche et développement pour la défense Canada ainsi qu'à l'Agence de la santé publique du Canada pour avoir posé cette importante question et avoir rendu notre travail possible.

Martha Crago, C.M., Ph. D., D. Sc., BVO
Présidente, comité d'experts sur la recherche sensible préoccupante

Personnel du projet du CAC

Équipe d'évaluation :	**Anita Melnyk,** directrice de projet **Anastasia Konina,** associée de recherche **Vasa Lukich,** associée de recherche **Ananda Fadila,** coordinatrice de projet
Édition et communications :	**Andrea Hopkins,** gestionnaire, planification et production **Brendan Fitzgerald,** spécialiste en communication
Avec la participation de :	**Alexei Halpin,** associé de recherche **Suzi Loney,** directrice de recherche

Examen par les pairs

La version préliminaire de ce rapport a été revue par des examinateurs choisis par le CAC pour la diversité de leurs points de vue et de leurs domaines d'expertise. Ils ou elles ont contribué à titre personnel et leurs commentaires ne reflètent pas les opinions de leurs organisations respectives. Leurs commentaires anonymisés ont été entièrement pris en compte par le comité d'experts. Le CAC ne leur a toutefois pas demandé de cautionner les conclusions du rapport et ils n'ont pas vu la version finale avant publication. La responsabilité du contenu final de ce rapport incombe au comité d'experts et au CAC.

Ingrid d'Hooghe, Ph. D., associée de recherche principale, Institut Clingendael (La Haye, Pays-Bas)

Charmaine B. Dean, Ph. D., vice-présidente, Recherche et affaires internationales, Université de Waterloo (Waterloo, Ont.)

Mylène Deschênes, LL.B, B.C.L., LL.M., directrice, Éthique et affaires juridiques, Fonds de recherche du Québec (Montréal, Qc)

Kenneth M. Evans, Ph. D., chercheur en politique scientifique et technologique, Baker Institute for Public Policy, Université Rice (Houston, TX)

David Gillum, Ph. D., vice-président associé, Conformité et administration de la recherche, Université du Nevada, Reno (Reno, NV)

Jennie Knopp, Ph. D., directrice communautaire et scientifique, Oceans North (Ottawa, Ont.)

Margaret E. Kosal, Ph. D., professeure, Sam Nunn School of International Affairs, Georgia Institute of Technology (Atlanta, GA)

Matt Malone, LL.B, B.C.L., professeur adjoint, Faculté de droit de l'Université d'Ottawa; directeur de la Clinique d'intérêt public et de politique d'Internet du Canada Samuelson-Glushko (Ottawa, Ont.)

Piers D. Millett, Ph. D., directeur exécutif, International Biosecurity and Biosafety Initiative for Science (Genève, Suisse)

David Moher, Ph. D., directeur du Centre de journalologie, Programme de recherche méthodologique et sur la mise en œuvre, Institut de recherche de l'Hôpital d'Ottawa (Ottawa, Ont.)

Kate Moran, O.C., PEng., FCAE, FAAAS, Ph. D., présidente et cheffe de la direction, Réseaux océaniques Canada (Victoria, C.-B.)

Tommy Shih, Ph. D., professeur agrégé, Université de Lund (Lund, Suède)

Akshay Singh, M.A., directeur, Sécurité de la recherche, Université de la Colombie-Britannique (Vancouver, C.-B.)

Le processus d'examen par les pairs a été supervisé au nom du CAC par **Benoît Dupont,** professeur à l'École de criminologie, titulaire de la Chaire de recherche du Canada en cybersécurité et de la Chaire de recherche en prévention de la cybercriminalité à l'Université de Montréal, et directeur scientifique du Human-Centric Cybersecurity Partnership.

Remerciements

Le comité d'experts et le personnel du CAC tiennent à exprimer leur sincère gratitude aux personnes et organisations suivantes qui ont apporté leurs connaissances et leurs points de vue :

Lukas Arenson, ingénieur géotechnique principal, BGC Engineering

David Barclay, professeur agrégé, Département d'océanographie, Université Dalhousie

Rocco Casagrande, directeur général, Deloitte

Sarah-Louise Decrausaz, responsable de projets stratégiques, Initiatives de recherche stratégique, Bureau du vice-président à la recherche et à l'innovation, Université de Victoria

Philip Ferguson, professeur agrégé, Département de génie mécanique, Université du Manitoba

Centre de gouvernance de l'information des Premières Nations (CGIPN)

Shayla Fitzsimmons, directrice générale, Association régionale de l'Atlantique, Système intégré d'observation des océans du Canada (SIOOC)

Volker Gerdts, directeur et PDG, Vaccine and Infectious Disease Organization (VIDO)

Relations gouvernementales et recherche sur les politiques, Collèges et instituts Canada (CICan)

Claire Herbert, responsable de la stratégie numérique, Centre des sciences de l'observation de la Terre, Faculté Clayton H. Riddell de l'environnement, de la terre et des ressources, Université du Manitoba

Maia Hoeberechts, directrice adjointe, Apprentissage et engagement communautaire, Réseaux océaniques Canada

Janet King, présidente du conseil d'administration, Savoir polaire Canada

Meghan Paulson, directrice générale, Opérations de l'observatoire, Réseaux océaniques Canada

Direction des politiques scientifiques, Secteur des sciences et de la recherche, Innovation, Sciences et Développement économique Canada

Kanta Subbarao, Chaire d'excellence en recherche du Canada sur la biologie et le contrôle des virus respiratoires zoonotiques et pandémiques et professeure, Faculté de médecine, Université Laval

Naluturuk Weetaluktuk

Dustin Whalen, scientifique en sciences physiques, Commission géologique du Canada, Ressources naturelles Canada

Résumé

L'écosystème de recherche du Canada s'appuie sur des collaborations nationales, internationales et intersectorielles pour mener des travaux de calibre mondial conférant des avantages scientifiques et sociétaux substantiels au Canada et à ses alliés. Cependant, la nature ouverte et collaborative de l'écosystème de recherche canadien en fait une cible potentielle pour des acteurs étatiques et non étatiques malveillants qui souhaitent l'exploiter afin d'en retirer des avantages économiques, politiques, technologiques ou stratégiques. Ces menaces exigent que les personnes qui participent à la recherche soient dotées des outils nécessaires pour reconnaître la recherche sensible, évaluer les risques connexes et adopter des mesures pour la protéger. L'évolution rapide du contexte géopolitique, le rythme effréné des progrès technologiques et l'intérêt manifeste d'un large éventail d'acteurs à abuser de la recherche canadienne ou à la détourner de son but soulignent la nécessité pour tous les participants à l'écosystème canadien d'adopter une approche proactive et collaborative et de veiller à ce que les mesures de sécurité répondent adéquatement aux menaces actuelles et potentielles, tout en maintenant un équilibre favorisant la science ouverte et l'innovation.

Recherche à double usage préoccupante (RDUP) : Terme dans le domaine des sciences de la vie désignant un sous-ensemble de la recherche à double usage[1] qui, « selon les connaissances actuelles, peut raisonnablement être considérée comme susceptible de fournir des savoirs, des informations, des produits ou des technologies pouvant être détournés pour causer un préjudice, sans modification ou avec seulement des modifications mineures, de manière à constituer une menace lourde de conséquences pour la santé et la sécurité publiques, les cultures agricoles et autres végétaux, les animaux, l'environnement, le matériel ou la sécurité nationale » (Gouv. des États-Unis, 2024a).

Sécurité de la recherche : Englobe un ensemble de mesures et d'activités visant à reconnaître et à protéger la recherche sensible contre les risques, notamment « l'influence indue, l'interférence ou

(continue)

1 La recherche à double usage, selon le contexte, désigne les connaissances scientifiques, les technologies, les données et les processus qui : (i) ont à la fois des applications civiles et militaires potentielles; ou (ii) peuvent être utilisés à des fins bienveillantes ou malveillantes (Kavouras et Charitidis, 2019) et sont susceptibles de causer un préjudice sur le plan physiologique, moral ou éthique (Evans et Commins, 2017).

(a continué)

l'appropriation illicite de la recherche, y compris le vol pur et simple d'idées, de résultats de recherche et de la propriété intellectuelle par des États, des armées et leurs mandataires, ainsi que par des acteurs non étatiques et des activités criminelles organisées; et d'autres activités et comportements clandestins ayant des répercussions négatives sur les implications économiques, stratégiques et au niveau de la sécurité nationale » (SIGRE, 2022).

Recherche sensible : Désigne le processus de recherche et ses résultats, notamment les connaissances, les biens, les technologies et les données – dans divers domaines – qui, bien que visant des fins bénéfiques, peuvent être utilisés par des acteurs malveillants ou à des fins malveillantes pour nuire au public, à la santé publique, à la sécurité publique, à l'environnement, à l'agriculture, à la pêche, à la souveraineté du pays et à sa sécurité économique et nationale, au Canada et à l'échelle internationale, ou présenter des risques pour la vie privée et l'éthique (Gouv. de la Nouvelle-Zélande, 2022; Leopoldina et DFG, 2022a; ISDE, 2023a,b; JASON, 2024). Le comité d'experts reconnaît que cette liste de préjudices et de risques n'est pas exhaustive et peut évoluer en fonction du contexte géopolitique.

Recherche sensible préoccupante : Constitue un sous-ensemble de la recherche sensible dont on peut raisonnablement prévoir qu'elle sera détournée ou utilisée abusivement, immédiatement ou à l'avenir, sans modification ou avec des modifications mineures, et qui doit faire l'objet de précautions supplémentaires (Leopoldina et DFG, 2022a; ISDE, 2023a,b; JASON, 2024)[2].

La science ouverte et la sécurité de la recherche vont de pair pour faciliter la mise en commun responsable de la recherche

Bien que la science ouverte et la sécurité de la recherche puissent être perçues comme des priorités contradictoires parce qu'elles mettent l'accent sur des objectifs différents, elles éclairent toutes deux les décisions concernant le moment où la recherche peut être mise en commun, les personnes avec lesquelles cela peut être fait, dans quelle mesure et sous quelle forme. Étant donné que le niveau de sensibilité de la recherche peut évoluer au fil du temps, une évaluation continue des risques tout au long du cycle de vie de la recherche

2 Les définitions de la recherche sensible et de la recherche sensible préoccupante ont été élaborées par le comité d'experts à partir de l'analyse des politiques en matière de sécurité de la recherche au Canada et dans d'autres pays (CAC, 2025).

est nécessaire pour éviter tout risque d'utilisation abusive et de sécurisation excessive. Certains types de recherche seront soumis à des restrictions nécessaires en matière de mise en commun, tandis que d'autres pourront être échangés ouvertement. Lorsque la recherche n'est pas soumise à des restrictions, sa diffusion peut contribuer à favoriser la transparence, les découvertes et l'accès équitable à l'information. Le fait de conclure qu'un type de recherche est sensible et soumis à des restrictions d'accès n'exclut aucunement qu'il puisse être financé ou mené à bien. En effet, la recherche sensible revêt souvent une importance cruciale pour l'innovation, la défense, la santé publique et l'agriculture, et ses constats contribuent à des avancées scientifiques plus larges. Toutefois, pour mener à bien des projets de recherche sensibles, les chercheurs et les établissements doivent minimiser les risques d'utilisation abusive en élaborant et en adoptant des mesures de sécurité appropriées, notamment en limitant l'accès lorsque cela est nécessaire.

La science ouverte est une combinaison de « différents mouvements et pratiques visant à rendre les connaissances scientifiques multilingues [...] librement accessibles à tous et réutilisables par tous, à renforcer la collaboration scientifique et le partage des informations au profit de la science et de la société, ainsi qu'à ouvrir les processus de création, d'évaluation et de diffusion des connaissances scientifiques aux acteurs de la société au-delà de la communauté scientifique traditionnelle. Elle inclut toutes les disciplines scientifiques et tous les aspects des pratiques savantes, y compris les sciences fondamentales et appliquées, les sciences naturelles et les sciences sociales et humaines, et repose sur les piliers essentiels suivants : les connaissances scientifiques ouvertes; les infrastructures de la science ouverte; la communication scientifique; la participation ouverte des acteurs de la société; et le dialogue ouvert avec les autres systèmes de connaissances » (UNESCO, 2021). La science ouverte favorise la découverte collaborative ainsi que la reproduction et la validation des résultats scientifiques.

À la demande de Recherche et développement pour la défense Canada (RDDC), de l'Agence de la santé publique du Canada (ASPC) et d'autres ministères et organismes de soutien[3] (ci-après dénommés « le commanditaire »), le Conseil

3 Pêches et Océans Canada; Environnement et Changement climatique Canada; Conseil national de recherches du Canada; Ressources naturelles Canada; Transports Canada; Agence canadienne d'inspection des aliments; Santé Canada; Innovation, Sciences et Développement économique Canada et Sécurité publique Canada.

des académies canadiennes (CAC) a formé un comité d'experts afin d'examiner les connaissances actuelles sur les politiques, les stratégies et les cadres permettant de reconnaître et de protéger la recherche sensible tout en maintenant un équilibre favorisant la science ouverte et l'innovation. S'appuyant sur des données publiées et des entretiens avec des décideurs, des praticiens et des universitaires, le comité d'experts a examiné les mesures permettant de reconnaître la recherche sensible, de déterminer quand elle est préoccupante et comment la protéger tout au long des trois phases du processus de recherche : la phase de conception, la phase active et la phase post-recherche. Le comité d'experts a également abordé les facteurs favorables à la mise en œuvre de ces mesures et à la science ouverte de manière générale. À la demande du commanditaire, le comité a appliqué ses conclusions à deux domaines, la recherche océanographique et la recherche sur les agents pathogènes, afin d'illustrer la manière de protéger la recherche susceptible d'être utilisée à des fins militaires ou ayant une valeur stratégique pour la santé, la sûreté ou la sécurité du public.

Le mandat

Quelles politiques, stratégies ou cadres pourraient être appliqués pour aider les chercheurs à déterminer si leurs travaux sont considérés comme de la recherche à double usage préoccupante (RDUP)[4]?

Afin de prendre une décision éclairée sur le niveau d'ouverture potentiel, les personnes qui participent à des activités de recherche et qui les supervisent doivent savoir comment reconnaître la recherche sensible et déterminer à quel moment elle devient préoccupante, parce qu'elle comporte des risques supplémentaires qui doivent être atténués. Les listes sont un outil couramment utilisé pour aider les chercheurs à déterminer si leur recherche est sensible et préoccupante. Divers ministères du gouvernement du Canada (p. ex. Innovation, Sciences et Développement économique Canada, Affaires mondiales Canada) ont adopté des listes qui encadrent les pratiques de la sécurité de la recherche. Ces listes couvrent notamment les biens et les articles soumis à des

4 Bien que le mandat fasse référence à la *recherche à double usage préoccupante (RDUP)*, ce terme est généralement utilisé pour faire référence à la recherche en sciences de la vie (Gouv. des États-Unis, 2024a). Tout au long du rapport, le comité d'experts utilisera un terme plus large, à savoir la *recherche sensible préoccupante*, afin d'englober divers domaines et disciplines qui participent au secteur de la recherche.

contrôles à l'exportation, les personnes et entités visées par des sanctions, ainsi que les technologies sensibles et les affiliations préoccupantes. Elles peuvent se recouper et être combinées pour indiquer qu'une recherche est non seulement sensible, mais qu'elle devient également préoccupante (p. ex. listes de domaines de recherche sensibles et d'affiliations préoccupantes). Outre ces listes, la communauté des chercheurs au Canada et dans d'autres pays s'appuie sur des évaluations des risques et des consultations avec des experts externes (p. ex. des experts sur les questions touchant les peuples autochtones, la défense ou le renseignement) pour déterminer les recherches sensibles préoccupantes. Une fois combinées, les listes, les évaluations des risques et l'expertise externe permettent de cerner de manière exhaustive les risques en fonction de facteurs pertinents pour le projet de recherche (p. ex. les domaines de recherche sensibles et les affiliations préoccupantes, la situation géographique des activités de recherche, les partenariats étrangers).

Quels principes ou stratégies pourraient être appliqués pour déterminer comment protéger la RDUP?

Une fois que la recherche sensible a été reconnue et jugée préoccupante, diverses mesures axées sur les personnes, les établissements et les projets de recherche peuvent la protéger tout au long de son cycle de vie et atténuer les risques détectés. Ces mesures comprennent notamment les contrôles de sécurité des chercheurs, la diligence raisonnable entourant les propositions de recherche et les partenariats, la cybersécurité et la sécurité physique, ainsi que l'examen préalable à la publication des résultats de recherche. Pour être efficaces, les mesures visant à protéger la recherche sensible préoccupante doivent être réévaluées en permanence tout au long du cycle de vie de la recherche, en tenant compte du contexte et de la nécessité de soutenir toutes les phases du processus. La plupart se concentrent sur les deux premières phases du processus, à savoir la conception et la phase active, afin de repérer et d'atténuer les risques le plus tôt possible. Des orientations supplémentaires axées sur la phase post-recherche permettent la mise en commun responsable des données et la communication des résultats, favorisant ainsi à la fois la science ouverte et la sécurité de la recherche.

Que suggèrent les données probantes actuelles pour reconnaître et protéger la RDUP tout en maintenant un équilibre favorisant la science ouverte et l'innovation?

Le comité d'experts a recensé de nombreuses mesures prometteuses pour reconnaître et protéger la recherche sensible et la recherche sensible préoccupante. Ces dernières années, le Canada et ses alliés ont accordé une attention accrue à la sécurité de la recherche, mais des études supplémentaires sont requises sur l'efficacité des mesures pertinentes. En améliorant notre compréhension des mesures les plus efficaces, ces études sont à même de favoriser l'apprentissage et l'amélioration continus, de contribuer à l'équilibre entre la sécurité de la recherche et la science ouverte, d'optimiser des ressources limitées et de réduire la charge relative à la conformité qui pèse sur les chercheurs et les établissements.

Une philosophie moderne de la recherche est essentielle pour bâtir un système de recherche ouvert, innovant et sécurisé

Les progrès technologiques rapides et l'évolution du contexte géopolitique soulignent la nécessité pour tous les acteurs de l'écosystème de la recherche d'adopter une philosophie moderne afin de répondre aux attentes en matière d'ouverture, de collaboration, de conduite éthique et de protection des informations sensibles.

Une **philosophie moderne de la recherche** signifie que tous les acteurs participant à l'écosystème de la recherche sont conscients du contexte dans lequel ils mènent leurs travaux, des impacts de ces travaux sur le monde, ainsi que des politiques, principes et pratiques pour y faire face, notamment sur le plan de la sécurité de la recherche, de la science ouverte, des droits des peuples autochtones, de la souveraineté des données, de l'éthique, du consentement et de l'intégrité de la recherche. Ces politiques, principes et pratiques permettent aux personnes d'évaluer le degré d'ouverture et de sécurité dont leurs travaux de recherche ont besoin.

La philosophie moderne de la recherche est une compétence clé dans le paysage actuel, qui privilégie la transparence et la collaboration tout en reconnaissant l'importance cruciale de reconnaître et de protéger la recherche sensible, de

respecter les protocoles de sécurité et d'atténuer les risques comme l'ingérence étrangère ou l'utilisation abusive des données. Il est essentiel de cultiver cette philosophie pour mettre en œuvre avec succès des mesures de sécurité de la recherche qui tiennent également compte des impératifs de la science ouverte et de l'innovation. Voilà qui favorise un engagement en faveur d'une responsabilité partagée, où la charge de maintenir la sécurité de la recherche est répartie entre les différents acteurs de l'écosystème, notamment les chercheurs, les dirigeants institutionnels, le personnel chargé de la sécurité de la recherche, les gouvernements et le secteur privé.

L'éducation, la communication et le renforcement des capacités peuvent contribuer à cultiver une philosophie moderne de la recherche afin de permettre aux chercheurs de combiner science ouverte et sécurité de la recherche

L'éducation, la communication et le renforcement des capacités aux niveaux individuel et institutionnel peuvent contribuer à cultiver une philosophie moderne de la recherche chez les personnes faisant partie de l'écosystème tout en élargissant la sensibilisation aux questions liées à la science ouverte et à la sécurité. Au Canada, des entités comme le Centre de la sécurité de la recherche de Sécurité publique Canada, les bailleurs de fonds fédéraux et provinciaux/territoriaux de la recherche, le programme Liaison-recherche et collaboration avec les intervenants du Service canadien du renseignement de sécurité et les unités institutionnelles chargées de la sécurité de la recherche peuvent fournir des conseils à la communauté. Les organismes de recherche de tout le Canada se sont également regroupés pour créer des communautés de pratique nationales et régionales. Ces groupes jouent un rôle essentiel dans l'échange de conseils et de pratiques exemplaires au sein de l'écosystème de la recherche. Le gouvernement du Canada a la possibilité d'améliorer ces services en accordant des fonds supplémentaires et en améliorant les voies de communication entre la communauté du renseignement, les chercheurs et l'administration des établissements.

Les directives et cadres relatifs à la sécurité de la recherche dans d'autres pays (p. ex. en Australie, en Allemagne, au Royaume-Uni et aux États-Unis) soulignent le rôle important des universités et de leurs dirigeants dans la fourniture d'un soutien, d'une formation et d'un enseignement adéquats au personnel et aux étudiants. En Allemagne, par exemple, certains établissements ont créé des comités spécialisés pour aider les chercheurs à reconnaître la recherche sensible qui suscite des préoccupations. Aux États-Unis, la National Science Foundation soutient les travaux du SECURE Center, un centre d'information dont l'objectif est de faciliter la collaboration sur les questions de sécurité de la recherche et de fournir des conseils et des informations à la

communauté des chercheurs. D'autres mesures de sécurité de la recherche comprennent des efforts de sensibilisation à l'échelle de l'organisation, des stratégies de communication et des formations générales régulières sur la sécurité de la recherche, l'intégrité de la recherche et les conflits d'intérêts ou d'engagement. Les formations générales peuvent être personnalisées afin de mieux répondre aux besoins de groupes particuliers (p. ex. les chercheurs, les étudiants, les services de soutien administratif). Des formations axées sur les exigences particulières des politiques sont également à même d'assurer la conformité dans tous les établissements de recherche au Canada.

L'harmonisation des approches en matière de sécurité de la recherche et de science ouverte peut améliorer l'efficacité des mesures pertinentes

Les approches en matière de sécurité de la recherche et de science ouverte diffèrent d'une région à l'autre au Canada, ce qui pose des défis pour les partenariats interinstitutionnels, la mise en œuvre cohérente des mesures de sécurité de la recherche, ainsi que les demandeurs et bénéficiaires de financement soutenus par plusieurs bailleurs de fonds. Ce manque d'harmonisation impose une charge administrative supplémentaire aux chercheurs et réduit l'adoption des initiatives. Une façon de remédier à ces problèmes consisterait à établir des critères de base communs fondés sur des principes et des approches partagés pour relever les principaux défis, tout en laissant une marge de manœuvre pour une mise en œuvre adaptée aux besoins propres aux différents contextes. Cela contribuerait à réduire les doubles emplois et la charge administrative pour les chercheurs et les établissements qui s'efforcent de mettre en œuvre à la fois des politiques de sécurité de la recherche et de science ouverte.

La participation du secteur privé aux pratiques de science ouverte et de sécurité de la recherche est nécessaire pour garantir la mise en commun responsable des résultats de la recherche

Le secteur privé apporte une contribution importante à l'écosystème de la recherche canadienne, notamment dans des domaines sensibles, comme les technologies quantiques, les agents pathogènes et les toxines, ainsi que l'IA. Or, les différents ordres de gouvernement exercent un contrôle limité sur la sécurité de la recherche et les pratiques de science ouverte en l'absence d'allocation de fonds publics, ce qui constitue une lacune dans l'approche nationale de sécurité de la recherche et de science ouverte. Ces dernières années, le gouvernement du Canada a intensifié son engagement sur le plan de la sécurité auprès des entreprises privées des secteurs biopharmaceutique, des sciences de la vie et des sciences des données, ainsi qu'auprès des petites et

moyennes entreprises qui utilisent les technologies émergentes. Une tendance similaire s'observe dans d'autres pays. Au Royaume-Uni, par exemple, la National Protective Security Authority et le National Cyber Security Centre ont créé la boîte à outils Secure Innovation à l'intention des innovateurs du secteur privé, tandis que l'Engineering Biology Responsible Innovation Advisory Panel du gouvernement intègre l'industrie dans la gouvernance des technologies à double usage. De 2020 à 2025, les National Academies of Sciences, Engineering, and Medicine des États-Unis ont organisé la table ronde sur la science, la technologie et la sécurité, au cours de laquelle des représentants du gouvernement, du monde universitaire et du secteur privé ont échangé des informations et des bonnes pratiques en matière de sécurité de la recherche. L'élaboration d'approches inclusives similaires au Canada pourrait faciliter la mise en commun d'informations et réduire l'exposition aux menaces dans l'ensemble de l'écosystème de la recherche.

Le succès des mesures favorisant les initiatives de science ouverte et de sécurité de la recherche nécessite un financement soutenu

Les politiques de sécurité de la recherche mises en œuvre par différents ordres de gouvernement alourdissent la charge administrative des organismes de recherche, ce qui souligne la nécessité d'un financement supplémentaire pour soutenir les programmes et les unités concernés dans les secteurs privé et public. Par exemple, des ressources supplémentaires sont nécessaires lorsque les politiques de sécurité de la recherche imposent des exigences physiques et de cybersécurité pour le stockage, la transmission et le traitement des données sensibles et la protection des équipements. La mise en œuvre des principes de science ouverte implique de rendre les données FAIR (faciles à trouver, accessibles, interopérables et réutilisables) et de respecter les principes dits TRUST (transparence, responsabilité, orientation vers l'utilisateur, soutenabilité/durabilité et technologie), ce qui nécessite des ressources financières et des infrastructures importantes.

Au Canada, le financement fédéral consacré à la sécurité de la recherche est calculé en pourcentage du financement direct admissible à la recherche de chaque établissement d'enseignement postsecondaire au-delà de 2 millions de dollars. Voilà qui entraîne des différences de capacité entre les grandes universités et les autres établissements, notamment les petites et moyennes universités, les établissements de santé et les instituts de recherche affiliés, ainsi que les collèges et les écoles polytechniques. Le soutien à la mise en place de capacités consacrées à la sécurité de la recherche et à la science ouverte dans tous les établissements d'enseignement postsecondaire pourrait contribuer à réduire ces disparités.

Comment les approches ci-dessus s'appliqueraient-elles aux études de cas portant sur des travaux susceptibles d'être utilisés à des fins militaires ou présentant une valeur stratégique pour la santé, la sûreté ou la sécurité publiques?

À la demande du commanditaire, le comité d'experts a appliqué ses conclusions à deux domaines – la recherche océanographique et la recherche sur les agents pathogènes – afin d'illustrer la manière de protéger les travaux de recherche susceptibles d'être utilisés à des fins militaires ou ayant une valeur stratégique pour la santé, la sûreté ou la sécurité publiques.

La sécurité de la recherche océanographique peut être renforcée grâce aux approches existantes qui s'appliquent à d'autres domaines de recherche et grâce au leadership autochtone

Les risques associés à la recherche océanographique ont fait l'objet de beaucoup moins d'attention dans les politiques et les lignes directrices que ceux touchant d'autres domaines, comme la recherche sur les agents pathogènes. De plus, il n'existe pas de mesures globales permettant de reconnaître la recherche océanographique sensible et de déterminer quand elle devient préoccupante. En effet, les mesures de protection s'appliquent à la recherche océanographique au cas par cas, en fonction des politiques applicables des établissements de recherche ou des exigences de financement.

Afin de renforcer la sécurité de la recherche, les océanographes doivent être conscients d'un certain nombre de facteurs de risque, dont la plupart ne sont pas propres à la recherche océanographique. Il s'agit notamment des partenariats internationaux, de la géographie (p. ex. la recherche dans l'Arctique), de la production et de l'utilisation de certains types de données et de grands ensembles de données (p. ex. les données personnelles, les données spatiales), ainsi que de la recherche concernant certaines technologies ou certains domaines de recherche (p. ex. certains types de sonars, les réseaux de capteurs sans fil sous-marins). Les politiques en matière de sécurité de la recherche promulguées par les gouvernements fédéral et provinciaux, ainsi que par certaines organisations menant des recherches océanographiques, peuvent toutefois fournir des orientations utiles pour la détermination des risques.

Les facteurs qui indiquent une sensibilité accrue peuvent justifier l'application directe de mesures de protection ou la réalisation d'une évaluation supplémentaire des risques. Des comités spécialisés sont à même d'aider les chercheurs à reconnaître la recherche sensible ou préoccupante, car il est possible d'anticiper raisonnablement un détournement ou une utilisation

abusive, immédiatement ou à l'avenir, avec peu ou pas de modifications. Les mesures de protection qui s'appliquent à d'autres types de recherche (incluant la recherche sur les agents pathogènes) peuvent quant à elles être étendues à la recherche océanographique reconnue comme sensible ou préoccupante.

Bien qu'il existe de nombreuses approches prometteuses pour garantir la sécurité de la recherche océanographique, seules les communautés autochtones elles-mêmes peuvent déterminer si elles conviennent à la recherche impliquant les Premières Nations, les Inuits et les Métis. Au Canada, un cadre fondé sur les droits pour la recherche impliquant les peuples autochtones découle de la Constitution et de la *Déclaration des Nations Unies sur les droits des peuples autochtones*, qui stipule que ceux-ci ont le droit à l'autodétermination dans tous les aspects de la recherche qui les concerne. De nombreux peuples autochtones du Canada dépendent des écosystèmes marins pour leur subsistance et leur sécurité. Dans ce contexte, les dirigeants autochtones jouent un rôle essentiel dans la reconnaissance et la résolution des défis uniques en matière de sécurité et de souveraineté auxquels sont confrontées les communautés côtières en raison des changements climatiques, de l'érosion côtière, de l'accès réduit aux ressources marines et des tensions géopolitiques croissantes dans l'Arctique.

Les approches visant à garantir la sécurité de la recherche sur les agents pathogènes peuvent être améliorées grâce à l'application volontaire des politiques gouvernementales entourant la sécurité de la recherche et à des évaluations multidisciplinaires des risques

Les listes proposées par le gouvernement du Canada constituent le principal mécanisme de reconnaissance de la recherche sensible portant sur certains types de toxines et d'agents pathogènes humains. Des mesures supplémentaires, comme l'examen de la recherche avant sa publication et le processus d'évaluation des risques de l'ASPC, complètent et renforcent l'application des listes. Cependant, la convergence de la recherche sur les agents pathogènes et des technologies émergentes (p. ex. la nanotechnologie, l'IA, la technologie quantique) remet en question les approches existantes pour reconnaître la recherche sensible préoccupante. En effet, les lois, règlements et politiques qui guident la détermination des risques ne suivent pas toujours le rythme rapide des progrès technologiques. Ces défis peuvent être relevés grâce à un processus d'évaluation des risques qui s'appuie sur une expertise multidisciplinaire et tient compte de facteurs de risque supplémentaires.

Dans le domaine de la recherche sur les agents pathogènes, une série de mesures visant à protéger la recherche sensible préoccupante s'appliquent à la conception et aux phases actives du processus de recherche. Ces mesures comprennent le filtrage des personnes travaillant avec des agents biologiques

sensibles sur le plan de la sécurité, l'octroi de permis de recherche, le contrôle de l'accès aux installations et des exigences supplémentaires de cybersécurité pour certaines installations. Outre les restrictions légales applicables aux partenariats et collaborations de recherche, les installations réglementées ont recours à des politiques et directives internes, à des accords de non-divulgation et à des formations pour protéger leur recherche et limiter la publication des résultats et des données. La Politique sur la recherche en technologies sensibles et sur les affiliations préoccupantes (PRTSAP) et les Lignes directrices sur la sécurité nationale pour les partenariats de recherche (LDSNPR) ne sont pas toujours directement applicables à la recherche sur les agents pathogènes; toutefois, elles peuvent fournir des orientations utiles sur la manière d'éviter ou d'atténuer les risques pour la sécurité posés par certaines collaborations et publications.

À l'instar de la recherche océanographique, le cadre juridique existant pour la recherche sur les agents pathogènes impliquant les peuples autochtones, leurs terres et leurs données défend les droits des Autochtones en affirmant que cette recherche doit être menée et développée conjointement avec les communautés, afin de respecter le principe de souveraineté des données.

Abréviations

ABCSE	agents biologiques à cote de sécurité élevée
ASPC	Agence de la santé publique du Canada
CGIPN	Centre de gouvernance de l'information des Premières Nations
DNUDPA	*Déclaration des Nations Unies sur les droits des peuples autochtones*
EPTC 2	Énoncé de politique des trois conseils : Éthique de la recherche avec des êtres humains
FAIR	Facile à trouver, Accessible, Interopérable et Réutilisable
FCI	Fondation canadienne pour l'innovation
FRQ	Fonds de recherche du Québec
GDR	gestion des données de recherche
IRSC	Instituts de recherche en santé du Canada
ISDE	Innovation, Sciences et Développement économique Canada
KEF	Kommissionen für Ethik sicherheitsrelevanter Forschung (comités d'éthique spécialisés dans la recherche liée à la sécurité, Allemagne)
LAPHT	*Loi sur les agents pathogènes humains et les toxines*
LDSNPR	Lignes directrices sur la sécurité nationale pour les partenariats de recherche
MDN	Ministère de la Défense nationale
NASEM	National Academies of Sciences, Engineering, and Medicine (États-Unis)
NMT	niveau de maturité technologique
ORN	organisation de recherche nommée
PGD	plan de gestion des données
PRTSAP	Politique sur la recherche en technologies sensibles et sur les affiliations préoccupantes
RAPHT	*Règlement sur les agents pathogènes humains et les toxines*
RDDC	Recherche et développement pour la défense Canada
RDUP	recherche à double usage préoccupante
SCRS	Service canadien du renseignement de sécurité
TRUST	Transparence, Responsabilité, orientation vers l'Utilisateur, Soutenabilité/durabilité et Technologie
VIDO	Vaccine and Infectious Disease Organization

Table des matières

1 Introduction 1
1.1 Le mandat du comité d'experts 4
1.2 Terminologie 5
1.3 Recherche sensible et droits des Autochtones 9
1.4 L'approche du comité d'experts 13
1.5 Structure du rapport. 19

2 Le paysage de la recherche au Canada. 20
2.1 Acteurs de l'écosystème de la recherche 22
2.2 Caractéristiques de l'écosystème de la recherche 24
2.3 Science ouverte 30
2.4 Sécurité de la recherche 36

3 Reconnaissance de la recherche sensible préoccupante . 43
3.1 Facteurs qui rendent la recherche sensible 47
3.2 Mesures et outils permettant de reconnaître la recherche sensible préoccupante. 53

4 Mesures de protection de la recherche sensible préoccupante 79
4.1 Phase de conception de la recherche 81
4.2 Phase de recherche active 91
4.3 Phase post-recherche 97
4.4 Protéger le cycle de vie de la recherche 102

5 Assurer la sécurité de la recherche tout en préservant l'ouverture scientifique. 104

5.1 Systèmes de soutien à la mise en commun des connaissances 106

5.2 Renforcement des capacités et formation 113

5.3 Ressources financières 118

5.4 Application de la conformité 122

5.5 Favoriser une philosophie moderne de la recherche . . . 128

6 Conclusion et réflexions finales 130

6.1 Application des mesures à la recherche sur les agents pathogènes et à la recherche océanographique 132

6.2 Réflexions du comité 139

Références 142

1

Introduction

1.1 Le mandat du comité d'experts

1.2 Terminologie

1.3 Recherche sensible et droits des Autochtones

1.4 L'approche du comité d'experts

1.5 Structure du rapport

Le concept de sécurité de la recherche, c'est-à-dire la protection de la recherche contre l'utilisation abusive, le vol ou d'autres activités malveillantes, n'est pas nouveau. Pendant la Seconde Guerre mondiale, les scientifiques employés au Laboratoire national de Los Alamos dans le cadre du projet Manhattan visant à créer la première bombe atomique du monde ont été la cible d'activités d'espionnage. Parmi les cas célèbres, le physicien théoricien allemand Klaus Fuchs a purgé une peine de neuf ans de prison au Royaume-Uni après la guerre pour avoir volé et fourni des secrets atomiques à l'Union soviétique (Laucht, 2012). La sécurité de la recherche s'est développée comme une extension de la sécurité nationale pendant la guerre froide afin de protéger les activités de recherche contre l'espionnage technologique militaire, souvent en mettant l'accent sur la recherche pouvant être considérée comme à double usage (c.-à-d. ayant des applications militaires et civiles) (Wilner *et al.,* 2022).

De nos jours, l'importance accrue accordée à la sécurité de la recherche découle de la nécessité de protéger l'environnement ouvert, international et collaboratif de la R-D au Canada contre les acteurs étatiques et non étatiques qui souhaitent l'exploiter afin d'en retirer un avantage économique, politique ou stratégique (SIGRE, 2022; ISDE, 2023c). Le Comité des parlementaires sur la sécurité nationale et le renseignement (CPSNR) du Canada a cerné plusieurs risques liés au contexte géopolitique, notamment l'espionnage visant les secteurs nationaux de la santé, des sciences et de la technologie; les cybermenaces pesant sur les infrastructures essentielles; l'utilisation potentielle d'armes nucléaires, chimiques et biologiques; ainsi que l'acquisition illicite et clandestine de technologies à double usage (CPSNR, 2021). Sur la base d'incidents documentés et d'informations rendues publiques, l'ingérence étrangère au Canada s'est manifestée par des collaborations de recherche non autorisées, l'abus de fonctions officielles au profit d'intérêts étrangers, le transfert clandestin de technologies sensibles et des cyberactivités ciblées, tous constituant une menace importante pour la sécurité nationale, la propriété intellectuelle (PI) et l'intégrité des institutions (CBC News, 2014, 2024; Centre pour la cybersécurité, 2024a; GRC, 2024).

Le concept de *sécurité de la recherche* comprend les politiques et les pratiques qui protègent la recherche sensible destinées à des fins bénéfiques (ISDE, 2023c) (p. ex. la préparation aux pandémies, la résilience aux catastrophes, la précision de la navigation) contre « les risques d'influence indue, d'ingérence ou d'appropriation illicite [...]; le vol pur et simple d'idées, de résultats de la recherche et de propriété intellectuelle [...]; et d'autres activités et comportements qui entraînent des répercussions négatives sur la sécurité économique, stratégique et/ou nationale » (SIGRE, 2022).

En tant qu'élément de la sécurité nationale, la sécurité de la recherche contribue à protéger les capacités technologiques et industrielles du Canada contre l'espionnage, le vol et d'autres menaces externes (CRSNG, 2024a). En tant qu'élément de la sécurité économique, elle favorise l'innovation; aide à prévenir la perte de propriété intellectuelle, d'occasions de brevets et de revenus potentiels; et protège la compétitivité des organisations (Asselin, 2024). La sécurité de la recherche est importante pour tous les chercheurs et toutes les organisations, car elle favorise la conduite responsable de la recherche, contribue à éviter les atteintes à la réputation et la responsabilité légale, et renforce la confiance du public (GC, 2022a; CRSNG, 2024a; SIGRE, 2024). De l'avis du comité d'experts, tous les acteurs de l'écosystème de la recherche bénéficient des mesures de sécurité de la recherche et partagent la responsabilité de leur mise en œuvre.

La sécurité de la recherche est étroitement liée à d'autres mouvements et pratiques qui sous-tendent le secteur de la recherche, notamment la science ouverte. La *science ouverte* vise « à rendre les connaissances scientifiques multilingues [...] librement accessibles à tous et réutilisables par tous, à renforcer la collaboration scientifique et le partage des informations au profit de la science et de la société, ainsi qu'à ouvrir les processus de création, d'évaluation et de diffusion des connaissances scientifiques aux acteurs de la société au-delà de la communauté scientifique traditionnelle » (UNESCO, 2021). En appliquant les pratiques de la science ouverte (p. ex. la recherche participative; ainsi que les logiciels, le matériel, les données, l'accès et les ressources éducatives en mode ouvert), la communauté scientifique peut accélérer les découvertes, faciliter l'élaboration de politiques fondées sur des données probantes, rendre la recherche plus accessible au grand public et renforcer la confiance de celui-ci envers la recherche (GC, 2020; UNESCO, 2021; COS, s.d.).

À une époque où la sécurité de la recherche revêt une importance croissante, la pratique de la science ouverte contribue à atténuer le risque de sécurisation excessive

De l'avis du comité d'experts, à une époque où la sécurité de la recherche revêt une importance croissante, la pratique de la science ouverte contribue à atténuer le risque de sécurisation excessive, garantit la mise en commun responsable de la recherche et des données afin de faire progresser les connaissances comme l'innovation, et soutient le droit de chacun « de participer au progrès scientifique et à ses avantages » (Assemblée générale des Nations Unies, 1948). En renforçant la responsabilité, la transparence et la reproductibilité du processus et des produits de la recherche, la science ouverte

favorise une *conduite responsable de la recherche*, c'est-à-dire « la connaissance et l'application des normes professionnelles établies, ainsi que des valeurs et des principes éthiques qui sont essentiels à l'exécution de toutes les activités liées à la recherche » (GC, 2022b). La conduite responsable de la recherche soutient en retour la science ouverte en garantissant que les données, les méthodes et les résultats sont transparents, exacts et traités conformément aux valeurs, principes et meilleures pratiques professionnelles qui guident les communautés de la recherche.

Bien que la science ouverte et la sécurité de la recherche puissent être perçues comme des priorités opposées parce qu'elles visent des objectifs différents, dans la pratique, elles sont interreliées, et contribuent ensemble à éclairer les décisions sur la manière dont la recherche peut être mise en commun, le moment où cela peut se faire, les personnes avec lesquelles cela est permis (CRSNG, 2024a) et la mesure où elle peut l'être. Ces décisions ne sont pas toujours simples : elles dépendent à la fois de facteurs objectifs et subjectifs (p. ex. le domaine de recherche, les développements géopolitiques, la conscience des risques par les chercheurs, l'accès aux ressources) et nécessitent une évaluation continue des risques tout au long du cycle de vie de la recherche (chapitre 3). À la suite de ces évaluations, certains travaux de recherche peuvent être soumis à des restrictions nécessaires en matière de mise en commun, par exemple parce qu'ils présentent des risques pour la santé publique ou la sécurité nationale ou économique. D'autres types de recherche peuvent en revanche faire l'objet d'une communication libre. Dans de nombreux cas, cependant, il est difficile de déterminer les politiques, stratégies ou cadres qui permettent de déterminer le degré d'ouverture de la recherche et de protéger celle jugée sensible, et qui est responsable de la mise en œuvre efficace de ces encadrements.

1.1 Le mandat du comité d'experts

Reconnaissant l'importance croissante accordée à la sécurité de la recherche et la nécessité de la garantir, ainsi que la valeur de la recherche ouverte et collaborative, Recherche et développement pour la défense Canada (RDDC) et l'Agence de la santé publique du Canada (ASPC), avec le soutien d'autres ministères et organismes[1] du gouvernement du Canada (ci-après dénommés « le commanditaire »), ont demandé au Conseil des académies canadiennes (CAC) de répondre à la question et aux sous-questions suivantes :

1 Pêches et Océans Canada; Environnement et Changement climatique Canada; Conseil national de recherches du Canada; Ressources naturelles Canada; Transports Canada; Agence canadienne d'inspection des aliments; Santé Canada; Innovation, Sciences et Développement économique Canada et Sécurité publique Canada.

Que suggèrent les données probantes actuelles pour reconnaître et protéger la recherche à double usage préoccupante (RDUP) tout en maintenant un équilibre favorisant la science ouverte et l'innovation?[2]

- Quelles politiques, stratégies ou cadres pourraient être appliqués pour aider les chercheurs à déterminer si leurs travaux sont considérés comme de la RDUP?
- Quels principes ou stratégies pourraient être appliqués pour déterminer comment protéger la RDUP?
- Comment les approches ci-dessus s'appliqueraient-elles aux études de cas portant sur des travaux susceptibles d'être utilisés à des fins militaires ou présentant une valeur stratégique pour la santé, la sûreté ou la sécurité publiques?

Le commanditaire a demandé au comité d'experts, dans sa réponse à la troisième sous-question, de se concentrer sur deux domaines : la recherche océanographique (incluant un large éventail de champs d'étude et de types de recherche) et la recherche sur les agents pathogènes[3] – et de démontrer l'application des mesures les plus susceptibles de reconnaître et de protéger la recherche sensible tout en favorisant la science ouverte et l'innovation. Le commanditaire a choisi ces domaines afin d'illustrer l'application des constats du rapport à des travaux de recherche soumis à différents niveaux de contrôle réglementaire. Pour s'acquitter de cet aspect du mandat, le comité d'experts présente des exemples de mesures et explique la manière dont elles peuvent être appliquées dans ces domaines.

1.2 Terminologie

Au cours de ses délibérations et de la collecte de données, le comité d'experts a pris note de plusieurs termes et définitions qui méritent d'être clarifiés (encadré 1.1). Certaines de ces définitions ont été tirées directement des politiques et de la littérature, tandis que d'autres ont été élaborées par le comité d'experts d'après l'analyse des politiques adoptées au Canada et dans

2 Bien que le mandat fasse référence à la *recherche à double usage préoccupante (RDUP)*, ce terme est généralement associé à la recherche en sciences de la vie (Gouv. des États-Unis, 2024a). Tout au long du rapport, le comité d'experts utilisera un terme plus large, à savoir *recherche sensible préoccupante*, afin d'englober divers domaines et disciplines qui participent à l'effort de recherche.

3 Le commanditaire utilise de manière variable les termes *biosécurité*, *biosûreté* et *recherche sur les agents pathogènes* pour désigner ce domaine de recherche. Toutefois, le terme *recherche sur les agents pathogènes* est utilisé tout au long du rapport, car il reflète l'objet principal de ce domaine de recherche.

certains pays (Aotearoa Nouvelle-Zélande, Australie, Union européenne, France, Allemagne, Pays-Bas, Royaume-Uni, États-Unis) (CAC, 2025).

Encadré 1.1 Définitions des termes clés

Biosécurité : « Ensemble des principes, des technologies et des pratiques liés au confinement mis en œuvre pour empêcher l'exposition involontaire à des matières réglementées, ou leur rejet accidentel. » (ASPC, 2022)

Biosûreté : « Ensemble des mesures de sûreté visant à prévenir la perte, le vol, le mésusage, le détournement ou le rejet volontaire de matières réglementées ou d'autres ressources connexes (p. ex. les membres du personnel, l'équipement, les matières non infectieuses, les animaux, les renseignements sensibles). » (ASPC, 2022)

Conduite responsable de la recherche : « Le comportement attendu de quiconque mène des activités de recherche ou de soutien à la recherche à quelque étape que ce soit d'un projet de recherche (c.-à-d. de la formulation de la question de recherche jusqu'à la rédaction du rapport, à sa publication et à sa diffusion, en passant par la planification, la réalisation, la collecte de données, l'analyse de la recherche et la bonne gestion des fonds de recherche). Ce comportement suppose la connaissance et l'application des normes professionnelles établies ainsi que des valeurs et des principes éthiques qui sont essentiels à l'exécution de toutes les activités liées à la recherche. Ces valeurs comprennent l'honnêteté, l'équité, la confiance, la responsabilité et l'ouverture. » (GC, 2022b)

Philosophie moderne de la recherche : Une approche dans laquelle tous les acteurs participant à l'écosystème de la recherche sont conscients du contexte dans lequel ils opèrent, de leur impact sur le monde et des politiques, principes et pratiques visant à atténuer cet impact, notamment la sécurité de la recherche, la science ouverte, les droits des Autochtones, la souveraineté des données, l'éthique, le consentement et l'intégrité de la recherche. Ces politiques, principes et pratiques permettent aux individus d'évaluer le degré d'ouverture et de sécurité dont leurs recherches ont besoin.

Recherche : Englobe à la fois le processus de recherche et ses résultats, notamment les connaissances, les biens, les technologies et les données, dans divers domaines. Elle comprend la recherche fondamentale et appliquée, ainsi que les activités de recherche financées par des fonds publics et privés.

(continue)

(a continué)

Recherche à double usage : Selon le contexte, désigne les connaissances scientifiques, les technologies, les données et les processus qui : (i) ont des applications civiles et militaires potentielles; ou (ii) peuvent avoir des applications bienveillantes et malveillantes (Kavouras et Charitidis, 2019) et la capacité de causer un préjudice sur le plan physiologique, moral ou éthique (Evans et Commins, 2017). Presque tous les travaux de recherche peuvent être à double usage dans la mesure où ils peuvent produire des connaissances scientifiques, des technologies, des données et des processus ayant des applications bienveillantes et malveillantes potentielles (Kavouras et Charitidis, 2019; Lev, 2019; Kosal, 2020a).

Recherche à double usage préoccupante (RDUP) : Expression utilisée dans les sciences de la vie pour désigner un sous-ensemble de la recherche à double usage qui, « selon les connaissances actuelles, peut raisonnablement être considérée comme susceptible de fournir des savoirs, des informations, des produits ou des technologies pouvant être détournés pour causer un préjudice, sans modification ou avec seulement des modifications mineures, de manière à constituer une menace lourde de conséquences pour la santé et la sécurité publiques, les cultures agricoles et autres végétaux, les animaux, l'environnement, le matériel ou la sécurité nationale » (Gouv. des États-Unis, 2024a).

Recherche autochtone : Ce terme a été défini comme la « recherche réalisée dans n'importe quel domaine ou discipline qui est menée par et avec des communautés, des sociétés ou des personnes des Premières Nations, des peuples inuit ou métis ou d'autres nations autochtones et qui les concerne et repose sur leur sagesse, leurs cultures, leurs expériences ou leurs systèmes de connaissances exprimés dans des formes dynamiques, passées et actuelles. La recherche autochtone peut englober les dimensions intellectuelles, physiques, émotionnelles et (ou) spirituelles du savoir de manière à créer des liens créatifs entre les personnes, les endroits et l'environnement naturel. » (Indigenous Advisory Circle et CRSH, 2025)

Recherche sensible : Désigne le processus de recherche et ses résultats, notamment les connaissances, les biens, les technologies et les données, dans divers domaines qui, bien que visant des fins bénéfiques, peuvent être utilisés par des acteurs malveillants ou à des fins malveillantes pour nuire au public, à la santé publique, à la sécurité publique, à l'environnement, à l'agriculture, à la pêche, à la souveraineté et à la sécurité économique et nationale au Canada et à l'échelle internationale, ou présenter des risques pour la vie privée et l'éthique

(continue)

(a continué)

(Gouv. de la Nouvelle-Zélande, 2022; Leopoldina et DFG, 2022a; ISDE, 2023a,b; JASON, 2024). Le comité d'experts reconnaît que cette liste de préjudices et de risques n'est pas exhaustive et peut évoluer en fonction du contexte géopolitique.

Recherche sensible préoccupante : Constitue un sous-ensemble de la recherche sensible dont on peut raisonnablement prévoir qu'elle sera détournée ou utilisée abusivement, immédiatement ou à l'avenir, sans modification ou avec des modifications mineures, et qui doit faire l'objet de précautions supplémentaires (Leopoldina et DFG, 2022a; ISDE, 2023a,b; JASON, 2024).

Science ouverte : Une combinaison de « différents mouvements et pratiques visant à rendre les connaissances scientifiques multilingues [...] librement accessibles à tous et réutilisables par tous, à renforcer la collaboration scientifique et le partage des informations au profit de la science et de la société, ainsi qu'à ouvrir les processus de création, d'évaluation et de diffusion des connaissances scientifiques aux acteurs de la société au-delà de la communauté scientifique traditionnelle. Elle inclut toutes les disciplines scientifiques et tous les aspects des pratiques savantes, y compris les sciences fondamentales et appliquées, les sciences naturelles et les sciences sociales et humaines, et repose sur les piliers essentiels suivants : les connaissances scientifiques ouvertes; les infrastructures de la science ouverte; la communication scientifique; la participation ouverte des acteurs de la société; et le dialogue ouvert avec les autres systèmes de connaissances. » (UNESCO, 2021)

Sécurité de la recherche : Englobe un ensemble de mesures et d'activités visant à reconnaître et à protéger la recherche sensible contre les risques, notamment « l'influence indue, l'interférence ou l'appropriation illicite de la recherche, y compris le vol pur et simple d'idées, de résultats de recherche et de la propriété intellectuelle par des États, des armées et leurs mandataires, ainsi que par des acteurs non étatiques et des activités criminelles organisées; et d'autres activités et comportements clandestins ayant des répercussions négatives sur les implications économiques, stratégiques et au niveau de la sécurité nationale » (SIGRE, 2022).

Souveraineté des données : Dans le contexte des droits des peuples autochtones, peut être définie comme « le droit des peuples autochtones de conserver, contrôler, protéger et développer leur patrimoine culturel, leurs connaissances traditionnelles et leurs expressions culturelles traditionnelles, ainsi que leur droit de conserver, contrôler, protéger et développer leur propriété intellectuelle par rapport à ces aspects » (Kukutai et Taylor, 2016).

Afin de fournir des orientations claires aux chercheurs, le comité d'experts a axé son évaluation sur les mesures visant à reconnaître et à protéger la recherche sensible préoccupante, car elle présente les risques les plus élevés en cas d'utilisation abusive ou détournée. Si le mandat confié par le commanditaire porte principalement sur la *recherche à double usage préoccupante*, ce terme est principalement associé aux sciences de la vie (Gouv. des États-Unis, 2024a). Le commanditaire a demandé au comité d'experts d'aborder les préoccupations en matière de sécurité de la recherche qui se posent dans divers domaines et disciplines et lui a laissé toute latitude pour choisir la terminologie qui lui permettrait de répondre pleinement aux questions du mandat. Ainsi, tout au long du rapport, le comité d'experts utilisera un terme plus large, *recherche sensible préoccupante*, plutôt que RDUP, afin de refléter le fait que la portée de l'évaluation s'étend aux questions de sécurité de la recherche qui se posent dans une variété de domaines, incluant les sciences sociales et humaines. Le comité d'experts note également que cette terminologie est en phase avec l'approche adoptée par le gouvernement du Canada, qui invite les chercheurs à évaluer la sensibilité de leurs projets de recherche (ISDE, 2024a; CRSNG, 2024b). Le comité reconnaît que, dans le contexte de la recherche sur les agents pathogènes, le terme RDUP reste largement utilisé dans les politiques et les lignes directrices (voir p. ex. ASPC, 2018a; NSABB, 2023). Les différences terminologiques seront signalées dans une note de bas de page lorsque les références citées utilisent un autre terme.

1.3 Recherche sensible et droits des Autochtones

Au Canada, les peuples autochtones participent à la recherche de diverses manières : en tant que chercheurs, communautés, participants et sujets de recherche. Les informations recueillies par, pour et sur les peuples et les communautés autochtones dans tout contexte de recherche, incluant celle portant sur les agents pathogènes et les océans, peuvent être sensibles et nécessiter une protection pour des motifs comme le respect de la vie privée, l'importance communautaire et culturelle, ainsi que le risque d'utilisation abusive et d'exploitation (ONU, 2007; de Beer et Dylan, 2015; CAC, 2023a). « La science ouverte et la sécurité de la recherche peuvent englober de nombreuses considérations interdépendantes, notamment la capacité des communautés à vivre en sécurité, à avoir accès à la nourriture et au logement; à garantir la sécurité physique des chercheurs; ainsi qu'à protéger le territoire, les droits à la vie privée – individuels et collectifs – de même que les données sur la santé contre l'exploitation » (N. Weetaluktuk, communication personnelle, 2025).

1.3.1 Un cadre fondé sur les droits

Les normes relatives à la recherche équitable impliquant les peuples autochtones et leurs terres sont énoncées dans la *Déclaration des Nations Unies sur les droits des peuples autochtones* (DNUDPA) (ONU, 2007). La DNUDPA a été codifiée dans la loi fédérale canadienne en 2021 et fournit une base juridique aux relations entre le gouvernement, les institutions et les peuples autochtones (JUS, 2021). Plusieurs dispositions de la DNUDPA (articles 3, 11.1, 13.1, 14.1, 18, 19, 26, 27, 28, 29.1, 31, 32) soutiennent le droit des peuples autochtones à l'autodétermination en ce qui concerne les activités de recherche qui les touchent, ainsi que leurs données, leurs connaissances et leurs terres (ONU, 2007). Les dispositions de la DNUDPA doivent être prises en compte lors de l'élaboration des politiques en matière de sécurité de la recherche et de science ouverte.

Au Canada, les terres sur lesquelles se déroulent les recherches peuvent être assujetties à des droits ancestraux et issus de traités protégés par la Constitution (GC, 1982). Ce cadre fondé sur les droits s'applique particulièrement aux deux domaines de recherche examinés dans le rapport. Dans la recherche océanographique, où l'accent est mis en particulier sur l'Arctique, une grande partie de cette région fait l'objet d'accords sur les revendications territoriales, qui définissent les droits ancestraux et la gouvernance des terres (ITK, 2018; RCAANC, 2022a). Par conséquent, la reconnaissance et la protection de la recherche sensible préoccupante dans ces régions (ainsi que dans toute autre région côtière et océanique impliquant des peuples ou des terres autochtones) exigent que les projets et protocoles soient élaborés et dirigés conjointement par les communautés autochtones – ceci pour refléter les contextes de recherche uniques et garantir la sécurité culturelle comme des produits de la recherche qui se révéleront mutuellement bénéfiques. Le leadership et la mobilisation des communautés sont essentiels pour comprendre les défis distincts en matière de sécurité et de souveraineté auxquels sont confrontées les communautés côtières autochtones, qui peuvent inclure les changements climatiques, l'érosion côtière et l'accès réduit aux ressources marines (Leonard *et al.,* 2022; Whalen *et al.,* 2022). Ces défis sont exacerbés dans l'Arctique, qui présente un intérêt particulier pour le commanditaire en raison des tensions géopolitiques croissantes (encadré 1.3).

À l'instar de la recherche océanographique, le cadre juridique canadien préconise une approche fondée sur les droits pour mener des recherches sur les agents pathogènes qui concernent les peuples autochtones, leurs terres et leurs données, et souligne que ces recherches doivent être menées et élaborées conjointement avec les communautés afin de respecter le principe de la souveraineté des données (ONU, 2007).

1.3.2 Souveraineté des données

Le concept de souveraineté des données désigne « le contrôle effectif, la propriété et d'autres revendications relatives aux données exprimées par divers agents, allant des individus aux pays » (Hummel *et al.*, 2021). Les interprétations et les applications du principe de souveraineté des données sont influencées par le contexte géopolitique et les priorités nationales, qui peuvent évoluer au fil du temps (Hummel *et al.*, 2021; Belli *et al.*, 2024; GC, 2025a). Dans le contexte des droits des peuples autochtones, la souveraineté des données peut être définie comme « le droit des peuples autochtones de conserver, contrôler, protéger et développer leur patrimoine culturel, leurs connaissances traditionnelles et leurs expressions culturelles traditionnelles, ainsi que leur droit de conserver, contrôler, protéger et développer la propriété intellectuelle sur ceux-ci » (Kukutai et Taylor, 2016) (encadré 1.2). Le principe de souveraineté des données s'applique à toutes les entités menant des recherches sur les peuples autochtones, incluant les ministères et organismes gouvernementaux qui ont l'obligation constitutionnelle de consulter les peuples autochtones et de leur offrir des accommodements appropriés lorsqu'ils planifient des activités susceptibles d'avoir une incidence sur leurs droits (ONU, 2007; GC, 2025b). De l'avis du comité d'experts, le principe de souveraineté des données et le droit inhérent des peuples autochtones de contrôler l'accès à leurs données comme leur utilisation sont essentiels à la conception et à la mise en œuvre de toute politique en matière de sécurité de la recherche et de science ouverte. Le droit des peuples autochtones à participer à l'élaboration conjointe de la recherche sur leurs terres sous-entend un examen de ce qu'est la sécurité de la recherche, de la manière dont la recherche est contrôlée et des entités contre lesquelles elle doit être protégée.

Le principe de souveraineté des données et le droit inhérent des peuples autochtones de contrôler l'accès à leurs données comme leur utilisation sont essentiels à la conception et à la mise en œuvre de toute politique en matière de sécurité de la recherche et de science ouverte

Encadré 1.2 Initiatives visant à promouvoir la souveraineté des données au Canada

Pour les Premières Nations du Canada, le Centre de gouvernance de l'information des Premières Nations (CGIPN) administre les principes de propriété, de contrôle, d'accès et de possession des données (communément appelés PCAP®[4]), qui affirment « que les Premières Nations sont les seules à contrôler les processus de collecte de données dans leurs communautés, et qu'elles possèdent et contrôlent la manière dont ces informations peuvent être stockées, interprétées, utilisées ou partagées » (CGIPN, s.d.). Les principes de PCAP® sont donc étroitement associés aux considérations de science ouverte et de sécurité de la recherche, la responsabilité et le droit de déterminer la sensibilité des informations des Premières Nations incombant aux individus ou aux communautés des Premières Nations concernés par la recherche. Les chercheurs ne doivent pas considérer les principes de PCAP® comme un obstacle à leurs activités de recherche, mais comme un tremplin pour établir des relations et faire progresser les perspectives des Premières Nations en matière de science ouverte et de sécurité de la recherche (Konczi et Bill, 2024).

Le Budget 2021 a alloué des fonds pour faire progresser la souveraineté des données pour les personnes et les communautés inuites et métisses « afin de renforcer les capacités des Inuits et de la Nation métisse en matière de données de base et d'élaborer des stratégies relatives aux données fondées sur les distinctions pour les Inuits et la Nation métisse » (GC, 2021a). En 2022, l'Inuit Tapiriit Kanatami s'est ainsi engagé à consacrer 4 millions de dollars à la création d'une stratégie inuite des données afin de soutenir des stratégies propres à chaque région de l'Inuit Nunangat (ITK, 2018; Jamal, 2022). De l'avis du comité d'experts, toute recherche impliquant les peuples autochtones ou leurs terres devrait être considérée comme sensible par défaut, car elle touche aux droits des Autochtones (qui peuvent dépasser les frontières des États) et nécessite le consentement des communautés concernées (IRSC *et al.*, 2022).

