RAPPORT DE CONFÉRENCE

2025

CONFÉRENCE SUR LA SÉCURITÉ DE LA RECHERCHE

explorer de nouveaux territoires nationaux et mondiaux

Vancouver, les 3 et 4 juin

THE UNIVERSITY OF BRITISH COLUMBIA

CONTENU

Reconnaissance territoriale

La Conférence sur la sécurité de la recherche 2025 a eu lieu les 3 et 4 juin 2025 au campus Point Grey de l'Université de la Colombie-Britannique, qui est situé sur les territoires traditionnels, ancestraux et non cédés des xwməθkwəy̓əm (Musqueam). Les participants et participantes à la conférence ainsi que les oratrices et orateurs se sont joints de près et de loin; nous reconnaissons aussi les propriétaires traditionnels et les gardiens de ces terres.

PRÉFACE

Ce rapport a été produit pour résumer les principales discussions de la Conférence sur la sécurité de la recherche 2025. Pour protéger la confidentialité des personnes qui ont participé à la conférence, le comité organisateur a mis en place la règle de Chatham House par laquelle les déclarations des personnes peuvent être partagées et discutées, toutefois, leur identité doit demeurer anonyme. De plus, le comité organisateur de la conférence s'est abstenu d'utiliser des enregistrements électroniques ou la prise de notes soutenue par l'intelligence artificielle, en respect de la protection de la vie privée des personnes qui ont pris la parole et de la sécurité des renseignements partagés. Les résumés inclus ci-dessous ont été produits à partir de notes manuscrites prises par le comité organisateur de l'événement et sont donc assujettis à leur interprétation. Les renseignements présentés ne devraient pas être considérés comme des faits sans consulter davantage les experts et professionnels appropriés de la sécurité de la recherche et des domaines connexes.

SOMMAIRE EXÉCUTIF

L'Université de la Colombie-Britannique (UBC) a accueilli la *Conférence sur la sécurité de la recherche 2025 : explorer de nouvelles frontières nationales et mondiales* les 3 et 4 juin au campus Point Grey de UBC. Cette conférence avait pour but de créer de la capacité et de partager des informations au sein de la communauté canadienne qui ne cesse de croître de professionnels de soutien à la recherche axés sur la sécurité de la recherche.

Les participants et participantes en personne à la conférence provenaient de :

- 54 établissements postsecondaires canadiens, dont 34 qui étaient des universités non membres du groupe des U15, des collèges et des polytechniques;
- 12 ministères et organismes du gouvernement du Canada;
- 4 gouvernements provinciaux;
- 13 organisations de la société civile et établissements nationaux de recherche importants;
- 6 entités internationales de l'Australie, de l'Allemagne, du Japon, du Royaume-Uni et des États-Unis d'Amérique;
- 3 entreprises du secteur privé qui fournissent des services liés à la sécurité de la recherche.

Au cours de deux jours de discussions, de panels et de séances simultanées, la conférence a présenté une variété d'approches et d'éléments à prendre en considération lors de la conception et de la mise en œuvre de programmes et de politiques de sécurité de la recherche dans divers établissements. Les personnes présentes ont profité d'une abondance de connaissances en provenance de multiples secteurs, tout en partageant des idées et en dialoguant ouvertement sur la façon d'aborder des questions importantes en matière de sécurité de la recherche.

Des séances simultanées leur ont permis de choisir parmi les thèmes de sécurité de la recherche les mieux alignés avec leurs intérêts professionnels. Les panels et discussions ont abordé une variété de sujets, tels que les pratiques exemplaires en matière de diligence raisonnable en source ouverte, les risques des chaînes d'approvisionnement, la création de capacité et les approches internationales à la protection de la recherche. Les séances ont aussi présenté des orateurs et oratrices en provenance d'une gamme d'établissements et de régions.

De multiples séances ont abordé les effets en aval des défis de la sécurité de la recherche qui peuvent survenir dans les milieux de la recherche et universitaires. Ces conséquences touchent les politiques internes, l'opinion des chercheuses et chercheurs sur la collaboration, la capacité à attirer et retenir des étudiantes et étudiants étrangers, en particulier depuis l'introduction de la Politique sur la recherche en technologies sensibles et sur les affiliations préoccupantes (RTSAP) du gouvernement canadien et l'expansion des Lignes directrices sur la sécurité nationale pour les partenariats de recherche (LDSNPR) en mai 2024.

ÉLÉMENTS RETENUS ET RECOMMANDATIONS

1. L'ouverture en recherche est essentielle afin de maintenir la compétitivité du Canada en matière de recherche. Le Canada doit collaborer avec des partenaires internationaux afin de réussir et les personnes présentes ont réitéré que la recherche ouverte et la sécurité de la recherche vont de pair.

2. Les ressources et les lignes directrices liées aux politiques du Canada, telles que les listes d'Organisations de recherche nommées (ORN) et de Domaines de recherche en technologies sensibles (DRTS), orientent le développement mondial de cadres de sécurité de la recherche. Toutefois, avec une plus grande adoption mondiale des pratiques en matière de sécurité de la recherche et de leurs exigences administratives, les spécialistes de la recherche et les établissements peuvent rencontrer des difficultés pour respecter divers cadres qui se chevauchent tout en étant quelques fois disparates. Il serait donc souhaitable que les autorités harmonisent les exigences lorsque possible.