4 PCAP® est une marque déposée du Centre de gouvernance de l'information des Premières Nations. Pour mieux comprendre ces principes, consultez son site Web à https://fnigc.ca/fr/les-principes-de-pcap-des-premieres-nations/.

1.4 L'approche du comité d'experts

Pour s'acquitter du mandat, le CAC a réuni un comité d'experts multidisciplinaire et multisectoriel composé de 13 membres (ci-après dénommé « le comité »). Les membres ont été sélectionnés pour leur expertise dans les domaines suivants : sécurité nationale et de la recherche, écosystème de la recherche postsecondaire, infrastructures de recherche, politique nucléaire, épidémiologie, recherche sur les agents pathogènes, océanographie, contributions à la science ouverte, biosécurité et bioéthique. À ces domaines s'ajoute leur expérience dans la mise en œuvre de politiques de sécurité de la recherche. Les membres du comité ont travaillé bénévolement et ont été chargés de procéder à une évaluation approfondie et objective des données disponibles. Le comité s'est réuni cinq fois virtuellement et deux fois en personne sur une période de 11 mois, entre juillet 2024 et juin 2025, afin d'élaborer le présent rapport.

Afin de garantir l'intégrité du processus d'évaluation, les membres du comité ont été tenus de signaler au CAC et aux autres membres tout conflit d'intérêts – réel, prévisible ou perçu – pertinent pour les questions examinées, afin que ceux-ci puissent être gérés avec transparence. Les membres ont respecté un accord de confidentialité et un code de conduite visant à favoriser un environnement propice à des délibérations collaboratives et respectueuses, au libre-échange des connaissances et à la synthèse des données probantes. Afin de préserver l'indépendance du comité, le commanditaire n'en a pas nommé les membres et n'est pas intervenu pendant le processus d'évaluation, à l'exception des cas suivants : (i) lors de la première réunion du comité, où le commanditaire a été invité à présenter le mandat, et (ii) lors d'une séance d'information prévue après que le comité eut officiellement approuvé le rapport avant sa publication, où le comité a présenté ses principaux constats au commanditaire.

Le rapport a fait l'objet d'un examen approfondi par des pairs, au cours duquel 13 experts supplémentaires, canadiens et étrangers, ont apporté des données, des compétences et des connaissances supplémentaires. À l'instar des membres du comité, les pairs évaluateurs ont participé à titre individuel et non en tant que représentants de leur organisation. Les pairs évaluateurs ont fourni des commentaires pour éclairer les délibérations du comité, mais n'ont pas été invités à approuver le rapport final. Ils sont restés anonymes jusqu'à la publication du rapport. Ce processus a été supervisé par un vérificateur indépendant de l'examen par les pairs, nommé par le comité consultatif scientifique du CAC, ce qui a encore renforcé l'intégrité de l'examen.

1.4.1 Données probantes et portée

L'évaluation du comité d'experts s'est fondée sur l'examen et la synthèse de diverses sources de données probantes, notamment des publications évaluées par des pairs et de la littérature grise (c.-à-d. documents d'orientation, publications gouvernementales, sites Web et rapports d'organisations et de comités nationaux et internationaux). Le comité a effectué des recherches par mots clés dans la littérature publiée à l'aide de plusieurs bases de données et a exploré les sites Web des ministères et organismes gouvernementaux pertinents au Canada et dans certains pays (Aotearoa Nouvelle-Zélande, Australie, l'UE, France, Allemagne, Pays-Bas, Royaume-Uni, États-Unis), en passant en revue la législation, les politiques et les lignes directrices pertinentes relatives aux mesures de sécurité de la recherche afin de constituer une base de données factuelles permettant de s'acquitter du mandat (CAC, 2025). Le présent rapport ne repose pas sur un examen systématique, mais plutôt sur une synthèse détaillée – éclairée par une analyse des pays – des références clés, telles que répertoriées par le comité (CAC, 2025) (le tout est disponible sur le site Web du CAC).

Le comité a recueilli des données supplémentaires au moyen d'entretiens semi-structurés afin de mieux comprendre l'étendue des points de vue sur la recherche sensible et les domaines connexes. Ses membres ont ainsi interrogé des chercheurs autochtones et des personnes travaillant avec des organisations autochtones dans les domaines de la souveraineté des données, de la science ouverte et de la sécurité de la recherche afin de s'assurer que ces points de vue étaient pris en compte parallèlement aux mesures visant à reconnaître et à protéger la recherche sensible préoccupante. En outre, le comité a interrogé des praticiens et des universitaires dans les deux domaines de recherche qui intéressent le commanditaire.

L'examen des données n'a pas porté sur les questions liées à la désinformation, à la mésinformation et à l'altération des données ou des connaissances par des acteurs malveillants ni sur l'évaluation exhaustive des programmes et des politiques, car ces domaines ont été jugés hors du champ de la présente étude.

Le comité a recueilli des données entre juillet 2024 et juin 2025. Il note que l'évolution rapide du contexte géopolitique pourrait entraîner la modification ou le retrait de certaines des mesures répertoriées dans le présent rapport dans un avenir proche.

1.4.2 Domaines de recherche

Le comité a été chargé de démontrer comment les mesures de sécurité de la recherche examinées dans le rapport pourraient être mises en œuvre dans deux domaines : la recherche océanographique et celle portant sur les agents pathogènes. Ces deux domaines présentent des niveaux très différents de surveillance et de sensibilisation par rapport aux enjeux ainsi qu'aux approches touchant la sécurité de la recherche.

La reconnaissance et la protection de la recherche sensible préoccupante sont officialisées dans le domaine des agents pathogènes, mais les cadres existants ne permettent pas de répondre pleinement à la complexité de l'ensemble du secteur de la recherche

La recherche sur les agents pathogènes est cruciale pour la société et l'économie canadiennes. Elle est un moteur essentiel de l'amélioration des soins de santé, de l'augmentation de la qualité de vie et de la longévité (Uhlenhaut *et al.,* 2013). Elle a également apporté d'énormes avantages à l'humanité grâce aux progrès de la biotechnologie, notamment dans la production alimentaire, la (bio)médecine, la synthèse de produits biopharmaceutiques, les (bio)matériaux, l'environnement, l'énergie et les mesures de lutte contre le bioterrorisme (Rappert et Selgelid, 2013; Rohden et Wieden, 2022). En outre, l'utilisation croissante des méthodes liées aux sciences de la vie dans les processus industriels jette les bases d'une bioéconomie en plein essor (Rohden et Wieden, 2022). La biotechnologie devrait également stimuler la recherche industrielle, l'éducation et l'emploi dans le domaine des sciences de la vie, à l'appui d'autres innovations et découvertes (RBC Thought Leadership, 2024).

La recherche sur les agents pathogènes classée comme recherche sensible préoccupante[5] peut être essentielle pour la santé publique, la préparation aux pandémies et l'agriculture, ses constats contribuant à des avancées scientifiques plus larges (NIH, 2014; Wang *et al.*, 2025). Compte tenu de ces avantages, le fait de conclure qu'un projet de recherche est préoccupant et que la recherche peut être utilisée à des fins néfastes n'exclut aucunement qu'il puisse être financé, mené à bien ou mis en commun. Cela signifie plutôt que les chercheurs et les établissements doivent minimiser les risques d'utilisation abusive en élaborant des mesures de protection appropriées et en les mettant en œuvre (NIH, 2014). On peut soutenir que les dommages éventuels pourraient être d'une échelle comparable aux avantages potentiellement conférés par des applications positives.

5 Les NIH (2014) utilisent le terme RDUP (« DURC » en anglais).

La reconnaissance et la protection de la recherche sensible préoccupante portant sur des agents pathogènes sont officialisées par des instruments internationaux (voir p. ex. OMS, 2022) et des lois, règlements et lignes directrices au niveau national (chapitres 3 et 4). Selon l'Indice de sécurité sanitaire mondial 2021, le Canada se classe au premier rang mondial en matière de biosécurité et au troisième rang en matière de biosûreté (GHS Index, 2021; SC et ASPC, 2022). Cependant, même lorsque la reconnaissance et l'évaluation des risques sont formalisées, les cadres existants ne permettent pas de répondre pleinement à la complexité du secteur de la recherche, des circonstances pouvant survenir tout au long du processus et entraîner des risques supplémentaires. Au Canada, les mesures existantes visant à protéger la recherche sensible préoccupante sont axées sur la biosécurité et la biosûreté, tandis que les règles relatives à la cybersécurité, aux collaborations en matière de recherche, à la mise en commun et à la communication responsables des données sont moins claires (chapitre 4).

Il existe un manque de lignes directrices sur la reconnaissance et la protection de la recherche océanographique sensible

La recherche océanographique, en particulier les travaux utilisant les sciences observationnelles et prédictives, est de plus en plus ouverte et accessible au public comme aux organismes internationaux dans l'intérêt de la modélisation climatique et de la sécurité de la navigation maritime (voir p. ex. SIOOC, s.d.-a,-b; ONC, s.d.-a). Les données en libre accès précisant l'emplacement de diverses ressources (p. ex. les bancs de poissons, les gisements minéraux) pourraient avoir une valeur énorme pour la gestion et l'exploitation de telles ressources (Loft et Saumweber, 2020). Les données cartographiques du fond océanique et de la profondeur de l'eau (données bathymétriques) contribuent à la gestion durable des océans, à la détection des risques géologiques et à la compréhension des changements climatiques (Wölfl *et al.,* 2019). Des prévisions actualisées et précises sont donc vitales au maintien des activités industrielles et économiques, de la sécurité environnementale et de la sécurité humaine (GC, 2025c). En outre, la surveillance des conditions océaniques revêt une importance critique pour la modélisation du climat et nécessite une coopération régionale et internationale afin d'obtenir des informations précises à l'échelle mondiale (voir p. ex. Fujii *et al.,* 2019; Révelard *et al.,* 2022). Les données océaniques sont collectées par de nombreux acteurs, notamment des chercheurs, le gouvernement (p. ex. le ministère de la Défense nationale, Transports Canada, la Garde côtière canadienne), des entreprises privées et des organisations non gouvernementales (Iverson *et al.,* 2019; RCAANC, 2022b; Moran *et al.,* 2022; RDDC, 2023; POLAIRE, 2023; GC, 2025d; GFW, s.d.).

Le Canada participe à des services internationaux de prévision océanique et à des réseaux d'observation, qui reposent tous sur un certain niveau d'ouverture et d'accessibilité des données océaniques canadiennes (p. ex. le Système mondial d'observation de l'océan, l'Organisation hydrographique internationale) (OHI, 2021; MPO, 2022; SIOOC, s.d.-a). On s'attend à ce que de nombreux produits de la recherche (p. ex. les données d'observation, de surveillance et de suivi des océans) soient rendus publics et accessibles afin d'atténuer les effets des changements climatiques et d'assurer la sécurité de la navigation. Cependant, ces données pourraient également être utilisées à des fins de navigation clandestine et pour échapper à la surveillance dans les eaux canadiennes.

L'accès libre aux données en temps réel sur la glace de mer et les prévisions météorologiques est un besoin essentiel dans l'océan Arctique (Smith *et al.*, 2019). La région subit en effet bon nombre des principaux effets des changements climatiques (voir p. ex. Rantanen *et al.,* 2022). Les coûts écologiques et sociaux de ces impacts, ainsi que les données physiques connexes décrivant cet environnement en mutation, sont des informations précieuses pour modéliser les scénarios climatiques futurs et les stratégies d'atténuation à différentes échelles (GIEC, 2019; Gaffey *et al.,* 2024). Les perturbations dans l'Arctique menacent également d'une manière appréciable la santé et le bien-être des peuples autochtones qui y vivent : ils sont en effet confrontés aux effets disproportionnés et interdépendants des changements climatiques sur la sécurité alimentaire et l'identité culturelle (POLAIRE, 2022). Lorsqu'ils sont envisagés globalement, ces facteurs soulignent l'importance de la recherche sur le climat de l'océan Arctique, incluant celle menée sous la direction des peuples autochtones ou en cogestion avec eux (POLAIRE, 2022).

Le commanditaire a demandé que, dans le cadre de l'examen de l'océanographie en tant que domaine d'intérêt, le comité accorde une attention particulière à la sécurité de la recherche menée dans l'océan Arctique. Le comité observe ce qui suit : (i) il s'agit d'une région où des intérêts divergents s'affrontent, au détriment d'une collaboration scientifique efficace, et (ii) le niveau d'ouverture de la recherche peut être influencé par des priorités nationales et un contexte géopolitique en mutation (encadré 1.3).

Encadré 1.3 Sécurité de la recherche dans l'Arctique

De nombreux pays ont défini la recherche scientifique comme un élément clé de leurs politiques arctiques (Heininen *et al.*, 2020). La Chine s'est concentrée sur l'élargissement de ses collaborations scientifiques avec les États arctiques dans les domaines de la télédétection, des observations spatiales et de la recherche sur les changements climatiques, ce qui suscite des inquiétudes quant aux applications militaires potentielles de ces activités (Robinson, 2020; Falco *et al.*, 2024; Weisko, 2025). De plus, ces dernières années, la Chine et la Russie ont intensifié leur collaboration dans l'Arctique, la Russie dépendant de plus en plus de la Chine pour financer et soutenir le développement de projets de recherche et d'infrastructures en raison des sanctions imposées par d'autres pays à la suite de l'invasion de l'Ukraine (Funaiole *et al.*, 2023; GC, 2024a). Ces tendances renforcent la présence de la Chine dans l'Arctique, ce qui représente potentiellement une importante menace pour la sécurité nationale du Canada (GC, 2024a). Parallèlement, la navigabilité accrue de l'Arctique maritime due aux changements climatiques soulève également des questions de sécurité nationale, notamment l'affirmation de la souveraineté du Canada dans la région et le renforcement des capacités en matière de sécurité (SECD, 2023).

La difficulté de fournir des orientations claires sur la reconnaissance et la protection de la recherche océanographique sensible est exacerbée par le fait que les sciences océaniques sont vastes et englobent « toutes les disciplines de recherche liées à l'étude de l'océan, du littoral et de leurs relations avec les sociétés : les sciences naturelles, les sciences de la santé et les sciences sociales, ainsi que l'ingénierie, les sciences humaines et la recherche multidisciplinaire » (CAC, 2013). Selon la Woods Hole Oceanographic Institution, la recherche océanographique englobe l'étude du climat et de la météorologie, les sciences côtières, les dangers océaniques, la chimie des océans, la circulation océanique, la vie océanique, les ressources et les politiques océaniques, les systèmes polaires, la pollution, les fonds marins, les technologies océaniques et l'archéologie sous-marine (WHOI, s.d.). Au sein de chacun de ces domaines, il existe des spécialisations de recherche plus poussées. Par exemple, le suivi des navires est un domaine de recherche important dans le domaine des technologies océaniques, car il contribue à assurer la sécurité maritime et à éclairer les décisions sur le plan

environnemental (Nicoll *et al.,* 2025). Au-delà de l'étendue et de la diversité des disciplines concernées, la recherche océanographique peut également être interdisciplinaire ou transdisciplinaire.

1.5 Structure du rapport

Le présent rapport décrit les mesures (c.-à-d. les politiques, les stratégies ou les cadres) qui pourraient aider la communauté scientifique à reconnaître et à protéger la recherche sensible tout en assurant un équilibre entre la science ouverte et l'innovation. Il applique ensuite ces mesures à la recherche sur les océans et les agents pathogènes. Le **chapitre 2** fournit le contexte du reste du rapport en se concentrant sur le paysage de la recherche au Canada sous l'angle de la sécurité et de la science ouverte. Les **chapitres 3 et 4** décrivent les mesures qui peuvent aider la communauté scientifique à reconnaître et à protéger la recherche sensible préoccupante tout au long du processus de recherche, c'est-à-dire la phase de conception, la phase active et la phase post-recherche. Ces mesures sont ensuite appliquées à la recherche sur les océans et les agents pathogènes à l'aide d'exemples actuels et hypothétiques. Le **chapitre 5** décrit les facteurs favorables qui peuvent contribuer à faciliter la mise en œuvre des mesures décrites dans les deux chapitres précédents. Le **chapitre 6** résume l'application des mesures à la recherche sur les océans et les agents pathogènes et se conclut par les réflexions générales du comité. Il souligne que, pour être pleinement efficaces, les mesures doivent être adoptées de manière holistique à toutes les étapes du processus de recherche et soutenues par un système de responsabilité partagée.

2

Le paysage de la recherche au Canada

2.1 Acteurs de l'écosystème de la recherche

2.2 Caractéristiques de l'écosystème de la recherche

2.3 Science ouverte

2.4 Sécurité de la recherche

Constatations du chapitre

- L'écosystème de la recherche décentralisé et internationalisé du Canada se prête à des travaux de recherche de calibre mondial dans des domaines technologiques sensibles qui présentent des avantages importants pour le développement scientifique et la société en général.
- L'approche actuelle de la sécurité de la recherche et de la science ouverte au Canada se traduit par une surveillance limitée de la part des autorités publiques relativement à la recherche sensible non financée par le gouvernement.
- Le secteur privé est un acteur important de l'écosystème de la recherche au Canada. Sa participation aux mesures favorisant la science ouverte et la sécurité de la recherche est nécessaire pour garantir la mise en commun responsable de tous les produits de la recherche.
- Le financement de la recherche par des entités multinationales étrangères ne relève pas de la compétence fédérale canadienne, ce qui constitue une lacune dans l'approche nationale de la sécurité de la recherche.
- Les efforts du gouvernement pour promouvoir l'adoption de la science ouverte au Canada se sont concentrés sur la publication en libre accès. Or, les mesures qui favorisent la gestion et la mise en commun responsables des données de recherche sont nouvelles et nécessitent des ressources, de la formation et des incitatifs pour être mises en œuvre avec succès dans l'ensemble de l'écosystème de la recherche.

L'écosystème de la recherche du Canada a produit des travaux de calibre mondial, notamment dans des domaines technologiques sensibles, qui ont profité à la science comme à la société. Cependant, à mesure que l'écosystème s'internationalise et se décentralise (section 2.1), les gouvernements et les établissements de recherche risquent de perdre le contrôle sur la manière dont la recherche, incluant la recherche sensible, est menée, protégée et mise en commun (section 2.2). Les gouvernements ont bien mis en œuvre des politiques favorisant la science ouverte et la sécurité de la recherche afin de remédier à ce problème, mais celles-ci doivent être mieux appliquées et interconnectées afin de concrétiser pleinement le principe selon lequel « la recherche doit être aussi ouverte que possible et aussi protégée que nécessaire » (ISDE, 2023a) (sections 2.3 et 2.4).

2.1 Acteurs de l'écosystème de la recherche

Le *secteur de l'enseignement supérieur*, qui inclut les universités, les collèges, les écoles polytechniques, les établissements de santé et les instituts de recherche affiliés, génère une grande partie de la recherche fondamentale et de nombreuses applications technologiques qui sont finalement commercialisées. Les dépenses de R-D du Canada dans le secteur de l'enseignement supérieur – plus de 18 milliards de dollars en 2024 (StatCan, 2024a) – sont proportionnellement plus élevées que dans la plupart des pays comparables[6]. Ainsi, en 2022, le Canada occupait le deuxième rang des pays du G7 pour l'intensité de la R-D dans l'enseignement supérieur (dépenses en pourcentage du PIB) (OCDE, 2025). Le gouvernement du Canada a consacré des investissements importants au maintien et au renforcement de la recherche postsecondaire dans les domaines où le Canada occupe une position de chef de file, des domaines où la recherche pourrait se révéler sensible dans bien des cas. Par exemple, en ce qui concerne les technologies quantiques, le Canada est un chef de file de la R-D dans les établissements publics, le gouvernement fédéral ayant récemment lancé une stratégie nationale en la matière (ISDE, 2022a; CAC, 2023b). L'IA est un autre domaine où le gouvernement fédéral a investi plus de 2 milliards de dollars depuis 2017 (CPM, 2024a) et il s'est engagé à investir plus de 2 milliards de dollars supplémentaires dans le budget 2024 (GC, 2024b).

Les établissements d'enseignement postsecondaire au Canada forment également des étudiants diplômés à un rythme croissant : plus de deux fois plus de doctorats ont été décernés en 2022 qu'en 2002 (StatCan, 2024b). La population étudiante diplômée du Canada est très cosmopolite, en particulier dans les domaines à forte intensité technologique; toutefois, les plafonds fédéraux imposés aux étudiants internationaux en 2024 et 2025, ainsi que les politiques de sécurité entourant la recherche, pourraient avoir une incidence sur cette tendance (GC, 2025e) (section 2.4). Plus de 50 % des doctorats décernés en 2021 dans les domaines des STIM et de la santé[7] l'ont été à des étudiants étrangers (StatCan, 2023). Le fait qu'ils peuvent choisir de quitter le Canada une fois leurs études terminées (CAC, 2021) contribue à la perte d'occasions pour la recherche et l'innovation canadiennes. Des facteurs comme les compétences linguistiques, les procédures d'immigration longues et

6 Selon Statistique Canada (StatCan, 2020), « le secteur de l'enseignement supérieur englobe toutes les universités, les collèges techniques et tous les instituts d'enseignement postsecondaire, quelles que soient leur source de financement ou leur forme juridique. En font également partie tous les instituts de recherche et centres ou ateliers expérimentaux qui sont administrés ou exploités directement par les établissements d'enseignement supérieur ».

7 Selon les catégories de Statistique Canada, « Sciences physiques et de la vie, et technologies », « Mathématiques, informatique et sciences de l'information » et « Santé et domaines connexes » (StatCan, 2023).

coûteuses, le temps passé dans le pays d'études, ainsi que les conditions socioéconomiques et politiques (tant dans le pays d'études que dans le pays d'origine) influent également sur la rétention des titulaires de doctorats internationaux (Trevena, 2019; Grewal, 2022; Malik *et al.*, 2022; Richardson et Hussain, 2022).

Le *secteur privé* (p. ex. l'industrie, les entreprises en démarrage, les multinationales étrangères) mène également des recherches fondamentales et appliquées, mais en 2022, l'intensité de la R-D des entreprises commerciales canadiennes se classait à l'avant-dernière place du G7 (OCDE, 2025). Malgré un niveau d'activité de recherche relativement faible, certains travaux de recherche privée pourraient être considérés comme sensibles, nécessitant donc une surveillance et une évaluation des risques minutieuses. Par exemple, les sociétés pharmaceutiques qui développent de nouvelles plateformes vaccinales – comme les vaccins à ARNm – travaillent sur des technologies qui préviennent les maladies infectieuses, mais qui ont également le potentiel d'être utilisées pour la manipulation génétique de pathogènes. Voilà qui pourrait nuire à la santé humaine si elles devaient servir des fins malveillantes (Musunuri *et al.*, 2021; Sandbrink et Koblentz, 2022). En 2019, on estimait que 70 % des permis de recherche sur les agents pathogènes et les toxines délivrés par l'ASPC avaient été accordés au secteur privé (ASPC, 2020; Gryphon Scientific, LLC, 2023). Le comité note toutefois que le nombre de permis délivrés ne reflète pas nécessairement la part du secteur privé dans les activités de recherche sur les agents pathogènes.

Divers *ordres de gouvernement* participent à l'écosystème de la recherche à titre de chercheurs, de bailleurs de fonds et de régulateurs. Ainsi, le gouvernement fédéral établit la politique commerciale internationale (incluant le contrôle des exportations de biens et de technologies) en créant des cadres stratégiques liés à la défense nationale, à la concurrence et à la propriété intellectuelle (GC, 1982, 1985a, 2025f; de Beer, s.d.). Il mène également des activités de R-D et de développement des talents afin d'appuyer le secteur privé et la réalisation des mandats publics (ISDE, 2025) tout en fournissant une infrastructure de recherche à l'échelle nationale, notamment 19 installations financées par la Fondation canadienne pour l'innovation (FCI) (FCI, s.d.-a). L'ASPC est quant à elle chargée de l'administration et de l'application des lois et règlements visant à « promouvoir et à protéger la santé, la sécurité et la sûreté des Canadiens » et qui minimisent les risques liés à la recherche sur les agents pathogènes et les toxines (ASPC, 2022, 2024a).

Les gouvernements provinciaux et territoriaux ont pour leur part un rôle à jouer dans l'éducation, la recherche interne, le financement et l'octroi de permis pour la recherche, la fourniture d'infrastructures scientifiques et de

services de santé, ainsi que le soutien aux centres d'expertise régionaux (CAC, 2017, 2023a). La compétence des provinces et des territoires en matière d'enseignement postsecondaire complique l'harmonisation des politiques de sécurité de la recherche à l'échelle du pays (section 5.1).

Enfin, en tant que détenteurs de droits, les *Premières Nations, les Inuits et les Métis* ont le droit de déterminer les activités de recherche pouvant être menées sur leurs terres; de contrôler les données relatives à leurs territoires, leurs terres, leurs connaissances et leurs langues; et de décider de l'utilisation des données et des connaissances acquises dans le cadre de ces activités de recherche (ONU, 2007). Les peuples autochtones participent également activement aux activités de recherche en tant que détenteurs de connaissances, chercheurs et sujets de recherche (GC, 2019a).

2.2 Caractéristiques de l'écosystème de la recherche

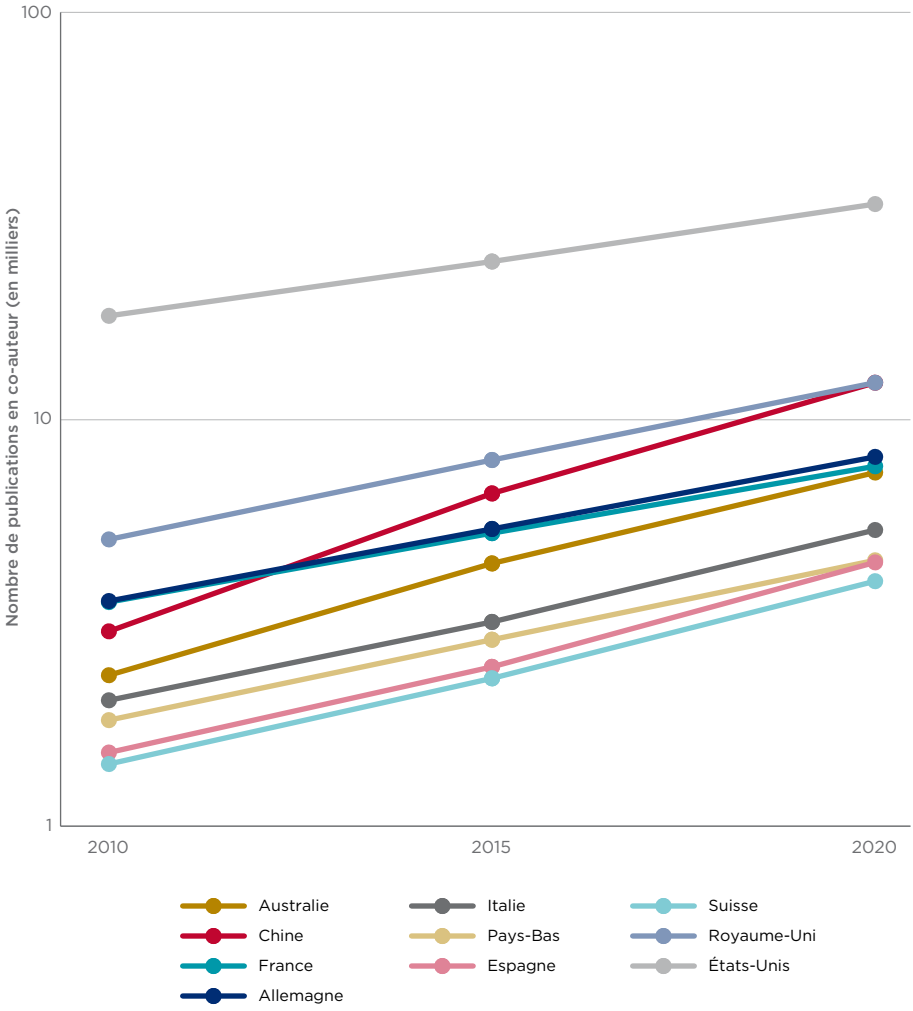
L'écosystème de recherche du Canada bénéficie de collaborations internationales et intersectorielles

Les collaborations interdisciplinaires et intersectorielles sont une caractéristique importante du paysage canadien de la recherche. Le Canada affiche en effet l'un des taux les plus élevés de l'OCDE pour ce qui a trait à l'investissement des entreprises dans la R-D menée dans l'enseignement supérieur, cet investissement représentant environ 7 à 8 % du financement entre 2010 et 2022 (OCDE, 2025). La recherche canadienne dans des domaines hautement concurrentiels comme l'IA bénéficie d'investissements des secteurs public, philanthropique et privé (notamment de multinationales étrangères) (Brandusescu, 2021; Université de Toronto, 2022; Geremia, 2024).

Les collaborations entre disciplines ou secteurs économiques sont soutenues par des programmes de subventions (p. ex. les subventions Alliance, le fonds Nouvelles frontières en recherche, le Fonds d'excellence en recherche Apogée Canada) afin d'encourager les percées technologiques et la recherche à haut risque et à haut rendement avec des partenaires internationaux et nationaux du secteur privé (GC, 2022c; CRSNG, 2024c; CRCRC, 2025). Le ministère de la Défense nationale (MDN) collabore avec les secteurs privé et universitaire afin de tirer parti des avantages de l'innovation. En 2018, le MDN a lancé le programme Innovation pour la défense, l'excellence et la sécurité (IDEeS) afin de renforcer les capacités de défense et de sécurité nationales en proposant aux innovateurs canadiens des défis axés sur la demande (MDN, 2023). En mars 2023, IDEeS avait lancé 75 défis et investi plus de 330 millions de dollars dans des projets. La majorité des fonds ont été alloués aux petites et moyennes entreprises (53 %), au milieu universitaire (27 %) et aux grandes industries

(17 %) (MDN, 2024a). Les chercheurs des ministères et organismes gouvernementaux à vocation scientifique peuvent collaborer à l'échelle internationale, incluant avec des partenaires du secteur privé. Par exemple, entre 2012 et 2023, les scientifiques de Pêches et Océans Canada ont coécrit 6 623 articles universitaires, dont 54 % faisant participer des collaborateurs internationaux et 11 % comprenant des auteurs affiliés à des organisations à but lucratif (Science-Metrix, 2024).

Les chercheurs canadiens participent également à de nombreuses collaborations internationales. D'après le nombre de publications corédigées répertoriées dans la plateforme Web of Science, les États-Unis sont le collaborateur le plus fréquent du Canada, avec 33 841 articles publiés en 2020 (figure 2.1). Le Royaume-Uni et la Chine occupent respectivement la deuxième et la troisième place. Entre 2010 et 2020, les collaborations entre chercheurs canadiens et chinois ont augmenté de plus de 75 % (CAC, 2024a), ce qui représente un changement par rapport aux collaborations bilatérales moins fréquentes au début des années 2000. Le comité note que ces publications reflètent les collaborations de recherche qui ont eu lieu avant l'introduction des politiques fédérales et provinciales entourant la sécurité de la recherche (section 2.4). Il n'est pas certain que cette tendance à la hausse se maintiendra en raison du refroidissement des relations entre le Canada et la Chine observé ces dernières années. Le gouvernement fédéral s'appuie sur des accords et des partenariats officiels en matière de science et de technologie conclus avec d'autres pays et régions afin de consolider la place du Canada au sein de la communauté mondiale de la recherche (voir p. ex. CPM, 2024b; GC, 1986). Par exemple, en 2024, le Canada et l'UE ont signé un accord qui permet aux organisations et aux chercheurs canadiens de participer au pilier 2 d'Horizon Europe selon les mêmes conditions que leurs homologues de l'UE (CE, s.d.-a).



Source : CAC (2024a)

Figure 2.1 Les dix principaux pays avec lesquels le Canada collabore à titre de coauteur

Principaux pays avec lesquels le Canada a collaboré en fonction du nombre de publications dont il a été coauteur entre 2010 et 2020, selon la plateforme Web of Science.

Les partenariats et la recherche collaborative sont souvent considérés comme des catalyseurs de découvertes et sont louangés pour leur capacité à tirer parti de compétences et de ressources complémentaires (TRIUMF, 2018; CAC, 2024a).

Cependant, l'écosystème de la recherche décentralisé du Canada est également vulnérable aux risques de sécurité posés par le nombre croissant de participants animés par des motivations, des valeurs et des incitatifs distincts. En raison d'un manque de surveillance centralisée, les données, les informations, les connaissances et la propriété intellectuelle peuvent être menacées par des entreprises malveillantes ou à cause d'une divulgation accidentelle (Wilner *et al.,* 2022). Dans les domaines de recherche où le Canada possède des atouts, les enjeux sont plus importants, car ces domaines sont plus susceptibles d'attirer des acteurs malveillants cherchant à utiliser les données, connaissances, technologies ou la propriété intellectuelle à mauvais escient ou à les détourner (voir p. ex. Centre pour la cybersécurité, 2024a). Le manque de sensibilisation des chercheurs aux menaces ou le rejet des procédures et protocoles de sécurité standard peuvent exacerber ces vulnérabilités (Centre pour la cybersécurité, 2024b; ISDE, 2024b).

Les activités de recherche sensibles se déroulent dans des contextes de plus en plus ouverts et échappent désormais à la portée des mécanismes actuels de surveillance gouvernementale

L'histoire de la recherche sensible est marquée par plusieurs exemples de technologies qui sont aujourd'hui omniprésentes dans la vie civile après avoir été découvertes ou étudiées pour la première fois dans le cadre de programmes de R-D militaires ou industriels financés par le gouvernement. Bien que l'Internet, les systèmes de positionnement GPS et les modèles d'IA soient le fruit de décennies de travaux de développement dans plusieurs secteurs, tous trois trouvent leur origine dans des activités de recherche menées ou financées par le gouvernement américain (Evan et Hays, 2006; Mowery, 2010; Lukasik, 2011; Ueno, 2023). De même, les programmes d'approvisionnement militaire américains ont soutenu des laboratoires privés, comme le Bell Labs, qui travaillaient sur l'électronique et les semi-conducteurs (Holbrook, 1995; Nokia Bell Labs, 2022). Les technologies et les processus élaborés ou financés par le gouvernement américain figurent toujours en bonne place sur les listes de contrôle des exportations (GC, 2025f).

Au cours des dernières décennies, des technologies sensibles ont également été développées indépendamment de la R-D financée par les pouvoirs publics. Par exemple, les technologies quantiques, la technologie CRISPR-Cas9 et les récentes applications de l'IA impliquent des activités de R-D à un stade précoce issues de la recherche fondamentale menée dans le secteur universitaire – qui est de plus en plus financée par le secteur privé (Zhang, 2019; Pannier, 2023; Major *et al*., 2024). Le développement de technologies à double usage potentiel en dehors d'un contrôle direct des autorités publiques réduit la capacité des

gouvernements à encadrer les activités de recherche et la mise en commun de ses résultats. Après avoir consulté des responsables de la politique étrangère de la Commission européenne, de la France et des États-Unis, Pannier (2023) a constaté que les gouvernements étaient inquiets du rôle important joué par les grandes entreprises multinationales (EMN), car leurs décisions concernant la localisation des activités de R-D et le choix des partenariats ne tiennent pas compte des alliances bilatérales existantes entre les États ni de la souveraineté ou des priorités relatives à la sécurité nationale d'un État. Ces défis peuvent être exacerbés par le fait que certaines entités à but lucratif sont susceptibles d'être entièrement ou partiellement détenues par un État *et al*ignées sur les intérêts de gouvernements étrangers (Jin *et al.*, 2022; Libman *et al.*, 2022). La participation de certaines entreprises privées étrangères à des recherches sensibles met encore plus en évidence les vulnérabilités liées à la perte de recherches, de données, de connaissances, d'informations et de propriété intellectuelle en raison d'actions malveillantes ou de divulgations involontaires (Wilner *et al.*, 2022; SCRS, 2024a).

Au Canada, les EMN ont été responsables de la grande majorité (76 %) des dépenses de R-D des entreprises en 2022, les EMN étrangères représentant la plus grande part (44 %), suivies des EMN canadiennes (32 %) et des entreprises non multinationales (24 %) (StatCan, 2024c). Le financement de la recherche par les EMN étrangères ne relève actuellement pas de la compétence fédérale canadienne. De l'avis du comité, cela représente une lacune dans l'approche nationale de la sécurité de la recherche, qui est axée uniquement sur la protection de certains travaux financés par des fonds publics. Le Conseil canadien des affaires, qui représente plus de 170 entreprises canadiennes, a suggéré que, pour garantir la sécurité économique, le gouvernement fédéral devrait concentrer ses efforts sur le soutien à la collaboration entre les secteurs privé, public et universitaire canadiens et sur l'adoption de politiques visant à remplacer les sources étrangères problématiques de financement de la recherche universitaire (Conseil canadien des affaires, 2023, s.d.). Toutefois, un certain nombre de facteurs favorables sont à même de renforcer la sécurité de la recherche nationale dans l'ensemble des secteurs tout en exploitant le potentiel de la recherche et de l'innovation non financées par le gouvernement (chapitre 5).

La recherche dans l'Arctique reste une priorité pour le Canada, mais elle s'accompagne de défis relevant de la sécurité géopolitique

Plusieurs pays ont renforcé leur présence dans l'Arctique par l'action de politiques stratégiques axées sur la recherche, la sécurité ou d'autres facteurs (Heininen *et al.*, 2020; POLAIRE, 2020; IARPC, 2021; Gouv. des États-Unis, 2022a;

Eiterjord, 2023; Lipunov et Devyatkin, 2023). Ces politiques sont motivées par des intérêts et des valeurs qui ne correspondent pas toujours à ceux du Canada et qui peuvent être source de tensions géopolitiques. Ainsi, les relations conflictuelles entre la Chine, la Russie et les États-Unis se répercutent dans l'Arctique pour des raisons stratégiques, mais aussi en raison des lacunes de gouvernance dans cette région (Zandee *et al.,* 2020; Cunningham, 2024; Tatlow, 2024). Bien que le Canada s'appuie sur des collaborations internationales pour améliorer ses connaissances sur la région arctique, notamment en ce qui concerne la biodiversité et les changements climatiques, les efforts visant à établir des partenariats de recherche risquent d'être entravés par l'évolution de la situation géopolitique (GC, 2024a). Par exemple, l'interruption des collaborations avec la Russie à la suite de son invasion de l'Ukraine a fait en sorte que la première a cessé de fournir sa part des données climatiques sur l'Arctique, qui couvrent près de la moitié de la région, au détriment des efforts de modélisation climatique dont les résultats sont largement utilisés (Breum, 2024).

Les efforts de recherche d'autres pays dans l'Arctique suscitent des préoccupations pour la sécurité nationale du Canada (Tatlow, 2024), car les données géoscientifiques physiques recueillies dans le cadre d'activités de recherche peuvent être utilisées pour affirmer une présence ou une domination dans des régions septentrionales contestées sur le plan géopolitique (Eiterjord, 2024). L'expansion des infrastructures de détection sans opérateur et la mise en place de stations satellitaires terrestres, prétendument utilisées à des fins scientifiques (p. ex. pour faciliter le transfert de données depuis les infrastructures de détection), constituent un exemple d'activités de recherche sensibles dans l'Arctique, les données collectées pouvant être utilisées à des fins de surveillance militaire (Thomson, 2017; Falco *et al.,* 2024). Un autre exemple est celui des technologies de détection sous-marine, qui risquent d'être utilisées par des acteurs étrangers dans la prospection des ressources minérales que recèlent les fonds marins de l'océan Arctique (Sun *et al.,* 2021; MDN, 2024b). Il a été avancé que la Chine mène des efforts de recherche dans l'Arctique afin de consolider sa position dans la région, de sécuriser les routes commerciales passant par le passage du Nord-Ouest et d'en explorer les ressources (voir p. ex. Brady, 2017; Eiterjord, 2023).

La recherche sur les agents pathogènes, qui est essentielle à la préparation aux pandémies, est la cible d'acteurs malveillants

La recherche sur les agents pathogènes est essentielle pour une préparation efficace aux pandémies, car elle permet une détection précoce; le développement d'outils diagnostiques, de traitements et de vaccins; ainsi que la

mise en place de stratégies d'intervention fondées sur des données probantes (NIAID, 2021). Le nombre de laboratoires menant des recherches sur les agents pathogènes a augmenté depuis la première identification du SARS-CoV-2, le virus responsable de la COVID-19, en 2019. En 2023, on comptait 51 laboratoires de niveau 4 en activité dans 27 pays, soit environ deux fois plus qu'il y a dix ans (Global BioLabs, 2023). Les laboratoires canadiens qui travaillent avec des agents pathogènes et des toxines ont apporté une contribution importante à la recherche nationale et internationale sur les pandémies, ce qui en fait des cibles privilégiées pour les activités malveillantes (Centre canadien pour la cybersécurité, 2024a). Pendant la pandémie de COVID-19, le Centre canadien pour la cybersécurité et des entreprises technologiques multinationales ont détecté une augmentation du volume des activités menaçantes menées contre des laboratoires canadiens et étrangers et d'autres entités participant aux efforts de lutte contre la pandémie (Centre canadien pour la cybersécurité, 2020). En juillet 2020, le Canada, les États-Unis et le Royaume-Uni ont publié une déclaration commune sur les activités de l'APT29, un groupe de cyberespionnage qui cible les organismes de recherche sur les vaccins afin de détourner la propriété intellectuelle (NCSC *et al.,* 2020). Les chercheurs et les organismes de recherche continuent d'être la cible de cybermenaces à des fins d'espionnage et d'enrichissement financier, ce qui a conduit à la mise en œuvre de mesures supplémentaires pour protéger la recherche sensible préoccupante (Centre pour la cybersécurité, 2024a).

2.3 Science ouverte

Les gouvernements soutiennent la science ouverte principalement en raison de ses promesses d'accélérer les progrès scientifiques et de promouvoir un impact sociétal positif (CE, 2019; GC, 2020; UKRI, 2024a). Fondamentalement, la science ouverte garantit la mise en œuvre d'un principe juridique internationalement reconnu : tous les êtres humains ont le droit de bénéficier des avantages des progrès scientifiques (Assemblée générale des Nations Unies, 1948, 1966; ISC, s.d.). Dans le domaine des soins de santé, par exemple, la mise en commun de données entre chercheurs peut accélérer l'innovation et les découvertes, ce qui se traduit par un accès plus rapide aux traitements ou aux remèdes pour les maladies rares (Rubinstein *et al.,* 2020). De plus, donner aux patients accès à la recherche signifie qu'ils peuvent devenir plus autonomes dans leur prise en charge (L'HO, 2021).

À cette fin, plusieurs pays, dont le Canada, ont adopté des politiques rendant obligatoire la mise en commun des publications ou d'autres résultats de la recherche (voir p. ex. SCT, 2014; ISDE, 2016; OSTP, 2022; cOAlition S, s.d.-a,-b). Au sein du gouvernement canadien, la Directive sur le gouvernement ouvert de

2014 a défini de nouveaux objectifs en matière de données ouvertes. Ces objectifs ont ensuite conduit à la Feuille de route pour la science ouverte de 2020 de la conseillère scientifique en chef, qui décrit plus en détail les responsabilités des ministères et organismes fédéraux relativement à la science ouverte (SCT, 2014, 2018; GC, 2020). Cette feuille de route a stimulé la création de plusieurs plans d'action coordonnés, mais distincts, en matière de science ouverte dans divers ministères et organismes (voir p. ex. MDN et FAC, 2021; ECCC, 2021; StatCan, 2024d). De l'avis du comité, la mise en œuvre de ces politiques par le gouvernement du Canada est essentielle pour améliorer l'accès du public à la recherche interne et l'application cohérente des principes de la science ouverte dans l'ensemble de l'écosystème de la recherche.

La science ouverte n'implique toutefois pas un accès universel; dans la pratique, l'accès est souvent limité et axé sur des aspects particuliers de la recherche. Les politiques d'ouverture par défaut ne garantissent donc pas un accès illimité aux données brutes, la disponibilité inconditionnelle des données et des métadonnées à des fins d'accès et d'utilisation étant considérée comme une exception plutôt que la règle dans un dépôt de données de recherche typique (CoreTrustSeal Standards and Certification Board, 2022). D'autre part, tous les chercheurs au Canada doivent se conformer aux lois fédérales, provinciales et territoriales entourant la protection de la vie privée et respecter le principe de la souveraineté des données autochtones, qui découle des droits des peuples autochtones à l'autonomie gouvernementale et à l'autodétermination (GC, 1982; ONU, 2007; CPVP, 2018; IRSC *et al.,* 2022; CGIPN, s.d.). En outre, l'Énoncé de politique des trois conseils : Éthique de la recherche avec des êtres humains (EPTC 2) énonce des considérations supplémentaires relatives à la confidentialité et d'autres mesures visant à restreindre l'accès à des données potentiellement sensibles ou personnelles et leur divulgation (IRSC *et al.,* 2022). Rappelons que la conformité à l'EPTC 2 est obligatoire pour les établissements admissibles à l'administration des fonds des trois organismes et pour les chercheurs qui mènent des recherches financées par ces derniers (IRSC *et al.,* 2022). Au sein du gouvernement fédéral, les chercheurs sont appelés au respect de « la vie privée, de la sécurité, des considérations éthiques et de la protection appropriée de la propriété intellectuelle » même s'ils adoptent une position d'ouverture par défaut (GC, 2020). Enfin, certains défenseurs de la science ouverte critiquent l'ouverture par défaut comme un paradigme potentiellement imprudent dont la

» La science ouverte n'implique toutefois pas un accès universel; dans la pratique, l'accès est souvent limité et axé sur des aspects particuliers de la recherche

justification éthique est étroite, compte tenu notamment de la puissance des technologies émergentes comme l'IA (Spitale *et al.*, 2024).

Les efforts récents du gouvernement du Canada pour promouvoir l'adoption de la science ouverte se sont concentrés sur la gestion et la mise en commun responsables des données

Un élément clé de la transition du Canada vers la science ouverte est le stockage, la gestion et la mise en commun responsables des données de recherche, soutenus par la Politique des trois organismes sur la gestion des données de recherche (politique sur la GDR) (GC, 2021b; Moher et Cobey, 2021). Cette politique, adoptée en 2021, exige que les établissements comme les chercheurs prennent des mesures de GDR et encourage la mise en commun des données, dans la mesure où les exigences éthiques, culturelles, juridiques et commerciales applicables le permettent (GC, 2021b) (encadré 2.1). L'adoption de ces mesures est à même de soutenir à la fois la science ouverte et la sécurité de la recherche en exigeant la prise en compte d'une mise en commun responsable de l'information.

Encadré 2.1 Éléments clés de la politique des trois organismes sur la GDR

- **Stratégie institutionnelle** : Tous les établissements d'enseignement postsecondaire et les hôpitaux de recherche admissibles à l'administration des fonds des trois organismes doivent publier une politique de GDR qui prévoit, entre autres, de « promouvoir, auprès des chercheurs, du personnel et des étudiants, l'importance de la gestion des données; [d']orienter leurs chercheurs sur la façon de gérer correctement les données, conformément aux principes énoncés dans la *Déclaration de principes des trois organismes sur la gestion des données numériques*, y compris pour élaborer des plans de gestion des données » et de « fournir ou appuyer un accès aux dépôts ou autres plateformes où sont conservées et organisées les données et où on peut avoir accès aux données de recherche de façon continue ».
- **Plans de gestion des données (PGD)** : Les meilleures pratiques en matière de GDR doivent être prises en compte dans toutes les propositions de recherche soumises aux trois organismes, et certaines propositions doivent inclure des PGD qui seront pris en considération dans le processus d'examen. Les PGD doivent décrire « comment les données seront recueillies, documentées, formatées, protégées, et conservées; comment seront utilisés les ensembles

(continue)

(a continué)

de données existants et quelles nouvelles données seront créées au cours du projet de recherche; comment les données seront communiquées, le cas échéant; et l'endroit où les données seront déposées ». Les PGD doivent également attribuer la responsabilité de la gestion des données, décrire les plans de succession et exposer les restrictions (éthiques, juridiques et commerciales) applicables aux données.

- **Dépôt des données** : Au moment de la publication, les bénéficiaires de fonds fédéraux doivent stocker dans un dépôt « les données de recherche, les métadonnées et les codes qui appuient directement les conclusions de la recherche publiées dans des revues de même que les préimpressions découlant de la recherche financée par les organismes subventionnaires ». Le dépôt choisi doit garantir le stockage, la conservation et la gestion sécurisés des données.

La politique prévoit également que les stratégies institutionnelles, les PGD et le dépôt doivent promouvoir le principe de souveraineté des données en ce qui concerne « les données créées dans le contexte de la recherche menée par et avec les collectivités, les regroupements collectifs et les organisations des Premières Nations, des Métis et des Inuits ».

(GC, 2021b)

Selon Moher et Cobey (2021), la mise en œuvre réussie de la politique de GDR au Canada dépend de plusieurs facteurs, notamment :

- la formation et l'éducation des chercheurs – élaboration d'un programme de base pouvant être adapté à différents établissements et disciplines;
- le financement de la mise en commun des données – soutenir les efforts des chercheurs par des subventions et des investissements dans les services de mise en commun des données;
- l'audit et le retour d'information – la mise en place de tableaux de bord permettant de suivre les taux de mise en commun des données, puis l'établissement de points de référence;
- la métascience – évaluer les progrès réalisés dans les différentes disciplines et au sein de l'écosystème de la recherche postsecondaire;
- l'avancement professionnel – utiliser d'autres critères pour évaluer les chercheurs en vue de leur avancement professionnel.

Ce dernier facteur est conforme aux recommandations de la Déclaration de San Francisco sur l'évaluation de la recherche (DORA), signée par plus de 22 300 personnes et organisations, dont la FCI, les Instituts de recherche en santé du Canada (IRSC), le Conseil de recherches en sciences naturelles et en génie du Canada (CRSNG), le Conseil de recherches en sciences humaines du Canada (CRSH) et le Fonds de recherche du Québec (FRQ) (DORA, 2012; FRQ, 2020; CRSNG, 2023). À défaut de quoi, les efforts déployés par les chercheurs pour mettre en commun leurs données et leurs documents de recherche pourraient ne pas être récompensés ou reconnus d'un point de vue professionnel dans la même mesure que les publications en libre accès (Moher et Cobey, 2021).

De l'avis du comité, la gestion des données est un élément important de la sécurité de la recherche, car elle permet aux chercheurs de stocker et d'utiliser les données tout au long du processus et, le cas échéant, de les partager. De plus, les pratiques rigoureuses en matière de gestion des données contribuent directement à la réalisation des objectifs des politiques fédérales récemment adoptées en matière de sécurité de la recherche (section 2.4), en fournissant aux chercheurs et aux établissements les moyens d'en maintenir l'intégrité (GC, 2024c).

Avant l'adoption de la politique de GDR, les mesures visant à encourager la science ouverte dans la recherche financée par des fonds publics se concentraient presque exclusivement sur les publications en libre accès

Actuellement, la politique des trois organismes exige que les publications soient mises en libre accès dans un délai de 12 mois (ISDE, 2016), bien que cette approche soit en cours de révision (ISDE, 2023d). Conformément aux engagements internationaux plus larges visant à maximiser la qualité et l'impact de la recherche, le FRQ demande aux bénéficiaires de fournir un accès libre immédiat aux publications évaluées par des pairs (CoARA, 2022, 2025; FRQ, 2022). Des mandats institutionnels sur le libre accès peuvent également exister en plus de ceux établis par le bailleur de fonds de la recherche (voir p. ex. SFU, 2023). Malgré ces politiques, la participation de la communauté de la recherche universitaire canadienne au libre accès reste inégale (Moskovkin *et al.,* 2021; Simard *et al.,* 2022). En effet, le bilan du Canada en ce qui concerne la publication en libre

Les pratiques rigoureuses en matière de gestion des données contribuent directement à la réalisation des objectifs des politiques fédérales récemment adoptées en matière de sécurité de la recherche

accès est médiocre par rapport à celui des pays membres de l'UE et des autres membres du G7 : environ la moitié des articles publiés entre 2015 et 2019 par des auteurs canadiens sont librement accessibles (Paquet *et al.*, 2022; CE, s.d.-b). D'autres pratiques de science ouverte, comme l'enregistrement des essais cliniques et la communication des résultats – pourtant essentielles pour appuyer la prise de décisions fondées sur des données probantes en médecine –, ne sont pas non plus largement mises en œuvre au Canada (Alayche *et al.*, 2023).

Les entreprises privées s'appuient sur divers mécanismes pour limiter l'accès à la recherche

Dans le domaine de la R-D privée (incluant les entreprises issues de la recherche universitaire), la mise en commun de l'accès à la recherche ou aux données de recherche se fait différemment, le gouvernement ne disposant pas des leviers nécessaires pour lier les conditions de financement à des politiques d'accès libre. L'accès à la recherche dans le secteur privé implique des incitatifs et des motivations moins bien définis que ceux des chercheurs financés par le gouvernement. Les connaissances, les logiciels, les résultats de recherche et les données sont tous des actifs intangibles vitaux pour les entreprises, en particulier sur le marché des technologies (Asselin et Speer, 2019; Lamb et Munro, 2020). Pour rester compétitives, elles doivent donc prendre des décisions stratégiques concernant la divulgation et la protection de ces actifs et d'autres qui constituent leur PI.

Certains résultats de recherche ayant une valeur économique sont gardés confidentiels et considérés comme des secrets commerciaux, ceux-ci constituant un élément clé de la stratégie de PI des entreprises (WIPO, s.d.). Les accords de partenariat entre les chercheurs universitaires et le secteur privé peuvent donc invoquer le secret commercial ou la confidentialité pour déroger aux politiques d'ouverture des données (Plomp *et al.*, 2019; MESR, 2021). Les accords de non-divulgation sont également couramment utilisés pour garantir la confidentialité dans le secteur privé (CE, 2022; van der Molen *et al.*, 2023). En outre, les réticences à mettre des données en commun dans le cadre de partenariats peuvent être renforcées par les conséquences juridiques du détournement de secrets commerciaux en vertu des principaux accords de libre-échange nord-américains (Malone, 2021; Akhtar, 2024).

Ces facteurs n'entraînent pas toujours le refus inconditionnel du secteur privé de divulguer les résultats de la recherche. Au contraire, certaines considérations stratégiques (p. ex. la possibilité de monétiser les produits de la recherche) peuvent guider les décisions de mise en commun ouverte (Pannier, 2023). Dans le domaine de la recherche sur l'IA, par exemple, certains grands développeurs de technologies prônent l'ouverture et publient de grandes quantités de logiciels et de données (voir p. ex. Heikkilä, 2024), tandis que leurs concurrents suivent

une voie opposée en raison des coûts de renonciation perçus qui résulteraient d'une transparence excessive (Heaven, 2023; Pannier, 2023; Tiku et de Vynck, 2023; Yao, 2023).

2.4 Sécurité de la recherche

En réponse au nombre croissant de risques pour la sécurité auxquels est confronté l'écosystème de la recherche au Canada, les différents ordres de gouvernement ont intensifié leurs efforts afin de gérer le détournement et l'utilisation indésirable des résultats de la recherche générés au Canada.

2.4.1 Contexte politique fédéral

Bien que la biosécurité soit au cœur des efforts entourant la sécurité depuis plusieurs décennies, en 2021 et en 2024, le gouvernement du Canada a mis en œuvre deux politiques majeures – les Lignes directrices sur la sécurité nationale pour les partenariats de recherche (LDSNPR) et la Politique sur la recherche en technologies sensibles et sur les affiliations préoccupantes (RTSAP) – tirant toutes deux parti du financement fédéral afin d'imposer des restrictions aux partenariats dans divers domaines de recherche sensibles.

La politique RTSAP interdit à ceux qui souhaitent faire progresser la recherche dans des domaines technologiques sensibles de maintenir des affiliations actives avec des organisations de recherche nommées

La politique RTSAP, entrée en vigueur en 2024, a introduit des critères d'admissibilité supplémentaires pour les partenariats de recherche financés par le gouvernement fédéral. Les projets de recherche ne sont pas admissibles à un financement fédéral s'ils répondent à deux critères : (i) un membre de l'équipe a une affiliation active avec une organisation de recherche nommée (ORN) étrangère « rattaché[e] à des organisations militaires, de défense nationale ou de sécurité d'État qui pourraient présenter un risque pour la sécurité nationale du Canada » (ISDE, 2023e) ou reçoit un financement ou une contribution en nature de la part d'une telle organisation; et (ii) la recherche est menée dans l'un des domaines technologiques sensibles définis (ISDE, 2023b). Bien que les exigences en termes d'affiliation, de financement et de contribution en nature s'appliquent à l'ensemble de l'équipe de recherche, seuls les chercheurs ayant des rôles désignés doivent présenter une attestation de conformité aux exigences de la politique RTSAP (ISDE, 2023f), ce qui peut entraîner une confusion quant à la responsabilité des autres membres de l'équipe et aux attentes par rapport à eux.

La politique RTSAP définit la liste des ORN et des domaines technologiques qu'elle considère comme sensibles afin de fournir des orientations aux chercheurs qui procèdent à une auto-évaluation lorsqu'ils sollicitent un financement fédéral (ISDE, 2023f). La liste des ORN a été élaborée par Sécurité publique Canada (SPC) sur la base d'un certain nombre d'indicateurs divulgués et confidentiels (SP, 2023). L'un des indicateurs divulgués est le fait qu'un établissement déclare publiquement qu'il mène des recherches pour le compte d'une organisation militaire ou de sécurité étrangère. Les entreprises privées sont actuellement exclues de la liste, et d'autres mécanismes, comme les LDSNPR, sont utilisés pour gérer les risques liés aux collaborations avec le secteur privé.

La liste des domaines technologiques sensibles a été élaborée par SP en collaboration avec d'autres ministères et organismes fédéraux et comprend les technologies qui peuvent être utilisées par des acteurs malveillants pour « miner les efforts de sécurité ou de défense du Canada ou des alliés ou renforcer les efforts de sécurité ou de défense d'un adversaire » (SP, 2023). Ces domaines technologiques sont les suivants :

- Technologie de l'infrastructure numérique de pointe
- Technologies énergétiques de pointe
- Matériaux et fabrication de pointe
- Détection et surveillance avancées
- Armes de pointe
- Technologies aérospatiales, spatiales et satellitaires
- Intelligence artificielle et technologie des mégadonnées
- Intégration homme-machine
- Technologies des sciences de la vie
- Science et technologie quantiques
- Robotique et systèmes autonomes

ISDE (2023b)

Reconnaissant qu'il s'agit de domaines très vastes, la politique RTSAP comprend également des sous-catégories et des exemples afin d'apporter un certain degré de spécificité aux chercheurs (ISDE, 2023b). Par exemple, la catégorie des technologies des sciences de la vie comprend deux sous-catégories, à savoir la biotechnologie et les technologies médicales et de la santé, qui englobent à leur tour des domaines de recherche plus pointus couverts par la politique RTSAP (p. ex. la biofabrication, la biologie synthétique,

la thérapie génique) (ISDE, 2023b). Cette liste ne s'applique pas aux technologies « omniprésentes et répandues », sauf s'il existe des raisons de craindre que de nouvelles applications présentent des risques (SP, 2023).

Les listes des ORN et des technologies sensibles sont permanentes et adaptées aux évolutions technologiques grâce aux efforts continus de plusieurs ministères et organismes gouvernementaux (SP, 2023). Dans ce contexte dynamique, l'application de la politique RTSAP nécessite une analyse au cas par cas par les chercheurs et les établissements d'enseignement supérieur. En 2025, le gouvernement du Canada a publié une liste des technologies sensibles (LTS), qui comprend les 11 mêmes catégories de technologies que celles figurant dans la politique RTSAP, mais qui fournit des informations plus détaillées et des exemples pour chaque catégorie. La LTS n'est pas directement liée aux politiques de sécurité de la recherche, mais elle pourrait être utilisée pour mettre à jour les futures versions de la politique RTSAP (GC, 2025g).

Les LDSNPR tiennent compte des considérations de sécurité nationale dans la création, l'évaluation et le financement de la recherche

En 2021, le gouvernement du Canada a publié les LDSNPR (ISDE, 2021), qui visent à protéger l'écosystème de recherche du Canada contre « l'interférence étrangère, l'espionnage et le transfert non désiré du savoir qui pourraient contribuer à : des avancées dans les forces militaires, la sécurité et les capacités de renseignement d'États ou de groupes qui présentent une menace pour le Canada; ou la perturbation de l'économie, de la société et de l'infrastructure essentielle canadienne » (ISDE, 2023a). Les LDSNPR s'appliquent à un certain nombre de programmes de recherche financés par le gouvernement fédéral, notamment les partenariats de recherche soutenus par les trois organismes (ISDE, 2023a). Mentionnons les subventions du programme Alliance du CRSNG, le programme de subventions Projet des IRSC, le Fonds de recherche biomédicale du Canada administré par le Secrétariat des programmes interorganismes à l'intention des établissements (phase 2); les organisations financées par le Fonds stratégique des sciences (p. ex. Génome Canada); et toutes les recherches financées par la FCI, à l'exception du Fonds des collèges (Génome Canada, 2024a,b; CRSNG, 2024b; FCI, s.d.-b). Bien que les délais exacts pour l'application des LDSNPR à certains programmes de la FCI, y compris le Fonds des initiatives scientifiques majeures, n'aient pas encore été déterminés, certaines installations de recherche ont pris des mesures pour renforcer la sécurité de la recherche conformément aux LDSNPR et à la politique RTSAP (FCI, s.d.-b; CLS, s.d.; GlycoNet, s.d.).

Les LDSNPR couvrent plus de types de risques liés à la sécurité de la recherche que la politique RTSAP et s'étendent à 11 domaines de recherche technologique

sensibles, ainsi qu'à d'autres, énumérés à l'annexe A, notamment les minéraux critiques, les infrastructures essentielles, les grands ensembles de données et les données personnelles qui « peuvent être considérées comme sensibles » (ISDE, 2023a). Les demandeurs doivent joindre un formulaire d'évaluation des risques à leur demande de subvention si la possibilité de financement relève des LDSNPR et s'ils prévoient de mener des recherches avec un partenaire visé (ISDE, 2024a). Ce qui constitue un partenaire visé dépend de la possibilité de financement, ce qui crée des complexités et des incertitudes pour les demandeurs (Université de l'Alberta, 2024a) (tableau 2.1), bien qu'une certaine harmonisation soit en cours.

Tableau 2.1 Quelques exemples de définitions de partenaire du secteur privé dans le cadre des LDSNPR, selon le bailleur de fonds de la recherche

Bailleur de fonds	Définitions
Trois organismes	« Organisations partenaires du secteur privé participant au projet de recherche proposé, incluant les associations industrielles et les groupes de producteurs » (CRSNG, 2024b).
FCI	• « Joue un rôle actif dans les activités de recherche décrites dans la proposition (p. ex. partage de la propriété intellectuelle, apport d'expertise, participation active aux activités de recherche, apport financier aux activités de recherche; ou • héberge toute l'infrastructure de recherche ou une partie de celle-ci; ou • contribue à plus de 500 000 dollars au coût d'un seul article d'infrastructure, que ce soit en espèces ou en nature » (FCI, s.d.-b).
Génome Canada (financé par le Fonds stratégique des sciences)	« Organisme à but lucratif ou organisme aidant, appuyant, structurant ou représentant les intérêts communs d'un groupe d'organismes incorporés à but lucratif, notamment des associations de l'industrie ou des consortiums officiels ou non officiels » (Génome Canada, 2024b).

Les listes d'articles à double usage, de personnes sanctionnées et d'entités visées par des sanctions limitent les collaborations en matière de recherche, ainsi que le transfert et la mise en commun des technologies comme des résultats de la recherche

Les restrictions fédérales en matière de recherche se limitent généralement à des listes, qu'il s'agisse de personnes, d'établissements ou de domaines de recherche. Ces listes sont ensuite référencées dans divers règlements. Par exemple, afin d'assurer la biosécurité, le gouvernement du Canada a adopté une liste d'agents biologiques à cote de sécurité élevée (ABCSE) et imposé des exigences en matière de permis et d'autres mesures de sécurité aux installations comme aux chercheurs qui travaillent avec ces agents (GC, 2009,

2024d; ASPC, 2023). Ces listes d'articles à double usage, de personnes sanctionnées et d'entités visées par des sanctions limitent les collaborations en matière de recherche, ainsi que le transfert et la mise en commun des technologies comme des résultats de la recherche. Elles sont adoptées en vertu de la *Liste des marchandises et technologies d'exportation contrôlées* (GC, 2021c), de la *Loi sur les agents pathogènes humains et les toxines* (GC, 2009), du *Règlement sur les agents pathogènes humains et les toxines* (GC, 2024d), de la *Loi sur la sûreté et la réglementation nucléaires* (GC, 1997), du *Règlement sur le contrôle de l'importation et de l'exportation aux fins de la non-prolifération nucléaire* (GC, 2010), de même que d'autres lois et règlements.

Toutefois, malgré les progrès considérables accomplis dans le domaine de la sécurité de la recherche, ces politiques et approches ont leurs limites. Les mesures de biosécurité et les listes d'articles à double usage/de personnes sanctionnées/d'entités visées par des sanctions confèrent une compétence fédérale fragmentée relativement à la sécurité de la recherche (Wagner et Zaia, 2023). De plus, les politiques de sécurité de la recherche liées au financement fédéral omettent de vastes segments de la recherche qui sont financés par d'autres sources, comme le secteur privé (Flagg et Arnold, 2021). L'approche actuelle est également insuffisante pour empêcher le transfert de technologies sensibles, développées grâce à des fonds publics, vers des entités préoccupantes par le biais de la commercialisation, ce qui pose des risques pour la sécurité nationale et économique (SRSR, 2024). Quel que soit le domaine de recherche, les progrès de la R-D et l'application de technologies en rapide évolution, comme l'IA et l'informatique quantique, peuvent créer de nouvelles situations dans lesquelles la reconnaissance des recherches sensibles devient difficile et les approches fondées sur des listes, désuètes (section 3.2.1).

2.4.2 Initiatives infranationales

Un nombre croissant d'exigences en matière de sécurité de la recherche ont été imposées par les gouvernements provinciaux. Ainsi, le gouvernement de l'Ontario a mis en œuvre ses propres mesures de sécurité liées au financement de la recherche (Gouv. de l'Ont., 2023). Ces mesures établissent des procédures d'évaluation et d'atténuation pour tous les projets de recherche financés par des fonds publics et exigent que les demandeurs (incluant les universités) divulguent leurs partenariats internationaux aux autorités provinciales (Gouv. de l'Ont., 2023, 2024a) (section 4.1.2). La sécurité de la recherche s'impose en Ontario comme un nouvel indicateur de reddition de comptes pour le financement opérationnel provincial reçu par les universités (voir p. ex. Université de Toronto, 2025). Ailleurs au Canada, le gouvernement de l'Alberta a ordonné aux quatre universités à vocation complète de recherche et

d'enseignement supérieur de la province (Université de l'Alberta, Université de Calgary, Université de Lethbridge et Université Athabasca) de suspendre les accords avec la Chine prévoyant des activités de recherche effectuées par des étudiants des cycles supérieurs, l'invitation de chercheurs étrangers et la participation de boursiers postdoctoraux dans les domaines de recherche sensibles précisés à l'annexe A des LDSNPR (Université de l'Alberta, 2024b). Dans le cadre du concours 2024-2025, le programme de capacité de recherche de l'Alberta exige que les candidats à certains volets de financement respectent des mesures visant à protéger la recherche (Gouv. de l'Alb., 2024). Si ces subventions soutiennent des projets interinstitutionnels, les exigences en matière de sécurité de la recherche s'appliquent aux chercheurs des établissements situés à l'extérieur de la province. Or, de telles divergences d'approche peuvent compliquer la mise en œuvre cohérente des mesures de sécurité de la recherche à l'échelle nationale (Université de Calgary et Université de l'Alberta, 2023) (section 5.1).

Les universités canadiennes ont intensifié leurs efforts en matière de sécurité de la recherche

Les universités canadiennes ont joué un rôle important dans l'élaboration des politiques gouvernementales en matière de sécurité de la recherche. Par exemple, le Groupe de travail mixte du gouvernement du Canada et des universités, créé en 2018, a contribué à l'élaboration du portail « Protégez votre recherche » du gouvernement du Canada et aux LDSNPR (U15, 2023). Les politiques institutionnelles sur l'intégrité de la recherche et la conduite responsable en la matière ont jeté les bases de l'élaboration de cadres, de politiques et de pratiques de gestion des risques – notamment ceux liés aux collaborations internationales – et d'autres politiques de protection des données de la recherche, des résultats de celle-ci et de la PI (U15, 2023).

Bien que les services de soutien à la recherche des universités aient l'habitude de traiter des données et des recherches sensibles, les politiques fédérales, provinciales et territoriales encouragent les universités à adopter une perspective géopolitique plus large dans leur approche de la sécurité (Owens, 2023a). Afin d'améliorer les services de soutien à la recherche existants, les universités ont donc créé des postes administratifs de haut niveau axés sur la sécurité de la recherche et mis en place des unités également chargées de la question. Les employés concernés participent désormais davantage à l'examen des propositions de recherche dans les domaines technologiques sensibles, ainsi qu'à la sélection des partenaires de recherche étrangers et des collaborations internationales (Owens, 2023a). Ces efforts ont été rendus possibles grâce à un financement spécial du gouvernement du Canada prévu dans le budget 2022 *et a*lloué par l'intermédiaire du Fonds de soutien à la recherche à 51 universités

en 2024–2025 (GC, 2024e,f). La méthode d'allocation, basée sur le montant du financement de la recherche reçu par les établissements d'enseignement supérieur de la part du gouvernement fédéral, a entraîné des disparités importantes en termes de capacités et d'approches entre les établissements (GC, 2024e; SPIIE, 2024). La création de bureaux et de fonctions administratives nécessite en effet des fonds supplémentaires, en particulier dans les petites et moyennes universités, les établissements de santé et les instituts affiliés, ainsi que dans les collèges et les écoles polytechniques (section 5.2).

Le comité reconnaît les tensions réelles entre la science ouverte et la sécurité de la recherche, tout en soulignant qu'il ne s'agit pas d'un problème à somme nulle. Au Canada, les politiques régissant la mise en commun des données dans les deux domaines d'intérêt – la recherche sur les agents pathogènes et la recherche océanographique – reflètent l'interdépendance entre la science ouverte et la sécurité de la recherche (section 4.3.2). Par exemple, la Ligne directrice canadienne sur la biosécurité : le double usage dans la recherche en sciences de la vie reconnaît que la décision de communiquer les résultats de la recherche impliquant des ABCSE est rarement facile à déterminer. Un plan de communication bien élaboré, précisant ce qui sera communiqué, à qui, comment et quand, est donc essentiel pour parvenir à un équilibre entre l'ouverture et la nécessité de protéger les informations sensibles (ASPC, 2018a). La politique sur les données de Réseaux océaniques Canada met pour sa part l'accent sur une position d'ouverture par défaut, avec des exceptions fondées sur des préoccupations clairement définies en matière de sécurité, d'éthique ou de droit – notamment les informations personnelles identifiables, les partenariats avec les peuples autochtones, les préoccupations militaires ou de sécurité nationale, la protection des espèces menacées ou les technologies sensibles (ONC, 2021a).

L'adoption de la science ouverte pourrait être limitée dans la recherche universitaire canadienne en raison de l'absence relative de politiques entourant la sécurité de la recherche. En France, les pratiques de science ouverte sont comparativement plus répandues, malgré des règles strictes en matière de sécurité de la recherche (Owens, 2023b; CNRS, 2024). Des mesures relatives aux infrastructures et à la conformité, comme le Baromètre français de la Science Ouverte, ont peut-être contribué à stimuler l'adoption de la science ouverte parmi les chercheurs (MESR, 2023; Owens, 2023b). Étant donné que la majorité des travaux de recherche ne sont vraisemblablement pas sensibles et que le Canada accuse un retard relatif dans la mise en commun des données, les décideurs politiques devraient s'attendre à réaliser des progrès tant sur le plan de la sécurité de la recherche que de l'accessibilité, tout en continuant de surveiller et de démêler les véritables zones de tension.

3

Reconnaissance de la recherche sensible préoccupante

3.1 Facteurs qui rendent la recherche sensible

3.2 Mesures et outils permettant de reconnaître la recherche sensible préoccupante

Constatations du chapitre

- Divers facteurs de risque sont utilisés pour reconnaître la recherche sensible, et une combinaison de ceux-ci, ainsi que le recours à des outils supplémentaires comme des listes, des évaluations des risques et une expertise pertinente, permettent de déterminer plus précisément si une recherche sensible est préoccupante. Les chercheurs, les établissements et les gouvernements partagent la responsabilité de ces activités.
- Il existe une tension entre le souhait des chercheurs de disposer de lignes directrices claires et précises sur la manière de reconnaître la recherche sensible (p. ex. des listes) et celui des décideurs politiques et des experts en sécurité de la recherche, qui préfèrent des évaluations dynamiques et réactives de la sensibilité.
- Le niveau de sensibilité d'une recherche peut évoluer tout au long du processus. Les mesures de reconnaissance peuvent donc être répétées avant, pendant et après chaque phase de recherche, en impliquant tous les acteurs du système à des degrés divers, à différentes étapes.
- Les groupes d'experts institutionnels ou régionaux chargés d'évaluer la sensibilité peuvent offrir avec succès une combinaison de connaissances sur le domaine et les risques liés à la recherche, apportant ainsi un soutien aux chercheurs. Ils peuvent également constituer un mécanisme supplémentaire pour reconnaître la recherche sensible tout au long du processus.

La première étape de la mise en œuvre des mesures de sécurité consiste à reconnaître la recherche sensible et à déterminer quand elle devient préoccupante. Cette étape est rendue difficile par le rythme rapide du développement et de la diffusion des technologies émergentes, qui accentue les tensions potentielles, ainsi que par les changements constants du paysage géopolitique (Kosal, 2020b). Pour chaque ambition de publier un article sur une nouvelle application, il pourrait raisonnablement y avoir une nouvelle voie d'utilisation abusive (voir p. ex. DiEuliis et Giordano, 2017; Spitale *et al.*, 2024). Le degré de sensibilité a des implications sur le niveau d'ouverture et d'accès aux résultats : il est donc essentiel de déterminer où se situent la recherche et les données sur le continuum allant de totalement ouvertes à totalement fermées, ce jugement étant influencé par la sensibilité de la recherche. De même, la détermination du point à partir duquel une recherche sensible devient préoccupante est influencée par plusieurs facteurs (section 3.1) et par les

risques documentés, ainsi que par la perception des risques par les acteurs chargés de reconnaître la recherche sensible. Rappelons que, pour qualifier une recherche sensible de préoccupante, il faut vérifier si elle peut être détournée ou utilisée abusivement, immédiatement ou à l'avenir, avec peu ou pas de modifications (section 1.2). Plusieurs des facteurs permettant de reconnaître la recherche sensible examinés ci-dessous (section 3.1), envisagés isolément ou en combinaison, peuvent également indiquer qu'une recherche est préoccupante. Enfin, d'autres outils existent pour aider à évaluer si un projet de recherche est préoccupant (section 3.2).

De plus en plus d'activités de recherche sont désormais soumises à des cadres de sécurité de la recherche, qui exigent une capacité à évaluer et à gérer les risques dans des contextes en évolution rapide et dans des domaines où cela n'était pas nécessaire auparavant

De plus en plus d'activités de recherche sont désormais soumises à des cadres de sécurité de la recherche (voir p. ex. ISDE, 2023f; CE, 2024a), qui exigent une capacité à évaluer et à gérer les risques dans des contextes en évolution rapide et dans des domaines où cela n'était pas nécessaire auparavant (chapitre 5). L'approche actuelle pour reconnaître la recherche sensible implique plusieurs acteurs de l'écosystème, notamment les chercheurs, les établissements et les gouvernements. Des cadres de sécurité ont ainsi été élaborés pour aider à déterminer où se situe la recherche sur l'échelle de sensibilité.

Les cadres visant à reconnaître la recherche sensible préconisent généralement des approches fondées sur les risques qui concilient les impératifs de liberté universitaire et de science ouverte avec la sécurité de la recherche, visant ainsi à éviter les scénarios où les chercheurs renoncent à publier ou évitent certains projets pour des raisons purement préventives (MPG, 2017; CNRS, 2024). Aux États-Unis, par exemple, le Federal Select Agent Program a vu le nombre d'entités enregistrées passer de 247 en 2019 à 226 en 2023 (HHS *et al.*, 2020, 2024). D'après l'expérience du comité, cette baisse pourrait s'expliquer par le renforcement des contrôles et la charge administrative, qui dissuadent les chercheurs d'entreprendre des travaux portant sur les agents biologiques et les toxines. À ce jour, les données sur l'impact des nouveaux cadres au Canada sont limitées, mais le projet pilote des LDSNPR (section 2.4.1) a révélé qu'environ 4 % des propositions traitées sur une période d'un an justifiaient une évaluation de la sécurité nationale par les organismes partenaires (ISDE, 2023c). Le comité note toutefois que, sans une surveillance et un suivi précis des répercussions des directives en matière de sécurité de la recherche (et de

science ouverte), il est difficile de déterminer leur efficacité et les meilleures pratiques pour leur mise en œuvre (section 5.1).

La recherche en sciences sociales et humaines est largement exclue de la politique canadienne entourant la recherche sensible (à quelques exceptions près, comme le développement d'outils d'IA pour analyser les données démographiques). En effet, cette politique se concentre plutôt sur l'avancement des technologies ou les risques associés aux partenariats (ISDE, 2023a,f). Néanmoins, les données recueillies par la recherche dans ces domaines pourraient servir des fins malveillantes (p. ex. comme source de désinformation ou de propagande, pour suivre les comportements dissidents) (Spitale *et al.,* 2024). Les risques pour les chercheurs eux-mêmes – et pour la liberté universitaire – sont également caractéristiques de la recherche sensible en sciences sociales et humaines, en particulier lorsqu'il s'agit de sujets liés à l'ingérence ou à l'influence d'États étrangers (voir p. ex. Harlan, 2019). Le vide sur le plan des politiques – explicite ou de facto – résultant de l'exclusion des disciplines des sciences sociales et humaines des cadres existants de sécurité de la recherche a été reconnu en France, avec une recommandation visant à les inclure dans certaines politiques nationales de sécurité de la recherche (Gattolin, 2021). En outre, les méthodologies et les pratiques utilisées dans les sciences sociales (p. ex. la psychologie, l'économie, la sociologie, les sciences politiques) peuvent être utiles pour concevoir et comprendre les pratiques fondées sur des données probantes en matière de sécurité de la recherche (Dao *et al.,* 2024) et pour promouvoir leur adoption par le biais de changements institutionnels ou culturels (Huising et Silbey, 2018; Huising, 2019) (section 5.4).

La recherche en sciences sociales et humaines est largement exclue de la politique canadienne entourant la recherche sensible

Pour combler ce vide, la définition de la recherche sensible préoccupante (encadré 1.1) adoptée par le comité englobe les menaces pour la santé et la sécurité publiques, y compris la vie privée et l'éthique, sans oublier les droits énoncés dans la DNUDPA, qui affirme que les peuples autochtones ont le droit de posséder et de contrôler les informations et les données les concernant (section 1.3). Les chercheurs en sciences sociales et humaines sont peut-être déjà conscients des risques éthiques ou liés à la vie privée, mais ils ne considèrent pas nécessairement que leurs travaux sont sensibles en ce qui a trait à la sécurité nationale. D'après l'expérience du comité, par exemple, la constitution de bases de données pour les organisations de santé nécessite la prévention des risques via des mesures de sécurité et la conception même de la

plateforme, l'ouverture étant pour sa part davantage limitée par des questions de confidentialité et de territoire de compétences que par les risques pour la sécurité nationale. Cette tension complique la reconnaissance de la recherche sensible.

Certains facteurs associés aux risques peuvent alerter les chercheurs, les établissements et les gouvernements sur la nécessité d'une analyse plus approfondie afin de déterminer le niveau de sensibilité et si la recherche est préoccupante. La définition de certains de ces facteurs peut immédiatement conduire à reconnaître une recherche comme sensible et préoccupante (p. ex. celle portant sur les armes), tandis que d'autres nécessitent une analyse supplémentaire ou des éclaircissements à l'aide de divers outils (p. ex. dans le cadre d'une évaluation des risques; section 3.2). Le présent chapitre examine certains de ces facteurs, ainsi que les outils qui peuvent ensuite aider la communauté des chercheurs à comprendre le niveau de risque et les prochaines étapes à suivre pour protéger la recherche au niveau approprié. Ces outils sont appliqués à des exemples et à des scénarios dans le domaine de la recherche sur les agents pathogènes et les océans, tant en ce qui concerne leur utilisation au Canada que la manière dont les pratiques pourraient être mises en œuvre à l'avenir. Ils figurent tout au long du présent chapitre et du chapitre suivant dans les encadrés intitulés *Application des mesures*.

Certains facteurs associés aux risques peuvent alerter les chercheurs, les établissements et les gouvernements sur la nécessité d'une analyse plus approfondie afin de déterminer le niveau de sensibilité et si la recherche est préoccupante

3.1 Facteurs qui rendent la recherche sensible

Divers facteurs indiquent aux chercheurs que certains types de travaux peuvent être sensibles et nécessiter une évaluation supplémentaire afin de déterminer si la recherche est préoccupante, ainsi que le niveau d'exposition au risque et les stratégies d'atténuation possibles. Par exemple, les partenariats de recherche avec des personnes ou des établissements de l'extérieur du Canada sont courants et encouragés, mais ils peuvent être considérés comme sensibles en raison des risques associés à d'éventuels acteurs malveillants, quelle que soit leur nationalité. Il est toutefois essentiel de noter que le degré de sensibilité peut être jugé très faible et ne nécessiter que des mesures de protection, comme des dispositifs de cybersécurité de base pour tous les partenaires concernés. Un autre facteur est la menace directe pour la santé ou la sécurité humaine; ainsi, le fait de travailler avec certains agents pathogènes indique en partant que la

recherche est préoccupante, le chercheur pouvant alors réfléchir aux meilleurs moyens de protéger ses travaux (chapitre 4).

Les deux domaines de recherche abordés dans le présent rapport peuvent être soumis à plusieurs facteurs de déclenchement particuliers. Par exemple, la recherche sur les agents pathogènes est sensible, car une grande partie des travaux menés dans ce domaine pourrait avoir des conséquences négatives pour les personnes en cas d'utilisation abusive. Les facteurs permettant d'évaluer si elle est préoccupante et le niveau approprié de mesures de protection sont propres au contexte et peuvent être déterminés à l'aide d'outils, comme ceux axés sur l'évaluation des risques (section 3.2.2). Cette évaluation pourrait amener le chercheur à réfléchir à la transmissibilité de certains agents pathogènes, ce qui conduirait alors à classer la recherche comme sensible et préoccupante. La recherche océanographique, un domaine d'étude plus vaste et moins clairement délimité, est soumise à différents types de facteurs révélant les risques en présence. Par exemple, la fréquence d'échantillonnage de certains signaux peut varier quant à la sensibilité, un faible taux d'échantillonnage étant considéré comme sensible, mais non préoccupant (p. ex. les capteurs de pression hydrostatique au fond de l'eau qui surveillent les vagues de tsunami), tandis qu'un taux d'échantillonnage plus élevé peut détecter une activité de nature sensible et fournir suffisamment de détails pour catégoriser les données comme étant préoccupantes (M. Paulson, communication personnelle, 2025). Dans ces deux domaines de recherche, l'évaluation porte sur la possibilité que la recherche soit détournée ou utilisée abusivement, immédiatement ou à l'avenir, sans modification ou avec des modifications mineures.

Le tableau 3.1 présente une série de facteurs qui indiquent la sensibilité de la recherche, dont certains peuvent être généraux et largement applicables, tandis que d'autres sont davantage propres à un domaine. Ces facteurs peuvent fournir à un chercheur un premier indice indiquant que sa recherche est (i) sensible, (ii) suffisamment risquée pour être également potentiellement préoccupante, ou (iii) certainement préoccupante lorsque des facteurs précis sont combinés. Le comité note que ce tableau n'est pas exhaustif et que de nombreux autres facteurs peuvent être utilisés dans l'écosystème de la recherche. En outre, ils ne sont pas équivalents en ce qui a trait aux degrés relatifs de sensibilité et varient en fonction du contexte ou du projet.

Tableau 3.1 Facteurs de sensibilité de la recherche

Facteur	Justification et applicabilité	Outils de reconnaissance
Partenariats Situations dans lesquelles les chercheurs collaborent avec des personnes ou des organisations extérieures à leur propre établissement ou situées hors du Canada.	Les chercheurs peuvent déterminer si les partenaires et leurs affiliés sont susceptibles d'être influencés, soumis à de l'ingérence ou contrôlés par des acteurs malveillants (y compris des gouvernements étrangers), ce qui pourrait « poser un risque pour la sécurité nationale si les connaissances, les technologies et la propriété intellectuelle découlant [du] projet de recherche étaient utilisées » (ISDE, 2024a).	Listes (p. ex. dans la politique sur la RTSAP) Évaluations des risques (p. ex. diligence raisonnable)
Recherche concernant les peuples autochtones La *Déclaration des Nations Unies sur les droits des peuples autochtones* (DNUDPA) stipule que les peuples autochtones ont le droit à l'autodétermination dans tous les aspects de la recherche qui les concerne eux, leurs connaissances et leurs terres (ONU, 2007).	Les chercheurs qui travaillent avec des peuples autochtones ou sur les terres de ces derniers sont tenus de consulter les communautés ou les personnes autochtones concernées et de collaborer avec elles afin de s'assurer que la recherche est menée de manière respectueuse, éthique et conformément aux souhaits des communautés en question.	Expertise pertinente (p. ex. comités d'éthique de la recherche, permis de recherche)
Recherche sur les êtres humains Toute recherche financée par les trois organismes est soumise à l'Énoncé de politique des trois conseils : Éthique de la recherche avec des êtres humains (EPTC 2) si elle implique des participants humains ou des matériaux biologiques humains (IRSC *et al.*, 2022).	Toute recherche répondant à ces conditions est soumise à l'approbation d'un comité d'éthique, qui peut à son tour imposer des conditions pour la protection de la recherche.	Expertise pertinente (p. ex. comités d'éthique de la recherche, permis de recherche)
Géographie Recherche menée dans un lieu géographique particulier.	Le lieu de la recherche peut conférer un certain degré de sensibilité, quels que soient le type de recherche et la personne qui la mène. L'Arctique, par exemple, est à la fois le théâtre de tensions géopolitiques croissantes et la terre natale de nombreux peuples autochtones.	Évaluation des risques

(continue)

(a continué)

Facteur	Justification et applicabilité	Outils de reconnaissance
Niveau de maturité technologique (NMT) Le NMT est une mesure systématique utilisée pour évaluer la maturité d'une technologie particulière, allant de la recherche fondamentale à la disponibilité commerciale (JASON, 2024).	Il a été suggéré de recourir à des évaluations du NMT pour évaluer l'impact potentiel des technologies, à différents stades de développement, sur la sécurité nationale (CE, 2021a; JASON, 2024). Les éléments affichant un NMT élevé ou les connaissances connexes peuvent nécessiter des mesures de protection supplémentaires compte tenu de la relative facilité avec laquelle la menace ou les effets d'une utilisation abusive pourraient se concrétiser.	Évaluations des risques
Applications potentiellement nocives de la recherche Évaluations propres à chaque projet visant à évaluer les applications nuisibles futures de la recherche, comme le double usage ou les applications contraires à l'éthique (JASON, 2019; Gouv. de la Nouvelle-Zélande, 2020, 2022).	L'impact potentiel de la recherche sur la sécurité économique et nationale (p. ex. augmentation du potentiel militaire offensif de nations étrangères, affaiblissement de la capacité de défense nationale) est souvent désigné comme étant un facteur distinct qui doit être pris en compte lors des évaluations des risques (CNRS, 2024; NPSA et NCSC, 2024).	Listes, évaluations des risques, expertise pertinente
Grands ensembles de données, données géospatiales et données à caractère personnel Les chercheurs sont invités à faire preuve d'une prudence toute particulière lorsqu'ils travaillent avec de grands ensembles de données et des données à caractère personnel (p. ex. des données sur la santé ou la génétique permettant d'identifier la personne, des données biométriques, des données financières, des communications privées) (ISDE, 2023a). Les données géospatiales peuvent également être sensibles, en particulier les données à haute résolution qui rendent possible l'identification des objets sensibles (voir p. ex. U.S. GAO, 2022).	Les ensembles de données « peuvent être analysés pour cerner des modèles, des tendances et des associations, particulièrement en ce qui a trait aux comportements humains et aux interactions entre les personnes. [Ces ensembles de données peuvent avoir] une incidence éthique, commerciale ou juridique à l'échelle individuelle, nationale ou internationale. » (ISDE, 2024a) L'utilisation abusive des données de recherche peut également soulever des préoccupations d'ordre éthique (GC, 2021d).	Évaluations des risques, expertise pertinente (p. ex. examen éthique)

(continue)

(a continué)

Facteur	Justification et applicabilité	Outils de reconnaissance
Atouts institutionnels ou nationaux Les établissements ou les pays qui possèdent des atouts dans des disciplines ou des domaines particuliers peuvent considérer ces domaines comme sensibles, notamment pour la sécurité économique.	Domaines de recherche dans lesquels l'établissement ou le pays peut avoir une capacité de pointe au niveau mondial ou qui recèlent une valeur particulièrement élevée pour d'autres raisons (Gouv. des Pays-Bas, 2022; VU Amsterdam, 2023).	Listes, évaluations des risques (p. ex. analyse des actifs), expertise pertinente (p. ex. organismes d'examen institutionnel)
Risques pour la sécurité des chercheurs Recherches susceptibles de porter préjudice aux chercheurs en raison du sujet de leurs travaux (p. ex. violations de la liberté universitaire).	Menaces pour la liberté universitaire, impliquant des recherches sur des sujets pouvant être considérés comme sensibles par certains gouvernements (suscitant une critique des politiques gouvernementales par exemple) ou dans des régions en conflit, où les chercheurs risquent de subir des atteintes physiques ou des persécutions (Gouv. des Pays-Bas, 2022; Heathershaw *et al.*, 2022).	Évaluation des risques

Certains des facteurs énumérés au tableau 3.1 sont généraux, mais visent à encourager une évaluation propre au contexte tenant compte de la nature de la recherche et de ses participants. Ces facteurs peuvent s'appuyer sur des informations, des ressources et des études de cas, qui fournissent aux chercheurs les outils nécessaires pour évaluer eux-mêmes les risques liés à leur programme de recherche (voir p. ex. GC, 2021d,e,f) ainsi que leur exposition aux risques. Celle-ci est influencée par des facteurs allant de la participation à des programmes de recrutement de talents étrangers à l'incapacité de mettre en place des protocoles efficaces de formation et de conformité en matière de biosécurité ou de cybersécurité (GC, 2024g).

3.1.1 Difficultés liées à la reconnaissance de la recherche sensible

Les différences dans la perception des risques et les incitatifs contradictoires compliquent le rôle des chercheurs dans la reconnaissance de la recherche sensible

Certains critères de reconnaissance peuvent ne pas correspondre aux incitatifs des demandes de subvention. Ainsi, le fait de demander aux chercheurs d'évaluer objectivement l'impact futur de leurs recherches peut s'avérer difficile, l'incitation à exagérer l'impact des travaux pouvant entrer en conflit avec le désir d'éviter un examen minutieux de la sécurité nationale. De l'avis du comité, former les chercheurs à anticiper les défis potentiels et les menaces

(section 5.2), puis élaborer des stratégies pour y faire face de manière proactive (chapitre 4) est susceptible de faire en sorte que la recherche reste à la fois innovante et sûre.

De plus, demander aux chercheurs si leurs projets peuvent être considérés comme sensibles fait peser la responsabilité de la reconnaissance entièrement sur eux, alors qu'ils ne sont peut-être pas conscients des risques au sens large associés à leurs activités (Kosal et Huang, 2015; Evans *et al.*, 2022). La France, par exemple, dispense largement les chercheurs de cette activité et transfère la responsabilité de la reconnaissance à des organismes gouvernementaux spécialisés (CNRS, 2024). Selon l'expérience du comité, un autre défi se pose lorsque les chercheurs ne sont pas informés d'une vulnérabilité connue, car la divulgation de son existence présente un risque pour la sécurité et n'est donc pas communiquée. Accroître la transparence et renforcer les partenariats avec le milieu universitaire, les gouvernements et les organisations autochtones ainsi que le secteur privé sont des objectifs clés du Service canadien du renseignement de sécurité (SCRS), qui pourraient contribuer à surmonter cet obstacle à l'avenir (SCRS, 2024b).

Outre les défis procéduraux dans ce domaine, les décisions relatives au niveau de risque tolérable seront influencées par la perception du risque. Il existe en effet des divergences entre les risques réels et les risques perçus (Dao *et al.*, 2024). Dans le contexte de la biosécurité, il a été démontré que la perception du risque est à la fois incohérente et variable dans la population générale ainsi qu'au sein des communautés d'experts (Engel-Glatter et Ienca, 2018; MacIntyre *et al.*, 2020). Or, ces questions ont une incidence sur la gouvernance des technologies émergentes (p. ex. l'IA; voir Brenneis, 2024) et contribuent aux difficultés liées à l'interprétation et à la gestion cohérentes des risques. La perception du risque concerne également la recherche impliquant des partenaires autochtones, qui peuvent déterminer, percevoir et hiérarchiser les risques liés à la recherche de manière différente. Par exemple, le Guide des politiques et procédures sur site du Centre de données des Premières Nations exige que les chercheurs tiennent compte des préjudices potentiels pour les communautés et des questions de confidentialité relatives aux groupes plutôt qu'aux individus (CGIPN, 2021, 2024). La méconnaissance de la nature des préjudices causés aux communautés ou aux droits collectifs

Les outils comme les listes et les évaluations des risques sont essentiellement des instantanés qui peuvent ne pas refléter le paysage des risques à chaque étape du cycle de vie d'un projet de recherche

pourrait donc créer des tensions lors de l'évaluation des risques liés à la recherche parallèlement aux risques économiques, de sécurité nationale ou autres.

Les facteurs permettant de reconnaître la recherche sensible évoluent constamment, ce qui justifie une réévaluation de la recherche à chaque étape

Une fois que les projets de recherche ont été conçus, financés et sont en cours, il est toujours utile de procéder à des évaluations régulières des risques, en particulier lorsque les participants ou les paramètres de la recherche changent ou que des résultats inattendus apparaissent. Ainsi, des tensions accrues dans une région (p. ex. l'Arctique) ou l'évolution de la situation politique avec des pays partenaires (p. ex. les États-Unis) sont susceptibles d'avoir des répercussions sur la probabilité et l'impact de certains risques pour la recherche, augmentant ainsi sa sensibilité et pouvant la rendre préoccupante. À l'inverse, certaines recherches considérées comme sensibles peuvent ne plus l'être, et les mesures de protection peuvent être assouplies, voire supprimées. La sensibilité de la recherche peut donc évoluer tout au long du processus, et il est utile de revoir régulièrement les mesures de reconnaissance. Il est important de garder à l'esprit que les outils comme les listes et les évaluations des risques sont essentiellement des instantanés qui peuvent ne pas refléter le paysage des risques à chaque étape du cycle de vie d'un projet de recherche.

En outre, différents acteurs du système de recherche joueront des rôles variables au fur et à mesure de l'avancement de la recherche. Pendant la durée des travaux, la surveillance descendante exercée par les pouvoirs publics s'affaiblira et les chercheurs pourraient être amenés à autoévaluer les risques à mesure que leur recherche progresse. Des organismes institutionnels, comme des groupes d'experts ou des bureaux de sécurité de la recherche, pourraient être appelés à aider les chercheurs ayant besoin d'aide pour caractériser adéquatement la sensibilité de leur recherche tout au long du processus.

3.2 Mesures et outils permettant de reconnaître la recherche sensible préoccupante

Les facteurs indiquant qu'une recherche peut être sensible et préoccupante peuvent être clarifiés, analysés et comparés à l'aide d'outils précis. Ces outils peuvent être autonomes (p. ex. des listes traitant d'un aspect de la sensibilité) ou combinés pour explorer pleinement le paysage des risques. Par exemple, l'inscription d'un domaine de recherche sur une liste de technologies critiques peut entraîner une évaluation des risques afin de déterminer le niveau de sensibilité et les types de risques les plus susceptibles de se manifester,

révélant si la recherche est préoccupante ou non. Trois grandes catégories d'outils permettant de reconnaître la recherche sensible préoccupante sont examinées ci-dessous : les listes, les évaluations des risques et les mécanismes d'expertise spécialisée.

3.2.1 Listes

Les listes sont un outil courant qui aide les chercheurs à déterminer si leurs recherches sont sensibles, ou encore à la fois sensibles et préoccupantes. Les listes découlent souvent d'approches descendantes : leur contenu est déterminé par un gouvernement ou un établissement (au moyen de leurs propres processus d'évaluation des risques), puis elles sont mises en œuvre par les chercheurs ou les établissements, en fonction du contexte. À ce titre, elles reflètent toute une série de facteurs de sensibilité. Les relations avec les autres pays sont régies par des listes de contrôle des exportations, d'autorisations et de sanctions. Les listes peuvent également être combinées pour indiquer un niveau de préoccupation plus élevé. La politique RTSAP, par exemple, comprend deux listes (section 2.4.1); si un chercheur souhaite travailler à l'avancement d'un domaine figurant sur la liste des recherches sensibles, mais sans s'associer avec une organisation de recherche nommée (ORN), aucune autre mesure n'est requise en vertu de la politique. Une recherche sensible préoccupante est toutefois signalée lorsque deux facteurs (avancement de technologies particulières et partenariat avec des ORN) sont combinés : la mesure de protection dissuade alors le chercheur de mener cette recherche en lui refusant tout financement.

Les approches fondées sur des listes sont couramment utilisées dans les différents pays pour reconnaître la recherche susceptible de porter atteinte aux personnes et aux populations

Dans divers contextes, des listes sont utilisées pour fournir des mesures accessibles permettant de reconnaître la recherche sensible : contrôles commerciaux réglementant les biens, les articles et les activités de recherche à double usage impliquant des personnes et des entités faisant l'objet de sanctions; listes de domaines de recherche ou technologiques sensibles ou de technologies critiques (voir p. ex. la politique RTSAP; section 2.4.1); listes d'entités ou d'affiliations préoccupantes; et listes d'ABCSE pertinents pour la biosécurité et la biosûreté (GC, 1992, 2025f; Gouv. de la France, 2020; ISDE, 2023f; BIS, 2024; Gouv. de l'Australie, 2024; Gouv. de la Nouvelle-Zélande, 2024). Un rapport de commission parlementaire de 2024 (*Les liens entre la science et la sécurité nationale au Canada : le cas du laboratoire national de microbiologie de Winnipeg*) recommande d'élargir la liste des ORN préoccupantes et de créer une liste supplémentaire de pays de confiance avec lesquels la PI et la recherche

peuvent être mises en commun plus librement (CACN, 2024), ce qui soutiendrait les principes de la science ouverte. Le Canada fournit déjà des listes de pays exemptés de contrôles à l'exportation pour certains biens (GC, 2021c), mais celles-ci pourraient être élargies pour inclure des dispositions relatives aux technologies en évolution rapide, comme le reflètent les modifications apportées aux contrôles à l'exportation (GC, 2025h,i).

Le travail avec des agents pathogènes et des toxines figurant sur les listes d'ABCSE nécessite le respect des exigences par les chercheurs et les installations de recherche en ce qui touche les permis et les habilitations de sécurité (voir p. ex. Gouv. de l'Australie, 2013; ASPC, 2018a). Si les listes de biens à double usage et d'ABCSE sont largement normalisés conformément aux traités internationaux de non-prolifération, d'autres listes sont adaptées aux préoccupations de sécurité nationale. Ces listes présentent toutefois certaines similitudes en ce qui concerne les domaines de recherche définis (p. ex. les technologies émergentes) et les pays d'affiliation des partenaires de recherche (p. ex. la Chine, l'Iran, la Corée du Nord, la Russie). De nombreux pays alliés ont adopté des listes de domaines ou de technologies de recherche sensibles, qui varient quant à la spécificité et l'applicabilité. En Australie, par exemple, la liste des technologies critiques d'intérêt national (*List of Critical Technologies in the National Interest*) décrit certains des avantages et des risques liés aux technologies critiques et vise à coordonner et à harmoniser le développement de ces domaines au sein du pays et des activités gouvernementales (Gouv. de l'Australie, 2023). Au Canada, l'obtention et le maintien de fonds pour la recherche provenant de volets de financement définis exigent le respect des politiques de sécurité en matière de recherche, y compris la politique RTSAP (section 2.4.1).

APPLICATION DES MESURES :

Listes pour la recherche sur les agents pathogènes

Les politiques et lignes directrices canadiennes portant particulièrement sur la recherche sur les agents pathogènes et les toxines comprennent la *Loi sur les agents pathogènes humains et les toxines* (LAPHT) (GC, 2009) et le *Règlement sur les agents pathogènes humains et les toxines* (RAPHT) (GC, 2024d), ainsi que la Ligne directrice canadienne sur la biosécurité – Le double usage dans la recherche en sciences de la vie (ASPC, 2018a). La LAPHT vise à « établir un régime pour promouvoir la sûreté des agents pathogènes humains et des toxines afin de protéger la

(continue)

(a continué)

santé et la sécurité publiques contre les risques qu'ils présentent » (ASPC, 2021), tandis que le RAPHT précise comment l'ASPC mettra en œuvre la LAPHT et autorisera les activités contrôlées impliquant des agents pathogènes humains et des toxines. Ces documents fournissent une liste des agents biologiques à cote de sécurité élevée (ABCSE) faisant l'objet de permis et d'autorisations de sécurité. Les chercheurs doivent demander une habilitation de sécurité auprès de l'ASPC pour mener certains types de recherches sur les agents pathogènes (une mesure de protection examinée à la section 4.1.1).

Rôles et responsabilités : « La LAPHT et le RAPHT s'appliquent aux organismes et aux personnes qui exercent des activités comportant la manipulation d'agents pathogènes humains et des toxines, dont les universités, les laboratoires de santé publique, le secteur privé, les hôpitaux et les services diagnostiques de santé humaine ou animale. » (ASPC, 2024b) Les deux sont maintenus et appliqués par l'ASPC.

Stade de la recherche concerné : Listes à prendre en considération et à appliquer lors de la phase de conception de la recherche.

APPLICATION DES MESURES :

Listes pour la recherche océanographique

En dehors de la recherche militaire explicitement couverte par la *Loi sur la production de défense* et les restrictions sur les marchandises contrôlées (GC, 1985b, 2016; SPAC, 2024), les restrictions sur la recherche océanographique au Canada trouvent leur origine dans la législation sur le contrôle des exportations et la politique RTSAP, où plusieurs technologies répertoriées peuvent s'appliquer ou concerner directement le développement des technologies marines (ISDE, 2023b; GC, 2025f). La majorité de ces technologies sont répertoriées dans la catégorie « détection et surveillance avancées » et comprennent les technologies qui « détectent, mesurent ou surveillent les conditions physiques, chimiques, biologiques ou environnementales et génèrent des données ou des informations à leur sujet » (ISDE, 2023b).
Les systèmes acoustiques (comme les sonars à faisceau unique, multifaisceaux et à balayage latéral), les capteurs optiques (comme les caméras, les LiDAR et les capteurs à fluorescence), les capteurs électromagnétiques (comme les magnétomètres et les profileurs de fond) ainsi que les technologies de navigation, de communication et de

(continue)

(a continué)

surveillance environnementale (incluant les capteurs CTD, les analyseurs chimiques et les systèmes de communication sous-marins) revêtent une importance particulière pour la recherche océanographique (Sun *et al.,* 2021). Ces technologies utilisent l'acoustique pour examiner les masses d'eau, obtenir des images du fond marin et communiquer, collecter ou transmettre des données à des fins de surveillance, d'exploration et de contrôle. Le développement de véhicules marins semi-autonomes ou sans équipage figure également sur cette liste (ISDE, 2023b). Si elles sont préoccupantes pour la sécurité nationale, ces technologies sensibles sont également d'une grande importance pour des usages civils ou de recherche scientifique.

Rôles et responsabilités : La politique RTSAP s'applique principalement aux chercheurs et aux organisations qui sollicitent un financement des trois organismes ou de la FCI, mais d'autres personnes et organisations peuvent également l'utiliser (voir p. ex. Génome Canada, 2024b). Cela exclut les entreprises privées et les particuliers qui développent et déploient ces technologies de manière indépendante, une pratique courante dans certains domaines du développement technologique marin, selon l'expérience du comité.

Stade de la recherche concerné : Listes à prendre en considération lors de la phase de conception de la recherche (avant l'octroi de la subvention).

À l'instar de la politique RTSAP, le département américain de l'Énergie restreint les collaborations dans certains domaines sensibles avec des chercheurs affiliés à la Chine, à l'Iran, à la Corée du Nord et à la Russie (COGR, 2023). Le département américain de la Défense, quant à lui, ne fait aucune distinction entre les domaines de recherche et se concentre sur les conflits d'intérêts et d'engagement potentiels des chercheurs qui sollicitent un financement pour la recherche fondamentale (DOD, 2023). L'Australian Research Council (ARC) adopte une approche différente : si des chercheurs demandent du financement pour des technologies figurant sur la *List of Critical Technologies in the National Interest* (liste des technologies critiques d'intérêt national), l'ARC examine une série de facteurs afin de déterminer les risques en présence (p. ex. le soutien financier étranger, la participation à des programmes de recrutement de talents étrangers, les liens avec des gouvernements ou des armées de l'étranger) (ARC, s.d.). Si l'ARC détecte un risque, les organismes de sécurité nationale peuvent être impliqués, et l'administration de l'université d'accueil sera informée et tenue de fournir une stratégie ou un plan d'atténuation des risques (ARC, s.d.).

Dans ce cadre, l'ARC exerce un certain contrôle sur la sécurité de la recherche en ayant la possibilité de suspendre le financement de certains travaux jusqu'à ce que des mesures d'atténuation des risques appropriées aient été démontrées (ARC, 2023).

Au niveau provincial, les candidats aux programmes de financement de la recherche de l'Ontario sont soumis à un examen de la sécurité de la recherche par le ministère du Solliciteur général de l'Ontario (SOLGEN) (Gouv. de l'Ont., 2024a). Le SOLGEN peut identifier comme à haut risque les projets de recherche qui impliquent des collaborations ou des relations bénéficiant d'un financement ou d'un soutien en nature de la part de tiers (p. ex. équipement de laboratoire, frais de déplacement, consultations) et dont le demandeur principal ou l'un des cochercheurs sont liés à « l'appareil militaire, de renseignement et de sécurité nationale d'un État hostile, à des organismes de recherche nationaux appartenant à l'État [...] [ou] sanctionnés par le gouvernement canadien » (Gouv. de l'Ont., 2024a). Le SOLGEN adhère aux deux listes prévues dans la politique RTSAP, mais peut également évaluer les risques à l'aide de ressources supplémentaires, comme celles fournies par les États-Unis et l'Australie, renforçant ainsi son évaluation des risques (Gouv. de l'Ont., 2024a).

Les listes de contrôle des exportations fournissent des indications détaillées sur les matériaux nécessitant des permis d'exporter

Bien que les chercheurs puissent participer à des recherches sensibles dans un pays donné, ils sont soumis à des restrictions en matière de transmission et d'exportation des résultats et des technologies développées une fois que la recherche ou le développement est achevé. Les listes de contrôle du commerce (ou des exportations) sont largement normalisées et limitent l'exportation des biens et articles à double usage précisés dans les régimes internationaux de contrôle des exportations aux fins de la non-prolifération (voir p. ex. The Australia Group, 2023; WAS, 2023). Au Canada, ces listes sont mises en œuvre par la *Loi sur les licences d'exportation et d'importation* (GC, 1985c), dont les détails figurent dans la *Liste des marchandises et technologies d'exportation contrôlée* (GC, 2021c), et par la *Loi sur la sûreté et la réglementation nucléaires*, dont les détails figurent dans le *Règlement sur le contrôle de l'importation et de l'exportation aux fins de la non-prolifération nucléaire* (GC, 1997, 2010).

Outre les listes adoptées en vertu d'accords internationaux, les pays mettent en œuvre des sanctions économiques et des contrôles généraux afin de limiter l'exportation d'articles non réglementés par les régimes de contrôle multilatéraux (CE, 2021b). La France, par exemple, a adopté une liste de technologies quantiques et de processus connexes soumis à un contrôle à l'exportation (Gouv. de la France, 2024). Des contrôles de l'utilisation finale, ou contrôles généraux, sont également en place lorsqu'il existe « des motifs

raisonnables de croire que ces articles pourraient être destinés à une utilisation en lien avec un programme d'armement nucléaire » (CCSN, 2014). Les catégories de biens et de technologies assujetties, dans certaines circonstances, à l'obtention de permis ou de licences d'exportation peuvent être désignées comme biens à double usage (encadrés par l'Arrangement de Wassenaar), munitions, biens visés par les régimes de non-prolifération nucléaire (en vertu du Traité sur la non-prolifération des armes nucléaires), biens à double usage liés au nucléaire, technologies relatives aux missiles, biens assujettis aux régimes de non-prolifération des armes chimiques et biologiques, ainsi que divers autres biens stratégiques (GC, 2021c). Une fois que des biens ou des articles ont été reconnus comme sensibles ou à double usage dans ces listes, un permis ou une licence d'exportation est nécessaire pour les commercialiser à l'extérieur du Canada.

APPLICATION DES MESURES :

Listes de contrôle des exportations pour la recherche sur les agents pathogènes

La recherche sur les agents pathogènes et les toxines est explicitement mentionnée dans le groupe 7 de *la Liste des marchandises et technologies d'exportation contrôlées* et englobe les biens et technologies que le Canada a accepté de contrôler

> *« […] conformément aux lignes directrices intitulées* Guidelines for Transfers of Sensitive Chemical or Biological Items *et aux listes désignées sous le nom de* Common Control Lists*, avec leurs modifications successives, préparées par le Groupe d'Australie pour contrôler l'exportation des armes chimiques et biologiques; et […] aux termes de la Convention sur l'interdiction de la mise au point, de la fabrication, du stockage et de l'emploi des armes chimiques et sur leur destruction signée à Paris, France, le 13 janvier 1993, avec ses modifications successives. »*
>
> (GC, 2021c)

Rôles et responsabilités : Tous les résidents du Canada sont tenus de respecter ces règles. Dans la pratique, les chercheurs qui étudient les agents pathogènes ont une capacité limitée à transmettre leurs résultats de recherche et leurs échantillons à d'autres, selon le type de recherche qu'ils mènent.

Stade de la recherche concerné : Bien que les chercheurs doivent savoir si leurs recherches sont soumises à des contrôles à l'exportation avant de commencer leurs travaux, ces contrôles n'entrent en vigueur qu'une fois la recherche terminée, si l'exportation de matériel est demandée.

Les listes peuvent simplifier la reconnaissance des recherches sensibles, permettant ainsi à un plus grand nombre de personnes de participer aux mesures de sécurité de la recherche

Les listes présentent plusieurs avantages. Par exemple, les chercheurs universitaires peuvent apprécier la réduction de la charge administrative liée au recoupement de leurs activités et de leurs partenaires avec les listes correspondantes, par rapport à la réalisation d'évaluations des risques à différents niveaux de formalité et de rigueur. Les chercheurs qui s'intéressent aux pathogènes et à l'océanographie interrogés dans le cadre de cette évaluation ont exprimé leur satisfaction à l'égard des listes en tant qu'outils permettant de simplifier les activités de reconnaissance, de promouvoir la clarté et de rationaliser le processus de recherche (D. Barclay et K. Subbarao, communication personnelle, 2024). De plus, les listes n'exigent pas des chercheurs ni des administrateurs qu'ils aient une compréhension poussée de l'évaluation des risques et des possibilités d'utilisation abusive. Elles peuvent aussi être utilisées par les administrateurs ou le personnel pour reconnaître la recherche sensible à différentes étapes du processus. Par exemple, les agents facultaires responsables des subventions peuvent examiner les demandes afin de vérifier leur conformité avec la politique RTSAP, ce qui constitue une étape supplémentaire dans le processus de préparation des subventions avant leur octroi (S. Decrausaz, communication personnelle, 2024). Toutefois, comme expliqué ci-dessous, les listes présentent également plusieurs inconvénients, ce qui conduit certains pays à recourir à des approches différentes ou complémentaires (Gouv. de la Nouvelle-Zélande, 2020; Gouv, des Pays-Bas, 2022; Leopoldina et DFG, 2022b).

Certains pays n'utilisent pas de listes, car elles peuvent donner un faux sentiment de sécurité et créer des vulnérabilités

Les listes permettant de reconnaître la recherche sensible ne sont pas utilisées dans tous les pays. Aux Pays-Bas, par exemple, les listes de pays, d'organisations partenaires ou de domaines de recherche sensibles ne sont généralement pas utilisées en dehors du cadre du contrôle des exportations, car elles sont considérées comme imparfaites et problématiques tant par les décideurs que par les organismes de recherche (AWTI, 2022; Gouv. des Pays-Bas, 2022; KNAW, 2023). En laissant entendre que les activités de recherche qui ne figurent pas sur les listes sont sûres, celles-ci peuvent contribuer à créer un faux sentiment de sécurité (KNAW, 2023). Selon le comité, les chercheurs qui ne se reconnaissent pas ou ne reconnaissent pas leurs recherches dans les documents de politiques n'évalueront pas la sensibilité et les risques de leurs travaux de la même manière que ceux dont les travaux sont mentionnés ou connexes, ce qui entraîne une vulnérabilité.

Les critères d'inscription sur les listes peuvent également fournir à des adversaires potentiels des informations détaillées susceptibles d'être utilisées pour contourner les politiques de sécurité (SP, 2023), tandis que les listes comportent le risque supplémentaire d'alimenter la discrimination à l'égard de groupes de chercheurs en fonction de leur nationalité (KNAW, 2023). Le filtrage faisant abstraction du pays, tel qu'il est pratiqué en France, évite la stigmatisation en exigeant que tous les chercheurs (français et internationaux) se soumettent à un contrôle de sécurité s'ils travaillent dans certains domaines sensibles (CNRS, 2024). À titre de compromis, certains pays, dont l'Aotearoa Nouvelle-Zélande, reconnaissent que les listes existent et peuvent être des ressources utiles, tout en encourageant les chercheurs à faire preuve de discernement (Gouv. de la Nouvelle-Zélande, 2020, 2022). Bon nombre de ces inconvénients se manifestent surtout lorsque l'on s'appuie trop fortement sur les listes, mais d'autres façons de les utiliser et de les constituer représentent des solutions de rechange prometteuses (section 3.2.2). De l'avis du comité, la forte dépendance du Canada à l'égard des listes (p. ex. la politique RTSAP) l'expose à ces inconvénients.

APPLICATION DES MESURES :

La plupart des domaines de la recherche océanographique ne figurent pas sur les listes de recherches sensibles

La recherche océanographique est un domaine où les listes actuelles peuvent donner un faux sentiment de sécurité aux chercheurs et aux établissements. Bien que certains types de technologies figurent bien dans la politique RTSAP (p. ex. les progrès des véhicules sous-marins sans pilote), d'autres domaines de recherche et de production de données reconnus comme étant sensibles dans une certaine mesure (p. ex. l'acoustique, le suivi des bancs de poissons) n'y figurent pas (ISDE, 2023b). Si bon nombre de ces domaines de recherche ne sont pas considérés comme préoccupants ou ne présentent pas de risques immédiats pour la santé humaine, le comité estime qu'un certain degré de sensibilité peut être justifié, en particulier dans certaines régions, comme l'Arctique.

Les listes peuvent devenir désuètes en raison des progrès rapides de la recherche ou parce qu'elles sont trop génériques ou trop spécifiques en partant

Le niveau de détail utilisé dans une liste de recherches sensibles est un facteur important pour son efficacité. Par exemple, des listes trop génériques entraînent une mesure d'ambiguïté pouvant conférer aux chercheurs une certaine latitude pour inclure ou exclure des activités ou des résultats de recherche, en fonction de la manière dont ils les présentent (JASON, 2024). Au Canada, la politique RTSAP pourrait ne pas reconnaître ou clarifier adéquatement la portée complète des recherches pouvant être considérées comme sensibles. Par exemple, la liste stipule que « une préoccupation particulière concerne le développement d'une technologie au cours de la recherche » (ISDE, 2023b). Or, ce qui constitue *un développement* peut être difficile à définir, en particulier dans les domaines où des technologies existantes sont utilisées dans des applications nouvelles (p. ex. les sonars à balayage latéral dans de nouvelles régions). En effet, elles ne sont alors peut-être pas perçues comme nouvelles en soi. Dans ces situations, les services de sécurité de la recherche des établissements ou les organisations régionales spécialisées peuvent être en mesure d'apporter un soutien supplémentaire pour aider à reconnaître la recherche sensible (SP, 2024a). Le comité note toutefois que toutes ces entités n'ont pas encore atteint leur plein potentiel en raison de ressources insuffisantes (section 5.1).

À l'inverse, les listes trop spécifiques risquent d'être difficiles à manier en raison de la quantité d'informations nécessaires pour garantir l'absence d'ambiguïté (JASON, 2024). La création et le maintien d'une base de données à l'appui de ces listes spécifiques nécessiteraient des efforts considérables, ainsi que des mises à jour régulières pour garantir qu'elles sont à jour (JASON, 2024). De telles listes pourraient également s'allonger considérablement en raison de la rapidité des progrès technologiques (Hähnel, 2024). Les progrès rapides de certaines technologies en particulier compliquent encore l'utilisation des listes, qui peuvent rapidement devenir obsolètes (KNAW, 2023). Dans le cas de la politique RTSAP – destinée à être mise à jour périodiquement afin de refléter les progrès technologiques et les changements dans les profils de risque des établissements étrangers –, toute modification sera uniquement prospective et ne s'appliquera pas rétroactivement (SP, 2023; CRSNG, 2025).

APPLICATION DES MESURES :

De nombreuses technologies émergentes contribuant à la recherche sur les agents pathogènes posent des défis pour la reconnaissance de la sensibilité

L'un des principaux défis à relever pour mesurer les risques liés à la recherche sur les agents pathogènes est la convergence de plusieurs technologies émergentes et sciences biologiques, qui a des implications pour la reconnaissance de la recherche sensible (Himmel, 2023). Les technologies quantiques, et plus particulièrement l'informatique quantique, devraient accélérer les tâches informatiques associées à l'étude des processus biologiques et à la conception de médicaments (Gunashekar *et al.*, 2022; CAC, 2023b). D'un autre côté, les technologies d'IA peuvent être combinées à la recherche sur les agents pathogènes pour en générer de nouveaux ou modifier la virulence des agents existants de manière ciblée (Brockmann *et al.,* 2019). Les technologies d'IA posent donc des défis pour ce qui est de l'évaluation des risques et de l'imposition de normes appropriées pour leur utilisation (Pouget et Zuhdi, 2024).

Rôles et responsabilités : Tous les acteurs du système peuvent être confrontés à cette question, mais les chercheurs issus de disciplines distinctes peuvent être particulièrement désavantagés, car ils risquent de ne pas disposer de l'expertise nécessaire pour avoir une vue d'ensemble des risques liés à la sécurité de la recherche dans le cadre de projets multidisciplinaires collaboratifs.

Stade de la recherche concerné : Le défi se pose lors de la phase de conception de la recherche, mais les chercheurs peuvent également y être confrontés durant la phase de recherche active si de nouveaux outils et technologies sont intégrés aux méthodologies au fur et à mesure de leur développement.

Les listes institutionnelles révisées périodiquement évitent plusieurs des inconvénients précités et sont à même de mieux s'adapter aux progrès technologiques comme au développement de la recherche

Au lieu des listes descendantes fournies par le gouvernement central, les équipes de sécurité de la recherche des établissements néerlandais sont encouragées à dresser des listes internes de thèmes de recherche, éclairées par une évaluation des risques, afin d'orienter les activités entourant la sécurité (Gouv. des Pays-Bas, 2022). Ce processus consiste à analyser les actifs de valeur

afin de reconnaître les domaines de recherche dans lesquels l'établissement peut avoir une capacité de pointe au niveau mondial ou présenter une valeur institutionnelle particulièrement élevée pour d'autres raisons (Gouv. des Pays-Bas, 2022; VU Amsterdam, 2023). Selon le comité, la reconnaissance des thèmes de recherche sensibles au niveau institutionnel et la possibilité de les réévaluer au fur et à mesure du développement de la recherche sont susceptibles d'éviter certains des inconvénients susmentionnés des listes, tout en clarifiant la situation pour les chercheurs et les départements. En revanche, la reconnaissance publique des actifs de valeur peut également attirer l'attention indésirable d'acteurs malveillants et comporte le risque de verser dans un protectionnisme excessif d'un point de vue économique.

Le département américain de l'Énergie ne s'appuie pas exclusivement sur des listes pour reconnaître la recherche potentiellement sensible (COGR, 2023; JASON, 2024). Ses experts en la matière procèdent plutôt à des évaluations périodiques afin de déterminer l'état d'avancement de plusieurs domaines de recherche liés à la compétitivité économique, à la sécurité nationale et/ou au leadership scientifique (p. ex. les batteries, la technologie quantique, l'IA) (JASON, 2024). Les recherches dans ces domaines sont ensuite classées en trois groupes : fondamentales et non sensibles, potentiellement sensibles d'un point de vue économique ou de sécurité nationale, ou nécessitant des mesures de protection supplémentaires. Cette classification est utilisée pour restreindre certaines activités comme les engagements et les voyages à l'étranger, les accords de coopération en R-D et l'accès aux projets et aux données impliquant des pays à risque (Chine, Iran, Corée du Nord, Russie) (COGR, 2023) (section 4.2). Les National Academies of Sciences, Engineering, and Medicine (NASEM[8]) (2022) recommandent l'adoption d'une approche similaire au sein du gouvernement fédéral américain, car elle met l'accent sur les catégories de technologies stratégiquement importantes plutôt que sur les listes de technologies critiques, ce qui est plus conforme à la protection des intérêts nationaux des États-Unis. JASON[9] (2024) soutient également l'adoption d'une approche plus souple et plus dynamique pour reconnaître la recherche potentiellement sensible en fonction de ses applications potentielles, de son NMT et de son impact direct et prévisible sur la sécurité nationale. Bien que les listes présentent de nombreux inconvénients, les approches ci-dessus peuvent améliorer leur utilité en tant que ressource plutôt qu'en tant qu'outil d'aide à la décision.

8 Académies nationales des sciences, de l'ingénierie et de la médecine des États-Unis.

9 JASON est un groupe indépendant, mis sur pied en 1960, qui conseille le gouvernement fédéral américain en matière de défense, de science et de technologie (DOD, 2022).

APPLICATION DES MESURES :

Analyse des actifs de valeur pour la recherche océanographique

Plusieurs établissements universitaires au Canada abritent des départements ou des facultés spécialisés dans la recherche océanographique. Ces entités peuvent être considérées comme des actifs importants si elles sont de renommée mondiale ou mènent des recherches d'une importance vitale pour le Canada et sa participation à des initiatives internationales comme les réseaux d'observation des océans (MPO, 2022; SIOOC, s.d.-a,-b; GOOS, s.d.). Le recensement des domaines d'excellence des établissements et la réalisation d'analyses des risques pour chacun de ces domaines sensibles peuvent aider à déterminer les mesures de protection appropriées pour la sécurité nationale, la sécurité du personnel et l'intégrité de la recherche (Gouv. des Pays-Bas, 2022). La sensibilité de la recherche pouvant évoluer au fil du temps, il est utile de réévaluer périodiquement ces listes institutionnelles (Gouv. des Pays-Bas, 2022).

Rôles et responsabilités : Les établissements sont chargés de mener l'analyse des actifs et peuvent être soutenus par les gouvernements qui fournissent des ressources pour mettre en œuvre les analyses des risques.

Stade de la recherche concerné : Tout au long du cycle de vie de la recherche.

3.2.2 Évaluation des risques

Une fois que le chercheur a cerné un facteur révélant la sensibilité, les évaluations des risques sont des outils utiles pour déterminer le niveau de sensibilité de la recherche, la manière dont les facteurs interagissent et si la recherche sensible est préoccupante. « L'évaluation du niveau de risque en matière de vraisemblance et de conséquences dans le but d'informer les décideurs est un processus officiel et systématique. » (SP, 2010) L'objectif est de fournir une compréhension claire des risques et de leur probabilité, ainsi que de leurs impacts possibles sur les résultats souhaités (SP, 2010). Une fois les risques reconnus, des mesures d'atténuation appropriées peuvent être mises en œuvre (chapitre 4). Cependant, les évaluations des risques peuvent exiger de ceux qui les utilisent une meilleure compréhension des risques pour la sécurité de la recherche; en comparaison, l'utilisation de listes ne nécessite pas un niveau de connaissance similaire.

Les principes fondamentaux de l'évaluation des risques sont adaptables à divers contextes

Si les évaluations des risques aident les chercheurs et les établissements à déterminer les cas où leurs recherches et leurs collaborations peuvent être préoccupantes, les évaluations varient en ce qui a trait à la spécificité. Certaines évaluations peuvent suivre des lignes directrices détaillées demandant aux chercheurs de prendre en compte des facteurs de risque supplémentaires – par exemple, le niveau de maturité technologique, les critères de détermination de l'autonomie institutionnelle – (Gouv. de l'Australie, 2021; JASON, 2024), tandis que d'autres s'appuient sur le jugement des chercheurs pour déterminer les risques d'après des lignes directrices générales (c.-à-d. les risques anticipés) (Gouv. de la Nouvelle-Zélande, 2020). Les informations accessibles au public fournissent aux chercheurs canadiens des lignes directrices pour mener leurs propres évaluations (ISDE, 2022b), mais les établissements et les administrateurs peuvent également avoir des responsabilités dans ce domaine. Aux Pays-Bas, par exemple, le National Contact Point for Knowledge Security « peut échanger les informations et l'expertise disponibles dans les ministères et les services du gouvernement central et donner des conseils sur les mesures d'atténuation qui pourraient être prises » (Gouv. des Pays-Bas, 2022).

La gouvernance de ces différents risques suit généralement un ensemble de processus largement utilisés qui peuvent être alignés sur les normes internationales (p. ex. ISO 2018). La terminologie précise utilisée dans ces processus (et la manière dont ils sont mis en œuvre) varie selon le domaine d'application et se reflète dans les différences entre les ministères et organismes fédéraux qui ont recours à la surveillance fondée sur les risques (voir p. ex. ASPC, 2018a; ARLA, 2024; SP, 2024b). Les facteurs révélant une sensibilité potentielle examinés à la section 3.1 peuvent servir de précurseurs ou de composantes majeures des évaluations des risques, selon la discipline.

Malgré l'influence du contexte sur les détails méthodologiques de la gouvernance des risques et son rôle dans la prise de décision, l'évaluation des risques est omniprésente et joue un rôle clé dans la reconnaissance de la recherche sensible. Afin de tenir compte des différences entre les domaines d'application, la première étape de l'évaluation des risques consiste généralement en un exercice de mise en contexte (SP, 2012). Cela permet de définir les thèmes d'intérêt pour l'évaluation des risques, les personnes ou groupes concernés et toute considération historique pertinente. Cette étape peut, par exemple, définir la portée et le calendrier de l'évaluation des risques (Verga, 2013).

APPLICATION DES MESURES :

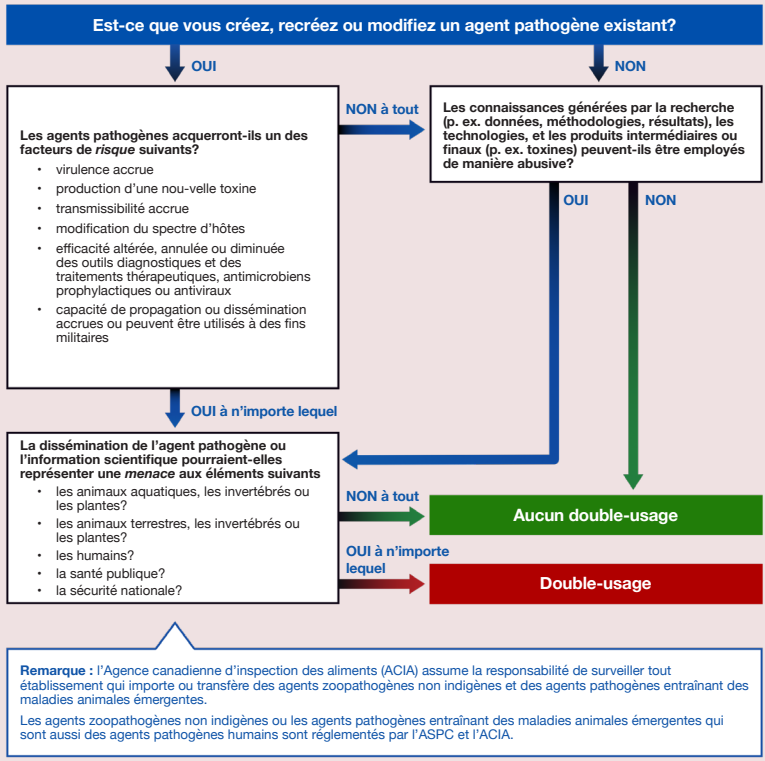
Risques pour la biosécurité dans la Ligne directrice canadienne sur la biosécurité

La Ligne directrice canadienne sur la biosécurité détaille la manière de reconnaître la recherche sur des agents pathogènes à double usage[10] potentiel en proposant un arbre décisionnel posant plusieurs questions sur les caractéristiques d'un organisme ou d'une toxine, notamment en ce qui a trait à la nocivité, à la nouveauté, aux risques de modification et au potentiel d'utilisation abusive (figure 3.1).

(continue)

10 Les termes « recherche à double usage » et « recherche à double usage préoccupante » sont utilisés dans cet encadré à la place du terme plus général « recherche sensible préoccupante » en raison de la spécificité du langage utilisé dans le processus de l'ASPC. L'ASPC définit le double usage potentiel comme les « propriétés d'un agent pathogène ou d'une toxine de pouvoir être utilisés autant pour mener des activités scientifiques légitimes (p. ex. à des fins commerciales ou médicales, aux fins de recherche) que pour créer sciemment une arme biologique ayant la capacité de causer une maladie (p. ex. le bioterrorisme) » (ASPC, 2018b).

(a continué)



©Tous droits réservés. Reproduit avec l'autorisation de l'ASPC (2015)

Figure 3.1 Processus de l'ASPC pour reconnaître le double usage potentiel de la recherche

Cet arbre décisionnel décrit comment les sujets de recherche (p. ex. les agents pathogènes) et les résultats peuvent entraîner ou exacerber des dangers. Dans la recherche sur les agents pathogènes et les toxines, on utilise les termes « double usage » et « recherche à double usage préoccupante » plutôt que « recherche sensible ».

ACIA – Agence canadienne d'inspection des aliments

ASPC – Agence de la santé publique du Canada

Le comité note toutefois qu'il existe d'autres facteurs de risque que ceux énumérés dans cet arbre décisionnel, notamment les méthodes de production uniques et la possibilité de recréer des agents pathogènes précédemment éradiqués. L'ASPC recommande que la recherche jugée à

(continue)

(a continué)

double usage sur la base des questions de la figure 3.1 fasse l'objet d'une évaluation des risques afin de déterminer si les mesures de biosécurité et de biosûreté existantes sont adéquates (ASPC, 2018a).

Rôles et responsabilités : L'ASPC est chargée d'élaborer ces évaluations des risques, tandis que les chercheurs sont responsables de leur mise en œuvre.

Stade de la recherche concerné : Phase de conception de la recherche.

Les évaluations des risques peuvent orienter les partenariats dans le cadre de collaborations de recherche

En dehors des listes, les facteurs de risque associés aux partenariats étrangers peuvent également être pris en compte dans le cadre de processus d'évaluation des risques à réaliser par les chercheurs ou les établissements. Ces évaluations peuvent ainsi inclure la vérification préalable (selon une approche de « diligence raisonnable ») des partenaires sur la base d'informations accessibles au public et de l'avis d'experts; la divulgation officielle par les chercheurs de leurs conflits d'intérêts et d'engagement lors de la demande de financement; et la détermination de l'autonomie institutionnelle des partenaires de recherche. Les informations accessibles au public, comme les affiliations et les projets actuels et passés, ainsi que les sources de financement divulguées de la recherche, peuvent suggérer l'existence de conflits d'intérêts réels ou potentiels (Gouv. de la Nouvelle-Zélande, 2020; Gouv. de l'Ont., 2023; ISDE, 2024a). Dans certains cas, la complexité législative des processus de diligence raisonnable nécessite une collaboration entre différents services au sein des établissements de recherche, notamment « les services juridiques, administratifs, financiers, internationaux, de développement et informatiques » (Marwaha *et al.*, 2023). Les évaluations des menaces menées par les services de renseignement sont également à même de fournir des informations pertinentes pour effectuer la vérification des partenaires potentiels et mieux comprendre la nature comme la portée des menaces (p. ex. les menaces liées à la cybersécurité) (SCRS, 2024b; Centre canadien pour la cybersécurité, 2024c). Dans le guide intitulé « Faire preuve de diligence raisonnable en utilisant des renseignements de sources ouvertes afin de protéger les partenariats de recherche », ISDE dresse une liste de plusieurs entreprises étrangères qui peuvent accélérer et compléter les activités de diligence raisonnable (ISDE, 2022c). Le comité note toutefois que le recours à des outils de diligence raisonnable étrangers peut être contraire aux valeurs et

aux priorités du Canada, en particulier dans un contexte géopolitique dynamique.

Les processus participatifs d'évaluation des risques permettent de recueillir des points de vue précieux qui ne proviennent ni des chercheurs ni des gouvernements

L'une des principales raisons pour lesquelles les chercheurs doivent évaluer eux-mêmes les risques et d'autres aspects de la recherche sensible est le fait qu'ils ont une compréhension plus approfondie de leur domaine que les évaluateurs externes (SIGRE, 2024). Cependant, les chercheurs peuvent avoir du mal à évaluer la sensibilité de leurs activités en raison d'une combinaison de facteurs, notamment le manque de formation, le temps insuffisant, l'ampleur des risques à évaluer et les préjugés. Dans ces circonstances, il peut être utile de se tourner vers l'évaluation participative des risques, qui est susceptible d'aider à détecter les dangers et à déterminer les stratégies pour une interaction efficace avec les communautés touchées en ce qui a trait aux risques (Stirling *et al.,* 2018). Lorsque les technologies en évolution peuvent avoir un impact sur les citoyens ou les patients, la participation des communautés et d'autres parties informées (p. ex. les professionnels de la santé) à l'évaluation peut conférer une description plus exhaustive des tolérances et des sensibilités aux risques, ce qui conduit à un processus décisionnel plus solide. Les exercices participatifs, comme les ateliers et la cartographie multicritères dans le cadre des évaluations des risques, se sont révélés efficaces pour éclairer les cadres de gouvernance relatifs aux technologies biologiques émergentes (voir l'analyse de Stirling *et al.,* 2018). Tirer parti des relations existantes pourrait être une voie à suivre pour cette méthode d'évaluation des risques. Par exemple, le comité de liaison avec la communauté de la Vaccine and Infectious Disease Organization (VIDO) en Saskatchewan fournit au public des informations et des ressources sur les recherches qu'elle effectue (VIDO, 2025), tout en relayant les préoccupations et les questions de la communauté à la VIDO (V. Gerdts, communication personnelle, 2025).

Les groupes d'experts peuvent renforcer les processus existants d'évaluation des risques et créer des communautés de pratique, à condition que les conflits d'intérêts soient gérés adéquatement

Dans certains pays, des groupes d'experts indépendants ont vu le jour. Ceux-ci présentent des similitudes avec les comités d'éthique de la recherche, à la différence qu'ils sont chargés de reconnaître la recherche sensible. Par exemple, l'Université Stanford a créé un comité d'éthique et de responsabilité sociale (ESR, *Ethics and Society Review Board*) afin d'évaluer la recherche en IA relativement à ses impacts potentiels sur la société (Bernstein *et al.*, 2021). Ce

processus est une étape obligatoire pour les chercheurs qui souhaitent bénéficier d'un financement institutionnel. Des enquêtes et des entretiens menés auprès de chercheurs ayant suivi le processus du ESR ont révélé que « 58 % d'entre eux estimaient que cela avait influencé la conception de leur projet de recherche [et que] 100 % sont disposés à continuer à lui soumettre leurs projets » (Bernstein *et al.*, 2021).

À l'échelle d'un pays entier, la Fondation allemande pour la recherche (DFG) et l'Académie nationale des sciences Leopoldina (Leopoldina) ont introduit en 2022 un cadre destiné aux chercheurs et aux établissements de recherche afin de superviser les « recherches pertinentes pour la sécurité » (Leopoldina et DFG, 2022b). Plus précisément, ces deux institutions définissent la recherche pertinente pour la sécurité comme « tout travail scientifique susceptible de produire des connaissances, des produits ou des technologies pouvant être directement utilisés de manière abusive par des tiers pour porter gravement atteinte à la dignité humaine, à la vie, à la santé, à la liberté, à la propriété, à l'environnement ou à la coexistence pacifique » (Leopoldina et DFG, s.d.-a). De tels travaux de recherche sont classés comme préoccupants car les dommages potentiels sont importants et leur utilisation abusive peut être envisagée dans l'immédiat. Les lignes directrices recommandent notamment aux établissements universitaires de créer des comités d'éthique de la recherche spécialisés, appelés *Kommissionen für Ethik sicherheitsrelevanter Forschung* (KEF), chargés de superviser les recherches pertinentes pour la sécurité et de contribuer à les classer éventuellement comme étant préoccupantes (Leopoldina et DFG, 2022b; Jakob *et al.*, 2024). Chaque établissement recrute des experts pour siéger à un KEF, qui peut ensuite conseiller d'autres chercheurs. Le KEF est habilité à prendre des décisions institutionnelles dans le domaine de la recherche pertinente pour la sécurité grâce à des politiques et à des règlements internes (Leopoldina et DFG, 2022b). Si un établissement ne dispose pas des capacités ni des ressources nécessaires pour accueillir un KEF, des coalitions peuvent se former afin de créer des KEF au service de plusieurs établissements, en mettant en commun leurs ressources. Les KEF sont en outre soutenus par le comité mixte DFG-Leopoldina sur le traitement de la recherche pertinente pour la sécurité, qui met en commun ses expériences et sert de point de contact (Leopoldina et DFG, 2022b).

L'une des principales responsabilités des KEF est de procéder à des évaluations de la recherche, qui consistent en une auto-évaluation réalisée par le chercheur, suivie d'évaluations par le KEF lui-même (Leopoldina et DFG, 2022a). Les KEF posent des questions sur la nature de la recherche et ses objectifs, ses participants et ses commanditaires. Ces questions portent sur plusieurs domaines éthiques liés aux avantages et aux risques (intentionnels ou non) et

visent à déterminer si les chercheurs disposent des connaissances ou des ressources nécessaires pour prendre des décisions éclairées et justes d'un point de vue éthique (Jakob *et al.,* 2024; Leopoldina et DFG, s.d.-b). Le KEF pose ensuite une série de questions afin d'éclairer une évaluation concluante, interrogeant les chercheurs sur les éventuelles utilisations abusives de la recherche, la nécessité d'une réévaluation par le KEF, la compatibilité avec les principes constitutionnels, les considérations éthiques et la possibilité de réduire suffisamment les risques en imposant les conditions proposées (Leopoldina et DFG, 2022a).

L'approche du KEF comble potentiellement les lacunes qui peuvent passer inaperçues dans les processus reposant strictement sur l'auto-évaluation. Jakob *et al.* (2024) soulignent toutefois que si l'expertise nécessaire à une évaluation ne peut être trouvée au sein d'un KEF, des experts externes provenant d'autres KEF ou d'ailleurs doivent être associés à l'évaluation, ce qui peut soulever des questions liées à la confidentialité ou à la protection des données. Ce modèle a suscité des inquiétudes parmi les membres du comité concernant les conflits d'intérêts, étant donné que les domaines dans lesquels la recherche sensible est menée ont tendance à être très concurrentiels, tant au niveau institutionnel qu'individuel. De plus, en tant que processus facultatif, le modèle KEF repose sur une culture où la sécurité est prise au sérieux; les obstacles ou les retards dans la recherche sont acceptés comme légitimes et nécessaires sur cette base, ce qui suppose la mise en place d'une culture institutionnelle particulière en matière de recherche (Jakob *et al.,* 2024). Le comité souligne également la nécessité de disposer de ressources et d'un soutien proportionnés afin de minimiser la charge administrative et les coûts en temps importants liés à un examen de type KEF, en particulier pour les chercheurs qui pourraient déjà être réticents à se soumettre à un examen ou à des tâches de recherche obligatoires. Le temps limité pour les demandes de subventions aurait un impact sur l'efficacité de ce type de comités, car tout allongement du processus de candidature serait susceptible d'être mal accueilli par les chercheurs. Néanmoins, la création de tels comités pourrait contribuer à la constitution de communautés de pratique, en particulier au niveau régional, car certaines considérations relatives aux risques (et aux menaces) peuvent être plus pertinentes que d'autres en matière de sécurité de la recherche (CNRS, 2024), et parce que les capacités et les ressources peuvent varier considérablement d'un établissement à l'autre (UNL, 2024) – en particulier au Canada (SPIIE, 2024).

Les groupes d'experts, comme les KEF, présentent à la fois des avantages et des inconvénients, mais leur multidisciplinarité inhérente et la participation d'experts en éthique constituent des atouts pour traiter les questions relevant de la sensibilité de la recherche. Les KEF offrent une solution de rechange aux

autres cadres nationaux de sécurité de la recherche examinés par le comité, qui se concentrent principalement sur les sciences naturelles et appliquées en raison de leur lien direct avec la technologie et de leur importance économique potentielle (voir p. ex. SGDSN, 2018; Gouv. de l'Australie, 2023; ISDE, 2023b; Gouv. du Royaume-Uni, 2024; UKRI, 2024b; ASIO, s.d.).

APPLICATION DES MESURES :

Comités d'examen des établissements pour la recherche océanographique

Comme pour l'analyse des actifs de valeur, les établissements qui possèdent déjà des atouts dans le domaine de la recherche océanographique pourraient faire appel à des comités d'examen pour les aider à déterminer le niveau de sensibilité de la recherche, ainsi que les mesures de protection appropriées si celle-ci est jugée préoccupante. Ces comités pourraient être composés de chercheurs issus des établissements, mais également bénéficier de la participation d'autres acteurs du système de recherche océanographique (p. ex. des représentants du secteur privé, des pêcheries, des gouvernements et des communautés autochtones côtières). Lorsque les établissements ne disposent pas des capacités suffisantes pour mener des examens internes, il serait possible de faire appel à des organisations régionales ou nationales ou d'en créer afin qu'elles assument cette fonction pour un plus grand nombre d'établissements ayant des atouts similaires. Par exemple, l'Alliance de la recherche océanique au Canada (AROC) a pour mandat de coordonner les efforts en matière de sciences et de technologies océaniques et sert de forum pour partager l'information et discuter des priorités dans le domaine de la recherche océanographique (AROC, 2022). L'AROC, dont le secrétariat est hébergé par Pêches et Océans Canada (AROC, 2023), pourrait soutenir un organisme d'examen afin d'aider les chercheurs et les établissements à évaluer la recherche sensible et à éviter la concurrence interne entre chercheurs, à même d'entraver les efforts visant à mettre en place des comités d'examen internes.

Les comités d'examen institutionnels pourraient également évaluer la sensibilité de la recherche dans certaines régions, comme l'Arctique. La souveraineté des peuples autochtones du Nord et leur droit à la recherche, ainsi que l'escalade des tensions géopolitiques, sont des facteurs qui compliquent la reconnaissance de la recherche sensible dans cette région. Les établissements et les organisations qui mènent des recherches dans l'Arctique pourraient tirer profit de la création de

(continue)

(a continué)

comités chargés de les aider à détecter les risques et à formuler des stratégies pour les atténuer, tout en tenant compte de cette complexité. Le comité met toutefois en garde contre le fait que tout organisme dictant la manière dont la recherche est menée dans le Nord (en particulier lorsqu'il s'agit des risques pour les populations nordiques) devrait être dirigé par des habitants du Nord, et plus précisément par les peuples autochtones du Nord, lorsque ceux-ci en ont la capacité (CAC, 2023a).

Rôles et responsabilités : Établissements et organismes de recherche régionaux ou nationaux.

Stade de la recherche concerné : Phase de conception de la recherche, avec possibilité de réévaluation pendant la phase active.

3.2.3 Expertise pertinente

L'expertise pertinente externe au chercheur ou à l'établissement qui mène la recherche est une autre mesure qui permet de reconnaître la sensibilité relative de la recherche en question et de la désigner comme préoccupante. Dans les situations où la responsabilité de reconnaître la recherche sensible est partagée avec des partenaires disposant de connaissances spécialisées, ces derniers peuvent signaler certains processus ou résultats de recherche comme sensibles à toutes les phases du processus.

Les détenteurs de connaissances autochtones sont les mieux placés pour reconnaître les informations sensibles qui les concernent ou qui concernent leurs terres

Lorsque les chercheurs travaillent en collaboration avec des peuples autochtones ou sur leurs terres, les détenteurs de connaissances autochtones peuvent parfois mettre leur expertise à profit pour reconnaître et protéger les informations sensibles. Par exemple, dans le cas d'une étude portant sur les processus d'érosion côtière dans la région de l'Inuvialuit, un chercheur fédéral de la Commission géologique du Canada s'est appuyé sur les connaissances et les conseils des membres des comités locaux de chasseurs et de trappeurs pour aider les chercheurs à interagir

Les détenteurs de connaissances autochtones peuvent parfois mettre leur expertise à profit pour reconnaître et protéger les informations sensibles

respectueusement avec les tombes qui s'érodaient en raison du dégel du pergélisol et de l'affaissement du sol (D. Whalen, communication personnelle, 2025). Une fois que les résultats et les données de la recherche ont été reconnus comme sensibles, des plans de gestion ou de gouvernance des données élaborés conformément aux protocoles des communautés autochtones et des détenteurs de droits (lors de la phase de conception de la recherche) peuvent être mis en œuvre afin de déterminer le niveau approprié d'accès et de partage, dans le cadre du processus de protection (section 4.2.4).

Les partenariats de recherche avec des acteurs militaires peuvent nécessiter la reconnaissance des données sensibles par des spécialistes disposant de connaissances classifiées

Dans les situations où les résultats de la recherche sont connus pour être potentiellement sensibles, des partenariats avec des organisations pertinentes peuvent être mis en place afin de reconnaître les données sensibles en temps réel. Par exemple, le comité a entendu plusieurs chercheurs océanographes dont les travaux étaient supervisés par les Forces armées canadiennes et le MDN, soit par le biais de protocoles d'entente (PE), soit par des accords de financement.

APPLICATION DES MESURES :

Filtrage des données de recherche océanographique par des partenaires militaires

Réseaux océaniques Canada (ONC) exploite un réseau de capteurs acoustiques au large des côtes canadiennes, qui produit des données accessibles au public en ligne (ONC, s.d.-a,-b). Cependant, certaines données peuvent être importantes pour la sécurité nationale et sont donc filtrées par des partenaires militaires afin d'en détecter le contenu sensible, un processus régi par un PE conclu entre ONC et le MDN (M. Paulson, communication personnelle, 2025). Les données collectées jugées sensibles sont conservées indéfiniment afin d'empêcher tout accès par des acteurs malveillants potentiels. Les données non sensibles sont quant à elles renvoyées à ONC pour être archivées et utilisées en tant que données ouvertes (M. Paulson, communication personnelle, 2025) (section 4.3).

Rôles et responsabilités : Les chercheurs, les établissements et les détenteurs d'expertise pertinente (c.-à-d. l'armée) peuvent conclure des accords à l'avance, éventuellement comme condition préalable au financement.

(continue)

(a continué)

Stade de la recherche concerné : Bien que les accords relatifs à la réalisation du filtrage soient conclus lors de la phase de conception de la recherche, le filtrage comme tel a lieu pendant la phase active, au fur et à mesure de la collecte des données.

Certaines revues ont pour politique éditoriale d'examiner les manuscrits soumis afin de détecter les recherches sensibles susceptibles de poser problème

Si relativement peu de revues ont publié des politiques sur l'examen des travaux de recherche sensibles, dans plusieurs cas, les comités de rédaction ont entrepris ce type d'examen (Musunuri *et al.*, 2021). Dans ces situations, les rédacteurs en chef, des comités spéciaux convoqués par les revues, des organismes gouvernementaux, des évaluateurs et les auteurs participent à la reconnaissance du niveau de sensibilité ou du risque lié à la publication des travaux et prennent des décisions sur la meilleure façon de les protéger (p. ex. en expurgeant certaines informations, en rejetant purement et simplement les articles soumis). La prolifération rapide des prépublications pendant la pandémie de COVID-19 a accru les inquiétudes quant à l'absence d'examen du double usage, un processus qui peut avoir lieu lors de la publication, mais qui est largement contourné par les prépublications (Musunuri *et al.*, 2021). Plusieurs serveurs de prépublications ont mis en place des processus de filtrage visant à détecter le double usage avant la soumission, mais les auteurs peuvent choisir de ne pas soumettre leurs articles à de tels serveurs offrant cette fonctionnalité (Yoshizawa *et al.*, 2023).

APPLICATION DES MESURES :

Évaluation du potentiel de RDUP[11] par les éditeurs de revues scientifiques

Certaines revues font appel à l'expertise de leurs évaluateurs pour déterminer le potentiel en matière de RDUP. En réponse aux recommandations du National Science Advisory Board for Biosecurity américain, les revues supervisées par l'American Society for Microbiology ont introduit en 2007 un questionnaire demandant aux

(continue)

11 Le terme « recherche à double usage préoccupante » (RDUP) est utilisé à la place du terme plus général « recherche préoccupante » en raison de la spécificité du langage utilisé dans ce processus, qui concerne la recherche sur les agents pathogènes.

(a continué)

évaluateurs de voir si les soumissions impliquaient des « expériences préoccupantes » (Casadevall *et al.,* 2015). Plus récemment, ces revues ont mis en place un processus plus formel pour traiter la RDUP en trois étapes : filtrage, discussion et décision (ASM Journals, 2021). Le processus de préfiltrage (c'est-à-dire la phase de reconnaissance) implique plusieurs acteurs et étapes clés. Tout d'abord, les auteurs peuvent déclarer eux-mêmes le caractère sensible du contenu dans la lettre d'accompagnement de leur soumission, afin d'alerter les éditeurs et les évaluateurs sur la nécessité de tenir compte des risques biologiques dans leurs évaluations. Le personnel éditorial consulte ensuite la *Select Agents and Toxins List* (liste des agents et toxines sélectionnés) américaine et recherche des expressions clés liées à une virulence accrue, à la transmission ou à des concepts connexes qui justifieraient un examen plus approfondi du manuscrit. Si un manuscrit est identifié comme RDUP, le personnel éditorial passe alors aux étapes suivantes de la discussion et de la décision afin de déterminer le niveau d'accès et de publication (c'est-à-dire la mise en commun) du manuscrit (Casadevall *et al.,* 2015; ASM Journals, 2021).

Rôles et responsabilités : Le personnel éditorial de la revue est impliqué dans cette mesure.

Stade de la recherche concerné : Dans la phase post-recherche, comme condition de publication.

Les partenaires de recherche autochtones ont le droit de déterminer comment les résultats de la recherche sont mis en commun

Les peuples autochtones ont le droit de dicter la manière dont la recherche et les informations les concernant – et concernant leurs terres – sont utilisées, incluant la manière dont elles sont mises en commun une fois collectées (section 1.3). Des protocoles d'accord, des accords d'accès et de partage des avantages et des plans de gouvernance des données peuvent être établis avant le début de la recherche afin de définir les rôles et les responsabilités concernant le traitement des résultats de la recherche une fois celle-ci terminée (CAC, 2023a). Dans de telles situations, la décision appartient aux communautés autochtones ou à des individus (p. ex. les Aînés, les membres des comités de chasseurs et de trappeurs) : ceux-ci déterminent alors le caractère sensible de certaines informations et dictent ensuite la façon dont elles peuvent être mises en commun afin de les protéger adéquatement (section 4.3.3).

APPLICATION DES MESURES :

Reconnaissance de la recherche sensible par les partenaires des communautés autochtones

Les chercheurs qui travaillent avec des communautés autochtones côtières ou sur les terres et les eaux des peuples autochtones doivent être conscients des sensibilités associées à la recherche océanographique. Par exemple, dans une situation où un chercheur cartographie les lieux de reproduction ou de frai des poissons, les communautés autochtones locales qui dépendent de ces ressources peuvent considérer les informations s'y rapportant comme sensibles étant donné leur importance culturelle et souhaiter par conséquent en contrôler l'accès, afin d'éviter des impacts négatifs comme la surpêche (M. Hoeberechts, communication personnelle, 2025).

Rôles et responsabilités : Les peuples autochtones et les détenteurs de connaissances peuvent exercer leur droit de protéger les informations les concernant et concernant leurs terres. Les chercheurs doivent être conscients des droits codifiés dans la DNUDPA et de leur responsabilité de mener leurs travaux dans le respect de ces droits.

Stade de la recherche concerné : Des accords et des relations doivent être établis avant le début de la recherche, les risques et résultats devant être communiqués tout au long de la phase active et post-recherche.

4

Mesures de protection de la recherche sensible préoccupante

4.1 Phase de conception de la recherche

4.2 Phase de recherche active

4.3 Phase post-recherche

4.4 Protéger le cycle de vie de la recherche

Constatations du chapitre

- Les mesures visant à protéger la recherche sensible préoccupante sont interdépendantes et contextuelles; elles doivent être réexaminées tout au long du processus de recherche afin de maintenir un équilibre entre ouverture et sécurité.
- La mise en œuvre et le respect des mesures visant à protéger la recherche sensible préoccupante relèvent de la responsabilité commune des chercheurs, des établissements et des gouvernements.
- Ces mesures se concentrent sur les deux premières phases du processus : la conception et la phase active. Il y a un manque de directives claires sur la mise en commun responsable des données et la publication des résultats dans la phase post-recherche.
- Les principes d'autonomie et d'autodétermination garantissent le droit des peuples autochtones de décider comment protéger la recherche sensible préoccupante qui les concerne. Or, le manque de soutien et de ressources, ainsi que la prédominance des établissements de recherche non autochtones, les empêchent de pleinement exercer ces droits.

La deuxième étape de la mise en œuvre des mesures de sécurité de la recherche consiste à protéger la recherche sensible une fois qu'elle a été jugée préoccupante. L'application de ces mesures dépend d'une série de facteurs, notamment la nature du projet de recherche (p. ex. le sujet, la méthodologie, les participants), les sources de financement et les partenaires. Ces mesures peuvent être considérées comme des pratiques exemplaires pour protéger au sens large les activités de recherche et s'appliquer à la fois à la recherche sensible et à la recherche sensible préoccupante, tout en assurant un équilibre entre science ouverte et innovation.

Les mesures examinées dans le présent chapitre sont classées selon les étapes du processus de recherche : la phase de conception (section 4.1), la phase de recherche active (section 4.2) et la phase post-recherche (section 4.3). Ces mesures sont interdépendantes et doivent être utilisées de manière cohérente pour être efficaces. Malgré les divers mécanismes qui peuvent être appliqués aux personnes, aux établissements et aux projets de recherche, la mise en œuvre des mesures de protection est souvent fragmentée et laissée à la discrétion des chercheurs et des établissements. De plus, les approches existantes se concentrent sur les deux premières phases du processus, ce qui

laisse les chercheurs et les établissements avec peu d'encadrement sur la mise en commun des données et la communication des résultats de la recherche. Le présent chapitre se termine par une discussion sur les considérations qui peuvent aider tous les acteurs de l'écosystème de la recherche à déterminer leurs rôles et leurs responsabilités dans la mise en œuvre des mesures de protection (section 4.4).

4.1 Phase de conception de la recherche

Au cours de la phase de conception de la recherche, les chercheurs prennent des décisions importantes concernant leur projet, notamment la détermination de la question de recherche et de la méthodologie, les partenariats et collaborations potentiels, de même que les sources de financement. Les chercheurs, les établissements, les gouvernements et les bailleurs de fonds ont la capacité de protéger la recherche sensible contre les utilisations abusives et les détournements en adoptant des mesures qui empêchent les acteurs malveillants d'accéder aux données, aux connaissances, aux informations et à la propriété intellectuelle dès le début du projet.

4.1.1 Sélection des chercheurs

Immigration, Réfugiés et Citoyenneté Canada (IRCC) procède à une évaluation de sécurité de tous les ressortissants étrangers (y compris les professeurs, les chercheurs invités et les étudiants) qui demandent à étudier ou à travailler au Canada, dans n'importe quel domaine ou discipline (SP, 2024c). Cette évaluation vise à déterminer si le demandeur a été impliqué dans des activités criminelles. En fonction des résultats de cette évaluation, certains chercheurs peuvent être déclarés admissibles au Canada, tandis que d'autres peuvent être soumis à un filtrage de sécurité approfondi faisant participer l'Agence des services frontaliers du Canada (ASFC) et le Service canadien du renseignement de sécurité (SCRS) (SP, 2024c). L'un des objectifs de l'examen approfondi est de déterminer si le demandeur présente un risque pour la sécurité nationale (et un risque pour la recherche sensible) en se basant sur plusieurs facteurs, notamment sa formation, ses antécédents professionnels et ses intérêts de recherche, ainsi que des informations provenant de sources ouvertes sur les activités hostiles de pays étrangers (voir p. ex. CF, 2023a,b). À la suite de cet examen, certains chercheurs peuvent être déclarés inadmissibles au Canada en vertu de *la Loi sur l'immigration et la protection des réfugiés* pour un certain nombre de raisons, notamment parce qu'ils constituent un risque pour la sécurité nationale ou se livrent à des activités d'espionnage (GC, 2001; SP, 2024c). Toutefois, cet examen ne représente qu'un instantané et ne peut tenir compte

ni de l'évolution de la situation ni des motivations des chercheurs, en raison, par exemple, de pressions et de menaces externes (SC et ASPC, 2022). Ces risques soulignent la nécessité de procéder à un examen périodique des mesures et des habilitations de sécurité, le cas échéant (SC et ASPC, 2022). Indépendamment des résultats des examens de sécurité effectués par IRCC, l'ASFC et le SCRS, les personnes activement affiliées à certaines organisations de recherche nommées (ORN) et travaillant dans des domaines de recherche sensibles mentionnés dans la politique RTSAP ne sont pas admissibles au financement des trois organismes dans ces domaines (ISDE, 2023f).

APPLICATION DES MESURES :

Filtrage de sécurité des océanographes

Les océanographes étrangers qui demandent à travailler et à étudier au Canada sont soumis à des évaluations de sécurité et peuvent également faire l'objet de filtrages de sécurité approfondis menés par IRCC, l'ASFC et le SCRS. Les océanographes et les organisations qui se consacrent à l'étude des océans peuvent se référer à la politique RTSAP pour éviter toute collaboration avec des chercheurs affiliés à des ORN qui présentent des risques pour la sécurité (ISDE, 2023f).

Contrairement au Canada, certains pays ont officiellement intégré les considérations relatives à la sécurité de la recherche dans le processus d'examen des demandes d'immigration et ont mis en place un filtrage ciblé pour les chercheurs de certains pays travaillant dans des domaines de recherche sensibles. Par exemple, le gouvernement du Royaume-Uni a introduit des exigences de certification dans le cadre du Academic Technology Approval Scheme (régime d'autorisation des technologies universitaires) pour les étudiants et les chercheurs étrangers de certains pays travaillant dans des domaines de recherche sensibles (Gouv. du Royaume-Uni, 2025). Un projet du gouvernement des Pays-Bas visant à instaurer un processus de filtrage des ressortissants de pays non membres de l'UE travaillant dans des domaines à haut risque a été critiqué pour son potentiel discriminatoire et les retards qu'il pourrait entraîner dans le traitement des demandes d'immigration (De Bruijn, 2023; Gouv. des Pays-Bas, 2025; Sharma, 2025).

APPLICATION DES MESURES :

Filtrages de sécurité des personnes travaillant avec des agents biologiques à cote de sécurité élevée (ABCSE)

Outre les contrôles de sécurité effectués par IRCC et ses partenaires, la *Loi sur les agents pathogènes humains et les toxines* (LAPHT) prévoit des procédures de sécurité spéciales pour tous les chercheurs (canadiens et étrangers) qui mènent des projets avec des ABCSE (GC, 2009). Les chercheurs doivent ainsi obtenir une habilitation de sécurité en vertu de la LAPHT (ASPC, 2024c). La demande d'habilitation est soumise à l'ASPC et comprend des renseignements sur le lieu de résidence, les antécédents professionnels et scolaires, le conjoint ou le conjoint de fait, ainsi qu'une vérification du casier judiciaire. Les ressortissants étrangers doivent fournir des documents supplémentaires, notamment une copie de leur curriculum vitae et des vérifications de leurs antécédents judiciaires à l'étranger (ASPC, 2024c). L'évaluation du cadre réglementaire de la *Loi sur les agents pathogènes humains et les toxines* et de son règlement d'application, réalisée par l'ASPC et Santé Canada en 2022, a soulevé des questions concernant les critères d'habilitation de sécurité (SC et ASPC, 2022). Les agents chargés de la sécurité biologique ont suggéré d'élargir la liste des personnes devant obtenir une habilitation de sécurité, c'est-à-dire au-delà de celles qui travaillent avec des ABCSE ou qui y ont accès, et de réaliser « un examen plus minutieux avant de délivrer une habilitation de sécurité à des étrangers ». L'évaluation a également suggéré de mettre en place un contrôle continu des habilitations de sécurité délivrées (généralement valables pour cinq ans), en soulignant que les circonstances peuvent changer au fil du temps (SC et ASPC, 2022).

4.1.2 Examen de sécurité des propositions de recherche

Les propositions de recherche peuvent faire l'objet de contrôles de sécurité supplémentaires avant d'être soumises à l'examen par les pairs. Par exemple, dans le cadre des LDSNPR, une évaluation des risques est effectuée indépendamment de l'examen du mérite et comprend les étapes suivantes :

1. *Examen administratif préliminaire.* L'organisme subventionnaire examine le formulaire d'évaluation des risques du demandeur afin de s'assurer qu'il est complet et procède à sa propre évaluation des risques en se basant sur des informations accessibles au public.

2. *Examen administratif supplémentaire.* Les demandes présentant des risques inconnus ou reconnus sont renvoyées pour un examen plus approfondi par le comité d'évaluation des risques de l'organisme subventionnaire, qui tient compte des éléments suivants : (i) la nature sensible de la recherche (conformément à l'annexe A des LDSNPR) et (ii) « selon des sources d'information en libre accès, [si] au moins un des organismes partenaires du secteur privé est peut-être associé à des organisations ou des pays visés par des sanctions, ou provenant de ces organisations ou pays; [ou] associé à des affaires non éthiques ou criminelles » (CRSNG, 2024b).
3. *Évaluation du mérite.* L'organisme subventionnaire procède à une évaluation du mérite, mais le formulaire d'évaluation des risques soumis par le demandeur et les résultats de l'examen du comité d'évaluation des risques ne sont pas communiqués aux pairs évaluateurs.
4. *Examen de certaines demandes par les organismes de sécurité.* À la suite d'un examen du mérite favorable, certaines demandes signalées par le comité d'évaluation des risques de l'organisme subventionnaire sont envoyées à SP pour une évaluation de la sécurité nationale qui peut impliquer le SCRS et le Centre de la sécurité des télécommunications Canada. SP peut consulter d'autres ministères (p. ex. Affaires mondiales Canada) afin d'examiner divers facteurs pertinents, comme les conséquences économiques et diplomatiques du financement de la demande.
5. *Décision de financement*. L'organisme subventionnaire tient compte des résultats de l'évaluation de la sécurité nationale et de l'examen du mérite pour prendre sa décision de financement. Les demandeurs retenus sont tenus de mettre en œuvre le plan d'atténuation des risques décrit dans leur demande de financement et, dans certains cas, des mesures supplémentaires d'atténuation des risques. Les demandeurs qui se sont vu refuser un financement sur la base des résultats de l'évaluation de la sécurité nationale peuvent demander des informations supplémentaires à l'organisme subventionnaire et au Centre de la sécurité de la recherche.

(GC, 2025j)

Entre juillet 2021 et juillet 2022, le CRSNG a utilisé les LDSNPR pour examiner les demandes soumises au programme de subventions Alliance (ISDE, 2023c). Sur les 1 158 demandes, 48 (environ 4 %) ont fait l'objet d'un contrôle de sécurité approfondi et, parmi celles-ci, 32 (soit environ 2,5 % de toutes) ont été rejetées pour des raisons de sécurité. Ces demandes concernaient des organisations partenaires du secteur privé pour lesquels on avait constaté « des liens publics avec des États étrangers reconnus pour cibler les

institutions universitaires, le secteur privé et le grand public, [et/ou] des antécédents publics de non-respect des régimes d'importation ou d'exportation » (ISDE, 2023c).

APPLICATION DES MESURES :

Examen de la sécurité des propositions de recherche dans le domaine de la recherche océanographique

Un océanographe qui sollicite un financement auprès des trois organismes (p. ex. une subvention Alliance du CRSNG) doit joindre un formulaire d'évaluation des risques à sa demande de subvention si son projet de financement relève des LDSNPR et s'il prévoit mener des recherches avec un partenaire visé (p. ex. une organisation du secteur privé). Ce formulaire d'évaluation des risques a pour objectif « d'identifier et d'évaluer les risques potentiels que les partenariats de recherche peuvent poser pour la sécurité nationale du Canada » (ISDE, 2024a). Les propositions de recherche font l'objet d'une évaluation des risques menée indépendamment de l'évaluation du mérite. Bien que les LDSNPR ne s'appliquent qu'à certaines recherches financées par des fonds publics, d'autres organisations qui financent la recherche océanographique peuvent s'en inspirer pour mener des examens de sécurité des propositions de recherche à partir de sources librement accessibles.

Les Lignes directrices sur la sécurité de la recherche pour les programmes de financement de la recherche en Ontario ont une portée plus large que les LDSNPR et la politique RTSAP

Les Lignes directrices sur la sécurité de la recherche pour les programmes de financement de la recherche en Ontario (LDSR) s'appliquent aux collaborations financées par le Fonds pour la recherche en Ontario (Gouv. de l'Ont., 2024a). L'approche du gouvernement de l'Ontario en matière de sécurité de la recherche est partiellement alignée sur la politique fédérale RTSAP (Gouv. de l'Ont., 2024a). Toutefois, les LDSR ont une portée plus large que la politique RTSAP et les LDSNPR : elles exigent que tous les chercheurs nommés dans toutes les demandes de financement soumettent un formulaire d'attestation reconnaissant qu'ils se conforment aux LDSR (Gouv. de l'Ont., 2024a,b). Ces exigences s'appliquent quels que soient le domaine de recherche et les affiliations (Gouv. de l'Ont., 2024a). Une autre différence réside dans le fait que la politique RTSAP ne considère que les affiliations actives avec des

organisations de recherche préoccupantes au moment de la demande et pendant la durée de la subvention (ISDE, 2023f). Les LDSR, en revanche, intègrent les collaborations au cours des deux années précédant la soumission de la proposition et pendant la durée du projet proposé. Ces collaborations comprennent, notamment celles « impliquant des coauteurs, des coéditions, des coorganisations de conférences internationales, des recherches conjointes ou des bénéficiaires de financements conjoints, […] un protocole d'accord, un partenariat, une coentreprise, un financement conjoint, un programme d'échange ou de diplôme conjoint, la supervision d'étudiants des cycles supérieurs, un chercheur invité ou la participation à un programme de talent bénéficiant d'un financement étranger » (Gouv. de l'Ont, 2024a). Il est important de tenir compte de ces différences si les chercheurs participent à des projets financés à la fois par le gouvernement fédéral et celui de l'Ontario. Il est possible que certains projets soient conformes aux politiques fédérales en matière de sécurité de la recherche, mais qu'ils soient considérés comme présentant un risque élevé en vertu des LDSR (Université de Victoria, 2024).

Une évaluation de la sécurité de certaines propositions de recherche est requise par les lois américaines

Aux États-Unis, des modifications ont été apportées à l'évaluation du mérite de certains projets financés par la National Science Foundation (NSF) en raison de préoccupations en matière de sécurité. Ces modifications ont été imposées par la *CHIPS and Science Act of 2022*, qui souligne qu'« un certain nombre de domaines de recherche émergents ont des implications potentielles […] en matière de sûreté et de sécurité qui pourraient apparaître dès le stade de la recherche fondamentale » (Gouv. des États-Unis, 2022b). La NSF examine la meilleure façon d'intégrer « les considérations éthiques, sociales, de sûreté et de sécurité dans […] le processus d'évaluation du mérite » afin d'atténuer « les dommages potentiels de la recherche scientifique » (NSF, 2024a). Cet examen s'ajoute aux autres exigences en matière de sécurité de la recherche imposées aux bénéficiaires de fonds fédéraux pour la recherche (incluant la NSF et les National Institutes of Health) en vertu des politiques et lignes directrices fédérales (NSTC, 2022; COGR, 2024).

APPLICATION DES MESURES :

Permis en vertu de la LAPHT

Dans le domaine de la recherche sur les agents pathogènes, un niveau supplémentaire d'examen de la sécurité et de la sûreté s'applique aux personnes et aux organisations qui proposent de mener des activités de recherche[12] avec des agents pathogènes humains et des toxines reconnus comme appartenant aux groupes de risque 2, 3 et 4 (ASPC, 2024d). Ces recherches nécessitent un permis en vertu de la LAPHT. Les conditions d'octroi des permis dépendent du groupe de risque de l'agent pathogène et du statut ABCSE de la toxine. Une installation souhaitant mener des recherches sur des agents pathogènes relevant de plusieurs groupes de risque et groupes d'ABCSE devra obtenir plusieurs permis (ASPC, 2024d). Avant d'en obtenir un, les demandeurs sont également tenus d'élaborer des plans d'action en matière de biosécurité et de biosûreté (ASPC, 2021).

4.1.3 Interdictions et autorisations préliminaires des partenariats et collaborations en matière de recherche

Les gouvernements du Canada et de l'Ontario peuvent refuser de financer des partenariats et des collaborations de recherche qui ne satisfont pas aux exigences en matière de sécurité (section 4.1.2). Toutefois, le refus du gouvernement d'allouer des fonds à la recherche n'interdit pas ces partenariats et collaborations, car les interdictions et les restrictions n'ont pas le même effet juridique que les décrets ou les lois. L'enseignement supérieur étant administré par les provinces et les territoires (GC, 1982), les gouvernements respectifs peuvent utiliser d'autres mécanismes que le financement pour exiger que le secteur de l'enseignement supérieur fasse preuve d'une plus grande prudence dans les collaborations internationales, voire suspende certaines d'entre elles ou y mette fin.

Par exemple, en 2021, le gouvernement de l'Alberta a ordonné aux quatre universités de recherche et d'enseignement supérieur de la province (l'Université de l'Alberta, l'Université de Calgary, l'Université de Lethbridge et l'Université Athabasca) de suspendre tout partenariat nouveau ou renouvelé lié au gouvernement chinois ou au Parti communiste chinois au pouvoir afin de garantir que ces partenariats respectent des procédures strictes d'évaluation

12 Définies de manière large comme « la possession, la manipulation, l'utilisation, la production, le stockage, l'autorisation d'accès à toute personne, le transfert, l'importation, l'exportation, la libération, l'abandon ou l'élimination » (ASPC, 2024d).

des risques et de diligence raisonnable (Chase, 2022). En 2022, ces universités ont été autorisées à reprendre les « accords à faible risque » avec la Chine, mais uniquement pour des arrangements relatifs à la « mobilité et la transférabilité des étudiants de premier cycle » et aux « possibilités de formation en entreprise » (SRSR, 2024). En 2023, les collèges et les universités de recherche de la province ont été invités à suspendre uniquement les accords avec la Chine qui concernent la recherche par les étudiants de cycles supérieurs, les chercheurs invités et les boursiers postdoctoraux dans les domaines de recherche sensibles précisés à l'annexe A des LDSNPR (Université de l'Alberta, 2024b).

APPLICATION DES MESURES :

Partenariats et collaborations entre les installations de recherche portant sur les agents pathogènes

« Les travaux sur les agents pathogènes au Canada sont tenus de se conformer aux lois et directives internationales, nationales et provinciales » (ASPC, 2025a), qui peuvent imposer des restrictions aux partenariats et collaborations à l'international (p. ex. contrôles à l'exportation) (GC, 2024h). Les installations réglementées ont également recours à des politiques et directives internes, à des accords de non-divulgation et à des formations pour protéger leurs recherches (ASPC, 2024e). Les installations peuvent utiliser la politique RTSAP comme guide pour éviter les collaborations qui présentent des risques pour la sécurité. En outre, les chercheurs qui effectuent des travaux sur les agents pathogènes et qui demandent un financement fédéral pour des projets impliquant l'application de technologies des sciences de la vie (telles que définies dans la politique RTSAP) ne peuvent collaborer avec des chercheurs affiliés à des ORN (ISDE, 2023b). Ils doivent enfin se conformer à la législation applicable qui couvre des sujets généraux, incluant la sécurité de la recherche.

Certains pays exigent des autorisations gouvernementales préliminaires pour les collaborations avec des établissements de recherche étrangers

Les gouvernements étrangers ont exploré et appliqué diverses approches réglementaires pour faire face aux risques liés à la sécurité des partenariats de recherche, notamment en introduisant des règles plus strictes que celles du Canada et en imposant l'obtention d'autorisations préliminaires pour les collaborations avec des établissements étrangers. En France, les établissements

de recherche menant des activités couvertes par le *Dispositif de protection du potentiel scientifique et technique de la nation* doivent faire approuver leurs accords de partenariat par le ministère de l'Enseignement supérieur et de la Recherche (Pannier, 2023). En Australie, les universités publiques doivent informer le ministre des Affaires étrangères avant de conclure un accord de partenariat avec une organisation étrangère (Gouv. de l'Australie, 2020). Le ministre peut interdire le partenariat s'il estime qu'une université étrangère ne dispose pas d'une autonomie institutionnelle suffisante, sur la base d'un ou plusieurs critères définis par la loi :

(a) *la majorité des membres du corps dirigeant de l'université sont tenus, en vertu d'une loi ou des documents constitutifs de l'université, d'être membres ou de faire partie (quelle que soit la forme que cela revêt) du parti politique qui forme le gouvernement étranger;*

(b) *l'enseignement dispensé ou la recherche menée à l'université est tenu, en vertu d'une loi ou des documents constitutifs de l'université, d'adhérer aux principes ou doctrines politiques : (i) du gouvernement étranger; ou (ii) du parti politique qui forme le gouvernement étranger;*

(c) *les enseignants et le personnel de recherche de l'université est tenu, en vertu d'une loi ou des documents constitutifs de l'université, d'adhérer aux principes ou doctrines politiques visés au paragraphe (b) ou d'être au service de ceux-ci dans son enseignement, ses recherches, ses discussions, ses publications ou ses commentaires publics.*

(Gouv. de l'Australie, 2020)

Certaines organisations et certains chercheurs ont accueilli avec résistance et critiques ce système de restrictions et d'autorisations imposées par la loi aux partenariats de recherche (Morris, 2020). Comme l'a fait remarquer Universities Australia (2024), la loi définit de manière trop large les notions d'« accord », d'« entité étrangère » et d'« autonomie institutionnelle », imposant ainsi aux universités une charge administrative inutile en matière de reddition de comptes. De plus, elle ne prévoit aucun mécanisme permettant de faire appel de la décision du ministre (Universities Australia, 2024). Il convient de tenir compte des différences entre les systèmes juridiques et les cultures lorsqu'on évalue dans quelle mesure les approches étrangères sont appropriées dans le contexte canadien.

4.1.4 Dispositions de sécurité des accords de coopération en matière de recherche

Les chercheurs peuvent atténuer les risques pour la sécurité dès le début d'un projet en incluant des dispositions pertinentes dans les accords de coopération avec leurs homologues. Par le biais de ces accords, il est possible d'établir des règles concernant l'utilisation des données et des infrastructures, la confidentialité, les permis et les transferts, l'inscription des droits de propriété, les garanties, la responsabilité, le droit applicable, le règlement des différends et une clause de sortie pour les partenaires qui ne respectent pas les règles (Leibniz Association, 2021). Toutefois, les chercheurs doivent savoir que « certains pays ont des lois ou des pratiques qui obligent les entités et les personnes à être assujetties aux instructions de leur gouvernement en vue de fournir les renseignements canadiens, le savoir issu de la recherche, la technologie et la propriété intellectuelle qui en découle » (ISDE, 2023a). Dans de tels cas, les dispositions contractuelles sont largement inapplicables, ce qui rend les partenariats risqués, et avantageux seulement pour une partie.

4.1.5 Examen éthique, autorisation de recherche et octroi de permis pour la recherche autochtone

Les principes d'autodétermination et d'autonomie gouvernementale des peuples autochtones, codifiés dans la DNUDPA, guident la recherche autochtone (voir la définition dans l'encadré 1.1) et signifient que ces peuples ont le droit de déterminer la manière de reconnaître et ensuite de protéger la recherche sensible préoccupante (ONU, 2007). Ce droit est pleinement réalisé lorsque les peuples autochtones participent équitablement au processus de recherche (ITK, 2018; GC, 2019a). Au Canada, il y a un manque de mécanismes d'examen éthique et d'octroi de permis de recherche qui soutiennent les mesures communautaires et centrées sur la communauté visant à protéger la recherche sensible préoccupante (CAC, 2023a).

Les mécanismes d'examen éthique et d'octroi de permis de recherche ne respectent pas pleinement les droits des peuples autochtones à l'autodétermination et à l'autonomie gouvernementale

L'Énoncé de politique des trois conseils : Éthique de la recherche avec des êtres humains (EPTC 2) comporte des considérations à l'intention des personnes qui reçoivent un financement des trois organismes pour des recherches impliquant les Premières Nations, les Inuits et les Métis (IRSC *et al.*, 2022). Toutefois, la Stratégie nationale inuite sur la recherche a explicitement déclaré qu'« il n'existe pas de directives éthiques connexes sur la recherche portant sur la faune et l'environnement » (ITK, 2018). Le système d'octroi de permis et de licences de recherche administré par les gouvernements territoriaux et, dans

certains cas, par les communautés autochtones (p. ex. le Nunatsiavut Government Research Advisory Committee, le Ittaq Heritage and Research Centre) comble en partie les lacunes des examens éthiques à cet égard (CAC, 2023a; IHRC, s.d.; NGRAC, s.d.). L'objectif de ce processus est de garantir une approche fondée sur les droits pour protéger la recherche sensible préoccupante :

> *La recherche sur l'érosion côtière qui n'implique pas d'êtres humains n'est pas soumise à un examen éthique institutionnel. Néanmoins, les chercheurs doivent obtenir un permis de recherche auprès de la région désignée des Inuvialuit s'ils mènent des recherches sur leurs terres. De même, les données physiques recueillies pour la recherche géologique peuvent être importantes pour la communauté pour des raisons de sécurité. Le système d'octroi de permis de recherche existe afin que le chercheur rende des comptes à la communauté.*
>
> (D. Whalen, communication personnelle, 2025)

Bien que les mécanismes d'octroi de licences et de permis de recherche marquent un tournant important quant à l'influence exercée sur la conduite des recherches en contexte autochtone, ces processus demeurent limités en raison de la capacité insuffisante des communautés et gouvernements autochtones « d'évaluer ou de participer à la recherche entrante » (CAC, 2023a). Par exemple, dans l'Arctique, « les délais courts, les limites de la dotation en personnel, la duplication des processus au niveau territorial et le manque de compréhension du contexte du Nord de la part des chercheurs du Sud posent des problèmes pour une évaluation efficace et opportune par les organisations autochtones » (CAC, 2023a). De plus, selon le comité, des mécanismes et des ressources supplémentaires sont nécessaires pour protéger les données autochtones contre toute utilisation abusive par des chercheurs non autochtones pendant la phase active et après la fin du projet de recherche.

4.2 Phase de recherche active

Pendant la phase active de la recherche, les chercheurs collectent des données, mènent des expériences, font des observations et réalisent d'autres activités afin de recueillir les informations nécessaires pour tester leurs hypothèses et répondre à la question de recherche. À ce stade, la gestion de l'accès aux installations physiques et aux données – par le biais du contrôle de l'accès, de la cybersécurité et de restrictions de déplacement – est essentielle pour protéger la recherche sensible préoccupante. En vertu de la politique RTSAP, les équipes de recherche doivent surveiller leurs collaborations et leurs

partenariats pendant la phase active de la recherche (ISDE, 2023f). Une surveillance continue du projet de recherche par les chercheurs et, le cas échéant, par les membres des peuples autochtones est nécessaire pour évaluer si les mesures de protection mises en œuvre sont appropriées.

4.2.1 Contrôle de l'accès aux installations de recherche

Le contrôle de l'accès aux installations de recherche est une mesure critique et couramment utilisée pour protéger la recherche sensible préoccupante. Elle s'applique tout au long du processus de recherche (COGR, 2023; CE, 2024b; JASON, 2024). Si le contrôle de l'accès aux installations de recherche, les habilitations de sécurité et d'autres mesures restrictives peuvent empêcher certains chercheurs de participer aux expériences, des règles claires en matière de sécurité physique et de cybersécurité sont également à même de favoriser le partage d'informations et la collaboration, en créant un environnement sûr où les chercheurs peuvent échanger librement leurs connaissances. « Dans le domaine de la recherche en technologie aérospatiale, une habilitation de sécurité est nécessaire pour travailler sur certains projets de recherche financés par RDDC et d'autres ministères. L'existence de règles claires concernant l'accès aux différentes parties du laboratoire permet aux chercheurs qui ne disposent pas de l'habilitation de sécurité nécessaire de poursuivre leurs travaux de recherche fondamentale » (P. Ferguson, communication personnelle, 2024).

APPLICATION DES MESURES :

Accès contrôlé aux installations de recherche portant sur les agents pathogènes

Il est courant que les installations publiques et privées menant des recherches sur les agents pathogènes établissent différents niveaux d'accès aux différentes parties de l'installation (voir p. ex. GC, 2009, 2024d; Gouv. de l'Australie, 2024). Les conditions d'accès établies dans la Norme canadienne sur la biosécurité (NCB) sont fondées sur le principe du besoin de savoir, qui « restreint l'accès à des espaces précis, des matières réglementées et des ressources connexes [...] aux personnes qui en ont besoin pour assumer les responsabilités relatives à leurs postes » (ASPC, 2024f). La NCB fait la distinction entre l'accès limité et l'accès restreint (ASPC, 2022) :

- *L'accès limité* s'applique au personnel et aux visiteurs autorisés et est contrôlé par l'application de moyens opérationnels (p. ex. la supervision par du personnel autorisé) ou à l'aide d'une barrière physique.

(continue)

(a continué)

- *L'accès restreint* s'applique au personnel autorisé et est contrôlé par une barrière physique. Les exigences en matière d'accès restreint s'appliquent aux parties de l'installation désignées comme zones de confinement et zones ABCSE.

4.2.2 Cybersécurité

Les stratégies de cybersécurité à l'échelle de l'organisation qui définissent les politiques, les normes, les rôles et les responsabilités; la gestion de l'identité numérique; les mesures visant à remédier aux vulnérabilités et à gérer les menaces; les programmes de formation et de sensibilisation; ainsi que la planification de la continuité des activités peuvent toutes aider les établissements de recherche à atténuer les risques liés à la cybersécurité (UFIT, 2021). Shankar et Drake (2022) font la distinction entre la cybersécurité institutionnelle et la cybersécurité de la recherche. Ils définissent cette dernière comme un sous-ensemble de la cybersécurité institutionnelle qui applique « la cybersécurité à la recherche de manière à accélérer cette dernière, tout en limitant les risques pour la mission de recherche ». Pour être efficace, un programme de cybersécurité appliqué à la recherche doit être conçu en tenant compte des chercheurs et de leur mission, réduire la charge que représentent la cybersécurité et la conformité pour les chercheurs et garantir la sécurité tout au long du processus de recherche (Shankar et Drake, 2022).

APPLICATION DES MESURES :

La cybersécurité au sein du réseau Ocean Tracking Network

Le réseau Ocean Tracking Network (OTN), financé par la FCI, comprend des infrastructures comme « des émetteurs acoustiques et satellitaires, des lignes de réception, une capacité de stockage de données et divers équipements océanographiques physiques ». Les données collectées à l'aide de cette infrastructure sont stockées dans une base de données. L'OTN a élaboré les documents suivants pour appuyer la préservation et la gestion des données océaniques : un plan de gestion des données; un plan de mise hors service des données; ainsi qu'un plan de cybersécurité qui répertorie les ressources et les actifs cybernétiques, décrit les risques et les stratégies d'atténuation et définit les mécanismes de contrôle des données.

(OTN, 2024)

Depuis le début de la pandémie de COVID-19, le Centre canadien pour la cybersécurité a observé un volume important d'activités malveillantes dirigées contre les organismes de recherche canadiens, incluant les laboratoires de recherche (Centre pour la cybersécurité, 2024a). La numérisation de la recherche et l'utilisation de systèmes informatiques intégrés pour mener des expériences avec des agents pathogènes et des toxines ont fait des laboratoires de recherche des cibles faciles pour les tentatives de cyberinterférence (Centre pour la cybersécurité, 2024a). Malgré les problèmes détectés par le Centre canadien pour la cybersécurité, la NCB et d'autres politiques qui encadrent les installations de recherche travaillant avec des agents pathogènes et des toxines ne prévoient pas d'exigences en matière de cybersécurité applicables à toutes les installations agréées.

APPLICATION DES MESURES :

Exigences en matière de cybersécurité pour les installations de niveau de confinement 4

L'ASPC prévoit d'introduire en 2026 des exigences supplémentaires en matière de cybersécurité pour les installations de niveau de confinement 4. Il existe actuellement une seule installation de ce type, le Laboratoire national de microbiologie situé au Centre scientifique canadien de santé humaine et animale à Winnipeg, au Manitoba (GC, 2019b; ASPC, 2024f, 2025b). En 2024, la Vaccine and Infectious Disease Organization (VIDO) était en train de mettre en place une autre installation de niveau 4 à Saskatoon (VIDO, s.d.). Les installations de niveau 4 devront mettre en œuvre un plan de cybersécurité, des politiques sur l'utilisation des appareils numériques et un système d'étiquetage, de traitement et de restriction d'accès relativement aux informations sensibles (ASPC, 2024f).

4.2.3 Politiques en matière de voyages

Au Canada, l'un des principaux documents régissant les voyages internationaux des chercheurs est le Guide sur la sécurité en voyage à l'intention du personnel et des chercheurs universitaires, élaboré par U15 (association de quinze grandes universités de recherche du Canada) et Universités Canada (U15 et Universities Canada, 2019a). Ce document, qui n'est pas propre à un pays en particulier et n'a pas force obligatoire, contient un certain nombre de recommandations sur la manière dont les chercheurs peuvent renforcer leur sécurité personnelle et leur cybersécurité lorsqu'ils voyagent à l'étranger, notamment :

- « Ne voyagez pas avec des appareils et des documents superflus (listes de contacts, fichiers électroniques, etc.). Avant de voyager, réfléchissez aux données dont vous aurez besoin. N'apportez que le minimum.
- « Chiffrez et transférez vos données sur un périphérique de stockage externe que vous garderez avec vous en tout temps pendant votre voyage. Conservez les mots de passe pour vos données dans un endroit distinct.
- « Ne laissez jamais vos appareils hors de votre vue pendant votre voyage. Si vous les perdez de vue, vous devez supposer qu'ils ont été exposés à des risques.
- « Ne branchez aucun appareil inconnu (clé USB, caméra, cadre pour photo numérique, etc.) à votre matériel. Si vous devez absolument le faire pour un exposé lors d'une conférence, vous devez supposer que votre appareil a été exposé à des risques.
- « Si possible, évitez d'accéder à des données stockées dans un nuage pendant vos déplacements. Si vous en avez absolument besoin, assurez-vous d'y accéder seulement à partir de vos appareils personnels et sécurisés.
- « Si votre appareil est perdu ou volé, informez immédiatement votre service de TI.
- « Évitez de parler des aspects délicats de vos travaux de recherche (ou de vos futurs travaux de recherche) dans les lieux publics ou avec des personnes que vous connaissez depuis peu de temps.
- « Portez attention à l'évolution de vos relations, surtout les nouvelles relations et celles avec des ressortissants étrangers. N'acceptez pas la compagnie de gens que vous ne connaissez pas pendant votre voyage. »

(U15 et Universities Canada, 2019a)

Le SCRS a également publié un guide sur la sécurité de la recherche destiné aux entreprises, aux industries et aux établissements d'enseignement (SCRS, 2020). Ce guide contient un large éventail de recommandations visant à atténuer les risques pour la sécurité personnelle et la cybersécurité liés au renseignement étranger, au terrorisme et aux menaces économiques lors de la préparation d'un voyage à l'étranger et pendant les visites internationales. Il couvre des sujets comme la protection des renseignements personnels et sensibles lors d'une demande de visa, la vigilance à exercer dans les aéroports et les hôtels, ainsi que la cybersécurité (SCRS, 2020). Plusieurs universités canadiennes ont également établi des politiques de sécurité des voyages qui désignent les bureaux responsables de la formation, de l'enregistrement des voyageurs à l'étranger et de la communication avec eux (voir p. ex. uOttawa, 2022; HEC Montréal, 2023).

Le gouvernement des États-Unis a introduit des exigences juridiquement contraignantes en matière de sécurité des voyages à l'étranger pour les organismes de recherche financés par le gouvernement fédéral (NSTC, 2022). Les organismes de recherche doivent établir des politiques en matière de voyage à l'étranger pour les membres du corps professoral et le personnel. Ces politiques peuvent inclure un registre des voyages et, si nécessaire, des exigences d'autorisation de voyage et d'enregistrement, une formation à la sécurité et une assistance relativement à la sécurité numérique (NSTC, 2022).

4.2.4 Surveillance de la recherche par les peuples autochtones

La surveillance de la recherche autochtone par les peuples autochtones leur permet de garder un contrôle permanent sur la manière dont leurs données sont stockées, traitées et mises en commun tout au long du processus de recherche (ITK, 2018; CGIPN, s.d.). Dans certains cas, cette surveillance a été officialisée. Par exemple, le Programme de lutte contre les contaminants dans le Nord du gouvernement du Canada, qui a été mis en place pour réduire la contamination des espèces sauvages, permet la communication entre les chercheurs et les communautés autochtones par l'intermédiaire de comités régionaux de lutte contre les contaminants (GC, 2024i). Aux États-Unis, des comités d'éthique tribaux contrôlés par les Nations tribales surveillent et examinent les recherches au nom de la communauté (Around Him *et al.*, 2019). Des systèmes officiels de surveillance autochtone des phases actives de la recherche pourraient être étendus au Canada, mais ils nécessitent des « ressources et des capacités adéquates, conformes aux valeurs des peuples autochtones concernés » (CAC, 2023a).

APPLICATION DES MESURES :

Étiquetage des données océaniques par les peuples autochtones

Les systèmes d'étiquetage des données contrôlés par les peuples autochtones peuvent également soutenir la surveillance continue de la phase active de la recherche, conformément au principe de souveraineté des données (ONC, 2023). En 2023, Réseaux océaniques Canada (ONC) et le Système intégré d'observation des océans du Canada (SIOOC) ont poursuivi un projet pilote en collaboration avec des communautés autochtones côtières, mettant en œuvre un outil d'étiquetage des ensembles de données développé par l'organisme Local Contexts. Les communautés peuvent créer et appliquer une

(continue)

(a continué)

étiquette personnalisée à un ensemble de données en ajoutant « des informations sur la provenance et des métadonnées contextuelles (y compris les noms des communautés), des protocoles, ainsi que des autorisations d'accès, d'utilisation et de diffusion ». Ce système d'étiquetage assure une accessibilité transparente, mais contrôlée des données conforme aux principes CARE de gouvernance des données autochtones (ONC, 2023). Ces principes renforcent la sécurité culturelle des données et contribuent à garantir que les peuples autochtones les contrôlent et tirent profit de leur mise en commun (Carroll *et al.,* 2021; GIDA, s.d.). Certains chercheurs estiment que les principes CARE constituent une base importante pour travailler avec les données autochtones et qu'ils évolueront et mûriront à mesure qu'ils seront appliqués dans les communautés autochtones (Carroll *et al.,* 2021).

En l'absence de mécanismes formels de suivi de la recherche, les chercheurs peuvent s'appuyer sur des lignes directrices élaborées conjointement avec les communautés autochtones (p. ex. le guide de l'Ocean Frontier Institute sur la participation des communautés autochtones) ainsi que sur une participation communautaire adaptée à la culture (p. ex. présentations communautaires, affiches, vidéos et films, émissions de radio, résumés de projets, brochures) afin de faciliter la communication continue et accessible des résultats de la recherche aux communautés (ITK et NRI, 2007; OFI, 2022). La rétroaction des communautés peut aider les chercheurs à reconnaître les aspects sensibles ou controversés de leurs recherches avant leur publication (ITK et NRI, 2007). « Le fait d'être accompagné par un membre du comité de chasseurs et de trappeurs lors de la prise d'images de l'érosion des falaises nous a aidés à garantir que nous traitions leurs données en respectant leur culture. Certaines images n'ont jamais été publiées en raison de leur caractère sensible et de leur importance pour la communauté » (D. Whalen, communication personnelle, 2025).

4.3 Phase post-recherche

La phase post-recherche du processus de recherche est axée sur les tactiques de mobilisation des connaissances susceptibles d'accélérer l'adoption et la mise en œuvre des résultats. Des approches responsables en matière de publication des résultats et de mise en commun des données (p. ex. par le biais de restrictions auto-imposées ou d'un examen externe) peuvent aider les chercheurs à faire progresser la science ouverte et à maximiser les avantages de la recherche

sensible, tout en veillant à ce qu'elle reste hors de portée des acteurs malveillants.

4.3.1 Restrictions auto-imposées en matière de publication et de mise en commun des données

Les chercheurs s'appuient sur diverses méthodes de mobilisation des connaissances, notamment des publications et des présentations, pour communiquer les résultats de leurs recherches au grand public et accélérer la mise en œuvre des résultats (CAC, 2024b). Cependant, ce ne sont pas tous les résultats de la recherche qui peuvent ou doivent être rendus publics (p. ex. auprès de personnes qui ne participent pas au projet ou qui ne disposent pas d'une habilitation de sécurité). Étant donné que les résultats de recherche seuls, sans description détaillée des données utilisées et de la méthodologie employée, peuvent dans certains cas présenter des risques importants ou causer des dommages, les chercheurs sont encouragés à évaluer les conséquences possibles de la publication dès le début du projet de recherche et à évaluer ces risques en continu tout au long du processus (ASPC, 2018a; Leopoldina et DFG, 2022b). Parfois, les chercheurs sont en mesure de modifier les données de recherche, de les expurger ou d'en limiter l'accès d'une autre manière sans nuire à leur capacité de publier dans l'ensemble (NPSA et NCSC, 2024). Selon Inglesby (2024), cette option est toutefois problématique dans bien des cas, car « toute tentative d'expurger ou de supprimer des résultats dans le domaine des sciences de la vie a provoqué d'énormes controverses scientifiques dans le passé. [...] Les revues ne sont pas susceptibles d'accepter de participer à ce genre de pratique et la communauté scientifique elle-même a sévèrement critiqué les scientifiques ayant tenté de le faire antérieurement ». En dernier recours, les chercheurs peuvent également envisager de retarder la publication des résultats ou de ne pas les publier du tout. Toutefois, la décision de ne pas publier doit être mûrement réfléchie au regard des politiques applicables en matière de financement de la recherche, sans oublier les principes régissant la conduite

Des approches responsables en matière de publication des résultats et de mise en commun des données (p. ex. par le biais de restrictions auto-imposées ou d'un examen externe) peuvent aider les chercheurs à faire progresser la science ouverte et à maximiser les avantages de la recherche sensible, tout en veillant à ce qu'elle reste hors de portée des acteurs malveillants

responsable de la recherche, la recherche ouverte et le libre-échange des informations (MPG, 2017; CRSNG, 2018; ASPC, 2018a; GC, 2022b).

4.3.2 Examen externe des résultats de recherche avant leur publication

L'examen préalable à la publication des résultats de recherche peut être exigé par les conditions générales des contrats de recherche, en particulier lorsque des recherches sensibles préoccupantes sont financées ou approuvées par des ministères et organismes gouvernementaux ou des bailleurs de fonds privés (Shea, 2006). « La technologie aérospatiale est un domaine de recherche sensible. Lorsque la recherche est financée par des fonds privés, l'examen préalable à la publication des articles par le bailleur de fonds peut être inclus dans les conditions du contrat de recherche. » (P. Ferguson, communication personnelle, 2024) Mentionnons que les lois et règlements fournissent des orientations plus claires sur les transferts de biens et de technologies que sur le partage des données et la publication des résultats de la recherche (GC, 2025f) (section 3.2.1).

APPLICATION DES MESURES :

Publication des résultats de la recherche océanographique

Dans le domaine de la recherche océanographique, des restrictions à la publication et à la mise en commun des données peuvent être imposées au cas par cas (p. ex. par le biais de contrats de recherche et du principe de souveraineté des données; section 4.3.3). Le comité et les experts interrogés n'ont pas connaissance de politiques ou de règlements limitant la mise en commun ouverte des données océanographiques. La plateforme nationale de données océaniques du SIOOC collabore ainsi au cas par cas avec les producteurs de données afin de traiter les questions sensibles liées à leurs données (SIOOC, s.d.-c). L'OTN traite pour sa part toutes les « informations sur la morphologie animale et toute information sur la localisation produite en continue » comme des données restreintes par défaut (OTN, 2024). Cela permet aux chercheurs de demander un embargo de deux ans (qui peut être prolongé au cas par cas) sur la publication des métadonnées relatives au marquage des animaux en raison de leur nature écologique sensible (OTN, 2024). La plupart des données collectées par les observatoires océaniques et côtiers exploités par l'ONC sont disponibles gratuitement en temps quasi réel et peuvent être utilisées par tout un chacun. Font notamment

(continue)

(a continué)

exception à cette règle certaines données sismiques et hydrophoniques, qui sont filtrées par les marines canadienne et américaine pour des raisons de sécurité nationale. En effet, de telles données courent le risque d'être détournées avant leur archivage (ONC, 2021a) (section 3.1).

APPLICATION DES MESURES :

Publication de la recherche sur les agents pathogènes

Les documents d'orientation publiés par l'ASPC ne contiennent pas de lignes directrices juridiquement contraignantes sur la manière dont l'examen préalable à la publication des données et des articles sur les agents pathogènes doit être effectué, ni sur les personnes qui doivent s'en charger (ASPC, 2018a). La Ligne directrice canadienne sur la biosécurité : le double usage dans la recherche en sciences de la vie (Ligne directrice sur le double usage) prévoit que chaque projet de recherche doit être examiné pour évaluer « la possibilité de double usage lors de l'étape de la planification, pendant toute la durée du travail (même lorsqu'il y a des résultats inattendus) et avant d'utiliser les résultats ou les diffuser (p. ex. la publication) ». Les établissements de recherche sont encouragés à adopter un plan de communication sur les informations (p. ex. les données de recherche, les protocoles expérimentaux) qui seront mises en commun, incluant le contenu à communiquer, le public cible et la méthode de communication. La Ligne directrice sur le double usage « vise à aider les parties réglementées à satisfaire aux exigences énoncées dans la NCB ». Les établissements de recherche peuvent toutefois choisir d'autres approches pour élaborer des plans de communication et gérer les risques liés à la communication (ASPC, 2018a).

La Ligne directrice sur le double usage de l'ASPC souligne le rôle des rédacteurs et des codes de conduite éditoriale dans la limitation de la publication des RDUP, mais ce rôle reste contesté (ASPC, 2018a). Si les rédacteurs peuvent fournir des commentaires sur les implications potentielles des articles de recherche, ils peuvent tout aussi bien ne pas disposer de l'expertise et de la formation nécessaires pour le faire (NASEM, 2017).

Le gouvernement des États-Unis a mis en place une surveillance plus stricte de la communication de la recherche à double usage financée

(continue)

(a continué)

par le gouvernement fédéral et portant sur les agents pathogènes et les toxines (Gouv. des États-Unis, 2024b). Le guide de mise en œuvre de la politique du gouvernement américain relative à la surveillance de la recherche à double usage préoccupante et des agents pathogènes présentant un potentiel pandémique accru[13] (le « Guide de mise en œuvre ») prévoit que les établissements de recherche doivent élaborer un plan de conduite et de communication de la recherche devant être approuvé par l'organisme de financement. Les chercheurs ont la responsabilité première de veiller à ce que toutes les communications, incluant celles traitant de la recherche, respectent le plan approuvé (Gouv. des États-Unis, 2024b). D'après l'expérience du comité, les articles de recherche sur le gain de fonction mentionnent souvent les pratiques de biosécurité et de biosûreté dans la section consacrée aux matériaux et méthodes, à titre de mesure de sécurité.

4.3.3 Examen préalable à la publication des résultats de recherche par les communautés autochtones

Afin de garantir la souveraineté des données, les données et les systèmes de connaissances autochtones doivent faire l'objet d'une attention particulière lors de la phase de publication du processus de recherche. La Global Indigenous Data Alliance souligne que « l'accent mis sur une mise en commun accrue des données crée à lui seul une tension pour les peuples autochtones qui revendiquent également un contrôle accru sur l'application et l'utilisation des données comme des connaissances autochtones pour le bénéfice de tous » (GIDA, s.d.). Les Autochtones et les non-Autochtones peuvent avoir des points de vue différents sur la vie privée et la confidentialité, qui font partie intégrante de la souveraineté des données (CAC, 2023a). Par exemple, le Guide des Premières Nations relatif à la Loi sur la protection des renseignements personnels rédigé par le CGIPN mentionne qu'une grande partie des données sur les Premières Nations détenues par la Couronne ne sont pas considérées comme des renseignements personnels au sens de la Loi et que cette dernière « ne reconnaît pas et ne prend pas en compte les droits collectifs des Premières Nations en matière de protection des renseignements personnels [...] [et leur refuse] le même respect que celui qu'elle accorde aux autres gouvernements, y compris les gouvernements étrangers, les provinces et les municipalités » (CGIPN, 2024). Or, la conception de la vie privée par les

13 *Implementation Guidance for the United States Government Policy for Oversight of Dual Use Research of Concern and Pathogens with Enhanced Pandemic Potential.*

communautés autochtones peut aller au-delà des données sur les personnes et inclure d'autres connaissances (p. ex. les pratiques de chasse et de cueillette, les cérémonies) (Snipp, 2016). La communication et la diffusion des résultats de la recherche aux communautés autochtones reposent souvent sur des méthodes semblables à celles utilisées pour la surveillance de la recherche (section 4.2.4), car ces deux phases du processus sont étroitement liées et doivent être guidées par les priorités comme les valeurs de la communauté.

4.4 Protéger le cycle de vie de la recherche

Au Canada, les chercheurs, les établissements, les gouvernements et les peuples autochtones ont mis en place des mesures pour protéger la recherche sensible préoccupante. Dans la pratique, la recherche sur les agents pathogènes fait l'objet d'une protection accrue en raison du risque élevé d'effets négatifs sur la santé humaine en cas d'incidents motivés – ou non – par des intentions malveillantes, par rapport à la recherche océanographique. Pour toute la recherche sensible préoccupante, il est important de réévaluer et, si nécessaire, de modifier ces mesures tout au long du processus afin d'assurer un juste équilibre entre la sécurité et la transparence. Bien que l'on suppose souvent que les chercheurs, en tant qu'experts en la matière et bénéficiaires de fonds de recherche, devraient assumer la responsabilité principale de la protection de la recherche sensible préoccupante, la mise en œuvre réussie de ces mesures repose sur la responsabilité partagée de tous les acteurs de l'écosystème : chercheurs, établissements, gouvernements et peuples autochtones.

La mise en œuvre réussie de ces mesures repose sur la responsabilité partagée de tous les acteurs de l'écosystème

La répartition des responsabilités au sein de l'écosystème de la recherche peut varier en fonction de la phase du processus, des types de recherche, de la source de financement et du fait que le projet implique ou non des peuples autochtones et leurs terres. Les considérations suivantes sont à même d'aider tous les acteurs de l'écosystème à évaluer qui doit participer pour garantir la mise en œuvre efficace des mesures visant à protéger la recherche sensible préoccupante :

- **Expertise** : La mise en œuvre efficace des mesures de protection dépend de l'expertise dans le domaine de recherche concerné, ainsi que des connaissances spécialisées relativement à la sécurité de la recherche et aux principes de science ouverte. Voici quelques exemples de mesures :

restrictions volontaires en matière de publication et de mise en commun des données, examen externe des résultats de la recherche avant leur publication.

- **Capacités et ressources** : Les acteurs ayant accès à des infrastructures, à des ressources (p. ex. du personnel, des outils, des programmes de formation) et à des communautés de pratique sont souvent mieux équipés pour soutenir la mise en œuvre des mesures de sécurité de la recherche. Voici quelques exemples de mesures : accès contrôlé aux installations de recherche, cybersécurité, politiques en matière de voyages.
- **Engagements juridiques :** Les lois, les règlements, les obligations contractuelles et les accords de financement peuvent attribuer la responsabilité et l'obligation de rendre compte de la mise en œuvre des mesures de protection à des acteurs précis. Voici quelques exemples de mesures : filtrage des chercheurs et des propositions de recherche, interdiction des partenariats et des collaborations, et dispositions de sécurité dans les accords de recherche.
- **Droits des peuples autochtones et souveraineté des données** : Les peuples autochtones devraient guider l'élaboration et la mise en œuvre de toutes les mesures visant à protéger la recherche sensible préoccupante qui est menée dans leurs communautés et sur leurs terres.

La clé du succès réside dans l'allocation de ressources et la mise en place de systèmes décisionnels qui soutiennent les chercheurs et les établissements dans ces efforts. Ces mêmes facteurs favorables devraient s'étendre aux Premières Nations, aux Inuits et aux Métis afin de garantir le droit des peuples autochtones à déterminer ce qui constitue une recherche sensible préoccupante dans leurs communautés et la manière de la protéger.

Les mesures visant à protéger la recherche sensible préoccupante varient quant à la portée et la complexité, mais se heurtent à des obstacles similaires en raison de la fragmentation du paysage de la sécurité de la recherche, de la répartition inéquitable des responsabilités touchant la protection de la recherche sensible, du manque de capacités et des effets dissuasifs de la sécurité de la recherche sur les collaborations et la recherche ouverte. Le chapitre 5 examine les facteurs qui permettraient de relever ces défis afin de mettre en place un système de recherche le plus ouvert et le plus sûr possible.

5

Assurer la sécurité de la recherche tout en préservant l'ouverture scientifique

5.1 Systèmes de soutien à la mise en commun des connaissances

5.2 Renforcement des capacités et formation

5.3 Ressources financières

5.4 Application de la conformité

5.5 Favoriser une philosophie moderne de la recherche

Constatations du chapitre

- Les facteurs qui favorisent les mesures de sécurité de la recherche peuvent également s'appliquer à la science ouverte. En effet, la détermination du niveau d'ouverture et de sécurité de la recherche repose sur les mêmes conditions favorables, notamment les ressources financières.
- Pour les chercheurs, la conciliation entre science ouverte et sécurité de la recherche repose sur l'éducation, la formation et le renforcement des capacités aux niveaux individuel et institutionnel.
- Les approches divergentes en matière de sécurité de la recherche au Canada et dans d'autres pays créent de la confusion et réduisent l'adhésion des chercheurs. L'harmonisation des systèmes de soutien à la mise en commun des connaissances dans l'ensemble de l'écosystème de la recherche et l'affectation de ressources à l'évaluation des résultats des mesures de sécurité peuvent améliorer l'efficacité.
- Pour généraliser la sensibilisation aux questions de sécurité, il faut changer la culture : la *philosophie moderne de la recherche* englobe en effet la conscience des risques, parallèlement à l'intégrité et à la conduite responsable.

L'impact et le succès éventuel des mesures visant à reconnaître et à protéger la recherche sensible (chapitres 3 et 4) dépendent en partie de facteurs favorables. Or, à l'heure actuelle, le soutien à la mise en œuvre de ces mesures est inégal et insuffisant dans certains secteurs, les divers acteurs du système étant touchés de manière différente. Les acteurs universitaires, gouvernementaux et privés sont soumis à des incitatifs variés et disposent de capacités différentes lorsqu'ils sont confrontés à la perspective d'adopter de nouvelles pratiques en matière de sécurité de la recherche ou de science ouverte, en particulier dans les domaines où ces pratiques sont nouvelles et où l'expérience est limitée. Dans plusieurs cas, les mêmes mesures de soutien s'appliquent à la sécurité de la recherche et à la science ouverte; la détermination du niveau d'ouverture et de sécurité repose donc sur les mêmes conditions favorables. Les systèmes de soutien à la mise en commun des connaissances (section 5.1), le renforcement des capacités et de la formation (section 5.2), le financement (section 5.3) et l'application des règles (section 5.4) sont tous nécessaires pour reconnaître et protéger la recherche sensible, tout en soutenant potentiellement la science ouverte et l'innovation.

5.1 Systèmes de soutien à la mise en commun des connaissances

Au Canada, les approches juridictionnelles en matière de sécurité de la recherche diffèrent, ce qui complique les partenariats interinstitutionnels et la mise en œuvre cohérente des politiques de sécurité de la recherche à l'échelle du pays (Université de Calgary et Université de l'Alberta 2023; SRO, 2024a). Cette variation a une incidence sur le financement public, car certains bailleurs de fonds alignent leurs efforts en matière de sécurité de la recherche sur les programmes fédéraux (p. ex. en utilisant la politique RTSAP et les LDSNPR comme référence) tout en imposant des exigences supplémentaires (Mitacs, 2023; Gouv. de l'Ont., 2024a). Parallèlement, les organismes et ministères fédéraux ont également leurs propres politiques en la matière (voir p. ex. CNRC, 2024). D'après l'expérience du comité, ce manque d'harmonisation impose des charges supplémentaires aux chercheurs, ce qui ralentit la recherche collaborative entre les établissements canadiens et réduit l'adhésion à la mise en œuvre de mesures de sécurité. Cette question ne se limite pas à la collaboration au sein du Canada : les différentes approches de la sécurité de la recherche entre les pays alliés peuvent réduire l'efficacité des efforts mondiaux et poser un défi aux chercheurs qui tentent de mener des collaborations internationales de manière responsable et sécuritaire. Au niveau international, le partenariat du Groupe des cinq et le G7 ont introduit des lignes directrices et des politiques à l'intention des chercheurs universitaires, des gouvernements et du secteur privé afin d'harmoniser les approches entre les États membres (SIGRE, 2022; SCRS, 2024a,c). Le comité souligne que l'harmonisation n'est pas synonyme de normalisation. L'utilisation de critères de base communs – constitués notamment de principes fondamentaux et d'approches permettant de relever les défis, tout en conservant des processus uniques adaptés à des circonstances particulières – serait un moyen de réduire les répétitions et la charge qui pèse sur les chercheurs et les

Au Canada, les approches juridictionnelles en matière de sécurité de la recherche diffèrent, ce qui complique les partenariats interinstitutionnels et la mise en œuvre cohérente des politiques de sécurité de la recherche à l'échelle du pays

Les différentes approches de la sécurité de la recherche entre les pays alliés peuvent réduire l'efficacité des efforts mondiaux et poser un défi aux chercheurs qui tentent de mener des collaborations internationales de manière responsable et sécuritaire

établissements chargés de mettre en œuvre les politiques entourant la sécurité de la recherche et la science ouverte.

Compte tenu de la nature fragmentée des mécanismes de reconnaissance et de protection de la recherche sensible, la création d'organismes de soutien chargés de recueillir et d'échanger des informations sur les approches existantes est essentielle pour favoriser la cohérence dans l'ensemble de l'écosystème de la recherche, tant au Canada que dans les autres pays. Parmi les stratégies susceptibles de remédier à cette fragmentation, on peut citer la création de centres spécialisés fournissant des conseils en matière de recherche, l'organisation de tables rondes et de groupes consultatifs nationaux, ainsi que la mesure et l'évaluation des activités de sécurité de la recherche.

Les centres spécialisés peuvent fournir des conseils adaptés sur la sécurité de la recherche et coordonner les efforts au sein des pays

Alors qu'au Canada, la sécurité de la recherche est répartie entre différents ministères et organismes (section 2.4), les Pays-Bas ont adopté une approche pangouvernementale et créé un point de contact national interministériel pour la sécurité des connaissances afin d'aider les établissements du savoir et leurs affiliés à évaluer les risques comme les opportunités découlant de la coopération internationale (OCW, s.d.-a). Ce service aide les établissements et les chercheurs à se tourner vers les publications et les outils produits par les organismes gouvernementaux et d'autres tiers de confiance, qui produisent par exemple des évaluations des menaces émanant d'acteurs étatiques (voir p. ex. AIVD *et al.*, 2022; OCW, 2023), des conseils sur la manière de concilier les besoins en matière de sécurité et les principes fondamentaux de la liberté et de l'intégrité de la recherche (AWTI, 2022), ainsi que des codes de conduite pertinents visant à compléter les lignes directrices nationales (KNAW *et al.*, 2018; OCW, s.d.-b). Cette approche est similaire à celle adoptée par le bureau de la biosécurité des Pays-Bas pour la surveillance de la recherche sensible préoccupante menée dans le domaine des sciences de la vie (RIVM, s.d.-a,-b). De même, le gouvernement de l'Australie a nommé un coordinateur national de la lutte contre l'ingérence étrangère afin de rationaliser les efforts visant à contrecarrer cette dernière au sein du gouvernement, ainsi qu'auprès des acteurs non gouvernementaux à haut risque, comme les établissements de recherche (UFIT, 2021; Gouv. de l'Australie, 2025).

Au Royaume-Uni, la Research Collaboration Advice Team [équipe consultative sur la collaboration en recherche] (RCAT) est une initiative de coopération mise en place entre le gouvernement et le monde universitaire pour fournir aux établissements des conseils officiels sur la sécurité de la recherche dans le cadre de partenariats internationaux (RCAT, s.d.). Cette initiative joue un rôle

important en aidant le gouvernement à comprendre la manière dont les universitaires conçoivent et gèrent les risques; elle se consacre à envisager des moyens d'améliorer initiatives et pratiques (d'Hooghe et Lammertink, 2022). La RCAT a été bien accueillie par la communauté scientifique britannique : on salue le fait qu'elle favorise la coordination entre les différents acteurs et qu'elle fait ressortir l'importance de la gestion des risques et de la sensibilisation (d'Hooghe et Lammertink, 2022; Department for Science, Innovation & Technology, 2023).

En 2024, la National Science Foundation (NSF) a annoncé la création du SECURE Center, piloté par l'Université de Washington et soutenu par neuf autres établissements (NSF, 2024b). Le SECURE Center a été créé pour servir de centre d'échange d'informations et aider la communauté scientifique à reconnaître et à atténuer l'ingérence étrangère. Il a pour mission de « publier des informations et des rapports sur les risques liés à la sécurité de la recherche, de dispenser des formations sur la sécurité de la recherche à la communauté scientifique et technique et de servir de pont entre la communauté scientifique et les organismes publics de financement ». Le SECURE Center servira également de plaque tournante pour plusieurs centres régionaux gérés par six universités du pays. Les experts de ces établissements « apporteront leur expertise sur la recherche sensible, les types de menaces, l'analyse géopolitique et la collaboration internationale », tandis que le NSF SECURE Analytics, dirigé par l'Université Texas A&M, prévoit de « fournir une expertise renforcée sous forme d'analyses du contexte, de modélisation des risques et de communication des données par l'intermédiaire du SECURE Center ». Ce centre n'étant pas encore pleinement opérationnel, son efficacité ne peut être évaluée (NSF, 2024b).

Au Canada, le Centre de la sécurité de la recherche, géré par SP, est chargé d'une mission semblable à celle du SECURE Center, à savoir fournir des orientations et des conseils à la communauté des chercheurs sur la manière de protéger leurs travaux (GC, 2024j). Le Centre de la sécurité de la recherche est composé d'un réseau de six conseillers en sécurité de la recherche répartis dans tout le Canada, avec un centre névralgique basé à Ottawa (SP, 2024a). Chaque conseiller est chargé de fournir des conseils aux établissements de sa région, mais le comité note que les régions sont très étendues géographiquement, ce qui fait qu'un conseiller doit s'occuper de nombreux établissements. Cette approche peut être particulièrement efficace lorsque les conseils doivent être fournis dans un délai précis. C'est par exemple le cas pour le point de contact national pour la sécurité des connaissances aux Pays-Bas, qui vise à fournir un service dans les 48 heures (OCW, s.d.-a,-c).

Le SCRS fait également progresser la sécurité de la recherche en offrant des ressources accessibles au public et en collaborant directement avec les communautés universitaires de recherche dans le cadre du programme Liaison-recherche et collaboration avec les intervenants (LRCI). Une liaison est également en place avec les investisseurs du secteur privé dans le cadre de l'initiative Innover en toute sécurité (SCRS, 2024a,d). Le programme LRCI organise des tables rondes et des ateliers, participe à des conférences et produit des documents sur demande afin de dialoguer avec divers secteurs concernés par la sécurité de la recherche (SCRS, 2024b, 2025). Cependant, les membres du comité soulignent que le SCRS ne peut diffuser que des informations limitées par le biais de ces ressources pour des raisons de sécurité, et que les informations disponibles ne parviennent pas toujours aux chercheurs du monde universitaire et de l'industrie.

De plus, le comité reconnaît que, lorsque des informations sur les menaces à la sécurité de la recherche sont communiquées au public, elles peuvent être exploitées par des acteurs malveillants pour causer du tort, et que ces risques doivent être soigneusement contrebalancés par les avantages de tenir l'écosystème de la recherche informé d'éventuelles menaces. La mise en commun d'informations par le SCRS pourrait être améliorée à l'avenir grâce à des modifications législatives apportées à la *Loi sur le Service canadien du renseignement de sécurité* par le biais du projet de loi C-70 afin de permettre « la divulgation d'informations, sous réserve des mesures de protection de la vie privée, à des personnes et à des organisations à l'extérieur du gouvernement du Canada, afin de les aider à renforcer leur résilience face aux menaces qui pèsent sur la sécurité du Canada » (SP, 2024d). De l'avis du comité, l'amélioration continue des canaux de communication entre la communauté du renseignement, les chercheurs et les administrations institutionnelles serait à même de sensibiliser les chercheurs et de les inciter à intégrer la sécurité de la recherche dans leurs activités quotidiennes.

Des communautés de pratique sur la sécurité de la recherche ont été créées pour établir des ponts entre différents secteurs et mettre en commun les connaissances

En 2020, le gouvernement des États-Unis a créé la National Science, Technology and Security Roundtable [table ronde nationale sur la science, la technologie et la sécurité], un forum permettant aux acteurs des secteurs gouvernemental, universitaire et industriel de mettre en commun leurs connaissances sur la sécurité de la recherche (NASEM, 2024). L'événement de clôture de 2024, qui a marqué la fin du mandat de quatre ans de la table ronde, a « examiné les approches efficaces pour communiquer les menaces et les risques [et] [...] mis

en commun les meilleures pratiques pour traiter et atténuer les menaces et les risques » (NASEM, 2024). Bien que cette table ronde soit désormais dissoute, les participants à l'événement de clôture ont souligné qu'« il sera important de disposer d'un forum où le monde universitaire, le secteur privé, les organismes fédéraux de financement de la recherche, les organismes de renseignement et les forces de l'ordre pourront continuer à se réunir pour mener des discussions continues et échanger des informations sur les menaces et les risques liés à la sécurité de la recherche » (NASEM, 2025). Au Royaume-Uni, l'Engineering Biology Responsible Innovation Advisory Panel [comité consultatif sur l'innovation responsable en génie biologique] (RIAP) conseille le gouvernement sur les risques émergents pour l'innovation dans ce domaine. Il est composé de leaders du monde universitaire et de l'industrie (Gouv. du Royaume-Uni, s.d.). Le RIAP assure une communication permanente entre le gouvernement, l'industrie et le monde universitaire, ce qui permet l'élaboration de politiques et la mobilisation de tous les secteurs sur les risques émergents (Gouv. du Royaume-Uni, s.d.). Au Japon, un consortium sur la sécurité et l'intégrité de la recherche au sein du système universitaire a également été proposé afin de soutenir les activités visant à répondre aux préoccupations sur ces sujets, qui suscitent un intérêt croissant dans le pays (Gouv. du Japon, 2023; Université de Tokyo, s.d.).

Enfin, des communautés de pratique ont également vu le jour dans d'autres domaines. Au Canada, les directeurs de la sécurité de la recherche de plusieurs établissements universitaires ont créé l'initiative Équipe Canada, réunissant ainsi des praticiens pour mettre en commun des ressources, discuter des meilleures pratiques et élaborer des stratégies – dans le but de répondre aux besoins des établissements du pays (Universités Canada, 2024). Cette démarche se ramifie à travers des communautés de pratique régionales (p. ex. l'Alberta Research Security Community of Practice; Université de Calgary, 2025).

Le secteur privé contribue considérablement à la recherche au Canada et a besoin d'orientations précises pour soutenir ses efforts sur le plan de la sécurité

Si les forums évoqués plus haut peuvent contribuer à l'élaboration de pratiques prometteuses, les besoins et les capacités du secteur privé diffèrent de ceux des universités et des autres établissements de recherche (CE, 2024a). Au Canada, le secteur privé est un élément important de l'écosystème de la recherche (section 2.1); il finance la majeure partie de la R-D, à hauteur de 32,9 milliards de dollars en 2024, contre 18,5 milliards de dollars pour le secteur de l'enseignement supérieur (StatCan, 2024a). Certains pays, y compris le Canada, ont donc renforcé leur engagement en matière de sécurité de la recherche avec

le secteur privé. Le SCRS organise des séances d'information sur la sécurité de la recherche à l'intention des entreprises du secteur privé qui mènent des recherches dans les domaines de la biopharmacie, des sciences de la vie et des sciences des données (SP, 2024e). En outre, des conseils et de l'éducation en sécurité sont proposés aux investisseurs dans les technologies émergentes, en particulier aux petites et moyennes entreprises, afin de les aider à reconnaître les menaces et les actifs susceptibles d'être compromis, de sécuriser les chaînes d'approvisionnement et de gérer les risques liés à la collaboration et à l'expansion internationale (SCRS, 2024a).

D'autres pays fournissent également des orientations au secteur privé. Au Royaume-Uni, la National Protective Security Authority [autorité nationale de sécurité et de protection] et le National Cyber Security Centre [centre national de cybersécurité] ont concentré leurs efforts sur la protection de jeunes entreprises innovantes et émergentes, dont des sociétés détachées, contre le vol de propriété intellectuelle. La boîte à outils Secure Innovation contient des conseils et des ressources adaptés aux petites entreprises qui pourraient autrement manquer d'expertise et de ressources sur le plan de la cybersécurité (NPSA, 2023). Aux États-Unis, le Center for Security and Emerging Technology[14] [centre pour la sécurité et les technologies émergentes] a recommandé la création d'un centre d'échange d'informations spécialisé dans la sécurité de la recherche, situé au sein des centres de R-D les plus actifs (Flagg et Arnold, 2021). L'objectif d'une telle organisation serait d'échanger des informations et des ressources (notamment pour la formation et l'aide à la décision) avec les chercheurs du secteur privé, tout en assurant la coordination avec les partenaires fédéraux (Flagg et Arnold, 2021). Il n'est toutefois pas certain que cette initiative sera mise en œuvre, ou si l'on prévoit son intégration dans les activités et le mandat du SECURE Center.

Les efforts visant à mesurer et à évaluer l'efficacité des stratégies de sécurité de la recherche en sont à leurs débuts et se heurtent à un manque de preuves et de clarté quant aux méthodes d'étude et aux approches théoriques appropriées

L'analyse des activités de sécurité de la recherche aide à évaluer l'efficacité des mesures

Les efforts visant à mesurer et à évaluer l'efficacité des stratégies de sécurité de la recherche en sont à leurs débuts et se heurtent à un manque de preuves et de clarté quant aux méthodes d'étude et aux approches théoriques appropriées

14 Le Center for Security and Emerging Technology est un organisme de recherche sur les politiques publiques rattaché à la Walsh School of Foreign Service de l'Université de Georgetown.

(Dao *et al.*, 2024). Cette question s'étend également aux directives et politiques entourant la science ouverte. La Politique des trois organismes sur la gestion des données de recherche exige que tous les établissements de recherche qui administrent des fonds de ces trois organismes élaborent une stratégie institutionnelle de gestion des données de recherche (GDR) et que la méthodologie de tous les travaux pour lesquels une demande de subvention est présentée reflète les pratiques exemplaires en matière de GDR. Dans certains cas, la politique exige que les demandeurs fournissent également un plan de gestion des données à l'organisme concerné (GC, 2021b). À l'instar des politiques de sécurité de la recherche, le non-respect de cette politique peut constituer un manquement à la conduite responsable de la recherche (GC, 2021b). Les trois organismes n'évaluent toutefois pas les stratégies institutionnelles (GC, 2024c), et rien n'indique qu'ils assurent une surveillance ou un suivi de la mise en œuvre de cette politique (Tayler *et al.*, 2020).

Les initiatives de science ouverte doivent aussi faire l'objet d'une surveillance afin de mieux comprendre les lacunes et de favoriser la mise en place de solutions (Cobey *et al.*, 2023); or, on sait peu de choses sur l'étendue du respect des politiques de gestion des données et de science ouverte de manière plus générale chez les bénéficiaires de subventions dans le système de recherche canadien (Tayler *et al.*, 2020). Notons que sans une forme d'audit ou d'analyse comparative, il est difficile de suivre les progrès et d'améliorer les processus (Tayler *et al.*, 2020; Moher et Cobey, 2021; Alayche *et al.*, 2023). Même lorsque les recherches financées par les trois organismes doivent être rendues publiques dans les 12 mois suivant leur publication, dans les faits, de nombreux chercheurs ne respectent pas la Politique des trois organismes sur le libre accès aux publications (Larivière et Sugimoto, 2018; Paquet *et al.*, 2022). Cette constatation s'étend également aux essais cliniques, dont l'enregistrement et la publication des résultats (qui sont des composantes de l'écosystème de la science ouverte) sont à la traîne au Canada par rapport à d'autres pays (Alayche *et al.*, 2023). Il semble que le non-respect des mandats n'entraîne pas de conséquences importantes, et que ces conséquences restent vagues (Paquet *et al.*, 2022).

De l'avis du comité, ces lacunes dans la mesure et le suivi de l'efficacité des initiatives en matière de science ouverte s'appliquent également aux mesures de sécurité de la recherche. Certains pays ont lancé des programmes de recherche particuliers pour combler le manque de preuves quant à l'efficacité des politiques de sécurité de la recherche. Ainsi, en 2023, la NSF a annoncé l'élaboration d'un nouveau programme (*The Research on Research Security Program*, RoRS) afin de « mieux comprendre la nature, la portée, les défis et le

potentiel de la sécurité de la recherche dans tous les domaines » (NSF, 2023). La NSF financera des recherches sur divers sujets, notamment :

> *la nature et l'omniprésence des menaces pour la sécurité de la recherche; les méthodes de reconnaissance des risques en la matière et les stratégies visant à les prévenir et à les atténuer; les méthodes de renforcement des protocoles et des approches de sécurité; les relations complexes entre le comportement humain et les politiques de sécurité; ces politiques et leurs implications; la recherche sur les changements organisationnels entourant les facteurs systémiques et culturels en rapport avec la sécurité de la recherche; la recherche sur la sécurité de la recherche dans le contexte d'un domaine ou d'une discipline donné, en particulier dans les domaines à haut risque; [et] les dimensions internationales de la sécurité de la recherche.*
>
> (NSF, 2025)

En Allemagne, l'Association Helmholtz, qui regroupe 18 centres de recherche scientifique, a lancé un programme intitulé « Further Development of Research Security in International Scientific Collaborations » [développement de la sécurité de la recherche dans les collaborations scientifiques internationales], qui soutient des programmes visant à renforcer la sécurité de la recherche dans plusieurs établissements (Helmholtz, s.d.). Parallèlement, l'UE met en place des initiatives visant à surveiller l'efficacité des mesures de sécurité de la recherche et à créer des centres stratégiques (CE, 2024a,b). Enfin, la Commission européenne surveille les progrès réalisés par les États membres dans la mise en œuvre de la recommandation du Conseil de l'Union européenne de 2024 sur la sécurité de la recherche – sur la base d'indicateurs établis – et est invitée à présenter tous les deux ans un rapport de mise en œuvre (CE, 2024a).

De l'avis du comité, la rationalisation et la centralisation des sources d'information sur la sécurité de la recherche au Canada à l'aide de centres spécialisés ou de groupes consultatifs pourraient faciliter l'échange d'informations entre tous les acteurs. L'harmonisation des approches aurait pour sa part l'effet de réduire au minimum la charge administrative qui pèse sur les établissements et les chercheurs. Rappelons que le suivi et la surveillance des approches en matière de sécurité de la recherche et de science ouverte sont nécessaires pour évaluer l'efficacité des différentes stratégies et mécanismes examinés dans le présent rapport, ainsi que pour mieux comprendre les besoins de renforcement des capacités et de formation.

5.2 Renforcement des capacités et formation

Toute mesure visant à reconnaître ou à protéger la recherche sensible doit disposer d'une capacité adéquate : le financement, la formation et les

infrastructures sont en effet indispensables pour garantir que les acteurs bénéficient d'un soutien dans le domaine de la sécurité de la recherche et des activités liées à la science ouverte. De l'avis du comité, l'un des objectifs du renforcement des capacités et de la formation pourrait être l'intégration de la sensibilité aux questions de sécurité. Il est toutefois essentiel que cela se fasse en minimisant la charge qui pèse sur les chercheurs.

Les outils de renforcement des capacités et de mise en œuvre constituent des appuis indispensables pour intégrer les politiques de sécurité de la recherche dans les cultures institutionnelles

Les gouvernements de nombreux pays offrent aux chercheurs des ressources pour reconnaître la recherche sensible. Dans certains cas, où la responsabilité de la reconnaissance incombe principalement aux chercheurs, on ne saurait trop insister sur l'importance d'une conception et d'une diffusion efficaces de l'information à l'appui de cette démarche. Par exemple, le gouvernement allemand ne participe pas directement à la reconnaissance de la recherche sensible ni à l'encadrement des partenariats de recherche en raison du droit à la liberté de la recherche protégé par la Constitution; toutefois, les ministères fédéraux fournissent un soutien et promeuvent les connaissances pertinentes pour la sécurité de la recherche (Gouv. de l'Allemagne, 1949; d'Hooghe et Lammertink, 2022). Bien qu'il existe des comités d'éthique de la recherche spécialisés (KEF) chargés de reconnaître la recherche sensible (section 3.2.2), le processus se déroule sur une base volontaire, le cadre allemand reposant sur la capacité de la communauté scientifique à reconnaître et à comprendre le paysage éthique de ses activités (Jakob *et al.*, 2024). Afin de garantir cette capacité d'autorégulation, des ressources détaillées sur la diligence raisonnable, les risques liés à la cybersécurité, les pratiques recommandées en contexte de collaboration et des modules de formation sur l'établissement de partenariats et d'accords internationaux sont mis à la disposition des chercheurs allemands (DLR, 2022, 2023, 2024; DAAD, s.d.). Des ressources en ligne similaires sont fournies par le gouvernement canadien à la communauté scientifique (GC, 2021e,f; CRSNG, 2024d), mais l'option de se soumettre à un examen de type KEF si un chercheur le souhaite n'existe pas.

Les établissements de recherche peuvent également avoir une certaine part de responsabilité en ce qui touche la formation ou le renforcement des capacités des chercheurs. Par exemple, le Royaume-Uni dispose de lignes directrices sur la sécurité de la recherche qui s'adressent explicitement aux instances dirigeantes des universités, les faisant participer à la fourniture d'un point de contact centralisé pour les chercheurs et d'un soutien adéquat (d'Hooghe et

Lammertink, 2022; Universities UK *et al.*, 2022). Le cadre de lutte contre l'ingérence étrangère de l'Australian Research Council (ARC) détaille quant à lui la responsabilité des universités bénéficiant de subventions de l'ARC pour ce qui est de la formation et de l'éducation du personnel en matière de divulgation appropriée. La détection et le signalement des risques relèvent également de leur responsabilité (ARC, 2023). De nombreux établissements de recherche au Canada disposent désormais de bureaux et de responsables de la sécurité de la recherche qui fournissent des conseils aux chercheurs et leur communiquent les meilleures pratiques et les exigences relatives à la protection de la recherche (voir p. ex. Université de l'Alberta, 2025; Université de Victoria, 2025; Université de Toronto, s.d.). Ces organismes peuvent se tenir informés des menaces et de l'évolution du paysage des risques et mettre au point des outils et des ressources pour les chercheurs de l'établissement concerné (V. Gerdts, communication personnelle, 2025; P. Ferguson, communication personnelle, 2024). L'IA a également été utilisée pour aider les établissements de recherche à gérer le nombre croissant d'exigences entourant la sécurité de la recherche dans certains pays; par exemple, l'Université Rice (É.-U.) utilise un outil d'IA appelé PRISM pour accélérer l'évaluation des risques liés à la sécurité de la recherche (Franklin, 2025).

Dans certains endroits, les ressources destinées au renforcement des capacités sont complétées par des points de contact centraux s'occupant de la sécurité de la recherche. Ils fournissent des conseils aux chercheurs qui se sentent mal préparés pour évaluer les risques ou gérer les vulnérabilités. Par exemple, aux Pays-Bas, le bureau de biosécurité de l'Institut national pour la santé publique et l'environnement propose un questionnaire pour aider les chercheurs à déterminer si leurs recherches sont à double usage (RIVM, s.d.-a,-c). Ce même bureau fait office de centre national d'information pour le gouvernement et les organisations qui travaillent avec des matières biologiques à haut risque. De même, au Canada, le Centre de sécurité de la recherche (CSR) est un point de contact national qui offre des orientations et des conseils (SP, 2024a).

Les collèges et les établissements qui mènent des recherches avec des délais d'exécution courts ont des besoins particuliers en matière de sécurité de la recherche

La recherche universitaire est menée en réponse aux besoins de la communauté et de l'industrie, souvent en partenariat avec des petites et moyennes entreprises canadiennes (Polytechnics Canada et BHER, s.d.). Selon l'enquête *La recherche appliquée dans les collèges et instituts* effectuée en 2023-2024 par Collèges et instituts Canada (CICan), environ 0,3 % des partenariats de recherche

appliquée des collèges ont une dimension internationale[15] (CICan, communication personnelle, 2025). Toutefois, compte tenu de l'incertitude économique et géopolitique croissante et de la complexité des relations de recherche, de nouvelles mesures de sécurité ont été jugées nécessaires pour protéger les chercheurs, les établissements et les bailleurs de fonds contre le détournement ou l'utilisation abusive des innovations issues des collèges (CICan, communication personnelle, 2025). Les collèges se spécialisent également dans les projets de recherche à court terme avec des délais d'exécution rapides (c.-à-d. achèvement du projet en moins d'un an) (CICan, 2023); ainsi, toute exigence en matière de sécurité de la recherche, comme les évaluations des risques qui impliquent de longs délais d'attente pour obtenir l'autorisation de poursuivre, pourrait entraver la capacité des collèges à entreprendre ce type de travaux.

À la suite d'une série de discussions tenues au sein de groupes de travail et de commentaires formulés par la communauté collégiale, ISDE a entendu que le principal obstacle aux initiatives en matière de sécurité de la recherche dans le secteur collégial était l'insuffisance des ressources, la capacité administrative et le budget limités rendant difficile la mise en œuvre de nouvelles mesures (ISDE, communication personnelle, 2025). Les représentants de la communauté collégiale ont indiqué à ISDE que les initiatives mises en œuvre devraient probablement tenir compte de la manière de réduire au minimum les contraintes et les délais afin d'être efficaces dans le contexte collégial. Depuis le 30 avril 2025, une approche de la sécurité de la recherche est à l'essai dans quatre établissements au Canada afin d'en déterminer la faisabilité ainsi que les ressources nécessaires. On cherche ainsi à tracer la voie la plus prometteuse pour l'ensemble du secteur collégial (ISDE, communication personnelle, 2025).

La protection de la recherche sensible nécessite la formation de tous les acteurs du système de la recherche, à intervalles réguliers, et par le biais de multiples modes de communication

Les mesures visant à protéger la recherche sensible comprennent des efforts de sensibilisation à l'échelle de l'organisation et des stratégies de communication, une formation sur la sécurité et l'intégrité de la recherche, ainsi que la transparence en ce qui touche les conflits d'intérêts et d'engagement (MPG, 2017; ASPC, 2018a; DOD, 2023; OSTP, 2024; ASIO, s.d.). Le Australia's University Foreign Interference Taskforce (groupe de travail australien sur l'ingérence étrangère dans les universités) recommande d'organiser régulièrement des formations générales à l'intention de tous les chercheurs, membres du

15 CICan définit les partenaires internationaux comme toute organisation basée à l'étranger ou détenue par des étrangers. Toutefois, les organisations ayant une succursale ou un bureau satellite au Canada en activité depuis au moins un an ont été classées comme partenaires canadiens.

personnel et étudiants afin de leur expliquer les attentes relatives à la conduite appropriée de la recherche, les manifestations de l'ingérence étrangère sur le campus et la façon de signaler les cas d'ingérence étrangère, d'intimidation et de harcèlement aux instances de l'université ou aux autorités compétentes (UFIT, 2021). La formation générale peut ensuite être adaptée pour répondre à des objectifs précis et cibler des groupes particuliers (comme les chercheurs, les étudiants, les services de soutien administratif). Par exemple, l'évaluation des risques liés à la géographie nécessite des considérations différentes de celles liées à l'évaluation des risques éthiques et peut exiger des ressources et des activités de sensibilisation différentes (voir p. ex. U15 et Universities Canada, 2019b; KNAW, 2023). Pour assurer l'efficacité, on recommande que les campagnes de formation et de sensibilisation aient lieu régulièrement et utilisent plusieurs canaux, tant en ligne (p. ex. communication par courriel, modules d'apprentissage) qu'en personne (p. ex. discussions et réunions d'équipe) (Gouv. des Pays-Bas, 2022).

Une formation axée sur les exigences précises, incluant les politiques gouvernementales qui imposent des obligations légales supplémentaires aux chercheurs, peut également être nécessaire pour garantir une conformité adéquate (JASON, 2024). Par exemple, la recommandation de l'UE accompagnant la réglementation qui entoure l'exportation décrit l'application de ces exigences aux produits de la recherche universitaire, dont les publications, les présentations, les logiciels et les données (CE, 2021a). Ce document décrit des exemples et les conditions déterminant un filtrage éventuel des éléments de recherche, tout en reconnaissant les tensions ainsi crées avec le libre accès à la recherche. Le document explique les conditions et les circonstances dans lesquelles certains résultats de recherche peuvent être exemptés des contrôles à l'exportation et décrit la procédure à suivre pour garantir la conformité, effectuer une évaluation des risques et gérer l'exportation d'articles à double usage qui ne figurent pas sur les listes connexes (CE, 2021a). Les établissements et les chercheurs canadiens ne sont pas suffisamment sensibilisés aux contrôles à l'exportation et aux régimes de sanctions, et pourraient donc bénéficier de conseils et de formations similaires (Université de Calgary et Université de l'Alberta, 2023). Le comité note également que la formation et l'éducation en matière de sécurité de la recherche ne sont pas l'apanage des établissements universitaires, et que les personnes participant à l'écosystème de la recherche au sein des gouvernements devraient également bénéficier de ces connaissances importantes.

L'un des risques liés à la généralisation de la formation à la sécurité de la recherche pourrait être la sensibilisation excessive des individus à certains profils de risque (p. ex. les pays où se trouvent des établissements à haut

risque), ce qui risquerait d'entraîner une discrimination et des obstacles à la participation de certains membres du personnel et étudiants aux activités de recherche (Gouv. des Pays-Bas, 2022). Comme indiqué au chapitre 3, les listes d'établissements de recherche interdits de partenariat peuvent désavantager les chercheurs de ces pays, même s'ils ne sont pas associés aux établissements en question (section 3.2.1). Les effets de ces politiques se font déjà sentir au Canada, où certains chercheurs font preuve d'une prudence excessive lorsqu'ils collaborent ou acceptent des étudiants : ils évitent tout simplement les personnes qui risquent de ne pas obtenir de visa (P. Ferguson, communication personnelle, 2025). Cette préoccupation excessive a atteint un paroxysme dans certains contextes, comme l'initiative américaine désormais abandonnée dite « U.S. China Initiative » qui, dans le but de lutter contre l'espionnage économique chinois, a plutôt donné lieu à un profilage racial généralisé des universitaires et des chercheurs (Prasso, 2021). Le harcèlement des ressortissants de certains pays peut également provenir de leur pays d'origine. En effet, il y a eu des cas où la Chine a fait pression sur des étudiants chinois travaillant ou étudiant dans des établissements nord-américains pour qu'ils fournissent au gouvernement chinois des informations sur leurs travaux (Molloy et Johnson, 2025).

Afin de lutter contre la discrimination, les établissements de recherche aux Pays-Bas sont encouragés à promouvoir « les valeurs de liberté, de respect et de débat ouvert propres au milieu de la recherche » dans la formation à la sensibilisation aux risques destinée aux chercheurs et au domaine de l'éducation en général (Gouv. des Pays-Bas, 2022). Une autre approche visant à éviter la discrimination à l'égard des ressortissants de certains pays a été adoptée en France, où le gouvernement peut restreindre l'accès physique à des installations désignées pour certaines personnes, sur la base d'évaluations des risques (Gouv. de la France, 2012; CNRS, 2024). Au Canada, l'élaboration de la politique RTSAP a été guidée par le principe de non-discrimination, de non-harcèlement et de non-coercition, stipulant explicitement qu'elle ne vise aucune nationalité (ISDE, 2023f). Les protocoles au niveau institutionnel peuvent également être explicites sur la manière de faire preuve de diligence raisonnable conformément aux exigences éthiques et juridiques, tout en respectant les principes d'équité, de diversité et d'inclusion (SRO, 2025).

5.3 Ressources financières

De l'avis du comité, il est essentiel de disposer de ressources financières durables pour les initiatives ciblant la science ouverte et la sécurité de la recherche. Demander aux chercheurs et aux établissements de s'engager dans le processus visant à déterminer le caractère sensible des recherches qu'ils

produisent, ainsi que la manière de les communiquer et de les protéger en toute sécurité – en assumant la responsabilité de tous ces aspects – sous-entend un financement à la hauteur, qui ne se limite pas à des sources ponctuelles ou précaires.

Le contrôle de l'accès à la recherche sensible nécessite des ressources financières, ce qui augmente le coût de la recherche

Les considérations financières sont particulièrement pertinentes lorsque les politiques de sécurité de la recherche imposent des exigences supplémentaires en termes de sécurité physique et de cybersécurité pour le stockage, de transmission et de traitement des données sensibles, ainsi que de protection des équipements (JASON, 2024). Les exigences relatives à la science ouverte impliquent également des infrastructures numériques supplémentaires (Goodchild *et al.*, 2023). Pour les organisations qui traitent d'énormes volumes de données (p. ex. le Système canadien d'observation intégrée de l'océan, Réseaux océaniques Canada), le mandat d'ouverture des données comprend la mise en place de données FAIR (faciles à trouver, accessibles, interopérables et réutilisables) et la mise en œuvre des principes TRUST (transparence, responsabilité, orientation vers l'utilisateur, soutenabilité/durabilité et technologie) (ONC, 2021a,b; SIOOC, s.d.-a,-c). La mise en œuvre de ces principes nécessite des ressources importantes pour « soutenir la production, la mise en commun et la réutilisation des données tout au long de leur cycle de vie », en particulier si la recherche est considérée comme sensible (Goodchild *et al.*, 2023).

» La répartition inéquitable du financement pour la sécurité de la recherche crée des vulnérabilités dans l'écosystème de la recherche postsecondaire canadien

Les politiques de sécurité de la recherche mises en œuvre par les gouvernements fédéral, provinciaux et territoriaux alourdissent le fardeau administratif des universités, soulignant la nécessité d'un financement supplémentaire pour soutenir les programmes et les bureaux chargés de la sécurité de la recherche. Cependant, en faisant preuve de rigueur en la matière, les établissements peuvent se positionner comme des partenaires de confiance pour la recherche sensible, ce qui leur ouvre des possibilités en termes de nouvelles collaborations et de nouveaux modes de financement (SRO, 2024b). Au niveau fédéral, les établissements d'enseignement postsecondaire qui reçoivent plus de 2 millions de dollars en financement de la recherche sont admissibles à un financement pour la sécurité de la recherche, qui est calculé en pourcentage de leur financement fédéral (SPIIE, 2022). Par conséquent, les grandes

universités reçoivent une part beaucoup plus importante du financement que celles de petite et moyenne taille, tandis que la plupart des collèges et des écoles polytechniques n'en reçoivent aucun (SPIIE, 2024). Il s'agit là d'une lacune dans le paysage actuel de la sécurité de la recherche, car les collèges participent au paysage canadien de la R-D et collaborent souvent avec le secteur privé, notamment avec des partenaires étrangers (CICan, 2023). De l'avis du comité, la répartition inéquitable du financement pour la sécurité de la recherche crée des vulnérabilités dans l'écosystème de la recherche postsecondaire canadien, les petites universités, les collèges et les écoles polytechniques étant souvent sollicités par des partenaires étrangers. Un financement de base pour mettre en place des capacités de sécurité de la recherche dans tous les établissements concernés pourrait contribuer à combler les lacunes dans l'écosystème et à garantir que tous bénéficient d'un soutien adéquat. D'autres formes de financement plus équitables déjà utilisées dans d'autres programmes de financement de la recherche (p. ex. le financement spécial des chaires de recherche du Canada, le modèle de subventions du Fonds de soutien à la recherche) pourraient également être appliquées pour soutenir les efforts dans les établissements de petite taille (GC, 2025k,l).

La formation à la sécurité de la recherche peut être exigée comme condition préalable à l'octroi d'un financement fédéral pour la recherche

Aux États-Unis, la directive NSPM-33 exige que les organisations mettent en œuvre un programme de sécurité de la recherche si elles reçoivent plus de 50 millions de dollars américains par an au total en financement fédéral pour la recherche (NSTC, 2022). Ces programmes doivent inclure une formation sur la sécurité de la recherche et le contrôle des exportations pour le personnel concerné, qui couvre la sensibilisation aux menaces et leur reconnaissance, la préparation aux incidents liés à la sécurité de la recherche, l'examen des partenariats étrangers et le respect des processus et protocoles de contrôle des exportations. Il est suggéré d'intégrer ces considérations dans les efforts de formation existants pour une conduite responsable et éthique de la recherche (NSTC, 2022). Selon le comité, ces initiatives s'inscrivent dans le concept du chercheur moderne, où la sensibilisation et la sensibilité à la sécurité de la recherche et à la science ouverte sont intégrées dans l'éducation et la formation (section 5.5).

Les ressources qui permettent de surmonter les obstacles à la communication d'informations favorisent à la fois la science ouverte et la sécurité de la recherche

Des ressources, des formations et des soutiens pour la protection et la mise en commun de la recherche sont nécessaires pour tous les types de recherche, quel que soit leur niveau de sensibilité. L'adoption de pratiques de science ouverte nécessite donc de surmonter plusieurs obstacles (Gownaris *et al.*, 2022; ISDE, 2024c). Or, les lacunes sur le plan des infrastructures de recherche numérique sont particulièrement marquées dans le contexte canadien (Northrup *et al.*, 2022; L'Alliance, 2024). Les ressources consacrées à la capacité de stockage dans le contexte de la GDR ne suivent pas le rythme auquel les données sont collectées ni l'éventail croissant des besoins correspondant à des domaines de recherche donnés (incluant les exigences particulières sur le plan de la protection de la recherche sensible) (L'Alliance, 2021; Goodchild *et al.*, 2023).

La publication en libre accès peut elle aussi nécessiter des ressources financières importantes (Owens, 2023b). Les publications dans des revues en libre accès exigent des frais de traitement des articles qui sont généralement prélevés sur les subventions de recherche. Si les chercheurs ne publient pas dans une revue en libre accès, ils doivent trouver un dépôt institutionnel approprié et y publier leurs travaux, éventuellement après une période d'embargo (Owens, 2023b). Une enquête a révélé que les questions du coût et d'accès aux dépôts sont des obstacles majeurs, parallèlement aux préoccupations concernant le manque d'incitatifs professionnels à la publication en libre accès au Canada et l'absence d'application des politiques existantes (ISDE, 2024c). Bien que le modèle de libre accès « diamant » soit gratuit pour les auteurs et les lecteurs, son fonctionnement nécessite tout de même des ressources financières provenant de bailleurs de fonds, des gouvernements ou de dons (Zheng, 2021; Bilodeau, 2024). Le financement du stockage et de l'accès à long terme fait également défaut dans toutes les disciplines de recherche, tout comme les fonds dédiés au personnel de soutien professionnel (L'Alliance, 2021).

Un autre défi consiste à fournir l'accès à des données correctement formatées dans les dépôts ou ailleurs. Voilà qui nécessite une expertise et des changements dans les flux de travail courants, ce qui peut être fastidieux en l'absence de contreparties. D'après l'expérience du comité, cette lacune entraîne des inégalités dans la manière dont certaines personnes et certains établissements sont en mesure de protéger ou de fournir l'accès aux connaissances et aux données. Cela est particulièrement vrai pour les gouvernements, les communautés et les chercheurs autochtones (encadré 5.1).

Encadré 5.1 Soutien à la gouvernance des données autochtones

Bien que le présent rapport ait mis en évidence des scénarios dans lesquels les détenteurs de droits autochtones entreprennent des efforts en matière de souveraineté et de gouvernance des données (sections 3.2, 4.1 à 4.3), ces efforts ont un coût. La création de plans de gestion des données et de mécanismes de gouvernance, l'achat et la maintenance des infrastructures, ainsi que le renforcement des capacités des personnes chargées de ces responsabilités nécessitent des ressources adéquates (CAC, 2023a). Plusieurs organisations ont élaboré ou élaborent activement des stratégies et des plans de gouvernance des données, notamment le Centre de gouvernance de l'information des Premières Nations (CGIPN), Inuit Tapiriit Kanatami (ITK) et le Ralliement national des Métis (MNC) (ITK, 2018; CGIPN, 2020; Gabel et Henry, 2024). Un financement durable est d'une importance critique pour atteindre les objectifs et les résultats visés en matière de gouvernance des données : « des instruments de financement pluriannuels (prévisibles) et souples seront essentiels pour soutenir une planification rentable, ainsi que pour allouer les fonds et en rendre compte en fonction des priorités et des besoins. La prévisibilité du financement sera essentielle pour attirer, développer et retenir les talents et les compétences. » (CGIPN, 2020) Le comité souligne toutefois que les coûts ne sont pas le seul obstacle aux efforts visant à garantir la souveraineté des données autochtones. En effet, l'agrégation des données, l'absence de transmission des données de recherche aux communautés, les politiques et la législation empêchent les peuples autochtones d'accéder à leurs propres données et de les utiliser. Mentionnons également la publication des résultats sans l'autorisation des personnes ou des organisations autochtones. Tous ces phénomènes persistent dans l'ensemble de l'écosystème de la recherche (ITK, 2018; CGIPN, 2020).

5.4 Application de la conformité

Il existe une grande variété d'approches dans l'application des mesures de sécurité de la recherche à l'étranger; toutefois, plusieurs pays ont recours à des approches fondées sur l'autorégulation du secteur pour protéger la recherche sensible (d'Hooghe et Lammertink, 2022). Voilà qui offre une certaine souplesse aux chercheurs et vise à réduire la charge liée à la mise en place d'une

surveillance externe. Cette approche est particulièrement marquée en Allemagne, où les chercheurs et les établissements assument collectivement la responsabilité de la protection de la recherche sensible, conformément à la législation applicable (Leopoldina et DFG, 2022b). En revanche, l'approche utilisée en France est descendante : la responsabilité du potentiel scientifique et technique de la nation est confiée au Secrétariat général de la Défense et de la Sécurité nationale (SGDSN), un organisme interministériel également chargé de la mise en œuvre et du développement des politiques de sécurité et de défense (d'Hooghe et Lammertink, 2022; SGDSN, s.d.). Le degré d'autorité attribué aux chercheurs détermine les leviers qui peuvent être utilisés pour les mesures de conformité et d'application.

Parmi les mesures de conformité actuellement en vigueur, plusieurs misent sur un effet dissuasif à l'endroit des chercheurs. Dans les pays où les chercheurs dépendent fortement d'un financement concurrentiel, les restrictions d'accès aux fonds ou aux programmes peuvent exercer une forte pression en faveur de la conformité. Cette approche est mise en œuvre de différentes manières : dans le cadre de la politique RTSAP au Canada, l'accès au financement fédéral peut être restreint pour les chercheurs en fonction du sujet et des affiliations des participants indiqués dans le projet proposé (ISDE, 2023f), tandis que le gouvernement australien a imposé des conditions d'accès aux subventions sur la base de la démonstration d'une planification adéquate de la gestion des risques liés à la sécurité de la recherche (ARC, 2023). La politique RTSAP s'inscrit dans le champ d'application du Cadre de référence des trois organismes sur la conduite responsable de la recherche, tout manquement à la RTSAP donnant lieu à des allégations de violation des politiques. De plus, l'établissement qui accueille le chercheur est chargé de mener une enquête préliminaire ou approfondie, si nécessaire (CRSNG, 2025). Le comité note toutefois que les enquêtes internes effectuées par les établissements relativement aux violations peuvent ne pas être aussi approfondies qu'elles le devraient, en raison de préoccupations liées à la préservation de leur réputation (voir p. ex. Molloy et Johnson, 2025), et qu'en dehors des recherches financées par les trois organismes, il n'existe aucun mécanisme d'application particulier pour garantir le respect des pratiques qui visent à préserver la sécurité de la recherche.

Le Secrétariat sur la conduite responsable de la recherche (SCRR) a pour mandat d'appuyer le Cadre de référence des trois organismes sur la conduite responsable de la recherche, « [d']étudier les rapports d'investigation des établissements afin de veiller à ce que le processus suivi par l'établissement soit conforme à sa politique sur la conduite responsable de la recherche et au Cadre; » et « [de] tirer parti des nouveaux enjeux dans le domaine de l'éthique

de la recherche et de la conduite responsable de la recherche, et d'y donner suite, dans un contexte national et international » (GC, 2024k). De l'avis du comité, le SCRR pourrait chercher à soutenir davantage les établissements et les chercheurs dans leurs activités de sécurité de la recherche, même s'il ne joue actuellement aucun rôle dans l'application des politiques.

D'autres mesures visant à encourager la conformité peuvent inclure la réduction des charges administratives supplémentaires, des sanctions juridiques et la mise en avant des risques pour la réputation. En France, les mesures de sécurité de la recherche numérique exigent que les données stockées dans les établissements réglementés soient étiquetées afin d'indiquer leur sensibilité, dans le cadre d'un plan de gestion des données plus large. L'absence d'un tel plan ou la présence de données non étiquetées entraîne la classification par défaut de toutes les données contenues dans cette installation comme sensibles, empêchant ainsi les chercheurs de diffuser les résultats de leurs recherches (SGDSN, 2018). Des sanctions peuvent également être prévues pour les activités contraires aux politiques de sécurité de la recherche. Par exemple, au Canada, le non-respect des conditions d'un permis de recherche sur les agents pathogènes humains et les toxines délivré par l'ASPC peut entraîner des mesures administratives (comme la suspension ou la révocation du permis et de l'habilitation de sécurité) ou des mesures pénales (comme une enquête et des poursuites) (ASPC, 2024a). Les sanctions juridiques varient d'un pays à l'autre, allant de l'amende à l'emprisonnement, leurs formes et leurs seuils étant définis par divers textes législatifs régissant différents aspects de la sécurité de la recherche (voir p. ex. Gouv. de la France, 1990, 2012; GC, 1992; Gouv. de l'Australie, 2018; Gouv. des États-Unis, 2022b; Gouv. des Pays-Bas, 2023; Gouv. de la Corée du Sud, 2023). L'atteinte à la réputation ou à l'image, avec des répercussions sur l'obtention de financement et l'attraction ou la rétention des étudiants et du personnel, est une autre conséquence négative qui peut être communiquée aux établissements et aux chercheurs comme étant un risque découlant de l'absence de mesures de sécurité de la recherche adéquates ou appropriées (Gouv. de la Nouvelle-Zélande, 2020; d'Hooghe et Lammertink, 2022; UNZ, 2022; NPSA et NCSC, 2024).

Les pratiques favorisant le respect et l'application des nouvelles politiques de sécurité de la recherche bénéficient d'une bonne compréhension du contexte de la recherche et des besoins des chercheurs

Il a été démontré que la conformité aux politiques de sécurité en laboratoire était améliorée par une meilleure compréhension des cultures disciplinaires, ce qui nécessite la participation d'experts engagés (Silbey, 2022). Par exemple, les biologistes et les chimistes sont tous tenus de se conformer à des pratiques de

sécurité strictes en laboratoire, mais les notions de contamination et de danger diffèrent entre ces domaines (Silbey, 2022). Ces distinctions, parmi d'autres, peuvent éclairer la conception et la mise en œuvre des mesures de conformité. La prise en compte des différences entre les disciplines et les contextes de recherche particuliers peut offrir d'autres possibilités, en explorant la manière dont les politiques de sécurité pourraient être déployées afin de répondre à un besoin non satisfait des chercheurs (Shankar et Drake, 2022).

Les politiques de cybersécurité peuvent quant à elles entraîner de nouvelles vulnérabilités si les chercheurs contournent les mesures perçues comme entravant la recherche ou comme étant disproportionnées. Une façon d'atténuer ce problème consiste à examiner les mesures de cybersécurité sous l'angle des flux de recherche et des cas d'utilisation propres aux disciplines, tout en tenant compte des infrastructures et des services informatiques existants, afin d'éviter d'imposer des conditions trop contraignantes aux chercheurs (Shankar et Drake, 2022). Cette méthode s'inspire de l'approche allemande de la sécurité de la recherche, qui intègre de telles considérations dans les procédures existantes entourant l'intégrité de la recherche, réduisant ainsi la charge qui pèse sur les chercheurs, tout en tirant parti de leur connaissance des politiques et des approches existantes (d'Hooghe et Lammertink, 2022).

Bien qu'il n'existe pas de solution unique pour surmonter efficacement les obstacles à la mise en commun des données, des stratégies comme l'adaptation des incitatifs à des contextes et des disciplines de recherche précis (Musker et Smith, 2021), parallèlement à la mise à disposition de ressources (financières et humaines) et d'infrastructures (Woods et Pinfield, 2022), se révèlent prometteuses. Il ne suffit pas de se concentrer uniquement sur les chercheurs individuels, car les changements culturels intervenant au sein des communautés de recherche peuvent être plus efficaces pour améliorer l'adoption (Plomp *et al.,* 2019; Woods et Pinfield, 2022). Au niveau international, certains établissements ont créé des rôles précis au sein des départements et unités de recherche : ils sont chargés de mettre en place un soutien à la gestion des données propre à chaque discipline (Plomp *et al.,* 2019; TU Delft, s.d.; Université de Cambridge, s.d.).

La protection des lanceurs d'alerte peut faciliter la divulgation d'informations aux organismes d'application de la loi

Dans certains pays, la coopération avec les organismes d'application de la loi et ceux chargés de la sécurité nationale est au cœur des politiques et des lignes directrices entourant la sécurité de la recherche (UFIT, 2021; NSTC, 2022; ARC, 2023). Ces interactions sont nécessaires pour tenir les chercheurs informés de l'ampleur et de la portée des problèmes posés par l'influence étrangère (JASON,

2024). Les politiques de dénonciation permettent aux chercheurs et aux membres du personnel de signaler en toute confiance des pratiques illégales ou contraires à l'éthique (Gouv. des Pays-Bas, 2022). Le gouvernement du Québec, par exemple, a adopté des mesures de protection spéciales pour les lanceurs d'alerte qui facilitent la divulgation d'actes répréhensibles commis ou sur le point de l'être à l'encontre d'organismes publics, y compris les universités. La *Loi facilitant la divulgation d'actes répréhensibles à l'égard des organismes publics* interdit à ces derniers d'exercer des représailles à l'encontre des personnes qui déposent une plainte de bonne foi et établit une présomption selon laquelle toute mesure ou activité disciplinaire qui affecte l'emploi d'une telle personne constitue une mesure de représailles (Gouv. du Québec, 2024a,b). Dans les situations où certains aspects de la sécurité de la recherche sont imposés par la loi, ces mesures de protection des lanceurs d'alerte peuvent aider les chercheurs qui tentent de se prévaloir de la loi, mais qui sont découragés ou empêchés de le faire par leur établissement.

La sensibilisation généralisée aux questions de sécurité nécessitera des changements dans la culture de la recherche

La création d'une culture de la recherche consciente des risques sur le plan de la sécurité peut contribuer à l'autorégulation de la sécurité de la recherche et à la science ouverte. Bien qu'un examen et une analyse approfondis de la question dépassent le cadre du présent rapport, les approches de gestion du changement offrent une voie possible pour atteindre certains de ces objectifs, même si elles ne sont pas exemptes de difficultés. Par exemple, la réussite individuelle et l'autonomie sont valorisées dans le milieu universitaire, ce qui peut rendre la culture réfractaire au changement en raison de plusieurs facteurs, notamment les préoccupations liées à la perte de temps; le manque de ressources et de soutien pour mettre en œuvre la démarche; la complexité ou l'incertitude qui y sont reliées; de même que la perception voulant que les changements proposés n'ont qu'une valeur minimale (Lane, 2007). Au-delà de la résistance culturelle, le comité note également que le système actuel d'incitations à la recherche et l'accent mis sur la maximisation des publications peuvent dissuader les chercheurs de mener des recherches responsables, tant en ce qui concerne la sécurité que les considérations relatives à la science ouverte. Le comité note toutefois que la signature de la Déclaration de San Francisco sur l'évaluation de la recherche (DORA) par les trois organismes (CRSNG, 2023) pourrait constituer une première étape pour relever ce défi à l'avenir, car la DORA souligne la « nécessité d'améliorer la façon dont les résultats de la recherche sont évalués » (DORA, 2012).

Un autre défi potentiel est le changement d'attitude à l'égard de la collaboration avec certains pays. Au cours des dernières décennies, le Canada a entretenu des relations solides avec la Chine dans les secteurs de l'innovation et de l'éducation, avec des programmes visant à renforcer les partenariats et l'échange de connaissances (GC, 2008; Davidson, 2017; Evans, 2022). L'accent mis récemment sur la limitation de la collaboration et de l'affiliation avec certains établissements, notamment ceux situés en Chine (voir p. ex. ISDE, 2023e), marque un revirement de cap. De l'avis du comité, les chercheurs qui étaient auparavant encouragés à nouer des relations avec leurs collègues et les établissements chinois pourraient avoir besoin d'un soutien supplémentaire pour s'adapter à l'évolution des politiques.

Lorsque le changement implique une nouvelle surveillance réglementaire, une communication insuffisante sur la portée et la nature de la réglementation peut créer de la confusion, en particulier lorsque la réglementation régissant l'ensemble d'un écosystème de recherche est interprétée de manière hétérogène d'un établissement à l'autre (Babb, 2020). Par exemple, au début des années 2000, le renforcement de l'application de la Common Rule – une politique fédérale américaine promulguée en 1991 visant à protéger les sujets de recherche humaine (Gouv. des États-Unis, 1991) – a suscité un mécontentement généralisé parmi les chercheurs (Babb, 2020). Cette levée de boucliers s'expliquait par un manque de clarté sur la manière de se conformer à la réglementation (censée offrir une certaine souplesse aux établissements) et par les sanctions prévues en cas de non-respect. Les efforts visant à améliorer la conformité ont été marqués par une volonté d'éliminer totalement les risques, mais ils ont également semé la confusion et causé de la frustration parmi les chercheurs dans des domaines qui seraient normalement exemptés de la Common Rule (en particulier les sciences sociales et humaines) (Babb, 2020). Bien que la sécurité de la recherche soit une question distincte des considérations éthiques énoncées dans la Common Rule, cet exemple illustre certains des risques liés à la mise en œuvre d'une réglementation de la recherche de large portée, ainsi que les défis liés à la définition de niveaux de conformité qui réduisent les risques à un niveau acceptable, sans pour autant nuire à la recherche.

Il est essentiel de comprendre la culture de l'environnement dans lequel le changement est recherché pour organiser la mise en œuvre et la planification de la communication (Berns *et al.*, 2007). Dans le contexte d'un établissement de recherche public, la création d'un organisme dédié au soutien de la gestion du changement est importante, car il agira comme une ressource centrale pour les différents départements de recherche. De plus, une communication efficace et claire ainsi qu'une formation des dirigeants sont essentielles à la mise en

œuvre, car les changements (et leurs conséquences) peuvent prendre le personnel au dépourvu (Berns *et al.,* 2007). Dans le cas de la sécurité de la recherche, des organismes institutionnels spécialisés (comme les bureaux de sécurité de la recherche) sont chargés de sensibiliser le corps enseignant et le personnel aux risques, mais le comité note que ces organismes ne détiennent pas nécessairement l'expertise pour mettre en œuvre le changement de manière optimale. En raison de ce manque d'expertise, ces bureaux peuvent avoir du mal à fonctionner efficacement dans les établissements dotés de structures organisationnelles décentralisées. L'intégration de l'expertise en matière de gestion du changement au sein des bureaux chargés de l'intégrité ou de la sécurité de la recherche et la prise en compte de ces principes dans l'élaboration et la mise en œuvre des politiques en la matière pourraient toutefois contribuer à faciliter l'adoption globale.

5.5 Favoriser une philosophie moderne de la recherche

La mise en œuvre de mesures visant à reconnaître et à protéger la recherche sensible peut être facilitée par des facteurs favorables applicables à la fois à la sécurité de la recherche et aux activités scientifiques ouvertes. La clé du succès de ces efforts réside dans la création de systèmes de responsabilité partagée, où la responsabilité de l'exécution des mesures est répartie entre les acteurs les mieux équipés pour assumer les rôles pertinents. Ce cadre se rapporte au concept de philosophie moderne de la recherche, selon lequel tous les acteurs participant à l'écosystème sont conscients non seulement de la sécurité et de leur rôle à cet égard, mais aussi des considérations de science ouverte, d'éthique et d'intégrité au sens large, ce qui permet à chacun d'évaluer le degré d'ouverture et de sécurité dont ses travaux ont besoin. L'évolution rapide du contexte géopolitique et le rythme effréné des progrès technologiques dans le domaine de la recherche contribuent à la nécessité pour les chercheurs d'adopter une philosophie moderne capable de s'adapter, et d'être équipés des outils et des ressources nécessaires pour concrétiser les aspects suivants :

La philosophie moderne de la recherche et le profil du chercheur moderne sont le résultat d'une formation, de ressources et d'un renforcement des capacités adéquats, tous nécessaires pour soutenir le développement des compétences essentielles à la participation à la recherche canadienne dans une perspective future

- Participation à la protection et à la préservation de l'écosystème de recherche canadien, ce qui englobe la sécurité de la recherche et la science ouverte, ainsi que l'innovation.
- Conscience du contexte mondial dans lequel s'inscrit la recherche et de la manière dont il peut influer sur la conduite responsable de la recherche.
- Application d'une perspective éthique, de confidentialité et de sécurité à la recherche, en particulier dans un contexte de partenariats et de collaborations (notamment avec les peuples autochtones et les partenaires étrangers).
- Priorité accordée à l'intégrité de la recherche dans tous les aspects de la conduite et du soutien de la recherche, et ce, tout au long du cycle de vie d'un projet.
- Évaluation continue de la sensibilité de ses propres travaux de recherche par rapport à l'évolution du contexte géopolitique.

De l'avis du comité, la philosophie moderne de la recherche et le profil du chercheur moderne sont le résultat d'une formation, de ressources et d'un renforcement des capacités adéquats, tous nécessaires pour soutenir le développement des compétences essentielles à la participation à la recherche canadienne dans une perspective future.

6

Conclusion et réflexions finales

6.1 Application des mesures à la recherche sur les agents pathogènes et à la recherche océanographique

6.2 Réflexions du comité

Bien que divers ordres de gouvernement aient mis en place des politiques de sécurité pour renforcer l'écosystème de la recherche au Canada, les progrès rapides dans certains domaines et l'évolution du contexte géopolitique nécessitent une approche en constante évolution pour reconnaître et protéger la recherche sensible tout en assurant un équilibre entre sécurité de la recherche, science ouverte et innovation. Sur la base de ce constat, Recherche et développement pour la défense Canada et l'Agence de la santé publique du Canada ont demandé au comité d'examiner les mesures visant à reconnaître et à protéger la recherche sensible préoccupante, ainsi que la manière d'appliquer de telles approches aux deux domaines de recherche suivants :

- **La recherche sur les agents pathogènes**, qui porte sur des matières comportant un risque élevé pour la santé humaine et qui fait donc l'objet de nombreux protocoles et cadres rigoureux pour la reconnaissance et la protection de la recherche. Ce type de recherche est représentatif d'autres domaines d'étude où les risques pour la santé et le bien-être humains sont bien connus.
- **La recherche océanographique**, qui couvre un large éventail de domaines d'étude présentant des degrés de sensibilité variables. Contrairement aux chercheurs qui se penchent sur les agents pathogènes, les océanographes font l'objet de beaucoup moins de surveillance et disposent de moins d'orientation pour évaluer la sensibilité de leurs recherches, juger de leurs impacts négatifs potentiels et mettre en œuvre des mesures de protection appropriées. Une grande partie de la recherche océanographique est axée sur la mise en commun d'informations avec un large éventail d'acteurs à l'échelle nationale et internationale. Il est donc possible que les chercheurs n'envisagent pas de mesures de sécurité visant à restreindre l'accès à ces informations.

À l'instar des océanographes, les chercheurs qui mènent de nombreux autres types de recherches, notamment en sciences sociales et humaines, peuvent ignorer les risques pour la sécurité associés à leurs travaux, même si les résultats ou les méthodes se révèlent possiblement sensibles sur le plan de la confidentialité ou de l'éthique.

Tout au long du rapport, divers moyens de reconnaître et de protéger la recherche sensible et la recherche sensible préoccupante ont été abordés, incluant les mesures utilisées au Canada et les approches d'autres pays. Dans la mesure du possible, l'applicabilité de ces mesures à la recherche sur les agents pathogènes ou à la recherche océanographique a été examinée. La section 6.1 résume ces mesures dans le contexte des deux domaines de recherche, en comparant et en opposant diverses approches et en évaluant les facteurs

nécessaires à leur mise en œuvre dans les phases de conception, de recherche active et de post-recherche. Les réflexions finales du comité sont présentées à la section 6.2.

6.1 Application des mesures à la recherche sur les agents pathogènes et à la recherche océanographique

Afin de prendre des décisions éclairées en matière de sécurité, les personnes entreprenant des travaux de recherche doivent savoir reconnaître la recherche sensible et déterminer quand elle présente des risques supplémentaires (c'est-à-dire quand elle devient *préoccupante*). L'équilibre entre les risques et les opportunités de la recherche est un élément essentiel de l'évaluation de la sensibilité et des mesures de protection appropriées. En effet, les travaux qui se révèlent extrêmement précieux pour la santé humaine et le bien-être mondial (p. ex. ceux portant sur les maladies infectieuses, les données géospatiales) sont souvent associés à des risques pour la sécurité. Les facteurs qui déclenchent la catégorisation d'une recherche comme sensible dépendent du domaine et du projet. Les listes de technologies sensibles, les évaluations des risques et la consultation de personnes détenant une expertise pertinente sont des outils couramment utilisés pour reconnaître la recherche sensible au Canada et dans d'autres pays. Une fois qu'une recherche a été reconnue comme sensible et préoccupante, des mesures de protection appropriées doivent être déterminées afin de garantir qu'elle est menée et mise en commun de manière responsable. Le comité souligne que toutes les mesures de protection ne sont pas appropriées pour tous les types de recherches sensibles préoccupantes, et lorsqu'elles sont applicables, leur mise en œuvre peut varier.

» Le comité souligne que toutes les mesures de protection ne sont pas appropriées pour tous les types de recherches sensibles préoccupantes, et lorsqu'elles sont applicables, leur mise en œuvre peut varier

6.1.1 Reconnaissance et protection de la recherche sensible préoccupante sur les agents pathogènes

Dans le domaine de la recherche sur les agents pathogènes, les facteurs indiquant la sensibilité comprennent les risques pour la santé humaine, les applications nocives de la recherche et des facteurs propres au contexte, comme la transmissibilité des agents pathogènes. Lorsque le risque lié à la conduite d'une recherche est évident et que les conséquences d'une utilisation abusive

potentielle peuvent menacer la santé et la sécurité publiques, les décideurs politiques établissent des listes d'éléments et de produits dangereux et restreignent l'accès à la recherche. C'est le cas pour la recherche portant sur certains types de toxines et d'agents pathogènes humains. Si l'approche fondée sur des listes est le principal mécanisme permettant de reconnaître la recherche sensible préoccupante liée aux agents pathogènes, elle est complétée par des mesures supplémentaires – évaluations des risques et examens par des experts aux compétences pertinentes – destinées à renforcer l'application des listes (tableau 6.1).

Tableau 6.1 Mesures visant à reconnaître la recherche sensible préoccupante dans le domaine des agents pathogènes

Mesure	Description	Phase du processus de recherche
Listes	La recherche sur les agents pathogènes et les toxines visée par la *Loi sur les agents pathogènes humains et les toxines* nécessite des mesures de protection particulières, notamment des permis et des habilitations de sécurité. Les matières visées figurent également sur les listes de contrôle des exportations, qui exigent une licence ou un permis pour qu'elles puissent sortir du pays, conformément aux listes d'armes chimiques et biologiques du Groupe d'Australie.	Phase de conception de la recherche; phase post-recherche
Évaluations des risques	Les Lignes directrices canadiennes sur la biosécurité fournissent un arbre décisionnel et un processus d'évaluation des risques pour aider à déterminer le niveau de sensibilité de certains types de recherche. Les considérations relatives à la nouveauté, à la nocivité, au risque de modification et au potentiel d'utilisation abusive sont toutes incluses dans le processus d'évaluation des risques. Une fois les risques reconnus, une étape supplémentaire est prévue pour déterminer si le niveau de biosécurité existant est adéquat, ou si des mesures de protection supplémentaires sont requises.	Phase de conception de la recherche
Expertise pertinente	Certaines revues passent au crible les articles soumis afin de détecter tout double usage potentiel et cherchent à reconnaître les travaux trop sensibles pour être publiés dans leur état actuel, voire pour être publiés tout court.	Phase post-recherche

Une fois que des travaux ont été reconnus comme étant sensibles et préoccupants dans le domaine de la recherche sur les agents pathogènes, une série de mesures de protection s'appliquent à la phase de conception. Dans de nombreux cas, ces mesures sont enchâssées dans les politiques (p. ex. la Norme canadienne sur la biosécurité) adoptées en vertu de la *Loi sur les agents pathogènes humains et les toxines (LAPHT)* et du *Règlement sur les agents pathogènes humains et les toxines (RAPHT)*. La phase de recherche active et la phase

post-recherche sont pour leur part moins réglementées. Par exemple, en matière de cybersécurité, l'Addenda de biosécurité apporté à la Norme canadienne sur la biosécurité, qui entrera en vigueur en 2026, ne s'appliquera qu'aux installations de recherche de niveau de confinement 4. Dans la phase post-recherche, l'élaboration de plans de communication est laissée à la discrétion des installations de recherche détentrices d'un permis (tableau 6.2).

Tableau 6.2 Mesures visant à protéger la recherche sensible préoccupante dans le domaine des agents pathogènes

Mesure	Description	Phase du processus de recherche
Filtrage des chercheurs et des partenaires	Les chercheurs qui entreprennent des recherches avec des ABCSE doivent obtenir une habilitation de sécurité spéciale, tandis que les ressortissants étrangers doivent fournir des documents supplémentaires.	Conception de la recherche
	Les chercheurs travaillant sur des agents pathogènes qui sollicitent un financement fédéral pour des projets comportant l'application de technologies des sciences de la vie (telles que définies dans la politique RTSAP) ne peuvent pas collaborer avec des chercheurs affiliés à des organisations de recherche nommées (ORN).	Conception de la recherche
Filtrage des projets de recherche	Des permis sont requis pour les recherches portant sur les agents pathogènes et les toxines classées dans les groupes de risque 2, 3 et 4.	Conception de la recherche
	Les installations de recherche qui adhèrent à la Norme canadienne sur la biosécurité sont tenues d'examiner tous les projets afin de déterminer leur double usage potentiel à toutes les étapes, incluant lors de la diffusion des résultats.	Phase de conception de la recherche; phase de recherche active; phase post-recherche
	L'ASPC recommande aux installations de recherche d'adopter des plans de communication précisant les informations qui peuvent être mises en commun et avec qui.	Phase post-recherche
Sécurité des installations et des infrastructures de recherche	Le contrôle de l'accès aux installations de recherche est une pratique courante dans les laboratoires publics et privés qui travaillent avec des agents pathogènes et des toxines.	Phase de recherche active
	Les exigences applicables aux installations de niveau 4 qui entreront en vigueur en 2026 comprendront un plan de cybersécurité, des politiques sur l'utilisation des appareils numériques et un système d'étiquetage, de traitement et de restriction de l'accès aux informations sensibles.	Phase de recherche active

6.1.2 Reconnaissance et protection de la recherche océanographique sensible préoccupante

Bien que les processus de haut niveau visant à reconnaître et à protéger la recherche sur les océans et les agents pathogènes soient harmonisés, la recherche océanographique diffère de celle sur les agents pathogènes en ce sens que les risques liés à la sensibilité de la première ne sont souvent pas aussi évidents, et entraînent moins de dommages, potentiels et immédiats, pour la santé ou le bien-être des humains. Certains facteurs peuvent rendre la recherche sensible, notamment les partenariats étrangers, la recherche concernant les peuples autochtones, la géographie, ainsi que la production et l'utilisation de grands ensembles de données. Dans le même temps, la mise en commun de grandes quantités de données d'observation océanique est fondamentale pour les partenariats internationaux qui font progresser la compréhension des changements climatiques et d'autres questions d'intérêt mondial. La sensibilité de la recherche peut dépendre du fait que le chercheur développe certaines technologies incluses dans la politique RTSAP, travaille dans des domaines de recherche sensibles ou utilise certains types de données. Des comités d'évaluation des risques peuvent être mis sur pied pour fournir des conseils supplémentaires aux chercheurs et déterminer si les recherches reconnues comme étant sensibles présentent des risques supplémentaires (c.-à-d. si elles sont préoccupantes) – parce qu'il est raisonnable de penser qu'elles pourraient être détournées ou utilisées abusivement, immédiatement ou à l'avenir, sans modification ou avec des modifications mineures (tableau 6.3).

Tableau 6.3 Mesures visant à reconnaître la recherche océanique sensible préoccupante

Mesure	Description	Phase du processus de recherche
Listes	La recherche océanique qui fait progresser certaines technologies est concernée par la politique RTSAP. Ces technologies (relevant de la catégorie « détection et surveillance avancées ») figurent sur la liste des technologies sensibles qui, en elles-mêmes, n'indiquent pas que la recherche est préoccupante, mais qui peuvent faire l'objet d'un recoupement avec la liste des ORN. Les établissements ont la possibilité d'évaluer leurs atouts à l'aide d'une analyse des actifs de valeur, ainsi que de créer et de réévaluer périodiquement des listes de domaines de recherche sensibles (qui pourraient inclure la recherche océanographique) nécessitant des mesures de protection supplémentaires.	Phase de conception de la recherche; phase de recherche active
Évaluations des risques	Les évaluations standardisées des risques ne sont pas couramment utilisées dans la recherche océanographique, en partie en raison du manque de connaissance des chercheurs individuels sur la sécurité de la recherche. Les comités d'éthique institutionnels pourraient être chargés d'évaluer les risques liés à des domaines de recherche particuliers en collaboration avec les chercheurs. Ces entités peuvent être internes aux établissements, régionales ou s'appuyer sur des organismes de recherche nationaux comme l'Alliance de la recherche océanographique au Canada (AROC) pour coordonner et fournir des services à la communauté des océanographes.	Phase de conception de la recherche; phase de recherche active
Expertise pertinente	Certains types de données de surveillance océanique (comme les données acoustiques) sont extrêmement précieuses car elles servent des objectifs scientifiques nationaux et internationaux, mais elles ont également des implications militaires. Un filtrage et une expertise pertinente de la part des forces armées sont nécessaires pour empêcher que certaines données ne soient incluses dans les flux de données accessibles au public, pour des raisons de sécurité nationale. Les partenaires de recherche autochtones possèdent également une expertise pertinente dans la reconnaissance des données ou des recherches qui peuvent être sensibles sur le plan culturel, ce qui dicte les conditions de mise en commun et d'accès.	Phase de conception de la recherche; phase de recherche active; phase post-recherche

La plupart des mesures visant à protéger la recherche océanographique sensible s'appliquent au cas par cas, en fonction des politiques applicables des établissements de recherche et de la sensibilisation des chercheurs aux risques liés à la sécurité. Les politiques promulguées par le gouvernement fédéral, comme les LDSNPR et la RTSAP, fournissent des orientations utiles à cet égard. Certaines mesures de protection sont associées à des financements privés et publics (p. ex. un processus d'évaluation des risques dans le cadre des LDSNPR ou des restrictions à la publication des résultats de recherche) (tableau 6.4).

Tableau 6.4 Mesures visant à protéger la recherche océanographique sensible préoccupante

Mesure	Description	Phase du processus de recherche
Filtrage des chercheurs et des partenaires	Les océanographes étrangers qui souhaitent travailler ou étudier au Canada sont soumis à des filtrages de sécurité par les organismes gouvernementaux.	Conception de la recherche
	Les chercheurs et les organisations océanographiques peuvent se référer à la liste des ORN pour éviter toute collaboration avec des chercheurs affiliés à des entités étrangères présentant des risques pour la sécurité.	Conception de la recherche
Filtrage des projets de recherche	Un océanographe qui sollicite un financement auprès des trois organismes doit joindre à sa demande de subvention un formulaire d'évaluation des risques si son projet relève des LDSNPR et s'il prévoit de mener des recherches avec un partenaire visé.	Conception de la recherche
	Les organismes qui financent la recherche océanographique peuvent utiliser les LDSNPR pour orienter l'examen de sécurité des propositions de recherche sur la base de sources accessibles au public.	Conception de la recherche
	Les systèmes d'étiquetage des données contrôlés par les peuples autochtones peuvent faciliter la surveillance continue de la phase active de la recherche, conformément au principe de souveraineté des données.	Phase de conception de la recherche; phase de recherche active; phase post-recherche
Restrictions relatives à la publication et à la mise en commun	Des restrictions à la publication et à la mise en commun des données peuvent être imposées au cas par cas (p. ex. par le biais de contrats de recherche ou en vertu du principe de souveraineté des données).	Phase post-recherche
Sécurité des installations et des infrastructures de recherche	Les organismes de recherche océanographique peuvent mettre en œuvre des politiques de cybersécurité et de gestion des données.	Phase de recherche active

6.1.3 Analyse comparative des approches

Les mesures visant à reconnaître et à protéger la recherche sensible préoccupante peuvent être largement appliquées dans de nombreux domaines de recherche, même si les modalités précises de mise en œuvre peuvent varier. Il n'existe pas de mesure unique adaptée à tous les types de recherche, ce qui va de soi, car les risques varient selon le domaine et le projet individuel. Il est essentiel de déterminer le niveau de risque de chaque projet et de mettre en œuvre les mesures et les protections appropriées afin d'éviter une sécurisation

excessive de la recherche et des chercheurs, et de garantir que la recherche et les données continuent d'être mises en commun pour faire progresser les connaissances et l'innovation. Dans le présent rapport, la recherche sur les agents pathogènes et la recherche océanographique peuvent être considérées comme des substituts d'autres domaines de recherche présentant différents niveaux de réglementation et de sensibilisation aux risques de la part des chercheurs et de leur établissement. Par exemple, la recherche nucléaire présente certaines similitudes avec celle sur les agents pathogènes en ce sens qu'elle est fortement réglementée et protégée, et que les risques pour l'humain sont largement connus. La recherche océanographique peut quant à elle être assimilée à de nombreux autres domaines de l'écosystème de la recherche où l'accent mis sur la sécurité est limité. Le comité souligne que son évaluation ne fournit pas une description exhaustive de toutes les mesures potentielles de reconnaissance et de protection, mais que celles qui y sont énumérées constituent un point de départ pour les chercheurs et les établissements afin de déterminer lesquelles sont les plus appropriées pour faire face aux risques liés aux domaines de recherche en question. D'autres types de déclencheurs de sensibilité (tableau 3.1) peuvent apparaître en fonction de la discipline ou du domaine, et les approches visant à reconnaître et à protéger la recherche peuvent être appliquées individuellement ou conjointement, de différentes manières. Quelle que soit la mesure adoptée, des politiques, des orientations, des ressources et un soutien adéquats sont la clé d'une mise en œuvre réussie.

Il n'existe pas de mesure unique adaptée à tous les types de recherche, ce qui va de soi, car les risques varient selon le domaine et le projet individuel

6.1.4 Conditions de réussite

Diverses initiatives sont en cours pour renforcer la sécurité de la recherche au Canada et dans d'autres pays, mais des efforts concertés sont requis pour évaluer ces mesures ainsi que leurs répercussions sur la science ouverte et l'innovation. Bien que limitées, les données indiquent que les mesures nécessitent des ressources financières (et autres); le renforcement des capacités; la formation; ainsi que la mise en commun des connaissances afin de permettre aux personnes, aux communautés et aux établissements qui entreprennent des travaux dans le domaine de la sécurité de la recherche et de la science ouverte de disposer des moyens nécessaires pour agir (chapitre 5). Bon nombre de ces considérations, bien que distinctes et impliquant des objectifs et des acteurs différents, peuvent relever de la conduite responsable de

la recherche. Pour garantir que les chercheurs, soutenus par leur établissement et leurs gouvernements, reçoivent une formation adéquate en matière de conduite responsable, il faut commencer par reconnaître et protéger la recherche sensible, ainsi que comprendre les impératifs de la science ouverte. Voilà qui leur permettra de mener des recherches les plus ouvertes possible, avec le niveau de sécurité qui s'impose.

6.2 Réflexions du comité

Au Canada, la sécurité de la recherche et la science ouverte relèvent de la responsabilité collective

La conduite responsable de la recherche est attendue de tous les acteurs du système de la recherche et implique un ensemble de mesures qui fonctionnent en tandem. Le comité comprend que, sur la base du travail déjà accompli au Canada pour faire progresser la sécurité de la recherche, il existe un potentiel de croissance et d'amélioration. Il n'y a pas de stratégie ni de mesure unique permettant de reconnaître ou de protéger efficacement toute la recherche sensible. De même, aucun acteur de l'écosystème de la recherche ne peut être seul responsable de l'élaboration et de la mise en œuvre de ces mesures. La collaboration en vue d'harmoniser les approches de sécurité de la recherche et de science ouverte au Canada contribuera à alléger le fardeau des chercheurs et à réduire la confusion lorsqu'ils tentent de travailler dans plusieurs territoires de compétence, tant au Canada qu'à l'étranger. Le comité suggère en outre que tous ceux qui se livrent à la recherche ont la responsabilité sociale et le devoir civique de rendre compte de la conduite appropriée de leurs travaux, notamment, et sans s'y limiter, la sécurité et l'ouverture de la recherche. Une grande partie de la recherche effectuée au Canada est financée par des fonds publics. Les chercheurs et les autres acteurs de l'écosystème devraient donc être encouragés à veiller à ce que leurs résultats soient non seulement utiles et bénéfiques pour la population canadienne, mais aussi, si nécessaire, à ce qu'ils soient protégés contre toute utilisation abusive. Parallèlement, les décideurs ont un rôle important à jouer pour veiller à ce que les lignes directrices soient claires, et que les chercheurs comme les établissements disposent d'un soutien adéquat pour se conformer aux directives encadrant la sécurité de la recherche et la science ouverte, tout en minimisant la charge administrative et les coûts financiers.

Une philosophie moderne de la recherche, englobant de multiples compétences, peut favoriser la conduite responsable de la recherche

Selon le comité, les concepts de philosophie moderne de la recherche et de chercheur moderne sont prometteurs pour apporter des changements qui favorisent à la fois la sécurité de la recherche et la science ouverte. Ces concepts font référence à la sensibilisation à la sécurité et à la science ouverte chez les chercheurs tout au long de leur carrière universitaire, ainsi que chez les personnes qui travaillent dans les établissements de recherche et les administrations en général. Ces compétences pourraient être introduites comme une exigence de formation par les établissements ou les départements universitaires, et soutenues par les gouvernements et les organes décisionnels. La formation pourrait également être appuyée au niveau du corps professoral en la rendant obligatoire pour l'obtention de fonds fédéraux voués à la recherche. Cette formation serait axée sur le principe selon lequel la conduite responsable de la recherche implique une sensibilité aux risques parallèlement à un engagement en faveur de la science ouverte et de l'intégrité de la recherche, afin d'éviter une sécurisation excessive. Les chercheurs, les établissements et les bailleurs de fonds doivent considérer la sensibilisation à la sécurité et la valeur de la science ouverte comme des compétences fondamentales dans l'écosystème de la recherche. Selon le comité, les hauts dirigeants ont un rôle essentiel à jouer dans ce processus; s'ils ne développent pas et ne valorisent pas eux-mêmes ces compétences, il sera beaucoup plus difficile de changer et d'adapter la culture institutionnelle.

La sécurité de la recherche est susceptible de gagner en importance à l'avenir, la mise en œuvre réussie des mesures nécessitant une évaluation, une surveillance et un suivi accrus des initiatives

Si les menaces qui pèsent actuellement sur les activités intellectuelles persistent, des conséquences dévastatrices et profondes pourraient s'ensuivre pour l'ensemble de la société, avec des répercussions négatives sur la santé, la richesse et nos modes de vie. En raison de ces répercussions potentielles, le comité considère le présent rapport comme un outil visant à appeler tous les acteurs à agir pour une meilleure reconnaissance de la sécurité dans l'ensemble de l'écosystème de la recherche. Pour être efficaces dans un contexte géopolitique en constante évolution, ces efforts doivent être déployés à l'échelle pancanadienne, et coordonner les approches des territoires de compétences alliés ou partenaires. L'évolution des facteurs externes justifie une réévaluation continue des risques afin de permettre une approche réactive et flexible de la sécurité de la recherche. Il est également nécessaire de poursuivre les discussions et le dialogue entre les chercheurs et les acteurs des communautés de la sécurité nationale et du renseignement afin que tous soient conscients de

l'évolution du contexte géopolitique et puissent réévaluer en permanence le caractère sensible de la recherche. L'Arctique en est un exemple frappant : certains domaines de recherche deviennent rapidement plus sensibles à mesure que les enjeux touchant le Nord se politisent de plus en plus.

Les initiatives en matière de sécurité et de science ouverte, qui s'inscrivent dans le concept plus large de conduite responsable et d'intégrité, sont essentielles à l'écosystème de la recherche. Cependant, il est difficile de déterminer les pratiques les plus prometteuses en raison du manque de recherches accessibles au public et d'évaluations des programmes actuels, tant au Canada qu'à l'étranger. Il est d'une importance capitale de surveiller et de suivre la conformité à ces politiques et programmes ainsi que leur efficacité, afin d'améliorer leur mise en œuvre et de garantir que tous les acteurs du système bénéficient d'un soutien adéquat pour rendre la recherche la plus ouverte et la plus sûre possible. L'écosystème de la recherche du Canada n'existe pas et n'existera jamais dans un vide national; par conséquent, un dialogue continu sur les approches permettant de reconnaître et de sécuriser la recherche sensible sans compromettre la science ouverte est nécessaire sur la scène internationale. Le Canada a l'occasion de jouer un rôle de premier plan dans ces discussions, en promouvant à la fois la science ouverte et la mise en commun lorsque cela est raisonnable, tout en sécurisant la recherche sensible préoccupante afin de garantir la sécurité comme le bien-être des personnes au Canada et dans le monde entier.

Il est d'une importance capitale de surveiller et de suivre la conformité à ces politiques et programmes ainsi que leur efficacité, afin d'améliorer leur mise en œuvre et de garantir que tous les acteurs du système bénéficient d'un soutien adéquat pour rendre la recherche la plus ouverte et la plus sûre possible

Références

AIVD, MIVD et NCTV – General Intelligence and Security Service, Military Intelligence and Security Service, et National Coordinator for Security and Counterterrorism, 2022. *Dreigingsbeeld Statelijke Actoren 2 [évaluation des menaces des acteurs étatiques]*, Zoetermeer, Pays-Bas, AIVD, MIVD et NCTV. https://www.nctv.nl/documenten/publicaties/2022/11/28/dreigingsbeeld-statelijke-actoren-2.

Akhtar, S. I., 2024. *USMCA: Intellectual Property Rights (IPR)*, Washington, D.C., U.S. Congressional Research Service. https://www.congress.gov/crs_external_products/IF/PDF/IF11314/IF11314.6.pdf.

Alayche, M., K. D. Cobey, J. Y. Ng, C. L. Ardern, K. M. Khan, A.-W. Chan, … D. Moher, 2023. « Evaluating prospective study registration and result reporting of trials conducted in Canada from 2009 to 2019 », *FACETS*, vol. 8, p. 1-10. https://doi.org/10.1139/facets-2022-0208.

ARC – Australian Research Council, 2023. *ARC Countering Foreign Interference Framework*, Canberra, Australie, ARC. https://www.arc.gov.au/sites/default/files/2023-12/ARC%20Countering%20Foreign%20Interference%20Framework.pdf.

ARC – Australian Research Council, s.d. Research security. https://www.arc.gov.au/funding-research/research-security (consulté en août 2024).

ARLA – Agence de réglementation de la lutte antiparasitaire, 2024. *Cadre d'évaluation et de gestion des risques liés aux produits antiparasitaires*, Ottawa, ON, Gouvernement du Canada. https://publications.gc.ca/collections/collection_2021/sc-hc/H114-41-2021-fra.pdf.

AROC – Alliance de la recherche océanique au Canada, 2022. Alliance de la recherche océanique au Canada.https://science.gc.ca/site/science/fr/alliance-recherche-oceanique-canada (consulté en juin 2024).

AROC – Alliance de la recherche océanique au Canada, 2023. *Rapport sommaire de la réunion nationale de l'AROC 2023*, St. John's, T.-N.-L., AROC. https://science.gc.ca/site/science/fr/alliance-recherche-oceanique-canada/reunion-nationale-aroc-2023/rapport-sommaire-reunion-nationale-laroc-2023.

Around Him, D., T. A. Aguilar, A. Frederick, H. Larsen, M. Seiber et J. Angal, 2019. « Tribal IRBs: A framework for understanding research oversight in American Indian and Alaska Native communities », *American Indian and Alaska Native Mental Health Research*, vol. 26, nº 2, p. 71-95. https://doi.org/10.5820/aian.2602.2019.71.

ASIO – Australian Security Intelligence Organisation, s.d. *Protect your Research, Collaborate with Care*, Canberra, Australie, ASIO. https://www.asio.gov.au/system/files/2023-05/Protect%20Your%20Research%2C%20Collaborate%20with%20Care%20-%20Booklet.pdf.

ASM Journals – American Society for Microbiology, 2021. Dual use research. https://journals.asm.org/dual-use-research (consulté en juin 2025).

ASPC – Agence de la santé publique du Canada, 2015. *Plan de surveillance administrative à l'égard des agents pathogènes et des toxines dans un contexte de recherche – Éléments requis et lignes directrices*, Ottawa, ON, Gouvernement du Canada. https://www.canada.ca/content/dam/phac-aspc/documents/services/laboratory-biosafety-biosecurity/licensing-program/plan-administrative-oversight-pathogens-toxins-a-research-setting-required-elements-guidance/admin_oversight-surveillance_admin-fra.pdf.

ASPC – Agence de la santé publique du Canada, 2018a. *Ligne directrice canadienne sur la biosécurité : le double usage dans la recherche en sciences de la vie*, Ottawa, ON, Gouvernement du Canada. https://publications.gc.ca/collections/collection_2020/aspc-phac/HP45-22-2018-fra.pdf.

ASPC – Agence de la santé publique du Canada, 2018b. *Ligne directrice canadienne sur la biosécurité: Effectuer une évaluation des risques de biosûreté*, Ottawa, ON, Gouvernement du Canada. https://shorturl.at/3IQVJ.

ASPC – Agence de la santé publique du Canada, 2020. *Centre de la biosûreté rapport annuel 2018-2019 – Maximiser L'effet*, Ottawa, ON, Gouvernement du Canada. https://www.canada.ca/content/dam/phac-aspc/documents/services/publications/health-risks-safety/centre-biosecurity-annual-report-2018-2019/phac-biosecurity-annual-report-fre.pdf.

ASPC – Agence de la santé publique du Canada, 2021. *Politique sur la recherche scientifique avec les agents pathogènes humains et les toxines*, Ottawa, ON, Gouvernement du Canada. https://www.canada.ca/fr/sante-publique/services/biosecurite-biosurete-laboratoire/politique-recherche-scientifique-agents-pathogenes-humains-toxines.html.

ASPC – Agence de la santé publique du Canada, 2022. *Norme canadienne sur la biosécurité, troisième édition*, Ottawa, ON, Gouvernement du Canada. https://www.canada.ca/content/dam/phac-aspc/migration/cbsg-nldcb/cbs-ncb/assets/pdf/norme-canadienne-biosecurite-troisieme-edition.pdf.

ASPC – Agence de la santé publique du Canada, 2023. Biosûreté – Foire aux questions. https://www.canada.ca/fr/sante-publique/services/biosecurite-biosurete-laboratoire/biosecurite/biosecurite-foire-questions.html (consulté en juin 2025).

ASPC – Agence de la santé publique du Canada, 2024a. Cadre de conformité et d'application des règlements de l'Agence de la santé publique du Canada. https://www.canada.ca/fr/sante-publique/organisation/transparence/ouverture-transparence-en-matiere-reglementation/cadre-conformite-d-application-des-reglements.html (consulté en mai 2025).

ASPC – Agence de la santé publique du Canada, 2024b. Foire aux questions (FAQ) : Règlements. https://www.canada.ca/fr/sante-publique/organisation/mandat/a-propos-agence/lois-reglements/politique-prestation-lignes-directrices-exigences-reglementaires/foire-questions-faq-reglements.html (consulté en août 2024).

ASPC – Agence de la santé publique du Canada, 2024c. Biosûreté. https://www.canada.ca/fr/sante-publique/services/biosecurite-biosurete-laboratoire/biosecurite.html (consulté en janvier 2025).

ASPC – Agence de la santé publique du Canada, 2024d. Programme de délivrance de permis. https://www.canada.ca/fr/sante-publique/services/biosecurite-biosurete-laboratoire/programme-delivrance-permis.html (consulté en janvier 2025).

ASPC – Agence de la santé publique du Canada, 2024e. Ce que nous avons entendu : Consultation thématique sur les modifications possibles au Règlement sur les agents pathogènes humains et les toxines. https://www.canada.ca/fr/sante-publique/services/biosecurite-biosurete-laboratoire/consultation-thematique-modifications-potentielles-apportees-reglement-agents-pathogenes-humains-toxines/ce-que-nous-avons-entendu-consultation-modifications-possibles-reglement.html (consulté en avril 2024).

ASPC – Agence de la santé publique du Canada, 2024f. *Addenda de biosûreté apporté à la Norme canadienne sur la biosécurité, troisième édition*, Ottawa, ON, Gouvernement du Canada. https://www.canada.ca/fr/sante-publique/services/normes-lignes-directrices-canadiennes-biosecurite/addenda-biosurete-apporte-norme-canadienne-biosecurite-troisieme-edition.html

ASPC – Agence de la santé publique du Canada, 2025a. Fiche Technique Santé-Sécurité : Agents Pathogènes.https://www.canada.ca/fr/sante-publique/services/biosecurite-biosurete-laboratoire/fiches-techniques-sante-securite-agents-pathogenes-evaluation-risques.html (consulté en juin 2024).

ASPC – Agence de la santé publique du Canada, 2025b. Publication de l'Addenda de biosûreté apporté à la Norme canadienne sur la biosécurité, troisième édition. https://training-formation.phac-aspc.gc.ca/mod/page/view.php?id=16605&lang=fr (consulté en juin 2025).

Asselin, R., 2024. *Moteurs de croissance*, Ottawa, ON, Conseil canadien des affaires. https://www.thebusinesscouncil.ca/fr/rapport/moteurs-de-croissance/.

Asselin, R., et S. Speer, 2019. *Une nouvelle étoile polaire : la compétitivité canadienne à l'ère de l'économie immatérielle*, Ottawa, ON, Forum des politiques publiques. https://ppforum.ca/fr/publications/une-nouvelle-etoile-polaire-et-la-competitivite-canadienne-economie-intangibles/.

Assemblée générale des Nations Unies, 1948. *Déclaration universelle des droits de l'homme*, New York, NY, Assemblée générale des Nations Unies. https://www.un.org/fr/about-us/universal-declaration-of-human-rights.

Assemblée générale des Nations Unies, 1966. *Pacte international relatif aux droits économiques, sociaux et culturels*, New York, NY, Assemblée générale des Nations Unies. https://www.ohchr.org/fr/instruments-mechanisms/instruments/international-covenant-economic-social-and-cultural-rights.

AWTI – Netherlands Advisory Council for Science, Technology and Innovation, 2022. *Knowledge in Conflict: Striking a Balance between Security and Liberty*, La Haye, Pays-Bas, AWTI. https://www.awti.nl/documenten/adviezen/2022/11/29/advice-knowledge-in-conflict.

Babb, S., 2020. *Regulating Human Research: IRBs from Peer Review to Compliance Bureaucracy*, Stanford, CA, Stanford University Press.

Belli, L., W. B. Gaspar et S. Singh Jaswant, 2024. « Data sovereignty and data transfers as fundamental elements of digital transformation: Lessons from the BRICS countries », *Computer Law & Security Review*, vol. 54, p. 106017. https://doi.org/10.1016/j.clsr.2024.106017.

Berns, K. A., D. Charboneau, C. J. Foth, J. Hesley, et P. Korsmo-Kennon, 2007. *Directing Change Management at the University of Minnesota*, Minneapolis, MN, University of Minnesota Twin Cities. https://conservancy.umn.edu/server/api/core/bitstreams/ec0e9e79-cd7a-45c8-a9e3-b2d3ad233542/content.

Bernstein, M. S., M. Levi, D. Magnus, B. Rajala, D. Satz, et C. Waeiss, 2021. « ESR: Ethics and society review of artificial intelligence research », *arXiv, Préimpression*. http://arxiv.org/abs/2106.11521.

Bilodeau, M., 2024 (21 août). « Libre accès : une mine de diamants sous ses pieds », *Affaires universitaires*. https://shorturl.at/RpfDx (consulté en juin 2025).

BIS – Bureau of Industry and Security of the U.S. Department of Commerce, 2024. *Export Administration Regulations*, 15 CFR.

Brady, A.-M., 2017. *China as a Polar Great Power*, Cambridge, Royaume-Uni, Cambridge University Press.

Brandusescu, A., 2021. *Artificial Intelligence Policy and Funding in Canada: Public Investments, Private Interests*, Montréal, QC, Centre des recherches interdisciplinaires en études montréalaises, Université McGill. https://www.mcgill.ca/centre-montreal/files/centre-montreal/publicaipolicyandfunding_report_updated_mar5.pdf.

Brenneis, A., 2024. « Assessing dual use risks in AI research: Necessity, challenges and mitigation strategies », *Research Ethics*, vol. 21, nº 2, p. 302-330. https://doi.org/10.1177/17470161241267782.

Breum, M., 2024 (23 janvier). « The lack of data from Russia may render Arctic climate forecasting meaningless », *Arctic Today*. https://www.arctictoday.com/the-lack-of-data-from-russia-may-render-arctic-climate-forecasting-meaningless/ (consulté en novembre 2024).

Brockmann, K., S. Bauer et V. Boulanin, 2019. *BIO PLUS X: Arms Control and the Convergence of Biology and Emerging Technologies*, Solna, Suède, Stockholm International Peace Research Institute (SIPRI). https://www.sipri.org/sites/default/files/2019-03/sipri2019_bioplusx_0.pdf.

CAC – Conseil des académies canadiennes, 2013. *Les sciences de la mer au Canada : Relever le défi, saisir l'opportunité*, Ottawa, ON, Comité d'experts sur les sciences de la mer au Canada, CAC. https://doi.org/10.60870/ycmk-d405.

CAC – Conseil des académies canadiennes, 2017. *Politique scientifique : Considérations pour les gouvernements infranationaux*, Ottawa, ON, Rapport du comité directeur de l'atelier, CAC. https://doi.org/10.60870/evab-1686.

CAC – Conseil des académies canadiennes, 2021. *Formés pour réussir*, Ottawa, ON, Comité d'experts sur la transition des titulaires de doctorat vers le marché du travail, CAC. https://doi.org/10.60870/a9pp-t168.

CAC – Conseil des académies canadiennes, 2023a. *Leadership et équité dans la recherche nordique*, Ottawa, ON, Comité d'experts sur l'avenir de la recherche dans l'Arctique et le Nord canadiens, CAC. https://doi.org/10.60870/23p9-tx16.

CAC – Conseil des académies canadiennes, 2023b. *Potentiel quantique*, Ottawa, ON, Comité d'experts sur l'adoption responsable des technologies quantiques, CAC. https://doi.org/10.60870/n41k-5d04.

CAC – Conseil des académies canadiennes, 2024a. *Évoluer dans des futurs collaboratifs*, Ottawa, ON, Comité d'experts sur les partenariats internationaux en science, technologie, innovation et production de connaissances, CAC. https://doi.org/10.60870/68cz-2y87.

CAC – Conseil des académies canadiennes, 2024b. *Équité, diversité et inclusion dans le système de recherche postsecondaire*, Ottawa, ON, Comité d'experts sur les pratiques d'EDI pour des changements porteurs, CAC. https://doi.org/10.60870/9m4s-yj08.

CAC – Conseil des académies canadiennes, 2025. *Sécurité de la recherche au Canada et à l'étranger*, Ottawa, ON, CAC. https://www.rapports-cac.ca/wp-content/uploads/2025/10/Balancing-Research-Security-and-Open-Science-FR.pdf.

CACN – Comité spécial sur la relation entre le Canada et la République populaire de Chine, 2024. *Les liens entre la science et la sécurité nationale au Canada : le cas du Laboratoire national de microbiologie de Winnipeg*, Ottawa, ON, Chambre des communes. https://www.ourcommons.ca/Content/Committee/441/CACN/Reports/RP13349277/cacnrp08/cacnrp08-f.pdf.

Carroll, S. R., E. Herczog, M. Hudson, K. Russell et S. Stall, 2021. « Operationalizing the CARE and FAIR Principles for Indigenous data futures », *Scientific Data*, vol. 8, p. 108. https://doi.org/10.1038/s41597-021-00892-0.

Casadevall, A., T. S. Dermody, M. J. Imperiale, R. M. Sandri-Goldin et T. Shenk, 2015. « Dual-use research of concern (DURC) review at American Society for Microbiology journals », *mBio*, vol. 6, nº 4, e01236-15. https://doi.org/10.1128/mBio.01236-15.

CBC News, 2014 (13 août). « Klaus Nielsen pleads guilty to trying to export infectious agent », *CBC News*. https://www.cbc.ca/news/canada/ottawa/klaus-nielsen-pleads-guilty-to-trying-to-export-infectious-agent-1.2735012 (consulté en juin 2025).

CBC News, 2024 (12 avril). « Former Canadian Space Agency engineer acquitted on charge of acting for Chinese firm », *CBC News*. https://www.cbc.ca/news/canada/montreal/space-agency-spying-quebec-1.7171861 (consulté en juillet 2025).

CCRC – Comité de coordination de la recherche au Canada, 2025. Caractéristiques du fonds Nouvelles frontières en recherche. https://sshrc-crsh.canada.ca/funding-financement/nfrf-fnfr/characteristics-caracteristiques-fra.aspx (consulté en novembre 2024).

CCSN – Commission canadienne de sûreté nucléaire, 2014. FAQs : Contrôles de l'utilisation finale. https://www.cnsc-ccsn.gc.ca/fra/nuclear-substances/import-and-export-controls/index-faq/ (consulté en février 2025).

CE – Commission européenne, 2019. Open science. https://www.cesaer.org/content/10-library/2023/ec-rtd-factsheet-open-science-2019.pdf (consulté en août 2024).

CE – Commission européenne, 2021a. *Recommandation (UE) 2021/1700 de la Commission du 15 septembre 2021 relative aux programmes internes de conformité pour les contrôles de la recherche portant sur les biens à double usage en vertu du règlement (UE) 2021/821 du Parlement européen et du Conseil instituant un régime de l'Union de contrôle des exportations, du courtage, de l'assistance technique, du transit et des transferts en ce qui concerne les biens à double usage*, Bruxelles, Belgique, Journal officiel de l'Union européenne. https://op.europa.eu/fr/publication-detail/-/publication/a5b08317-1c07-11ec-b4fe-01aa75ed71a1.

CE – Commission européenne, 2021b. *Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast).*

CE – Commission européenne, 2022. *Open Science and Intellectual Property Rights: How Can They Better Interact? State of the Art and Reflections*, Bruxelles, Belgique, Office des publications de l'Union européenne. https://data.europa.eu/doi/10.2777/347305.

CE – Commission européenne, 2024a. *Recommandation du conseil sur le renforcement de la sécurité de la recherche*, Bruxelles, Belgique, CE. https://data.consilium.europa.eu/doc/document/ST-9097-2024-INIT/fr/pdf.

CE – Commission européenne, 2024b. Fact sheet: Council recommendation on research security. https://research-and-innovation.ec.europa.eu/document/download/09a49b8b-ddc8-43eb-856f-73ffbe5076c8_en?filename=ec_rtd_council-recommendation-research-security-fs.pdf (consulté en août 2024).

CE – Commission européenne, s.d.-a. Canada. https://research-and-innovation.ec.europa.eu/strategy/strategy-research-and-innovation/europe-world/international-cooperation/bilateral-cooperation-science-and-technology-agreements-non-eu-countries/canada_en (consulté en juin 2025).

CE – Commission européenne, s.d.-b. Trends for open access to publications. https://web.archive.org/web/20240921011832/https://research-and-innovation.ec.europa.eu/strategy/strategy-2020-2024/our-digital-future/open-science/open-science-monitor/trends-open-access-publications_en (consulté en septembre 2024).

Centre pour la cybersécurité – Centre canadien pour la cybersécurité, 2020. *Bulletin sur les cybermenaces : L'incidence continue de la COVID-19 sur les activités de cybermenaces*, Ottawa, ON, Gouvernement du Canada. https://www.cyber.gc.ca/fr/orientation/bulletin-sur-les-cybermenaces-lincidence-continue-de-la-covid-19-sur-les-activites-de.

Centre pour la cybersécurité – Centre canadien pour la cybersécurité, 2024a. *The Cyber Threat to Research Laboratories*, Ottawa, ON, Gouvernement du Canada. https://www.cyber.gc.ca/en/guidance/cyber-threat-research-laboratories.

Centre pour la cybersécurité – Centre canadien pour la cybersécurité, 2024b. Security considerations for research and development organizations (ITSAP.00.130). https://www.cyber.gc.ca/en/guidance/security-considerations-research-and-development-itsap00130 (consulté en juin 2025).

Centre pour la cybersécurité – Centre canadien pour la cybersécurité, 2024c. *National Cyber Threat Assessment 2025–2026*, Ottawa, ON, Centre canadien pour la cybersécurité. https://www.cyber.gc.ca/sites/default/files/national-cyber-threat-assessment-2025-2026-e.pdf.

CF – Cour fédérale, 2023a. *Jahantigh c. Canada (Citoyenneté et Immigration)*, 2023 CF 1253.

CF – Cour fédérale, 2023b. *Li c. Canada (Citoyenneté et Immigration)*, 2023 CF 1753.

CGIPN – Le Centre de gouvernance de l'information des Premières Nations, 2020. *Stratégie de gouvernance des données des Premières Nations*, Ottawa, ON, CGIPN. https://fnigc.ca/wp-content/uploads/2020/06/fnigc_fndgs_fr_final.pdf.

CGIPN – Le Centre de gouvernance de l'information des Premières Nations, 2021. *The First Nation Data Centre (FNDC) On-Site Policies and Procedures Guide*, Ottawa, ON, FNIGC. https://fnigc.ca/wp-content/uploads/2022/01/FNDC_On-site-Policies-and-Procedures-Nov_2021.pdf.

CGIPN – Le Centre de gouvernance de l'information des Premières Nations, 2024. *Guide des Premières Nations relatif à la Loi sur la protection des renseignements personnels*. Ottawa, ON, CGIPN. https://fnigc.ca/wp-content/uploads/2024/08/FNIGC_FN_Guide_Privacy_Act_FR-1.pdf.

CGIPN – Le Centre de gouvernance de l'information des Premières Nations, s.d. Les principes de PCAP® des Premières Nations. https://fnigc.ca/fr/les-principes-de-pcap-des-premieres-nations/ (consulté en octobre 2022).

Chase, S., 2022 (9 août). « Alberta relaxes some restrictions on university partnerships with links to Chinese government », *The Globe and Mail*. https://www.theglobeandmail.com/politics/article-alberta-university-partnerships-chinese-government/ (consulté en janvier 2025).

CICan – Collèges & instituts Canada, 2023. *Canadian Colleges: Creating IP and Powering Commercialization: Submission to the House of Commons Standing Committee on Science and Research – Study on the Commercialization of Intellectual Property*, Ottawa, ON, CICan. https://www.ourcommons.ca/Content/Committee/441/SRSR/Brief/BR12369907/br-external/CollegesandInstitutesCanada-e.pdf.

CLS – Canadian Light Source, s.d. Research security. https://www.lightsource.ca/users/your-cls-experiment/practical-information/research-security.php (consulté en mars 2025).

CNRC – Conseil national de recherches Canada, 2024. Énoncé sur la sécurité de la recherche. https://nrc.canada.ca/fr/organisation/valeurs-ethique/enonce-securite-recherche (consulté en mai 2025).

CNRS – Centre national de la recherche scientifique, 2024. *Call for evidence. Boosting research security in the EU.* Contribution du Centre national de la recherche scientifique. https://international.cnrs.fr/wp-content/uploads/2024/01/Contribution-du-CNRS-au-Call-for-Evidence-on-Research-Security-FR.pdf (consulté en août 2024).

cOAlition S, s.d.-a. Organisations endorsing Plan S and working jointly on its implementation. https://www.coalition-s.org/organisations/ (consulté en septembre 2024).

cOAlition S, s.d.-b. Plan S: Making full and immediate open access a reality. https://www.coalition-s.org/ (consulté en juin 2025).

CoARA – Coalition for Advancing Research Assessment, 2022. *Agreement on Reforming Research Assessment*, s.l., CoARA. https://coara.eu/app/uploads/2022/09/2022_07_19_rra_agreement_final.pdf.

CoARA – Coalition for Advancing Research Assessment, 2025. Signatories. https://coara.eu/agreement/signatories/ (consulté en juin 2025).

Cobey, K. D., S. Haustein, J. Brehaut, U. Dirnagl, D. L. Franzen, L. G. Hemkens, … D. Moher, 2023. « Community consensus on core open science practices to monitor in biomedicine », *PLOS Biology*, vol. 21, nº 1, p. e3001949. https://doi.org/10.1371/journal.pbio.3001949.

COGR – Council on Governmental Relations, 2023. *Multi-Agency Panel on Research Security Risk Assessment & Analysis*, Washington, D.C., COGR. https://www.cogr.edu/sites/default/files/Multi-Agency%20Research%20Security%20Panel_0.pdf.

COGR – Council on Governmental Relations, 2024. *Overview of OSTP Guidelines for Research Security Programs at Covered Institutions*, Washington, D.C., COGR. https://www.cogr.edu/sites/default/files/Overview%20of%20OSTP%20Guidelines%20for%20Research%20Security%20Programs%20at%20Covered%20Institution%20clean%20copy%20july%2012%202024%20REVISED.pdf.

Conseil canadien des affaires, 2023. *La sécurité économique est la sécurité nationale les arguments en faveur d'une stratégie canadienne*, Ottawa, ON, Conseil canadien des affaires. https://www.thebusinesscouncil.ca/fr/rapport/strongla-securite-economique-est-la-securite-nationale-strong/.

Conseil canadien des affaires, s.d. Nos membres. https://www.thebusinesscouncil.ca/fr/a-propos-de-nous/nos-membres/ (consulté en juin 2025).

CoreTrustSeal Standards and Certification Board, 2022. « CoreTrustSeal Requirements 2023–2025 », *Zenodo, Préimpression*. https://zenodo.org/record/7051011.

COS – Center for Open Science, s.d. What is open science? https://www.cos.io/open-science (consulté en août 2024).

CPM – Cabinet du Premier ministre du Canada, 2024a. Pour un avantage canadien en matière d'intelligence artificielle. https://www.pm.gc.ca/fr/nouvelles/communiques/2024/04/07/pour-avantage-canadien-matiere-dintelligence-artificielle (consulté en juin 2024).

CPM – Cabinet du Premier ministre du Canada, 2024b. Déclaration commune du premier ministre Trudeau et de la présidente von der Leyen concernant l'association du Canada à Horizon Europe. https://www.pm.gc.ca/fr/nouvelles/declarations/2024/07/03/declaration-commune-du-premier-ministre-trudeau-et-de-la (consulté en novembre 2024).

CPSNR – Comité des parlementaires sur la sécurité nationale et le renseignement, 2021. *Le Comité des parlementaires sur la sécurité nationale et le renseignement Rapport annuel 2020*, Ottawa, ON, CPSNR. https://nsicop-cpsnr.ca/reports/rp-2021-04-12-ar/annual_report_2020_public_fr.pdf.

CPVP – Commissariat à la protection de la vie privée du Canada, 2018. Aperçu des lois sur la protection des renseignements personnels au Canada. https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-renseignements-personnels-au-canada/02_05_d_15/ (consulté en novembre 2024).

CRSNG – Conseil de recherches en sciences naturelles et en génie du Canada, 2018. Politique sur la propriété intellectuelle. https://www.nserc-crsng.gc.ca/NSERC-CRSNG/policies-politiques/ip-pi_fra.asp?utm_source=chatgpt.com (consulté en juin 2025).

CRSNG – Conseil de recherches en sciences naturelles et en génie du Canada, 2023. Déclaration de San Francisco sur l'évaluation de la recherche (DORA) https://www.nserc-crsng.gc.ca/NSERC-CRSNG/policies-politiques/DORA-DORA_fra.asp (consulté en novembre 2023).

CRSNG – Conseil de recherches en sciences naturelles et en génie du Canada, 2024a. Sécurité de la recherche : Orientations des trois organismes concernant la sécurité de la recherche. https://www.nserc-crsng.gc.ca/InterAgency-Interorganismes/RS-SR/index_fra.asp (consulté en avril 2024).

CRSNG – Conseil de recherches en sciences naturelles et en génie du Canada, 2024b. Sécurité de la recherche : Orientations des trois organismes concernant Les Lignes directrices sur la sécurité nationale pour les partenariats de recherche. https://www.nserc-crsng.gc.ca/InterAgency-Interorganismes/RS-SR/nsgrp-ldsnpr_fra.asp (consulté en janvier 2025).

CRSNG – Conseil de recherches en sciences naturelles et en génie du Canada, 2024c. Subventions Avantage du programme Alliance. https://www.nserc-crsng.gc.ca/innovate-innover/alliance-alliance/index_fra.asp (consulté en novembre 2024).

CRSNG – Conseil de recherches en sciences naturelles et en génie du Canada, 2024d. Sécurité de la recherche : Ressources. https://www.nserc-crsng.gc.ca/InterAgency-Interorganismes/RS-SR/resources-ressources_fra.asp (consulté en novembre 2024).

CRSNG – Conseil de recherches en sciences naturelles et en génie du Canada, 2025. Sécurité de la recherche : Orientations des trois organismes concernant la Politique sur la recherche en technologies sensibles et sur les affiliations préoccupantes. https://www.nserc-crsng.gc.ca/InterAgency-Interorganismes/RS-SR/strac-rtsap_fra.asp (consulté en juin 2025).

Cunningham, A., 2024 (14 mai). « Shifting ice: How the Russian invasion of Ukraine has changed Arctic Circle governance and the Arctic Council's path forward », *The Arctic Institute—Center for Circumpolar Security Studies*. https://www.thearcticinstitute.org/shifting-ice-russian-invasion-ukraine-arctic-circle-governance-arctic-councils-path-forward/ (consulté en novembre 2024).

d'Hooghe, I., et J. Lammertink, 2022. *How National Governments and Research Institutions Safeguard Knowledge Development in Science and Technology*, Leiden, Pays-Bas, Leiden Asia Centre & Netherlands Advisory Council for Science, Technology and Innovation. https://leidenasiacentre.nl/wp-content/uploads/2022/11/How-National-Governments-and-Research-Institutions-Safequard-Knowledge-Development-in-Science-and-Technology.pdf.

DAAD – German Academic Exchange Service Support, s.d. Kompetenzzentrum Internationale Wissenschaftskooperationen (KIWi) [centre d'excellence de coopération scientifique internationale]. https://www.daad.de/de/infos-services-fuer-hochschulen/kompetenzzentrum/ (consulté en août 2024).

Dao, T. K., K. M. Evans, M. D. Shannon, C. Bronk, C. Neuhauser et E. Roberts, 2024. *Responsible Collaboration Through Appropriate Research Security: A Workshop To Discuss and Study the Emergent Discipline of Research on Research Security*, Houston, TX, Rice University's Baker Institute for Public Policy. https://www.bakerinstitute.org/research/responsible-collaboration-through-appropriate-research-security.

Davidson, P., 2017 (1er décembre). « Beyond the basics: Taking Canada–China collaboration to the next level », *Hill Times*. https://univcan.ca/news/beyond-basics-taking-canada-china-collaboration-next-level/ (consulté en mai 2025).

de Beer, J. et D. Dylan, 2015. « Traditional knowledge governance challenges in Canada », dans Rimmer, M. (dir.), *Indigenous Intellectual Property*. Cheltenham, Royaume-Uni, Edward Elgar Publishing.

de Beer, J., s.d. Who has jurisdiction over intellectual property law and policy in Canada's federal system? https://www.jeremydebeer.ca/intellectual-property-a-canadian-federalism/ (consulté en juin 2025).

De Bruijn, A., 2023 (30 mai). « New knowledge security screening is counterproductive », *Delta*. https://delta.tudelft.nl/en/article/new-knowledge-security-screening-counterproductive (consulté en août 2024).

Department for Science, Innovation & Technology, 2023. *RCAT update August 2023*, Londres, Royaume-Uni, Gouvernement du Royaume-Uni. https://assets.publishing.service.gov.uk/media/654a2f1be2e16a000d42aae4/research_collaboration_advice_team_update_report.pdf.

DiEuliis, D., et J. Giordano, 2017. « Why gene editors like CRISPR/Cas may be a game-changer for neuroweapons », *Health Security*, vol. 15, nº 3, p. 296-302. https://doi.org/10.1089/hs.2016.0120.

DLR – German Aerospace Center, 2022. *Annotated Collection of Guidance for Secure and Successful International R&I Cooperation*, Bonn, Allemagne, DLR. https://www.safeguarding-science.eu/wp-content/uploads/annotated-collection-2022.pdf.

DLR – German Aerospace Center, 2023. *Open Source Intelligence (OSINT) Application to Illustrate the Potential Compromise of Academic Knowledge Security Systems*, Bonn, Allemagne, DLR. https://www.safeguarding-science.eu/wp-content/uploads/OSINT_report_exec_sum-11-2023.pdf.

DLR – German Aerospace Center, 2024. *Due Diligence in Science*, Bonn, Allemagne, DLR. https://www.safeguarding-science.eu/wp-content/uploads/Due-Diligence-in-Science_Manual2024.pdf.

DOD – Department of Defense, 2022. JASON Defense Advisory Panel reports. https://irp.fas.org/agency/dod/jason/ (consulté en septembre 2024).

DOD – Department of Defense, 2023. *Policy for Risk-Based Security Reviews of Fundamental Research*, Washington, D.C., DOD. https://media.defense.gov/2023/Jun/29/2003251160/-1/-1/1/COUNTERING-UNWANTED-INFLUENCE-IN-DEPARTMENT-FUNDED-RESEARCH-AT-INSTITUTIONS-OF-HIGHER-EDUCATION.PDF.

DORA – Declaration on Research Assessment, 2012. Déclaration de San Francisco sur l'évaluation de la recherche. https://sfdora.org/read/ (consulté en novembre 2024).

ECCC – Environnement et Changement climatique Canada, 2021. *Plan d'action pour la science ouverte d'Environnement et changement climatique Canada : 2021-2026*, Gatineau, QC, Gouvernement du Canada. https://publications.gc.ca/collections/collection_2021/eccc/En4-446-2021-fra.pdf.

Eiterjord, T., 2023 (23 novembre). « What the 14th Five-Year Plan Says About China's Arctic Interests », *The Arctic Institute—Center for Circumpolar Security Studies*. https://www.thearcticinstitute.org/14th-five-year-plan-chinas-arctic-interests/ (consulté en novembre 2024).

Eiterjord, T., 2024. « Securitise the volume: Epistemic territorialisation and the geopolitics of China's Arctic research », *Territory, Politics, Governance*, vol. 12, nº 1, p. 93-111. https://doi.org/10.1080/21622671.2023.2179535.

Engel-Glatter, S., et M. Ienca, 2018. « Life scientists' views and perspectives on the regulation of dual-use research of concern », *Science and Public Policy*, vol. 45, nº 1, p. 92-102. https://doi.org/10.1093/scipol/scx050.

Evan, W. M., et B. B. Hays, 2006. « Dual-use technology in the context of the non-proliferation regime », *History and Technology*, vol. 22, nº 1, p. 105-113. https://doi.org/10.1080/07341510500517850.

Evans, N. G. et A. Commins, 2017 (2 février). « Defining dual-use research: When scientific advances can both help and hurt humanity », *The Conversation*. http://theconversation.com/defining-dual-use-research-when-scientific-advances-can-both-help-and-hurt-humanity-70333 (consulté en mars 2024).

Evans, N. G., M. J. Selgelid et R. M. Simpson, 2022. « Reconciling regulation with scientific autonomy in dual-use research », *The Journal of Medicine and Philosophy: A Forum for Bioethics and Philosophy of Medicine*, vol. 47, nº 1, p. 72-94. https://doi.org/10.1093/jmp/jhab041.

Evans, P., 2022 (19 septembre). « Canadian universities & China: Research collaborations in question », *The Institute for Peace and Diplomacy*. https://peacediplomacy.org/2022/09/19/canadian-universities-china-research-collaborations-in-question/.

Falco, G., N. Boschetti et I. Nikas, 2024. *Undercover Infrastructure: Dual-Use Arctic Satellite Ground Stations*, Waterloo, ON, Centre for International Governance Innovation. https://www.cigionline.org/publications/undercover-infrastructure-dual-use-arctic-satellite-ground-stations/.

FCI – Fondation canadienne pour l'innovation, s.d.-a. Fonds des initiatives scientifiques majeures : https://www.innovation.ca/fr/appel-gestion/financement/fonds-initiatives-scientifiques-majeures (consulté en mars 2025).

FCI – Fondation canadienne pour l'innovation, s.d.-b. Sécurité de la recherche. https://www.innovation.ca/fr/appel-gestion/ressources-lien-avec-appels-propositions-gestion-financement/securite-recherche (consulté en février 2025).

Flagg, M., et Z. Arnold, 2021. *A New Institutional Approach to Research Security in the United States*, Washington, D.C., Center for Security and Emerging Technology. https://cset.georgetown.edu/publication/a-new-institutional-approach-to-research-security-in-the-united-states/.

Franklin, A. R., 2025 (29 janvier). « How Rice is using generative AI to enhance research security, saving hundreds of expert hours each week », *Rice University*. https://news.rice.edu/news/2025/how-rice-using-generative-ai-enhance-research-security-saving-hundreds-expert-hours-each (consulté en juin 2025).

FRQ – Fonds de recherche du Québec, 2020. Les Fonds de recherche du Québec adhèrent à la Déclaration de San Francisco sur l'évaluation de la recherche. https://frq.gouv.qc.ca/les-fonds-de-recherche-du-quebec-adherent-a-la-declaration-de-san-francisco-sur-levaluation-de-la-recherche/ (consulté en février 2024).

FRQ – Fonds de recherche du Québec, 2022. *Politique de diffusion en libre accès (version révisée)*, Québec, QC, FRQ. https://frq.gouv.qc.ca/app/uploads/2022/06/politique-libre-acces-revisee_vf.pdf.

Fujii, Y., E. Rémy, H. Zuo, P. Oke, G. Halliwell, F. Gasparin, … N. Usui, 2019. « Observing system evaluation based on ocean data assimilation and prediction systems: On-going challenges and a future vision for designing and supporting ocean observational networks », *Frontiers in Marine Science*, vol. 6, p. 417. https://doi.org/10.3389/fmars.2019.00417.

Funaiole, M. P., B. Hart, J. S. Bermudez Jr., et A. Powers-Riggs, 2023 (18 avril). « Frozen frontiers: China's great power ambitions in the polar regions », *Center for Strategic and International Studies*. https://features.csis.org/hiddenreach/china-polar-research-facility (consulté en mai 2025).

Gabel, C. et R. Henry, 2024. *National Métis Health Data Strategy and Principles*, Ottawa, ON, Métis National Council. https://macsphere.mcmaster.ca/bitstream/11375/30688/2/MNC_Final_Draft_Report_March_2024.pdf.

Gaffey, C. B., N. Bax, N. Krauzig, et K. Tougeron, 2024. « A call to strengthen international collaboration to assess climate change effects in polar regions », *PLOS Climate*, vol. 3, nº 10, e0000495. https://doi.org/10.1371/journal.pclm.0000495.

Gattolin, A., 2021. *Mission d'information « Influences étatiques extra-européennes dans le monde universitaire et académique français et leurs incidences »*, Paris, France, Le Sénat. https://www.senat.fr/rap/r20-873/r20-8731.pdf.

GC – Gouvernement du Canada, 1982. *Loi constitutionnelle de 1982, constituant l'annexe B de la Loi de 1982 sur le Canada (R.-U.), 1982, c 11.*

GC – Gouvernement du Canada, 1985a. *Loi sur la concurrence,* L.R.C. 1985, ch. C-34.

GC – Gouvernement du Canada, 1985b. *Loi sur la production de défense*, L.R.C. 1985, ch. D-1.

GC – Gouvernement du Canada, 1985c. *Loi sur les licences d'exportation et d'importation*, L.R.C. 1985, ch. E-19.

GC – Gouvernement du Canada, 1986. *Accord entre le Gouvernement du Canada et le Gouvernement du Japon sur la coopération scientifique et technologique*, Ottawa, ON, GC. https://www.treaty-accord.gc.ca/text-texte.aspx?id=102070&Lang=fra.

GC – Gouvernement du Canada, 1992. *Loi sur les mesures économiques spéciales,* L.C. 1992, ch. 17.

GC – Gouvernement du Canada, 1997. *Loi sur la sûreté et la réglementation nucléaires*, L.C. 1997, ch. 9.

GC – Gouvernement du Canada, 2001. *Loi sur l'immigration et la protection des réfugiés*, L.C. 2001, ch. 27.

GC – Gouvernement du Canada, 2008. *Accord de coopération scientifique et technique entre le Canada et la Chine*, Ottawa, ON, GC. https://www.canada.ca/fr/environnement-changement-climatique/organisation/affaires-internationales/partenariats-pays-regions/asie/canada-chine-cooperation-scientifique-technique.html.

GC – Gouvernement du Canada, 2009. *Loi sur les agents pathogènes humains et les toxines*, L.C. 2009, ch. 24.

GC – Gouvernement du Canada, 2010. *Règlement sur le contrôle de l'importation et de l'exportation aux fins de la non-prolifération nucléaire*, DORS/2000-210.

GC – Gouvernement du Canada, 2016. *Règlement sur les marchandises contrôlées*, DORS/2001-32.

GC – Gouvernement du Canada, 2019a. *Établir de nouvelles orientations à l'appui de la recherche et de la formation en recherche autochtone au Canada*, Ottawa, ON, GC. https://www.canada.ca/fr/comite-coordination-recherche/priorites/recherche-autochtone/plan-strategique-2019-2022.html.

GC – Gouvernement du Canada, 2019b. Laboratoire 101 : Que faut-il pour entreposer les agents pathogènes les plus dangereux au monde? https://science.gc.ca/site/science/fr/blogues/science-sante/laboratoire-101-faut-il-pour-entreposer-agents-pathogenes-plus-dangereux-monde (consulté en janvier 2025).

GC – Gouvernement du Canada, 2020. *Feuille de route pour la science ouverte*, Ottawa, ON, Bureau de la Conseillère scientifique en chef. https://science.gc.ca/site/science/fr/bureau-conseillere-scientifique-chef/science-ouverte/feuille-route-pour-science-ouverte.

GC – Gouvernement du Canada, 2021a. *Budget 2021 : une relance axée sur les emplois, la croissance et la résilience*, Ottawa, ON, GC. https://publications.gc.ca/collections/collection_2021/fin/F1-23-3-2021-fra.pdf.

GC – Gouvernement du Canada, 2021b. Politique des trois organismes sur la gestion des données de recherche. https://science.gc.ca/site/science/fr/financement-interorganismes-recherche/politiques-lignes-directrices/gestion-donnees-recherche/politique-trois-organismes-gestion-donnees-recherche (consulté en août 2024).

GC – Gouvernement du Canada, 2021c. *Liste des marchandises et technologies d'exportation contrôlée*, DORS/89-202.

GC – Gouvernement du Canada, 2021d. Évaluez votre profil de risque. https://science.gc.ca/site/science/fr/protegez-votre-recherche/lignes-directrices-outils-pour-mise-oeuvre-securite-recherche/evaluez-votre-profil-risque (consulté en mai 2024).

GC – Gouvernement du Canada, 2021e. Quels sont les risques? https://science.gc.ca/site/science/fr/protegez-votre-recherche/renseignements-generaux-securite-recherche/quels-sont-risques (consulté en mars 2024).

GC – Gouvernement du Canada, 2021f. Qui constitue une menace? https://science.gc.ca/site/science/fr/protegez-votre-recherche/renseignements-generaux-securite-recherche/qui-constitue-menace (consulté en mars 2024).

GC – Gouvernement du Canada, 2022a. Pourquoi devriez-vous protéger votre recherche? https://science.gc.ca/site/science/fr/protegez-votre-recherche/renseignements-generaux-securite-recherche/pourquoi-devriez-vous-proteger-votre-recherche (consulté en mars 2024).

GC – Gouvernement du Canada, 2022b. *Cadre de référence des trois organismes sur la conduite responsable de la recherche (2021)*, Ottawa, ON, GC. https://rcr.ethics.gc.ca/fra/framework-cadre-2021.html.

GC – Gouvernement du Canada, 2022c. Fonds d'excellence en recherche Apogée Canada : Présentation des demandes – Concours de 2022. https://www.cfref-apogee.gc.ca/program-programme/competitions-concours/2022/apply-demande-fra.aspx#2.6 (consulté en février 2025).

GC – Gouvernement du Canada, 2024a. *La Politique étrangère du Canada pour l'Arctique*, Ottawa, ON, GC. https://www.international.gc.ca/gac-amc/publications/transparency-transparence/arctic-arctique/arctic-policy-politique-arctique.aspx?lang=fra.

GC – Gouvernement du Canada, 2024b. *Budget de 2024 : Une chance équitable pour chaque génération*, Ottawa, ON, GC. https://www.canada.ca/fr/ministere-finances/nouvelles/2024/04/une-chance-equitable-pour-chaque-generation.html.

GC – Gouvernement du Canada, 2024c. Politique des trois organismes sur la gestion des données de recherche – Foire aux questions. https://science.gc.ca/site/science/fr/financement-interorganismes-recherche/politiques-lignes-directrices/gestion-donnees-recherche/politique-trois-organismes-gestion-donnees-recherche-foire-aux-questions (consulté en février 2025).

GC – Gouvernement du Canada, 2024d. *Règlement sur les agents pathogènes humains et les toxines*, DORS/2015-44.

GC – Gouvernement du Canada, 2024e. Fonds de soutien à la recherche. https://www.rsf-fsr.gc.ca/apply-demande/research_security-securite-recherche-fra.aspx (consulté en février 2025).

GC – Gouvernement du Canada, 2024f. Financement de la sécurité de la recherche attribué en 2024-2025. https://www.rsf-fsr.gc.ca/apply-demande/grants-subventions/rs2024-fra.aspx (consulté en juin 2025).

GC – Gouvernement du Canada, 2024g. Études de cas – scénarios. https://science.gc.ca/site/science/fr/protegez-votre-recherche/lignes-directrices-outils-pour-mise-oeuvre-securite-recherche/etudes-cas-comment-atteinte-securite-peut-avoir-repercussions-votre-recherche (consulté en mai 2024).

GC – Gouvernement du Canada, 2024h. *Guide de la Liste des marchandises et technologies d'exportation contrôlée du Canada—Janvier 2024*, Ottawa, ON, GC. https://www.international.gc.ca/trade-commerce/assets/pdfs/guides/export-control-list-guide-2024-fra.pdf.

GC – Gouvernement du Canada, 2024i. Plan directeur du sous-programme communications, capacités et sensibilisation. https://science.gc.ca/site/science/fr/programme-lutte-contre-contaminants-dans-nord/appel-propositions-2025/programme-lutte-contre-contaminants-dans-nord-2025-appel-propositions#section9 (consulté en janvier 2025).

GC – Gouvernement du Canada, 2024j. Centre de la sécurité de la recherche. https://science.gc.ca/site/science/fr/protegez-votre-recherche/lignes-directrices-outils-pour-mise-oeuvre-securite-recherche/centre-securite-recherche (consulté en novembre 2024).

GC – Gouvernement du Canada, 2024k. Le Secrétariat sur la conduite responsable de la recherche (SCRR). https://rcr.ethics.gc.ca/fra/srcr-scrr_staff-personnel.html (consulté en juin 2025).

GC – Gouvernement du Canada, 2025a. Le gouvernement du Canada finalise son investissement pour soutenir Cohere, une entreprise phare en matière d'intelligence artificielle fondée au Canada. https://www.canada.ca/fr/innovation-sciences-developpement-economique/nouvelles/2025/03/le-gouvernement-du-canada-finalise-son-investissement-pour-soutenir-cohere-une-entreprise-phare-en-matiere-dintelligence-artificielle-fondee-au-canada.html (consulté en mai 2025).

GC – Gouvernement du Canada, 2025b. Le gouvernement du Canada et l'obligation de consulter. https://www.rcaanc-cirnac.gc.ca/fra/1331832510888/1609421255810 (consulté en janvier 2025).

GC – Gouvernement du Canada, 2025c. Prévisions opérationnelles océan-glace. https://science.gc.ca/site/science/fr/concepts/previsions-operationnelles-ocean-glace (consulté en mai 2024).

GC – Gouvernement du Canada, 2025d. Plan de protection des océans. https://tc.canada.ca/fr/campagnes/plan-protection-oceans (consulté en juin 2025).

GC – Gouvernement du Canada, 2025e. Attributions provinciales et territoriales de 2025 dans le cadre du plafond d'étudiants étrangers. https://www.canada.ca/fr/immigration-refugies-citoyennete/nouvelles/avis/attributions-provinciales-territoriales-2025-cadre-plafond-etudiants-etrangers.html (consulté en juin 2025).

GC – Gouvernement du Canada, 2025f. *Guide de la Liste des marchandises et technologies d'exportation contrôlée du Canada*, Ottawa, ON, Affaires mondiales Canada. https://www.international.gc.ca/trade-commerce/assets/pdfs/guides/export-control-list-guide-2025-fra.pdf.

GC – Gouvernement du Canada, 2025g. Liste de technologies sensibles. https://www.canada.ca/fr/services/defense/securitenationale/liste-technologies-sensibles.html (consulté en juin 2025).

GC – Gouvernement du Canada, 2025h. Décret modifiant la Liste des marchandises et technologies d'exportation contrôlée : DORS/2025-89. https://gazette.gc.ca/rp-pr/p2/2025/2025-03-26/html/sor-dors89-fra.html (consulté en juin 2025).

GC – Gouvernement du Canada, 2025i. Document d'information : modification du Guide de la Liste des marchandises et technologies d'exportation contrôlée du Canada. https://www.international.gc.ca/trade-commerce/controls-controles/ecl-lec/backgrounder-document-information-2025.aspx?lang=fra (consulté en juin 2025).

GC – Gouvernement du Canada, 2025j. Processus d'examen de l'évaluation des risques. https://science.gc.ca/site/science/fr/protegez-votre-recherche/lignes-directrices-outils-pour-mise-oeuvre-securite-recherche/lignes-directrices-securite-nationale-pour-partenariats-recherche/formulaire-devaluation-risques-lignes-directrices-securite-nationale-pour-partenariats-0 (consulté en février 2025).

GC – Gouvernement du Canada, 2025k. Chaires de recherche du Canada : Méthode utilisée pour l'attribution des chaires. https://www.chairs-chaires.gc.ca/program-programme/allocation-attribution-fra.aspx (consulté en mai 2025).

GC – Gouvernement du Canada, 2025l. Fonds de soutien à la recherche : Calcul des subventions. https://www.rsf-fsr.gc.ca/apply-demande/calculations-fra.aspx (consulté en mai 2025).

Génome Canada, 2024a. *Rapport annuel 2023-2024 Exploiter la génomique pour un meilleur impact*, Ottawa, ON, Génome Canada. https://genomecanada.ca/wp-content/uploads/2024/07/GC-AnnualReport-2023-24_FR_web.pdf.

Génome Canada, 2024b. *Research Security Plan*, Ottawa, ON, Génome Canada. https://genomecanada.ca/wp-content/uploads/2024/12/Research-Security-Plan-2024-Dec.pdf.

Geremia, S., 2024 (18 mars). « New research grants to bolster Canada's AI ecosystem », *Google Canada*. https://blog.google/intl/en-ca/company-news/outreach-initiatives/new-research-grants-to-bolster-canadas-ai-ecosystem/ (consulté en novembre 2024).

GFW – Global Fishing Watch, s.d. Home. https://globalfishingwatch.org/ (consulté en juin 2025).

GHS Index – Global Health Security Index, 2021. 2021 GHS Index country profile for Canada. https://ghsindex.org/country/canada/ (consulté en mai 2025).

GIDA – Global Indigenous Data Alliance, s.d. CARE Principles for Indigenous Data Governance. https://www.gida-global.org/care (consulté en janvier 2025).

GIEC – Groupe d'experts intergouvernemental sur l'évolution du climat, 2019. « Summary for policymakers », dans Pörtner, H.-O., D.C. Roberts, V. Masson-Delmotte, P. Zhai, M. Tignor, E. Poloczanska, … N.M. Weyer (dir.), *The Ocean and Cryosphere in a Changing Climate: Special Report of the Intergovernmental Panel on Climate Change*, 1re édition, Cambridge, Royaume-Uni et New York, NY, Cambridge University Press.

Global BioLabs, 2023. *Global BioLabs Report 2023*, Londres, Royaume-Uni, King's College London. https://static1.squarespace.com/static/62fa334a3a6fe8320f5dcf7e/t/6412d3120ee69a4f4efbec1f/1678955285754/KCL0680_BioLabs+Report_Digital.pdf.

GlycoNet – Canadian Glycomics Network, s.d. Research security. https://canadianglycomics.ca/research/research-security/ (consulté en mars 2025).

Goodchild, M., S. Khair, A. Leahey, K. Newson, et L. Wilson, 2023. « Research data sharing and reuse in Canada: Practice and policy », dans Thompson, K., E. Hill, E. Carlisle-Johnston, D. Dennie, et E. Fortin (dir.), *Research Data Management in the Canadian Context: A Guide for Practitioners and Learners*, 1re édition, London, ON, Université Western, Western Libraries.

GOOS – Global Ocean Observing System, s.d. What we do. https://goosocean.org/what-we-do/ (consulté en novembre 2024).

Gouv. de l'Alb. – Gouvernement de l'Alberta, 2024. *Research Capacity Program*, Edmonton, AB, Gouv. de l'Alberta. https://open.alberta.ca/dataset/faf898eb-ed6b-4fae-ae39-f2aa7efcf6d2/resource/5460ea77-829e-4dcc-b5d8-2173308df567/download/ti-research-capacity-program-guidelines-2024-2025.pdf.

Gouv. de l'Allemagne – Gouvernement de l'Allemagne, 1949. *Basic Law for the Federal Republic of Germany in the revised version published in the Federal Law Gazette Part III, classification number 100-1, as last amended by the Act of 19 December 2022 (Federal Law Gazette I p. 2478).*

Gouv. de l'Australie – Gouvernement de l'Australie, 2013. *Security Sensitive Biological Agent (SSBA) Standards*, Canberra, Australie, Gouv. de l'Australie. https://www.health.gov.au/sites/default/files/documents/2022/06/ssba-standards.pdf.

Gouv. de l'Australie – Gouvernement de l'Australie, 2018. Foreign Influence Transparency Scheme Act 2018.

Gouv. de l'Australie – Gouvernement de l'Australie, 2020. *Australia's Foreign Relations (State and Territory Arrangements) Act 2020* No. 116.

Gouv. de l'Australie – Gouvernement de l'Australie, 2021. *Australia's Foreign Relations (State and Territory Arrangements) Act 2020: Fact Sheet 4 - Australian Universities*, Canberra, Australie, Department of Foreign Affairs and Trade. https://www.foreignarrangements.gov.au/resources/fact-sheets.

Gouv. de l'Australie – Gouvernement de l'Australie, 2023. List of critical technologies in the national interest. https://www.industry.gov.au/publications/list-critical-technologies-national-interest (consulté en septembre 2024).

Gouv. de l'Australie – Gouvernement de l'Australie, 2024. Security Sensitive Biological Agents (SSBA) Regulatory Scheme. https://www.health.gov.au/our-work/ssba-regulatory-scheme (consulté en août 2024).

Gouv. de l'Australie – Gouvernement de l'Australie, 2025. National Counter Foreign Interference Coordinator. https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/countering-foreign-interference (consulté en septembre 2024).

Gouv. de l'Ont. – Gouvernement de l'Ontario, 2023. *Mitigating Economic and Geopolitical Risk Checklist for Ontario Research Fund Applications*, Toronto, ON, Gouv. de l'Ont. https://forms.mgcs.gov.on.ca/en/dataset/on00352.

Gouv. de l'Ont. – Gouvernement de l'Ontario, 2024a. *Research Security Guidelines for Ontario Research Funding Programs*, Toronto, ON, Ministère des Collèges et Universités. https://forms.mgcs.gov.on.ca/en/dataset/on00708.

Gouv. de l'Ont. – Gouvernement de l'Ontario, 2024b. *Formulaire d'attestation pour les chercheurs qui présentent une demande dans le cadre de programmes de financement de la recherche de l'Ontario*, Toronto, ON, Ministère des Collèges et Universités. https://forms.mgcs.gov.on.ca/fr/dataset/on00694.

Gouv. de la Corée du Sud – Gouvernement de la Corée du Sud 2023. *Act on Protection of Industrial Technology.*

Gouv. de la France – Gouvernement de la France, 1990. *Code pénal*.

Gouv. de la France – Gouvernement de la France, 2012. *Circulaire interministerielle de mise en œuvre du dispositif de protection du potentiel scientifique et technique de la nation*, Paris, France, Secrétariat général de la défense et de la Sécurité nationale. https://www.legifrance.gouv.fr/download/pdf/circ?id=36329.

Gouv. de la France – Gouvernement de la France, 2020. *Décret nº 2020-1481 du 30 novembre 2020 portant mesure nationale autorisée par le paragraphe 3 de l'article 6 du règlement (CE) nº 428/2009 du Conseil du 5 mai 2009 instituant un régime communautaire de contrôle des exportations, des transferts, du courtage et du transit de biens à double usage*.

Gouv. de la France – Gouvernement de la France, 2024. *Arrêté du 2 février 2024 relatif aux exportations vers les pays tiers de biens et technologies associés à l'ordinateur quantique et à ses technologies habilitantes et d'équipements de conception, développement, production, test et inspection de composants électroniques avancés*.

Gouv. de la Nouvelle-Zélande – Gouvernement de la Nouvelle-Zélande, 2020. *Trusted Research: Guidance for Institutions and Researchers*, Wellington, Nouvelle-Zélande, Centre for the Protection of National Infrastructure, Science New Zealand et Universities New Zealand. https://www.protectivesecurity.govt.nz/assets/protective-security-requirements/resources/psr-trusted-research-guidance-spreads.pdf.

Gouv. de la Nouvelle-Zélande – Gouvernement de la Nouvelle-Zélande, 2022. *Due Diligence Assessments for Espionage and Foreign Interference Threats*, Wellington, Nouvelle-Zélande, Protective Security Requirements. https://www.protectivesecurity.govt.nz/assets/protective-security-requirements/resources/psr-due-diligence-assessments.pdf.

Gouv. de la Nouvelle-Zélande – Gouvernement de la Nouvelle-Zélande, 2024. *New Zealand Strategic Goods List*, Wellington, Nouvelle-Zélande, Ministry of Foreign Affairs and Trade. https://www.mfat.govt.nz/assets/Trade-General/Brokering-weapons-AND-Trading-weapons-and-controlled-chemicals/NZ-Strategic-Goods-List-November.pdf.

Gouv. des États-Unis – Gouvernement des États-Unis, 1991. *Protection of Human Subjects*, 45 CFR 46.

Gouv. des États-Unis – Gouvernement des États-Unis, 2022a. *National Strategy for the Arctic Region*, Washington, D.C., Gouv. des États-Unis. https://bidenwhitehouse.archives.gov/wp-content/uploads/2022/10/National-Strategy-for-the-Arctic-Region.pdf.

Gouv. des États-Unis – Gouvernement des États-Unis, 2022b. *CHIPS and Science Act* PL 117-167.

Gouv. des États-Unis – Gouvernement des États-Unis, 2024a. *United States Government Policy for Oversight of Dual Use Research of Concern and Pathogens with Enhanced Pandemic Potential*, Washington, D.C., Gouv. des États-Unis. https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/05/USG-Policy-for-Oversight-of-DURC-and-PEPP.pdf.

Gouv. des États-Unis – Gouvernement des États-Unis, 2024b. *Implementation Guidance for the United States Government Policy for Oversight of Dual Use Research of Concern and Pathogens with Enhanced Pandemic Potential*, Washington, D.C., Gouv. des États-Unis. https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/05/USG-DURC-PEPP-Implementation-Guidance.pdf.

Gouv. des Pays-Bas – Gouvernement des Pays-Bas, 2022. *National Knowledge Security Guidelines: Secure International Collaboration*, La Haye, Pays-Bas, Gouv. des Pays-Bas. https://english.loketkennisveiligheid.nl/site/binaries/site-content/collections/documents/2022/04/07/national-knowledge-security-guidelines/National+Knowledge+Security+Guidelines.pdf.

Gouv. des Pays-Bas – Gouvernement des Pays-Bas, 2023. *Besluit toepassingsbereik sensitieve technologie*.

Gouv. des Pays-Bas – Gouvernement des Pays-Bas, 2025. Screening for researchers wis[h]ing to handle sensitive knowledge. https://www.government.nl/latest/news/2025/04/07/screening-for-researchers-wising-to-handle-sensitive-knowledge (consulté en juin 2025).

Gouv. du Japon – Gouvernement du Japon, 2023. *Checklist for New Risks Associated with Increasing Internationalization and Openness of Research (Template)*, Tokyo, Japon, Cabinet Office. https://www8.cao.go.jp/cstp/english/doc/checklist_for_univ_en.pdf.

Gouv. du Qc – Gouvernement du Québec, 2024a. *Loi sur la protection contre les représailles liées à la divulgation d'actes répréhensibles* P-33.01.

Gouv. du Qc – Gouvernement du Québec, 2024b. *Loi facilitant la divulgation d'actes répréhensibles à l'égard des organismes publics* D-11.1.

Gouv. du Royaume-Uni – Gouvernement du Royaume-Uni, 2024. National Security and Investment Act: Details of the 17 types of notifiable acquisitions. https://www.gov.uk/government/publications/national-security-and-investment-act-guidance-on-notifiable-acquisitions/national-security-and-investment-act-guidance-on-notifiable-acquisitions (consulté en juin 2025).

Gouv. du Royaume-Uni – Gouvernement du Royaume-Uni, 2025. Academic Technology Approval Scheme (ATAS). https://www.gov.uk/guidance/academic-technology-approval-scheme (consulté en août 2024).

Gouv. du Royaume-Uni – Gouvernement du Royaume-Uni, s.d. Engineering Biology Responsible Innovation Advisory Panel. https://www.gov.uk/government/groups/engineering-biology-responsible-innovation-advisory-panel (consulté en mai 2025).

Gownaris, N. J., K. Vermeir, M.-I. Bittner, L. Gunawardena, S. Kaur-Ghumaan, R. Lepenies, … I. S. Zakari, 2022. « Barriers to full participation in the open science life cycle among early career researchers », *Data Science Journal*, vol. 21, nº 2, p. 1–15. https://doi.org/10.5334/dsj-2022-002.

GRC – Gendarmerie royale du Canada, 2024. Accusations d'espionnage contre un employé d'Hydro-Québec. https://www.rcmp-grc.gc.ca/fr/nouvelles/2022/accusations-despionnage-employe-dhydro-quebec (consulté en juin 2025).

Grewal, S., 2022. « International students for long-term prosperity in Canadian economy: Expanding pathways to permanence for international students in Canada », *Crossings: An Undergraduate Arts Journal*, vol. 2, p. 140-146. https://doi.org/10.29173/crossings45.

Gryphon Scientific, LLC, 2023. *Characterizing Private-Sector Research on Human Pathogens in the United States*, Takoma Park, MD, Gryphon Scientific, LLC. https://pandorareport.org/wp-content/uploads/2023/10/private-sector-research-final.pdf.

Gunashekar, S., C. d'Angelo, I. Flanagan, D. Motsi-Omoijiade, M. Virdee, C. Feijao et S. Porter, 2022. *Using Quantum Computers and Simulators in the Life Sciences: Current Trends and Future Prospects*, Cambridge, Royaume-Uni, RAND Corporation. https://www.rand.org/pubs/research_reports/RRA1899-1.html.

Hähnel, M., 2024. « Conceptualizing dual use: A multidimensional approach », *Research Ethics*, vol. 21, nº 2, p. 205-227. https://doi.org/10.1177/17470161241261466.

Harlan, T., 2019 (25 octobre). « State of sensitivity: Navigating fieldwork in an increasingly authoritarian China », *Made in China Journal*. https://madeinchinajournal.com/2019/10/25/state-of-sensitivity-navigating-fieldwork-in-an-increasingly-authoritarian-china/ (consulté en juin 2025).

Heathershaw, J., J. Chalcraft, A. Chubb, A. Fulda, C. Hughes, K. Kaczmarska, … Y. Y. Yıldız, 2022. « Model code of conduct: Protection of academic freedom and the academic community in the context of the internationalisation of the UK HE sector », *The International Journal of Human Rights*, vol. 26, nº 10, p. 1858-1865. https://doi.org/10.1080/13642987.2022.2148977.

Heaven, W. D., 2023 (12 mai). « The open-source AI boom is built on Big Tech's handouts. How long will it last? », *MIT Technology Review*. https://www.technologyreview.com/2023/05/12/1072950/open-source-ai-google-openai-eleuther-meta/ (consulté en novembre 2024).

HEC Montréal – Hautes études commerciales de Montréal, 2023. *Politique sur la sécurité des activités à l'international*, Montréal, QC, HEC Montréal. https://www.hec.ca/direction_services/secretariat_general/juridique/reglements_politiques/documents/politique-securite-activites-international.pdf.

Heikkilä, M., 2024 (18 octobre). « The race to find new materials with AI needs more data. Meta is giving massive amounts away for free », *MIT Technology Review*. https://www.technologyreview.com/2024/10/18/1105880/the-race-to-find-new-materials-with-ai-needs-more-data-meta-is-giving-massive-amounts-away-for-free/ (consulté en novembre 2024).

Heininen, L., K. Everett, B. Padrtova et A. Reissell, 2020. *Arctic Policies and Strategies — Analysis, Synthesis, and Trends*, Laxenburg, Autriche, International Institute for Applied Systems Analysis. https://pure.iiasa.ac.at/id/eprint/16175/1/ArticReport_WEB_new.pdf.

Helmholtz – Helmholtz Association of German Research Centres, s.d. Research security in international scientific collaborations. https://www.helmholtz.de/en/international/research-security/ (consulté en août 2024).

HHS, CDC, et USDA – U.S. Department of Health and Human Services, Centers for Disease Control and Prevention, et U.S. Department of Agriculture, Animal and Plant Health Inspection Service, 2020. *2019 Annual Report of the Federal Select Agent Program*, Washington, D.C., HHS, CDC, et USDA. https://www.selectagents.gov/resources/publications/docs/FSAP_Annual_Report_2019_508.pdf.

HHS, CDC, et USDA – U.S. Department of Health and Human Services, Centers for Disease Control and Prevention et U.S. Department of Agriculture, Animal and Plant Health Inspection Service, 2024. *2023 Annual Report of the Federal Select Agent Program*, Washington, D.C., HHS, CDC, et USDA. https://www.selectagents.gov/resources/publications/docs/FSAP-Annual-Report-2023_508.pdf.

Himmel, M., 2023. *Biosecurity Risk Assessment in the Life Sciences: Towards a Toolkit for Individual Practitioners*, Stockholm, Suède, Stockholm International Peace Research Institute. https://www.sipri.org/publications/2023/other-publications/biosecurity-risk-assessment-life-sciences-towards-toolkit-individual-practitioners.

Holbrook, D., 1995. « Government support of the semiconductor industry: Diverse approaches and information flows », *Business and Economic History*, vol. 24, nº 2, p. 133-165. https://www.jstor.org/stable/23703131.

Huising, R. et S. S. Silbey, 2018. « From nudge to culture and back again: Coalface governance in the regulated organization », *Annual Review of Law and Social Science*, vol. 14, p. 91-114. https://doi.org/10.1146/annurev-lawsocsci-110615-084716.

Huising, R., 2019. « Pragmatic regulatory design: The case of human pathogens and toxins regulations in Canada », *Entreprises et histoire*, vol. 97, nº 4, p. 58-69. https://doi.org/10.3917/eh.097.0058.

Hummel, P., M. Braun, M. Tretter, et P. Dabrock, 2021. « Data sovereignty: A review », *Big Data & Society*, vol. 8, nº 1, 2053951720982012. https://doi.org/10.1177/2053951720982012.

IARPC – Interagency Arctic Research Policy Committee, 2021. *Arctic Research Plan 2022–2026*, Washington, D.C., National Science and Technology Council, Office of Science and Technology Policy. https://www.iarpccollaborations.org/plan/index.html.

IHRC – Ittaq Heritage & Research Centre, s.d. Research. https://ittaq.ca/research/ (consulté en juin 2025).

Indigenous Advisory Circle et CRSH – Conseil de recherches en sciences humaines, 2025. Recherche autochtone. https://sshrc-crsh.canada.ca/fr/financement/terminologie.aspx#0 (consulté en janvier 2025).

Inglesby, T., 2024 (7 mai). « Take-aways from strong new OSTP policy on DURC and pathogens with pandemic potential », *LinkedIn*. https://www.linkedin.com/pulse/take-aways-from-strong-new-ostp-policy-durc-pathogens-tom-inglesby-3lrje (consulté en août 2024).

IRSC, CRSNG et CRSH – Instituts de recherche en santé du Canada, Conseil de recherches en sciences naturelles et en génie du Canada et Conseil de recherches en sciences humaines, 2022. *Énoncé de politique des trois conseils : Éthique de la recherche avec des êtres humains – EPTC 2*. Ottawa, ON, Gouvernement du Canada. https://ethics.gc.ca/fra/policy-politique_tcps2-eptc2_2022.html.

ISC – Conseil scientifique international, s.d. *The International Science Council's Interpretation of the Right to Participate in and Benefit from Science*, Paris, France, ISC. https://council.science/wp-content/uploads/2024/11/The-Right-to-Participate-in-and-Benefit-from-Science_ISC.pdf.

ISDE – Innovation, Sciences et Développement économique Canada, 2016. Politique des trois organismes sur le libre accès aux publications (2015). https://ised-isde.canada.ca/site/science/fr/financement-interorganismes-recherche/politiques-lignes-directrices/libre-acces/politique-trois-organismes-libre-acces-aux-publications-2015 (consulté en juin 2024).

ISDE – Innovation, Sciences et Développement économique Canada, 2021. Le gouvernement du Canada agit pour protéger la recherche et la propriété intellectuelle au Canada. https://www.canada.ca/fr/innovation-sciences-developpement-economique/nouvelles/2021/07/le-gouvernement-du-canada-agit-pour-proteger-la-recherche-et-la-propriete-intellectuelle-au-canada.html (consulté en juin 2025).

ISDE – Innovation, Sciences et Développement économique Canada, 2022a. *Stratégie quantique nationale du Canada*, Ottawa, ON, Gouvernement du Canada. https://ised-isde.canada.ca/site/strategie-quantique-nationale/fr/strategie-quantique-nationale-canada.

ISDE – Innovation, Sciences et Développement économique Canada, 2022b. *Utiliser les renseignements de sources ouvertes pour faire preuve de diligence raisonnable*, Ottawa, ON, Gouvernement du Canada. https://science.gc.ca/site/science/fr/protegez-votre-recherche/lignes-directrices-outils-pour-mise-oeuvre-securite-recherche/faire-preuve-diligence-raisonnable-utilisant-renseignements-sources-ouvertes/resume-utiliser-renseignements-sources-ouvertes-pour-faire-preuve-diligence.

ISDE – Innovation, Sciences et Développement économique Canada, 2022c. *Faire preuve de diligence raisonnable en utilisant des renseignements de sources ouvertes afin de protéger les partenariats de recherche*, Ottawa, ON, Gouvernement du Canada. https://science.gc.ca/site/science/fr/protegez-votre-recherche/lignes-directrices-outils-pour-mise-oeuvre-securite-recherche/faire-preuve-diligence-raisonnable-utilisant-renseignements-sources-ouvertes/faire-preuve-diligence-raisonnable-utilisant-renseignements-sources-ouvertes.

ISDE – Innovation, Sciences et Développement économique Canada, 2023a. *Lignes directrices sur la sécurité nationale pour les partenariats de recherche*, Ottawa, ON, Gouvernement du Canada. https://science.gc.ca/site/science/sites/default/files/documents/lignes_directrices_sur_la_securite_nationale_pour_les_partenariats_de_recherche_jan2024.pdf.

ISDE – Innovation, Sciences et Développement économique Canada, 2023b. *Domaines de recherche en technologies sensibles*, Ottawa, ON, ISDE. https://science.gc.ca/site/science/fr/protegez-votre-recherche/lignes-directrices-outils-pour-mise-oeuvre-securite-recherche/recherche-technologies-sensibles-affiliations-preoccupantes/domaines-recherche-technologies-sensibles.

ISDE – Innovation, Sciences et Développement économique Canada, 2023c. *Rapport sur l'état d'avancement de la mise en œuvre des Lignes directrices sur la sécurité nationale pour les partenariats de recherche et de l'appui aux efforts de sécurité de la recherche*, Ottawa, ON, Gouvernement du Canada. https://science.gc.ca/site/science/sites/default/files/documents/2023-11/1077-rapport-sur-letat-davancement-2021-2023-23nov23.pdf.

ISDE – Innovation, Sciences et Développement économique Canada, 2023d. Les présidents respectifs des organismes fédéraux de financement de la recherche au Canada annoncent une révision de la Politique des trois organismes sur le libre accès aux publications. https://science.gc.ca/site/science/fr/financement-interorganismes-recherche/politiques-lignes-directrices/libre-acces/presidents-respectifs-organismes-federaux-financement-recherche-canada-annoncent-revision-politique (consulté en novembre 2024).

ISDE – Innovation, Sciences et Développement économique Canada, 2023e. *Organisations de recherche nommées*, Ottawa, ON, Gouvernement du Canada. https://science.gc.ca/site/science/fr/protegez-votre-recherche/lignes-directrices-outils-pour-mise-oeuvre-securite-recherche/recherche-technologies-sensibles-affiliations-preoccupantes/organisations-recherche-nommees.

ISDE – Innovation, Sciences et Développement économique Canada, 2023f. *Politique sur la recherche en technologies sensibles et sur les affiliations préoccupantes*, Ottawa, ON, Gouvernement du Canada. https://science.gc.ca/site/science/sites/default/files/documents/2024-01/1154-politique-rtsap-fr-final-09jan2024.pdf.

ISDE – Innovation, Sciences et Développement économique Canada, 2024a. Formulaire d'évaluation des risques des Lignes directrices sur la sécurité nationale pour les partenariats de recherche. https://science.gc.ca/site/science/fr/protegez-votre-recherche/lignes-directrices-outils-pour-mise-oeuvre-securite-recherche/lignes-directrices-securite-nationale-pour-partenariats-recherche/formulaire-devaluation-risques-lignes-directrices-securite-nationale-pour-partenariats (consulté en mai 2024).

ISDE – Innovation, Sciences et Développement économique Canada, 2024b. Études de cas : comment une atteinte à la sécurité peut avoir des répercussions sur votre recherche. https://ised-isde.canada.ca/site/science/fr/protegez-votre-recherche/lignes-directrices-outils-pour-mise-oeuvre-securite-recherche/etudes-cas-comment-atteinte-securite-peut-avoir-repercussions-votre-recherche (consulté en janvier 2025).

ISDE – Innovation, Sciences et Développement économique Canada, 2025. Plan ministériel d'Innovation, Sciences et Développement économique Canada pour 2024–2025. https://ised-isde.canada.ca/site/planification-rapports-rendement/fr/plans-ministeriels/plan-ministeriel-dinnovation-sciences-developpement-economique-canada-pour-2024-2025 (consulté en juin 2025).

ISDE Innovation, Sciences et Développement économique Canada, 2024c. Résultats du sondage sur la révision de la Politique des trois organismes sur le libre accès aux publications. https://science.gc.ca/site/science/fr/financement-interorganismes-recherche/politiques-lignes-directrices/libre-acces/resultats-sondage-revision-politique-trois-organismes-libre-acces-aux-publications (consulté en juin 2024).

ISO – International Organization for Standardization, 2018. *ISO 31000:2018 Risk Management — Guidelines*, Genève, Suisse, ISO. https://www.iso.org/standard/65694.html.

ITK – Inuit Tapiriit Kanatami, 2018. *Stratégie nationale inuite sur la recherche*, Ottawa, ON, ITK. https://www.itk.ca/wp-content/uploads/2018/03/Strat%C3%A9gie-nationale-inuite-sur-la-recherche.pdf.

ITK et NRI – Inuit Tapiriit Kanatami et Nunavut Research Institute, 2007. *Negotiating Research Relationships with Inuit Communities: A Guide for Researchers*, Ottawa, ON et Iqaluit, NU, ITK et NRI. https://itk.ca/wp-content/uploads/2016/07/Negotitiating-Research-Relationships-Researchers-Guide_0.pdf.

Iverson, S. J., A. T. Fisk, S. G. Hinch, J. Mills Flemming, S. J. Cooke, et F. G. Whoriskey, 2019. « The Ocean Tracking Network: Advancing frontiers in aquatic science and management », *Canadian Journal of Fisheries and Aquatic Sciences*, vol. 76, p. 1041–1051. https://doi.org/10.1139/cjfas-2018-0481.

Jakob, U., F. Kraemer, F. Kraus et T. Lengauer, 2024. « Applying ethics in the handling of dual use research: The case of Germany », *Research Ethics*, vol. 21, nº 2, p. 228–244. https://doi.org/10.1177/17470161241261044.

Jamal, M., 2022 (27 avril). « ITK looking to make it easier for organizations to share information across Inuit Nunangat », *Nunatsiaq News*. https://nunatsiaq.com/stories/article/itk-looking-to-make-it-easier-for-organizations-to-share-information-across-inuit-nunangat/ (consulté en juin 2023).

JASON, 2019. *Fundamental Research Security*, McLean, VA, MITRE Corporation. https://nsf-gov-resources.nsf.gov/files/JSR-19-2IFundamentalResearchSecurity-12062019FINAL.pdf.

JASON, 2024. *Safeguarding the Research Enterprise*, McLean, VA, MITRE Corporation. https://nsf-gov-resources.nsf.gov/files/JSR-23-12-Safeguarding-the-Research-Enterprise-Final.pdf?VersionId=ZVhvRaTIrxMsdZql6E_yz5pN6Ssw0fSl.

Jin, X., L. Xu, Y. Xin et A. Adhikari, 2022. « Political governance in China's state-owned enterprises », *China Journal of Accounting Research*, vol. 15, 100236. https://doi.org/10.1016/j.cjar.2022.100236.

JUS – Justice Canada, 2021. Document d'information : *Loi sur la Déclaration des Nations Unies sur les droits des peuples autochtones*. https://www.justice.gc.ca/fra/declaration/apropos-about.html (consulté en avril 2024).

Kavouras, P., et C. A. Charitidis, 2019. « Dual use in modern research: Taming the Janus of technological advance », dans Iphofen, R. (dir.), *Handbook of Research Ethics and Scientific Integrity*. Cham, Suisse, Springer International Publishing.

KNAW – Royal Netherlands Academy of Arts and Sciences, 2023. *Knowledge Security: Academy Position Paper*. Amsterdam, Pays-Bas, KNAW. https://www.knaw.nl/en/publications/knowledge-security-academy-position-paper.

KNAW, NFU, NWO, TO2-federatie, Vereniging Hogescholen et VSNU – Royal Netherlands Academy of Arts and Sciences, Netherlands Federation of University Medical Centres, Netherlands Organisation for Scientific Research, Associated Applied Research Institutes, Association of Universities in the Netherlands et Netherlands Association of Universities of Applied Sciences, 2018. *Netherlands Code of Conduct for Research Integrity*. s.l.: KNAW, NFU, NWO, TO2-federatie, Vereniging Hogescholen & VSNU. https://easy.dans.knaw.nl/ui/datasets/id/easy-dataset:110600.

Konczi, A. E., et L. Bill, 2024. « Advancing First Nations Principles of OCAP® », dans Garvey, G. (dir.), *Indigenous and Tribal Peoples and Cancer*. Cham, Suisse, Springer Nature.

Kosal, M. E., 2020a. « Emerging life sciences and possible threats to international security », *Orbis*, vol. 64, nº 4, p. 599-614. https://doi.org/10.1016/j.orbis.2020.08.008.

Kosal, M. E., 2020b. « CRISPR and new genetic-engineering techniques: Emerging challenges to strategic stability and nonproliferation », *Nonproliferation Review*, vol. 27, nº 4-6, p. 389-408. https://doi.org/10.1080/10736700.2020.1879464.

Kosal, M. E., et J. Y. Huang, 2015. « Security implications and governance of cognitive neuroscience: An ethnographic survey of researchers », *Politics and the Life Sciences*, vol. 34, nº 1, p. 93-108. https://doi.org/10.1017/pls.2015.4.

Kukutai, T., et J. Taylor, 2016. « Data sovereignty for Indigenous Peoples: Current practice and future needs », dans Kukutai, T. et J. Taylor (dir.), *Indigenous Data Sovereignty: Toward an Agenda*. Canberra, Australie, Australian National University Press.

L'Alliance – Alliance de recherche numérique du Canada, 2021. *Researcher Needs Assessment: Summary of What We Heard*, Toronto, ON, L'Alliance. https://alliancecan.ca/sites/default/files/2022-03/needsassessment_alliance_20220126.pdf.

L'Alliance – Alliance de recherche numérique du Canada, 2024. *Résultats du concours pour l'allocation de ressources pour 2024*, Toronto, ON, L'Alliance. https://alliancecan.ca/fr/resultats-du-concours-pour-lallocation-de-ressources-pour-2024.

L'HO – L'Hôpital d'Ottawa, 2021 (17 mars). « La science ouverte permet de poser un diagnostic qui change la vie d'une patiente », *L'Hôpital d'Ottawa*. https://www.ottawahospital.on.ca/fr/avenir-en-sante/la-science-ouverte-permet-de-poser-un-diagnostic-qui-change-la-vie-dune-patiente/ (consulté en novembre 2024).

Lamb, C., et D. Munro, 2020. *The Intangible Shift: Changing Gears to Compete in the New Economy*, Toronto, ON, Brookfield Institute for Innovation+Entrepreneurship. https://brookfieldinstitute.ca/wp-content/uploads/2023/10/The-Intangible-Shift-ONLINE-1.pdf.

Lane, I. F., 2007. « Change in higher education: Understanding and responding to individual and organizational resistance », *Journal of Veterinary Medical Education*, vol. 34, nº 2, p. 85-92. https://doi.org/10.3138/jvme.34.2.85.

Larivière, V., et C. R. Sugimoto, 2018. « Do authors comply when funders enforce open access to research? », *Nature*, vol. 562, nº 7728, p. 483-486. https://doi.org/10.1038/d41586-018-07101-w.

Laucht, C., 2012. *Elemental Germans: Klaus Fuchs, Rudolf Peierls and the Making of British Nuclear Culture 1939-59*, New York, NY, Palgrave Macmillan.

Leibniz Association, 2021. *Risk Management in International Scientific Collaboration*, Berlin, Allemagne, Leibniz Association. https://www.leibniz-gemeinschaft.de/fileadmin/user_upload/Bilder_und_Downloads/%C3%9Cber_uns/Internationales/Risk_management_in_international_scientific_cooperation.pdf.

Leonard, K., P. L. Buttigieg, M. Hudson, K. Paul, J. Pearlman et S. K. Juniper, 2022. « Two-eyed seeing: Embracing the power of Indigenous knowledge for a healthy and sustainable Ocean », *PLOS Biology*, vol. 20, nº 10, e3001876. https://doi.org/10.1371/journal.pbio.3001876.

Leopoldina et DFG – German National Academy of Sciences Leopoldina et German Research Foundation, 2022a. *The Handling of Security-Relevant Research in Germany—An Overview*, Berlin, Allemagne, Joint Committee on the Handling of Security-Relevant Research. https://www.sicherheitsrelevante-forschung.org/wp-content/uploads/2022/10/The-Handling-of-Security-Relevant-Research-in-Germany-An-Overview.pdf.

Leopoldina et DFG – German National Academy of Sciences Leopoldina et German Research Foundation, 2022b. *Scientific Freedom and Scientific Responsibility: Recommendations for Handling of Security-Relevant Research*, Halle, Allemagne, Leopoldina et DFG. https://www.dfg.de/resource/blob/176010/0f6dbcaa5e6b5b032bc24772cbf73a83/empfehlungen-de-en-data.pdf.

Leopoldina et DFG – German National Academy of Sciences Leopoldina et German Research Foundation, s.d.-a. Frequently asked questions about security-relevant research and the KEFs. https://www.security-relevant-research.org/faq-eng/ (consulté en août 2024).

Leopoldina et DFG – German National Academy of Sciences Leopoldina et German Research Foundation, s.d.-b. Research assessment and international collaborations. https://www.security-relevant-research.org/research/ (consulté en août 2024).

Lev, O., 2019. « Regulating dual-use research: Lessons from Israel and the United States », *Journal of Biosafety and Biosecurity*, vol. 1, p. 80-85. https://doi.org/10.1016/j.jobb.2019.06.001.

Libman, A., R. W. Stone et E. Vinokurov, 2022. « Russian power and the state-owned enterprise », *European Journal of Political Economy*, vol. 73, p. 102122. https://doi.org/10.1016/j.ejpoleco.2021.102122.

Lipunov, N. et P. Devyatkin, 2023 (30 mai). « The Arctic in the 2023 Russian Foreign Policy Concept », *The Arctic Institute—Center for Circumpolar Security Studies*. https://www.thearcticinstitute.org/arctic-2023-russian-foreign-policy-concept/ (consulté en novembre 2024).

Loft, T., et W. Saumweber, 2020 (22 avril). « Are we moving toward an ocean data dystopia? », *Stephenson Ocean Security Project*. https://ocean.csis.org/commentary/are-we-moving-toward-an-ocean-data-dystopia/ (consulté en novembre 2024).

Lukasik, S., 2011. « Why the Arpanet was built », *IEEE Annals of the History of Computing*, vol. 33, p. 4-21. https://doi.org/10.1109/MAHC.2010.11.

MacIntyre, C. R., D. C. Adam, R. Turner, A. A. Chughtai, et T. Engells, 2020. « Public awareness, acceptability and risk perception about infectious diseases dual-use research of concern: A cross-sectional survey », *BMJ Open*, vol. 10, e029134. https://doi.org/10.1136/bmjopen-2019-029134.

Major, R. M., A. M. Davis, G. E. Henderson, G. Inamine, et J. M. Conley, 2024. « The public–private research ecosystem in the genome editing era », *iScience*, vol. 27, 109896. https://doi.org/10.1016/j.isci.2024.109896.

Malik, M., E. Agudelo et R. Kunjwal, 2022. « Quantum researcher mobility: The wonderful wizard of Oz who paid for Dorothy's visa fees », *Quantum Science and Technology*, vol. 7, 034005. https://doi.org/10.1088/2058-9565/ac77b3.

Malone, M., 2021. « Consequences of the criminalization of trade secret theft in Canada », *UBC Law Review*, vol. 54, nº 3, p. 889-933. https://commons.allard.ubc.ca/ubclawreview/vol54/iss3/7.

Marwaha, S., J. Timlin, L. Dickson, E. Kagiri-Kalanzi et J. Johnson, 2023. *Complex Collaborations: Efficiency, Equity, Quality and Security in International Research*, Stow-cum-Quy, Royaume-Uni, Association of Research Managers and Administrators. https://arma.ac.uk/wp-content/uploads/2023/03/Trusted-Report_Booklet_v7.pdf.

MDN – Défense nationale, 2023. *Évaluation du programme IDEeS*, Ottawa, ON, Gouvernement du Canada. https://www.canada.ca/fr/ministere-defense-nationale/organisation/rapports-publications/verification-evaluation/eval-programme-idees.html.

MDN – Défense nationale, 2024a. *Rapport annuel IDEeS 2022-2023*, Ottawa, ON, Gouvernement du Canada. https://www.canada.ca/fr/ministere-defense-nationale/organisation/rapports-publications/rapport-annuel-idees-2022-2023.html.

MDN – Défense nationale, 2024b. *Notre Nord, fort et libre : Une vision renouvelée pour la défense du Canada*, Ottawa, ON, Gouvernement du Canada. https://www.canada.ca/fr/ministere-defense-nationale/organisation/rapports-publications/nord-fort-libre-2024.html.

MDN et FAC – Défense nationale et Forces armées canadiennes, 2021. *Plan d'action du ministère de la Défense nationale et des Forces armées canadiennes en matière de science ouverte*, Ottawa, ON, Gouvernement du Canada. https://www.canada.ca/fr/ministere-defense-nationale/organisation/rapports-publications/plan-d-action-science-ouverte.html.

MESR – Ministère chargé de l'Enseignement Supérieur et de la Recherche, 2021. Deuxième Plan national pour la science ouverte : *Généraliser la science ouverte en France 2021-2024*, Paris, France, MESR. https://www.ouvrirlascience.fr/wp-content/uploads/2021/06/Deuxieme-Plan-National-Science-Ouverte_2021-2024.pdf.

MESR – Ministère chargé de l'Enseignement Supérieur et de la Recherche, 2023. Baromètre français de la Science ouverte. barometredelascienceouverte.esr.gouv.fr (consulté en novembre 2024).

Mitacs, 2023. *Sécurité de la recherche*, Montréal, QC, Mitacs. https://www.mitacs.ca/fr-ca/securite-de-la-recherche/.

Moher, D., et K. D. Cobey, 2021. « Ensuring the success of data sharing in Canada », *FACETS*, vol. 6, p. 1534-1538. https://doi.org/10.1139/facets-2021-0031.

Molloy, G., et E. Johnson, 2025 (7 mai). « Investigation: Uncovering Chinese academic espionage at Stanford », *The Stanford Review*. https://stanfordreview.org/investigation-uncovering-chinese-academic-espionage-at-stanford/ (consulté en mai 2025).

Moran, K., S. K. Juniper, S. Bligh, D. Loock, I. Kulin, M. Paulson, et B. Pirenne, 2022. « Canada's internet-connected ocean », *Frontiers in Marine Science*, vol. 8, p. 805134. https://doi.org/10.3389/fmars.2021.805134.

Morris, N., 2020 (9 septembre). « Why unis are worried about a federal power to cancel their foreign "arrangements" », *The Conversation*. http://theconversation.com/why-unis-are-worried-about-a-federal-power-to-cancel-their-foreign-arrangements-145689 (consulté en janvier 2025).

Moskovkin, V. M., T. V. Saprykina, M. V. Sadovski et O. V. Serkina, 2021. « International movement of open access to scientific knowledge: A quantitative analysis of country involvement », *The Journal of Academic Librarianship*, vol. 47, 102296. https://doi.org/10.1016/j.acalib.2020.102296.

Mowery, D. C., 2010. « Military R&D and innovation », dans Hall, B.H. et N. Rosenberg (dir.), *Handbook of the Economics of Innovation*. Amsterdam, Pays-Bas, North-Holland.

MPG – Max Planck Society, 2017. *Guidelines and Rules of the Max Planck Society on a Responsible Approach to Freedom of Research and Research Risks*, Munich, Allemagne, MPG. https://www.mpg.de/197392/researchFreedomRisks.pdf.

MPO – Pêches et Océans Canada, 2022. À propos du Service hydrographique du Canada. https://www.cartes.gc.ca/help-aide/about-apropos/index-fra.html#legal (consulté en mai 2024).

Musker, R., et F. Smith, 2021. *Incentive Systems for Research Data Sharing in Funded Projects*, Wallingford, Royaume-Uni, CAB International. https://gatesopenresearch.org/documents/5-84.

Musunuri, S., J. B. Sandbrink, J. T. Monrad, M. J. Palmer et G. D. Koblentz, 2021. « Rapid proliferation of pandemic research: Implications for dual-use risks », *mBio*, vol. 12, nº 5, e0186421. https://doi.org/10.1128/mBio.01864-21.

NASEM – National Academies of Sciences, Engineering, and Medicine, 2017. *Dual Use Research of Concern in the Life Sciences: Current Issues and Controversies*, Washington, D.C., The National Academies Press. https://doi.org/10.17226/24761.

NASEM – National Academies of Sciences, Engineering, and Medicine, 2022. *Protecting U.S. Technological Advantage*, Washington, D.C., The National Academies Press. https://doi.org/10.17226/26647.

NASEM – National Academies of Sciences, Engineering, and Medicine, 2024. National Science, Technology, and Security Roundtable-Capstone Workshop. https://www.nationalacademies.org/our-work/national-science-technology-and-security-roundtable-capstone-event (consulté en novembre 2024).

NASEM – National Academies of Sciences, Engineering, and Medicine, 2025. *National Science, Technology, and Security Roundtable Capstone: Proceedings of a Workshop*, Washington, D.C., The National Academies Press. https://doi.org/10.17226/27976.

NCSC, CSE et DHS CISA – National Cyber Security Centre, Communications Security Establishment Canada et Department of Homeland Security's Cybersecurity and Infrastructure Security Agency des É.-U., 2020. *Advisory: APT29 Targets COVID-19 Vaccine Development*, Londres, Royaume-Uni; Ottawa, ON et Washington, D.C., NCSC. https://www.ncsc.gov.uk/files/Advisory-APT29-targets-COVID-19-vaccine-development.pdf.

NGRAC – Nunatsiavut Government Research Advisory Committee, s.d. NGRAC. https://nunatsiavut.com/research/ngrac/ (consulté en juin 2025).

NIAID – National Institute of Allergy and Infectious Diseases, 2021. Pandemic preparedness research approach. https://www.niaid.nih.gov/research/pandemic-preparedness-research-approach (consulté en juin 2025).

Nicoll, A., J. Dawson, J. Marty, M. Sawada et L. Copland, 2025. « Comparative and critical analysis of data sources used for ship traffic spatial pattern analysis in Canada and across the global Arctic », *Maritime Transport Research*, vol. 8, 100129. https://doi.org/10.1016/j.martra.2025.100129.

NIH – National Institutes of Health, 2014. *Implementation of the U.S. Government Policy for Institutional Oversight of Life Sciences DURC: Frequently Asked Questions*, Bethesda, MD, NIH.

Nokia Bell Labs, 2022. The transistor: 75 years since the famed Nokia Bell Labs invention changed the world. https://www.bell-labs.com/institute/blog/the-transistor-75-years-since-the-famed-nokia-bell-labs-invention-changed-the-world/#gref (consulté en novembre 2024).

Northrup, S., C. Lovekin, B. Blais, R. Chartier, R. Davis, P. Mann, … S. Sahrakorpi, 2022. *Stratégie de calcul de haute performance de l'Alliance de recherche numérique du Canada*, Toronto, ON, Alliance de recherche numérique du Canada. https://shorturl.at/8JhiS.

NPSA – National Protective Security Authority, 2023. Five Eyes launches the Five Principles of Secure Innovation. https://www.npsa.gov.uk/blog/news/five-eyes-launches-five-principles-secure-innovation (consulté en novembre 2024).

NPSA et NCSC – National Protective Security Authority et National Cyber Security Centre, 2024. *Trusted Research: Guidance for Academics*, Londres, Royaume-Uni, NPSA et NCSC. https://www.npsa.gov.uk/system/files/trusted-research-guidance-for-academia-digital-july24.pdf.

NSABB – National Science Advisory Board for Biosecurity, 2023. *Proposed Biosecurity Oversight Framework for the Future of Science*, Bethesda, MD, NSABB. https://osp.od.nih.gov/wp-content/uploads/2023/03/NSABB-Final-Report-Proposed-Biosecurity-Oversight-Framework-for-the-Future-of-Science.pdf.

NSF – U.S. National Science Foundation, 2023. Dear colleague letter: Workshop to inform development of the NSF Research on Research Security Program (RRSP). https://www.nsf.gov/pubs/2023/nsf23126/nsf23126.jsp (consulté en novembre 2024).

NSF – U.S. National Science Foundation, 2024a. Dear colleague letter: Request for Information on the CHIPS and Science Act Section 10343. Research Ethics. https://www.nsf.gov/pubs/2024/nsf24127/nsf24127.jsp (consulté en novembre 2024).

NSF – U.S. National Science Foundation, 2024b. NSF-backed SECURE Center will support research security, international collaboration. https://new.nsf.gov/news/nsf-backed-secure-center-will-support-research (consulté en octobre 2024).

NSF – U.S. National Science Foundation, 2025. The Research on Research Security Program (RoRS). https://www.nsf.gov/funding/opportunities/rors-research-research-security-program (consulté en mai 2025).

NSTC – National Science and Technology Council, 2022. *Guidance for Implementing National Security Presidential Memorandum 33 (NSPM-33) on National Security Strategy for United States Government-Supported Research and Development*, Washington, D.C., Subcommittee on Research Security & Joint Committee on the Research Environment. https://bidenwhitehouse.archives.gov/wp-content/uploads/2022/01/010422-NSPM-33-Implementation-Guidance.pdf.

OCDE – Organisation de coopération et de développement économiques, 2025. Principaux indicateurs de la science et de la technologie. https://www.oecd.org/fr/data/datasets/main-science-and-technology-indicators.html (consulté en janvier 2025).

OCW – Ministry of Education, Culture and Science, 2023. DBSA 2 published. https://english.loketkennisveiligheid.nl/latest/news/2023/01/17/dbsa-2-published (consulté en août 2024).

OCW – Ministry of Education, Culture and Science, s.d.-a. Contact Point for Knowledge Security. https://english.loketkennisveiligheid.nl/ (consulté en août 2024).

OCW – Ministry of Education, Culture and Science, s.d.-b. Legal frameworks and codes of conduct. https://english.loketkennisveiligheid.nl/tools-and-frameworks/legal-frameworks-and-codes-of-conduct (consulté en mai 2025).

OCW – Ministry of Education, Culture and Science, s.d.-c. About us: Submit your question to the National Contact Point. https://english.loketkennisveiligheid.nl/about-us (consulté en mai 2025).

OFI – Ocean Frontier Institute, 2022. *Indigenous Engagement Guide*, Halifax, NS, OFI. https://www.ofi.ca/impact/indigenous-engagement/guide.

OHI – L'Organisation hydrographique internationale, 2021. A propos de l'OHI. https://iho.int/fr/a-propos-de-l-ohi-0 (consulté en mai 2024).

OMS – Organisation mondiale de la Santé, 2022. *Cadre d'orientation mondial pour l'usage responsable des sciences de la vie : atténuer les risques biologiques et régir la recherche duale*, Genève, Suisse, OMS. https://iris.who.int/bitstream/handle/10665/369131/9789240067219-fre.pdf?sequence=1.

ONC – Ocean Networks Canada, 2021a. *ONC Data Policy*, Victoria, BC, ONC. https://www.oceannetworks.ca/data/data-policy/.

ONC – Ocean Networks Canada, 2021b. Building TRUST to be FAIR: Data stewardship for a sustainable ocean economy. https://www.oceannetworks.ca/news-and-stories/stories/building-trust-to-be-fair-data-stewardship-for-a-sustainable-ocean-economy/ (consulté en décembre 2024).

ONC – Ocean Networks Canada, 2023. Decolonizing data. https://www.oceannetworks.ca/news-and-stories/stories/decolonizing-data/ (consulté en janvier 2025).

ONC – Ocean Networks Canada, s.d.-a. Our story. https://www.oceannetworks.ca/about-onc/our-story/ (consulté en juin 2024).

ONC – Ocean Networks Canada, s.d.-b. Cabled networks. https://www.oceannetworks.ca/observatories/physical-infrastructure/cabled-networks (consulté en novembre 2024).

ONU – Nations Unies, 2007. *Déclaration des Nations Unies sur les droits des Peuples autochtones*, New York, NY, ONU. https://www.un.org/development/desa/indigenouspeoples/wp-content/uploads/sites/19/2018/11/UNDRIP_F_web.pdf.

OSTP – White House Office of Science and Technology Policy, 2022. *Desirable Characteristics of Data Repositories for Federally Funded Research*, Washington, D.C., OSTP. https://repository.si.edu/handle/10088/113528.

OSTP – White House Office of Science and Technology Policy, 2024. *Guidelines for Research Security Programs at Covered Institutions*, Washington, D.C., OSTP. https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/07/OSTP-RSP-Guidelines-Memo.pdf.

OTN – Ocean Tracking Network, 2024. *Ocean Tracking Network Data Policy*, Halifax, NS, OTN. https://members.oceantrack.org/data/policies/.

Owens, B., 2023a (14 juin). « La sécurité nationale et la recherche font-ils bon ménage? », *Affaires universitaires*. https://shorturl.at/B5sKe (consulté en mars 2024).

Owens, B., 2023b (19 avril). « L'heure est au rattrapage en matière de libre accès », *Affaires universitaires*. https://shorturl.at/tpQrT (consulté en novembre 2024).

Pannier, A., 2023. *Balancing Security and Openness for Critical Technologies: Challenges for French and European Research*, Paris, France, French Institute of International Relations. https://www.ifri.org/sites/default/files/migrated_files/documents/atoms/files/ifri_pannier_balancing_security_openness_critical_technologies_2023.pdf.

Paquet, V., S. Van Bellen, et V. Larivière, 2022. « Measuring the prevalence of open access in Canada: A national comparison », *The Canadian Journal of Information and Library Science*, vol. 45, nº 1, p. 1–21. https://doi.org/10.5206/cjilsrcsib.v45i1.14149.

Plomp, E., N. Dintzner, M. Teperek et A. Dunning, 2019. « Cultural obstacles to research data management and sharing at TU Delft », *Insights*, vol. 32, nº 29, p. 1–11. https://doi.org/10.1629/uksg.484.

POLAIRE – Savoir polaire Canada, 2020. *Savoir polaire Canada: Plan stratégique*, Ottawa, ON, Gouvernement du Canada. https://www.canada.ca/fr/savoir-polaire/rapports/plan-strategique.html.

POLAIRE – Savoir polaire Canada, 2022. *Savoir polaire : Rapport Aqhaliat – volume 4*, Ottawa, ON, Gouvernement du Canada. https://www.canada.ca/fr/savoir-polaire/publications/aqhaliat/volume-4.html.

POLAIRE – Savoir polaire Canada, 2023. Canadian Ranger Ocean Watch (CROW). https://www.canada.ca/content/dam/polar-polaire/documents/publications/aqhaliat/volume-4/infosheets/crow-english.pdf (consulté en juin 2025).

Polytechnics Canada et BHER – Business + Higher Education Roundtable, s.d. *Guide to Research Partnerships with Canada's Colleges & Polytechnics*, Ottawa, ON, Polytechnics Canada et BHER. https://bher.ca/assets-documents/resource/Research-Partnerships-Guide-Colleges-Sept.pdf.

Pouget, H., et R. Zuhdi, 2024 (5 mars). « AI and product safety standards under the EU AI Act », *Carnegie Endowment for International Peace*. https://carnegieendowment.org/research/2024/03/ai-and-product-safety-standards-under-the-eu-ai-act?lang=en

Prasso, S., 2021 (14 décembre). « China Initiative set out to catch spies. It didn't find many », *Bloomberg Businessweek*. https://www.bloomberg.com/news/features/2021-12-14/doj-china-initiative-to-catch-spies-prompts-fbi-misconduct-racism-claims (consulté en mai 2025).

Rantanen, M., A. Y. Karpechko, A. Lipponen, K. Nordling, O. Hyvärinen, K. Ruosteenoja, … A. Laaksonen, 2022. « The Arctic has warmed nearly four times faster than the globe since 1979 », *Communications Earth & Environment*, vol. 3, p. 168. https://doi.org/10.1038/s43247-022-00498-3.

Rappert, B., et M. J. Selgelid, 2013. *On the Dual Uses of Science and Ethics: Principles, Practices, and Prospects*, Canberra, Australie, ANU E Press.

RBC Thought Leadership, 2024 (28 novembre). « Canada's biotech reboot: How to keep the vital life sciences sector strong ». https://www.rbc.com/en/thought-leadership/the-growth-project/canadas-biotech-reboot-how-to-keep-the-vital-life-sciences-sector-strong/ (consulté en mai 2025).

RCAANC – Relations Couronne-Autochtones et Affaires du Nord Canada, 2022a. *Politique sur l'Inuit Nunangat*, Ottawa, ON, Gouvernement du Canada. https://www.rcaanc-cirnac.gc.ca/fra/1650556354784/1650556491509.

RCAANC – Relations Couronne-Autochtones et Affaires du Nord Canada, 2022b. Navigation dans l'Arctique. https://www.rcaanc-cirnac.gc.ca/fra/1648145733596/1648145784817 (consulté en juin 2025).

RCAT – Research Collaboration Advice Team, s.d. About us. https://www.gov.uk/government/organisations/research-collaboration-advice-team/about (consulté en septembre 2024).

RDDC – Recherche et développement pour la défense Canada, 2023. Capacités de recherche et de développement. https://www.canada.ca/fr/recherche-developpement-defense/services/capacites.html (consulté en juin 2024).

Révelard, A., J. Tintoré, J. Verron, P. Bahurel, J. A. Barth, M. Belbéoch, … B. Williams, 2022. « Ocean integration: The needs and challenges of effective coordination within the ocean observing system », *Frontiers in Marine Science*, vol. 8, 737671. https://doi.org/10.3389/fmars.2021.737671.

Richardson, B. et Y. Hussain, 2022 (1er septembre). « Course correction: How international students can help solve Canada's labour crisis », *RBC*. https://thoughtleadership.rbc.com/course-correction-how-international-students-can-help-solve-canadas-labour-crisis/ (consulté en février 2025).

RIVM – Dutch National Institute for Public Health and the Environment, s.d.-a. Biosecurity Office. https://www.bureaubiosecurity.nl/en (consulté en août 2024).

RIVM – Dutch National Institute for Public Health and the Environment, s.d.-b. Dual-use animation. https://www.bureaubiosecurity.nl/en/dual-use-animatie (consulté en août 2024).

RIVM – Dutch National Institute for Public Health and the Environment, s.d.-c. Dual-Use Quickscan. https://dualusequickscan.com/en/ (consulté en mai 2024).

Robinson, J., 2020. *Arctic Space Challenge for NATO Emerging from China's Economic and Financial Assertiveness*, Kalkar, Allemagne, Joint Air Power Competence Centre. https://www.japcc.org/articles/arctic-space-challenge-for-nato-emerging-from-chinas-economic-and-financial-assertiveness/.

Rohden, F., et H.-J. Wieden, 2022. « Introduction: Dual use in life science research », *Biochemistry and Cell Biology*, vol. 100, p. 266-267. https://doi.org/10.1139/bcb-2022-0082.

Rubinstein, Y. R., P. N. Robinson, W. A. Gahl, P. Avillach, G. Baynam, H. Cederroth, … M. A. Haendel, 2020. « The case for open science: Rare diseases », *JAMIA Open*, vol. 3, nº 3, p. 472-486. https://doi.org/10.1093/jamiaopen/ooaa030.

Sandbrink, J. B., et G. D. Koblentz, 2022. « Biosecurity risks associated with vaccine platform technologies », *Vaccine*, vol. 40, p. 2514-2523. https://doi.org/10.1016/j.vaccine.2021.02.023.

SC et ASPC – Santé Canada et Agence de la santé publique du Canada, 2022. *Évaluation de la Loi sur les agents pathogènes humains et les toxines et de son règlement d'application 2015-2016 à 2020-2021*, Ottawa, ON, Gouvernement du Canada, Bureau de l'audit et de l'évaluation. https://www.canada.ca/fr/sante-publique/organisation/transparence/rapports-gestion/evaluation/loi-agents-pathogenes-humains-toxines-reglement-d-application-2015-2016-2020-2021.html.

Science-Metrix, 2024. *Bibliometric Analysis for the Expert Panel on the State of Science, Technology, and Innovation in Canada*. Montréal, QC, partagé en ligne par le CAC. https://www.rapports-cac.ca/wp-content/uploads/2025/11/science-metrix-bibliometric-analysis-for-the-expert-panel-on-the-state-of-science-technology-and-innovation-in-canada-2025.pdf.

SCRS – Service canadien du renseignement de sécurité, 2020. *À L'étranger – Directives de sécurité sur les voyages*, Ottawa, ON, Gouvernement du Canada. https://www.canada.ca/fr/service-renseignement-securite/organisation/publications/a-letranger.html.

SCRS – Service canadien du renseignement de sécurité, 2024a. Innover en toute sécurité : Conseils de sécurité à l'intention des investisseurs dans le secteur des nouvelles technologies. https://www.canada.ca/fr/service-renseignement-securite/organisation/publications/innover-en-toute-securite-investisseurs.html (consulté en février 2025).

SCRS – Service canadien du renseignement de sécurité, 2024b. *Rapport public du SCRS 2023*, Ottawa, ON, Gouvernement du Canada. https://www.canada.ca/fr/service-renseignement-securite/organisation/publications/rapport-public-du-scrs-2023.html.

SCRS – Service canadien du renseignement de sécurité, 2024c. Les partenaires en renseignement du Groupe des cinq lancent une initiative conjointe offrant conseils de sécurité aux entreprises, chercheurs et investisseurs du secteur des technologies. https://www.canada.ca/fr/service-renseignement-securite/nouvelles/2024/10/les-partenaires-en-renseignement-du-groupe-des-cinq-lancent-une-initiative-conjointe-offrant-conseils-de-securite-aux-entreprises-chercheurs-et-inv.html (consulté en mai 2025).

SCRS – Service canadien du renseignement de sécurité, 2024d. *Need to Know September 2024*, Ottawa, ON, Gouvernement du Canada. https://www.citt.ca/insights/resources/csis-september-2024.

SCRS – Service canadien du renseignement de sécurité, 2025. *Rapport public du SCRS 2024*, Ottawa, ON, Gouvernement du Canada. https://www.canada.ca/fr/service-renseignement-securite/organisation/publications/rapport-public-du-scrs-2024.html.

SCT – Secrétariat du Conseil du Trésor du Canada, 2014. *Directive sur le gouvernement ouvert*, Ottawa, ON, Gouvernement du Canada. https://www.tbs-sct.canada.ca/pol/doc-fra.aspx?id=28108.

SCT – Secrétariat du Conseil du Trésor du Canada, 2018. Plan d'action national du Canada pour un gouvernement ouvert de 2018-2020. https://ouvert.canada.ca/fr/contenu/plan-daction-national-du-canada-pour-un-gouvernement-ouvert-de-2018-2020 (consulté en novembre 2024).

SECD – Standing Senate Committee on National Security, Defence and Veterans Affairs, 2023. *Arctic Security under Threat: Urgent Needs in a Changing Geopolitical and Environmental Landscape*, Ottawa, ON, SECD. https://sencanada.ca/content/sen/committee/441/SECD/reports/2023-06-28_SECD_ArcticReport_e.pdf.

SFU – Université Simon Fraser, 2023. SFU Open Access Policy. https://www.lib.sfu.ca/help/publish/scholarly-publishing/open-access/open-access-policy (consulté en novembre 2024).

SGDSN – Secrétariat général de la défense et de la Sécurité nationale, 2018. *La protection numérique du potentiel scientifique et technique de la nation*, Paris, France, SGDSN. https://www.sgdsn.gouv.fr/files/files/Nos_missions/guide_protection_scientifique_technique_nation_anssi-pa-049_v1.pdf.

SGDSN – Secrétariat général de la défense et de la Sécurité nationale, s.d. *La protection du potentiel scientifique et technique de la nation*, Paris, France, SGDSN. https://www.sgdsn.gouv.fr/files/files/Nos_missions/a5-ppst-v5.pdf.

Shankar, A., et W. Drake, 2022. *Effective Cybersecurity for Research*, Bloomington, IN, Center for Applied Cybersecurity Research, Indiana University. https://library.educause.edu/-/media/files/library/2022/6/researchcybersecurity.pdf.

Sharma, Y., 2025 (17 avril). « Academics say draft screening law could deter foreign talent », *University World News*. https://www.universityworldnews.com/post.php?story=20250417132055569 (consulté en juin 2025).

Shea, D. A., 2006. *Balancing Scientific Publications and National Security Concerns: Issues for Congress*, Washington, D.C., U.S. Congressional Research Service. https://sgp.fas.org/crs/secrecy/RL31695.pdf.

SIGRE – Groupe de travail sur la sécurité et l'intégrité de l'écosystème de la recherche, 2022. *Valeurs communes et principes du G7 en matière de sécurité et d'intégrité de la recherche*, s.l., SIGRE. https://science.gc.ca/site/science/sites/default/files/attachments/2023/1135-valeurs-communes-et-principes-du-g7-en-mati%C3%A8re-de-s%C3%A9curit%C3%A9-et-d%E2%80%99int%C3%A9grit%C3%A9-de-la-recherche.pdf.

SIGRE – Groupe de travail sur la sécurité et l'intégrité de l'écosystème de la recherche, 2024. *Meilleures pratiques du G7 pour une recherche sécuritaire et ouverte*, s.l., SIGRE. https://www.science.gc.ca/site/science/sites/default/files/documents/1136-meilleures-pratiques-du-g7-pour-une-recherche-securitaire-et-ouverte-octobre-2024.pdf.

Silbey, S. S., 2022. « Why do biologists and chemists do safety differently? The reproduction of cultural variation through pragmatic regulation », dans Gross, N., I.A. Reed, et C. Winship (dir.), *The New Pragmatist Sociology: Inquiry, Agency, and Democracy*, 1re édition, New York, NY, Columbia University Press.

Simard, M.-A., G. Ghiasi, P. Mongeon et V. Larivière, 2022. « National differences in dissemination and use of open access literature », *PLOS ONE*, vol. 17, no 8, e0272730. https://doi.org/10.1371/journal.pone.0272730.

SIOOC – Système intégré d'observation des océans du Canada, s.d.-a. À propos de SIOOC. https://cioos.ca/fr/a-propos/(consulté en novembre 2024).

SIOOC – Système intégré d'observation des océans du Canada, s.d.-b. Des milliers de données sur nos océans. https://www.cioos.ca/fr/accueil/ (consulté en novembre 2024).

SIOOC – Système intégré d'observation des océans du Canada, s.d.-c. Ressources pour la gestion de données. https://cioos.ca/fr/gestion-de-donnees/(consulté en février 2025).

Smith, G. C., R. Allard, M. Babin, L. Bertino, M. Chevallier, G. Corlett, … the WWRP PPP Steering Group, 2019. « Polar ocean observations: A critical gap in the observing system and its effect on environmental predictions from hours to a season », *Frontiers in Marine Science*, vol. 6, p. 429. https://doi.org/10.3389/fmars.2019.00429.

Snipp, C. M., 2016. « What does data sovereignty imply: What does it look like? », dans Kukutai, T. et J. Taylor (dir.), *Indigenous Data Sovereignty: Toward an Agenda*. Canberra, Australie, Australian National University Press.

SP – Sécurité publique Canada, 2010. *Guide pour la planification de la gestion des urgences 2010-2011*. Ottawa, ON, Gouvernement du Canada. https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/mrgnc-mngmnt-pnnng/index-fr.aspx.

SP – Sécurité publique Canada, 2012. *Lignes directrices sur la méthodologie d'évaluation tous risques 2012-2013*, Ottawa, ON, Gouvernement du Canada. https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/archive-ll-hzrds-ssssmnt/index-fr.aspx.

SP – Sécurité publique Canada, 2023. Notes des comités parlementaires : Comité permanent de la science et de la recherche (SRSR) Questions et réponses. https://www.securitepublique.gc.ca/cnt/trnsprnc/brfng-mtrls/prlmntry-bndrs/20240321/04-fr.aspx (consulté en février 2025).

SP – Sécurité publique Canada, 2024a. À propos du Centre de la sécurité de la recherche. https://www.canada.ca/fr/services/defense/securiterecherche/apropos.html (consulté en mai 2024).

SP – Sécurité publique Canada, 2024b. *Profil national des risques : Un outil national de préparation et de sensibilisation aux situations d'urgence*, Ottawa, ON, Gouvernement du Canada. https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/2023-nrp-pnr/2023-npr-pnr-fr.pdf.

SP – Sécurité publique Canada, 2024c. Notes des comités parlementaires : Filtrage de sécurité en matière d'immigration – Un programme trilatéral. https://www.securitepublique.gc.ca/cnt/trnsprnc/brfng-mtrls/prlmntry-bndrs/20241227/14-fr.aspx (consulté en janvier 2025).

SP – Sécurité publique Canada, 2024d. Lignes médiatiques – Projet de loi C-70, *Loi concernant la lutte contre l'ingérence étrangère*. https://www.justice.gc.ca/eng/trans/bm-mb/other-autre/c70/media-mediatiques.html (consulté en mai 2025).

SP – Sécurité publique Canada, 2024e. Notes des comités parlementaires : Sécurité de la recherche. https://www.securitepublique.gc.ca/cnt/trnsprnc/brfng-mtrls/prlmntry-bndrs/20240813/03-fr.aspx (consulté en novembre 2024).

SPAC – Services publics et Approvisionnement Canada, 2024. Marchandises contrôlées : examen, possession ou transfert. https://www.canada.ca/fr/services-publics-approvisionnement/services/securite-industrielle/marchandises-controlees.html (consulté en juillet 2024).

SPIIE – Secrétariat des programmes interorganismes à l'intention des établissements, 2022. Sécurité de la recherche. https://www.rsf-fsr.gc.ca/apply-demande/research_security-securite-recherche-fra.aspx (consulté en octobre 2024).

SPIIE – Secrétariat des programmes interorganismes à l'intention des établissements, 2024. Research security funding for 2023–24. https://www.rsf-fsr.gc.ca/apply-demande/grants-subventions/rs2023-fra.aspx (consulté en octobre 2024).

Spitale, G., F. Germani et N. Biller-Andorno, 2024. « Disruptive technologies and open science: How open should open science be? A "third bioethics" ethical framework », *Science and Engineering Ethics*, vol. 30, p. 36. https://doi.org/10.1007/s11948-024-00502-3.

SRO – Safeguarding Research Office, 2024a. *Understanding and Adhering to Government of Ontario Research Security Requirements*, Edmonton, AB, Office of the Vice-President (Research & Innovation), University of Alberta.

SRO – Safeguarding Research Office, 2024b. *2024 Impact Report*, Edmonton, AB, Office of the Vice-President (Research & Innovation), University of Alberta. https://www.ualberta.ca/en/research/media-library/services/2024-safeguarding-research-office-impact-report.pdf.

SRO – Safeguarding Research Office, 2025. *Responsible Open Source Due Diligence Protocol*, Edmonton, AB, Office of the Vice-President (Research & Innovation), University of Alberta. https://www.ualberta.ca/en/research/media-library/services/responsible-open-source-due-diligence-protocol.pdf.

SRSR – Comité permanent de la science et de la recherche, 2024. *La sécurité des partenariats de recherche des universités et des établissements de recherche canadiens avec des entités liées à la république populaire de chine*, Ottawa, ON, Chambre des communes. https://www.noscommunes.ca/documentviewer/fr/44-1/SRSR/rapport-10.

StatCan – Statistique Canada, 2020. Estimations des dépenses de recherche et développement (R-D) effectuées dans le secteur de l'enseignement supérieur. https://www.statcan.gc.ca/fr/programmes-statistiques/document/5109_D3_T9_V1(consulté en juin 2025).

StatCan – Statistique Canada, 2023. Tableau 37-10-0020-01: Diplômés postsecondaires, selon le type d'établissement, le statut de l'étudiant au Canada et le genre de la personne. https://www150.statcan.gc.ca/t1/tbl1/fr/cv.action?pid=3710002001&request_locale=fr (consulté en novembre 2024).

StatCan – Statistique Canada, 2024a. Tableau 27-10-0273-01 (anciennement CANSIM 358-0001) : Dépenses intérieures brutes en recherche et développement, selon le type de science et selon le secteur de financement et le secteur d'exécution (x 1 000 000). https://www150.statcan.gc.ca/t1/tbl1/en/tv.action?pid=2710027301 (consulté en juin 2025).

StatCan – Statistique Canada, 2024b. Tableau 37-10-0135-01: Diplômés postsecondaires, selon le domaine d'études, la classification Internationale Type de l'Éducation, le groupe d'âge et le genre de la personne. https://www150.statcan.gc.ca/t1/tbl1/fr/tv.action?pid=3710013501&request_locale=fr (consulté en juin 2025).

StatCan – Statistique Canada, 2024c. Tableau 36-10-0604-01: Activités des entreprises multinationales au Canada, multinationales canadiennes et étrangères, selon le secteur et l'industrie. https://www150.statcan.gc.ca/t1/tbl1/fr/cv.action?pid=3610060401&request_locale=fr (consulté en septembre 2024).

StatCan – Statistique Canada, 2024d. Plan d'action pour la science ouverte de Statistique Canada. https://www.statcan.gc.ca/fr/apercu/paso (consulté en novembre 2024).

Stirling, A., K. R. Hayes et J. Delborne, 2018. « Towards inclusive social appraisal: Risk, participation and democracy in governance of synthetic biology », *BMC Proceedings*, vol. 12, suppl. 8, p. 15. https://doi.org/10/gr5fcp.

Sun, K., W. Cui et C. Chen, 2021. « Review of underwater sensing technologies and applications », *Sensors*, vol. 21, 7849. https://doi.org/10.3390/s21237849.

Tatlow, D. K., 2024 (21 juillet). « China's expanding Arctic ambitions challenge the U.S. and NATO », *Newsweek* : https://www.newsweek.com/2024/08/09/china-russia-us-arctic-north-pole-strategy-svalbard-norway-sea-route-1916641.html (consulté en août 2024).

Tayler, F., D. Moher et K. Cobey, 2020. « Creating an Audit and Feedback Loop to Monitor and Enhance Data Sharing in Canada », *Université d'Ottawa, Préimpression*. https://ruor.uottawa.ca/handle/10393/41562.

The Australia Group, 2023. Control list of dual-use biological equipment and related technology and software. https://www.dfat.gov.au/publications/minisite/theaustraliagroupnet/site/en/dual_biological.html (consulté en mai 2024).

Thomson, J., 2017 (2 août). « Canadian military developing surveillance system to monitor Arctic waters », *CBC News*. https://www.cbc.ca/news/canada/north/cause-array-drdc-test-1.4232348 (consulté en novembre 2024).

Tiku, N., et G. de Vynck, 2023 (4 mai). « Google shared AI knowledge with the world—until ChatGPT caught up », *The Washington Post*. https://www.washingtonpost.com/technology/2023/05/04/google-ai-stop-sharing-research/ (consulté en juin 2025).

Trevena, P., 2019. *Post Study Work Visa Options: An International Comparative Review*, Édinbourg, Royaume-Uni, Gouvernement de l'Écosse. https://dera.ioe.ac.uk/id/eprint/33953/1/post-study-work-visa-options-international-comparative-review.pdf.

TRIUMF, 2018. *TRIUMF Strategic Plan 2020–2025*, Vancouver, BC, TRIUMF. https://fiveyearplan.triumf.ca/wp-content/uploads/2019/05/TRIUMF-Strategic-Plan-Web-Pages.pdf.

TU Delft – Delft University of Technology, s.d. Data stewardship. https://www.tudelft.nl/en/library/research-data-management/r/support/data-stewardship (consulté en novembre 2024).

U.S. GAO – U. S. Government Accountability Office, 2022. National security space: Actions needed to better use commercial satellite imagery and analytics. https://www.gao.gov/products/gao-22-106106 (consulté en juin 2025).

U15 – Les grandes universités de recherche du Canada, 2023. *Protéger la recherche au Canada : Guide des politiques et des pratiques universitaires*, s.l., U15. https://u15.ca/wp-content/uploads/2023/06/2023-06-22.-Proteger-la-recherche-au-Canada-Guide-des-politiques-et-des-pratiques-universitaires-FINAL.pdf.

U15 et Universities Canada, 2019a. *Guide sur la sécurité en voyage à l'intention du personnel et des chercheurs universitaires*, Ottawa, ON, U15 et Universités Canada. https://univcan.ca/wp-content/uploads/2020/08/guide-sur-la-securite-en-voyage-a-lintention-du-personnel-et-des-chercheurs-universitaires-dec-2019.pdf.

U15 et Universities Canada, 2019b. *Atténuer les risques économiques et géopolitiques associés aux projets de recherche sensibles — Guide à l'intention des chercheurs universitaires*, Toronto, ON, U15 et Universités Canada. https://univcan.ca/wp-content/uploads/2020/08/attenuer-les-risques-economiques-et-geopolitiques-associes-aux-projets-de-recherche-sensibles-dec-2019.pdf.

Ueno, H., 2023. « Artificial intelligence as dual-use technology », dans Hatzilygeroudis, I.K., G.A. Tsihrintzis, et L.C. Jain (dir.), *Fusion of Machine Learning Paradigms: Theory and Applications*. Cham, Switzerland, Springer.

UFIT – University Foreign Interference Taskforce, 2021. *Guidelines to Counter Foreign Interference in the Australian University Sector*, Canberra, Australie, Gouvernement de l'Australie. https://www.education.gov.au/countering-foreign-interference-australian-university-sector/resources/guidelines-counter-foreign-interference-australian-university-sector.

Uhlenhaut, C., R. Burger et L. Schaade, 2013. « Protecting society: Biological security and dual-use dilemma in the life sciences—status quo and options for the future », *EMBO Reports*, vol. 14, nº 1, p. 25-30. https://doi.org/10.1038/embor.2012.195.

UKRI – United Kingdom Research and Innovation, 2024a. Ensuring open research. https://www.ukri.org/what-we-do/supporting-healthy-research-and-innovation-culture/open-research/ (consulté en août 2024).

UKRI – United Kingdom Research and Innovation, 2024b. Trusted research and innovation. https://www.ukri.org/manage-your-award/good-research-resource-hub/trusted-research-and-innovation/ (consulté en août 2024).

UNESCO – Organisation des Nations Unies pour l'éducation, la science et la culture, 2021. *Recommandation de l'UNESCO sur une science ouverte*, Paris, France, UNESCO. https://unesdoc.unesco.org/ark:/48223/pf0000379949_fre.

Université de Calgary et Université de l'Alberta, 2023. *Research Security Conference Summary: Mitigating Risk in a Changing World*, Calgary, AB, Université de Calgary et Université de l'Alberta. https://www.ualberta.ca/en/research/media-library/services/2023-rs-conference-summary-notes.pdf.

Université de Calgary, 2025. Alberta Research Security Community of Practice Workshop/AGM. https://events.ucalgary.ca/event/494400-alberta-research-security-community-of-practice (consulté en mai 2025).

Université de Cambridge, s.d. Data champions. https://www.data.cam.ac.uk/intro-data-champions (consulté en novembre 2024).

Université de l'Alberta, 2024a. *Research Security Requirements At-a-Glance Tool*, Edmonton, AB, Safeguarding Research Office. https://www.ualberta.ca/en/research/media-library/services/updated-october-2024-research-security-at-a-glance-tool.pdf.

Université de l'Alberta, 2024b. *Safeguarding Research: Research Security Overview Presentation*, Edmonton, AB, Safeguarding Research Office.

Université de l'Alberta, 2025. Safeguarding your research. https://www.ualberta.ca/en/research/services/safeguarding-your-research.html (consulté en mars 2025).

Université de Tokyo, s.d. U.S.–Canada–Japan International Workshop on Research Security and Integrity. https://ifi.u-tokyo.ac.jp/en/event/13105/ (consulté en mai 2025).

Université de Toronto, 2022. *Canada's AI Ecosystem: Government Investment Propels Private Sector Growth*, Toronto, ON, Université de Toronto. https://gro.utoronto.ca/wp-content/uploads/2022/04/Canadas_AI_Ecosystem-_Government_Investment_Propels_Private_Sector_Growth.pdf.

Université de Toronto, 2025. Report Number 215 of the Planning & Budget Committee. https://governingcouncil.utoronto.ca/secretariat/page/governance-bodies/planning-and-budget-committee/reports/feb-12-2025 (consulté en juin 2025).

Université de Toronto, s.d. Research security: Safeguarding research. https://research.utoronto.ca/safeguarding-research/research-security-safeguarding-research (consulté en mars 2025).

Université de Victoria, 2024. Implication of Ontario research security guidelines. https://www.uvic.ca/research-services/funding/research-security/announcements/ontario-research-security.php (consulté en février 2025).

Université de Victoria, 2025. Research security. https://www.uvic.ca/research-services/funding/research-security/index.php (consulté en mars 2025).

Universités Canada, 2024. *Briefing Note on New Research Security Measures*, Ottawa, ON, Universités Canada. https://www.ulethbridge.ca/sites/default/files/2024/02/universities_canada_-_research_security_goc_announcement_briefing_note_to_member_insititutions.pdf.

Universities Australia, 2024. *Legislative review of the Australia's Foreign Relations (State and Territory Arrangements) Act 2020*, Deakin, Australie, Universities Australia. https://universitiesaustralia.edu.au/wp-content/uploads/2024/08/Submission-to-the-review-of-Australias-Foreign-Relations-State-and-Territory-Arrangements-Act-2020.pdf.

Universities UK, CPNI, et UKRI – Centre for the Protection of National Infrastructure et UK Research and Innovation, 2022. *Managing Risks in International Research and Innovation: An Overview of Higher Education Sector Guidance*, Londres, Royaume-Uni, Universities UK, CPNI et UKRI. https://www.universitiesuk.ac.uk/sites/default/files/field/downloads/2022-06/managing-risks-in-international-research-and-innovation-uuk-cpni-ukri_1.pdf.

UNL – Universities of the Netherlands, 2024. *Capability Maturity Model: Knowledge Security*, La Haye, Pays-Bas, UNL. https://www.universiteitenvannederland.nl/files/publications/UNL%20Capability%20Maturity%20Model%20Knowledge%20Security%20ENG-DEF.pdf.

UNZ – Universities New Zealand – Te Pōkai Tara, 2022. *Trusted Research – Protective Security Requirements: Guide for Senior University Leaders in Aotearoa New Zealand*, Wellington, Nouvelle-Zélande, UNZ. https://www.universitiesnz.ac.nz/sites/default/files/uni-nz/Main%20guide_as%20single%20pages.pdf.

uOttawa – Université d'Ottawa, 2022. *Règlement 128 : Règlement sur la sécurité relative aux voyages internationaux*, Ottawa, ON, uOttawa. https://www.uottawa.ca/notre-universite/leadership-gouvernance/politiques-reglements/reglement-128-securite-voyages-internationaux.

van der Molen, I., D. Gheorghe, C. Daouti et V. Eechaudt, 2023. *Keeping Science Open? Current Challenges in the Day-to-Day Reality of Universities*, Louvain, Belgique, Conference of European Schools for Advanced Engineering Education and Research (CESAER). https://zenodo.org/doi/10.5281/zenodo.8355324.

Verga, S., 2013. *A Holistic, Cross-Government All Hazards Risk Assessment*, Ottawa, ON, Recherche et développement pour la défense Canada, Centre des sciences pour la sécurité. https://publications.gc.ca/collections/collection_2017/rddc-drdc/D69-26-2013-eng.pdf.

VIDO – Vaccine and Infectious Disease Organization, 2025. Community Liaison Committee. https://www.vido.org/about/community-liaison-committee.php (consulté en mars 2025).

VIDO – Vaccine and Infectious Disease Organization, s.d. Facilities. https://www.vido.org/about/facilities.php (consulté en janvier 2025).

VU Amsterdam – Vrije Universiteit Amsterdam, 2023. Sleuteltechnologieën [Key technologies]. https://assets-us-01.kc-usercontent.com/d8b6f1f5-816c-005b-1dc1-e363dd7ce9a5/2db06628-bbe9-43cb-8ee9-8064899405ca/Sleuteltechnologie%C3%ABn%20-%20Key%20technology%202023.pdf (consulté en août 2024).

Wagner, W. J., et R. Zaia, 2023 (17 novembre). « The intersection between national security research guidelines and export/import laws in Canada: What institutions should know », *Gowling WLG*. https://gowlingwlg.com/en/insights-resources/articles/2023/national-security-research-guidelines/ (consulté en juin 2024).

Wang, L.-F., S. R. Lewin, N. Zhong, L. Zhang, Z. Chen, K.-Y. Yuen et D. D. Ho, 2025. « Pandemic research: The need for a paradigm shift », *The Lancet Microbe*, vol. 6. https://doi.org/10.1016/j.lanmic.2024.101048.

WAS – Wassenaar Arrangement Secretariat, 2023. *Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies*, Vienne, Autriche, WAS. https://www.wto.org/english/res_e/booksp_e/int_exp_regs_part3_5_e.pdf.

Weisko, P., 2025 (25 mars). « Dragon on ice: China's geostrategic interests in the Arctic », *Institute for National Security Studies, Tel Aviv University*. https://www.inss.org.il/publication/north-pole/ (consulté en mai 2025).

Whalen, D., D. L. Forbes, V. Kostylev, M. Lim, P. Fraser, M. R. Nedimović et S. Stuckey, 2022. « Mechanisms, volumetric assessment, and prognosis for rapid coastal erosion of Tuktoyaktuk Island, an important natural barrier for the harbour and community », *Canadian Journal of Earth Sciences*, vol. 59, p. 945-960. https://doi.org/10.1139/cjes-2021-0101.

WHOI – Woods Hole Oceanographic Institution, s.d. Areas of research. https://www.whoi.edu/what-we-do/understand/areas-of-research/ (consulté en juin 2025).

Wilner, A., S. Beach-Vaive, C. Carbonneau, G. Hopkins et F. Leblanc, 2022. « Research at risk: Global challenges, international perspectives, and Canadian solutions », *International Journal*, vol. 77, nº 1, p. 26-50. https://doi.org/10.1177/00207020221118504.

WIPO – World Intellectual Property Organization, s.d. WIPO Guide to Trade Secrets and Innovation—Part II: Strategic roles of trade secrets in the innovation ecosystem. https://www.wipo.int/web-publications/wipo-guide-to-trade-secrets-and-innovation/en/part-ii-strategic-roles-of-trade-secrets-in-the-innovation-ecosystem.html (consulté en novembre 2024).

Wölfl, A.-C., H. Snaith, S. Amirebrahimi, C. W. Devey, B. Dorschel, V. Ferrini, … R. Wigley, 2019. « Seafloor mapping—The challenge of a truly global ocean bathymetry », *Frontiers in Marine Science*, vol. 6, p. 283. https://doi.org/10.3389/fmars.2019.00283.

Woods, H. B., et S. Pinfield, 2022. « Incentivising research data sharing: A scoping review », *Wellcome Open Research*, vol. 6, p. 355. https://doi.org/10.12688/wellcomeopenres.17286.2.

Yao, D., 2023 (8 mai). « Google to halt sharing AI research—Until product is developed », *AI Business*. https://aibusiness.com/companies/google-to-halt-sharing-ai-research-until-product-is-developed (consulté en novembre 2024).

Yoshizawa, G., N. Shinomiya, S. Kawamoto, N. Kawahara, D. Kiga, K.-I. Hanaki et J. Minari, 2023. « Limiting open science? Three approaches to bottom-up governance of dual-use research of concern », *Pathogens and Global Health*. https://doi.org/10.1080/20477724.2023.2265626.

Zandee, D., K. Kruijver et A. Stoetman, 2020. *The Future of Arctic Security: The Geopolitical Pressure Cooker and the Consequences for the Netherlands*, La Haye, Pays-Bas, The Netherlands Institute of International Relations (Clingendael). https://www.clingendael.org/sites/default/files/2020-04/Report_The_Future_of_Arctic_Security_April_2020.pdf.

Zhang, F., 2019. « Development of CRISPR-Cas systems for genome editing and beyond », *Quarterly Reviews of Biophysics*, vol. 52, nº e6, p. 1-31. https://doi.org/10.1017/S0033583519000052.

Zheng, E., 2021 (28 octobre). « Choosing open: How to find an open access route that works for you », *University of Alberta Library News*. https://news.library.ualberta.ca/blog/tag/scholarly-comms-and-open/ (consulté en juin 2025).

Conseil d'administration*

Soheil Asgarpour, FACG, (président), Président et chef de direction sortant, Petroleum Technology Alliance Canada et Président sortant du conseil d'administration, Académie canadienne du génie (Vancouver, C.-B.)

Brian Fleck, Professeur, Faculté de génie, Département de génie mécanique, Université de l'Alberta (Edmonton, Alb.)

Pascal Grenier, Vice-président principal, Solutions aériennes et Exploitation mondiale, CAE (Montréal, Qc)

Jawahar (Jay) Kalra, M.D., MACSS, (vice-président), Professeur, Département de pathologie et de médecine de laboratoire, Université de la Saskatchewan (Saskatoon, Sask.)

Catherine Karakatsanis, FACG, Cheffe de l'exploitation, Stantec (Morrison Hershfield Group Inc.) (Toronto, Ont.)

Catherine Middleton, Professeure, École de gestion des technologies de l'information Ted Rogers, Université métropolitaine de Toronto (Toronto, Ont.)

Hasna Rouighi, Directrice du Bureau de l'innovation, ministère de la Santé et des Services sociaux, gouvernement du Québec (Montréal, Qc)

Donna Strickland, C.C., MSRC, FACG, Professeure, Département de physique et d'astronomie, Université de Waterloo (Waterloo, Ont.)

Christine Thomas, Vice-présidente, Gouvernance et Conseillère juridique, Association médicale canadienne (Ottawa, Ont.)

Gisèle Yasmeen, Global Fellow, Wilson Center (Ottawa, ON)

*en juillet 2025

Comité consultatif scientifique*

Maydianne C. B. Andrade (présidente), Professeure universitaire de sciences biologiques (Toronto, Ont.)

Peter Backx, MSRC, Professeur, Département de biologie; titulaire, Chaire de recherche du Canada en biologie cardiovasculaire, Université York (Toronto, ON)

Kyle Bobiwash, Professeur adjoint, érudit autochtone, Entomologie, Université du Manitoba (Winnipeg, Man.)

Bing Chen, Professeur de génie civil, titulaire de la Chaire UArctic en génie de l'environnement marin et côtier, directeur du Northern Region Persistent Organic Pollution Control (NRPOP) Lab et doyen associé de la faculté de génie et des sciences appliquées, Université Memorial de Terre-Neuve (St. John's, T.-N.-L.)

Benoît Dupont, Professeur, École de criminologie, Chaire de recherche du Canada en cybersécurité, Chaire de recherche en prévention de la cybercriminalité, Université de Montréal; directeur scientifique, Réseau intégré sur la cybersécurité (Montréal, Qc)

Jaigris Hodson, Chaire de recherche de niveau 2 du Canada sur la communication numérique au service de l'intérêt public et professeure agrégée, Collège des études interdisciplinaires, Université Royal Roads (Victoria, C.-B.)

Digvir S. Jayas, O.C., MSRC, FACG, Président et vice-chancelier, Université de Lethbridge (Lethbridge, Alb.)

Catherine L. Mah, Professeur et titulaire de la Chaire de recherche du Canada sur la promotion des populations en santé, École d'administration de la santé, Faculté de la santé, Institut des populations en santé, Université Dalhousie (Halifax, N.-É.)

Louise Poissant, MSRC, Directrice scientifique du Fonds de recherche du Québec – Société et culture (Montréal, QC)

Nicole Redvers, Professeure agrégée, Chaire de recherche à Western, École de médecine et de médecine dentaire Schulich, Université Western ; V.-P., recherche, L'Association des facultés de médicine du Canada (London, Ont.)

Madison Rilling, Directrice Générale, Optonique (Québec, Qc)

David A. Wolfe, Professeur émérite et codirecteur, Innovation Policy Lab à la Munk School of Global Affairs and Public Policy, Université de Toronto (Toronto, ON)

*en juillet 2025

Des données probantes pour le bien public.

Le **Conseil des académies canadiennes (CAC)** est une voix de confiance à l'intersection de la recherche, des enjeux sociaux et des politiques publiques. Il rassemble l'expertise et évalue les connaissances afin de faire progresser la prise de décision fondée sur des données probantes au Canada comme à l'étranger.

Grâce à des évaluations multidisciplinaires menées par des experts s'appuyant sur des données probantes en provenance de différents secteurs et communautés, le CAC apporte clarté, rigueur et équilibre dans la compréhension de sujets de politiques complexes dans divers domaines comme la santé, l'environnement, la sécurité publique, l'innovation et l'économie.

Organisation de bienfaisance sans but lucratif, le CAC est guidé par les principes d'indépendance, d'excellence et d'intégrité dans tous ses travaux, offrant ainsi une valeur constante à ceux qui utilisent ses rapports pour éclairer les politiques et le débat public.

www.rapports-cac.ca

Council of Canadian Academies | Conseil des académies canadiennes