3. Le financement des programmes de sécurité de la recherche au Canada, par l'entremise du Fonds de soutien à la recherche (FSR), a été essentiel afin de créer de la capacité au sein de nombreux établissements. Toutefois, les plus petits établissements ont des ressources (financières) limitées et peinent à aborder pleinement les enjeux émergents ou pour créer de la capacité en matière de sécurité de la recherche. De plus, alors que les considérations de sécurité de la recherche et leurs exigences administratives se sont régulièrement accrues au cours des dernières années, le financement total dédié à la sécurité de la recherche dans le FSR (25 millions de dollars canadiens) n'a pas changé. En tenant compte du fait que la sécurité de la recherche et les exigences administratives qui y sont associées sont en croissance, les établissements de petite et moyenne envergure pourraient particulièrement profiter de ressources supplémentaires et de soutien des gouvernements pertinents.

4. La mise en œuvre de la politique sur la RTSAP et des LDSNPR a fourni aux universités et aux organismes de recherche du Canada un cadre utile pour mettre en œuvre des pratiques afin de protéger la recherche et d'atténuer les risques tout en réalisant leur recherche de premier plan. Les spécialistes en sécurité de la recherche, partout au pays, continuent d'échanger des informations et de développer leurs compétences par le biais de diverses activités, telles que des webinaires ou des ateliers destinés aux analystes, afin de contribuer à clarifier les politiques et les lignes directrices gouvernementales.

5. La communauté de la recherche canadienne, composée des administrateurs d'établissements et des spécialistes de la recherche du pays, a observé des effets inattendus découlant de la mise en œuvre de la Politique sur la RTSAP et des LDSNPR. Certains de ces effets semblent être liés à des malentendus liés aux cadres; par exemple, comme certaines personnes à la conférence ont dit :

    I. Certains chercheurs et chercheuses ont tenu pour acquis que tous les partenariats de recherche avec des ORN ne seraient pas admissibles au financement du gouvernement fédéral, peu importe la sensibilité de la recherche. De plus, certains d'entre eux pourraient éviter des partenariats dans certaines régions (p. ex., la République populaire de Chine) en tenant pour acquis que de telles collaborations sont interdites. Ceci malgré le fait que la Politique sur la RTSAP n'interdit pas de telles collaborations;

    II. Les spécialistes de la recherche, et particulièrement les chercheurs principaux, peuvent tenir pour acquis qu'ils feront l'objet d'une plus grande surveillance de la part des organismes de financement ou des entités

gouvernementales lors de l'embauche de titulaires de diplômes en provenance des ORN, peu importe si leur recherche fait progresser un domaine de recherche de technologie sensible ou si elle reçoit du financement du gouvernement fédéral. Certaines de ces inquiétudes sont probablement alimentées par des lignes directrices précises de certaines provinces. Les personnes en début de carrière de recherche ainsi que les étudiantes et étudiants internationaux peuvent être particulièrement affectés par ces hypothèses.

6. La communauté de pratique informelle, rassemblée sous le nom de « Équipe Canada » comme réseau de professionnels de soutien à la recherche, fournit un modèle pour renforcer les approches de sécurité de la recherche dans les établissements postsecondaires et d'autres établissements par l'entremise de la collaboration. Les communautés de pratique régionales et plus petites peuvent aussi fournir beaucoup de valeur.

RÉSUMÉ DE L'ALLOCUTION LIMINAIRE

L'allocution liminaire portait sur les collaborations avec des établissements de recherche en République populaire de Chine (RPC), dont plusieurs ont des profils de recherche qui prennent de l'envergure ou qui sont déjà reconnus mondialement comme chefs de file dans certains domaines. Selon des données de l'Organisation de coopération et de développement économiques (OCDE), la montée du secteur de la recherche en Chine correspond à une hausse de 164 % des dépenses de recherche-développement entre 2012 et 2023. En comparaison, les augmentations en dépenses de recherche-développement dans des pays comme les États-Unis (hausse de 68 pour cent), le Canada (hausse de 26 pour cent) et le Japon (hausse de 17 pour cent) n'ont pas correspondu aux fonds investis par la RPC, ce qui a eu pour effet de limiter la croissance du secteur.

Plusieurs établissements en RPC ont également fait l'objet de préoccupations liées à la sécurité de la recherche, étant donné l'adoption par le pays de politiques qui font la promotion de la fusion civile et militaire et des collaborations étroites entre certains établissements et l'Armée populaire de libération. Alors qu'il y avait plusieurs facteurs et acteurs à considérer lors de l'évaluation des risques liés à la sécurité de la recherche sur une échelle mondiale, des entités basées en RPC ont été la cause des plus grandes inquiétudes.

Plusieurs établissements en RPC ont accru le nombre de leurs publications, ce qui a mené à leur hausse dans les rangs internationaux en matière d'innovation et de développement scientifique. Une grande partie de cette activité a ciblé les technologies émergentes considérées comme sensibles par les gouvernements, tels que les États-Unis et le Canada. Ces tendances reflètent la direction du haut vers le bas du gouvernement de la RPC et les efforts conscients de l'État central pour accroître la gestion et les priorités de développement scientifique. Cela vise à pousser les établissements chinois vers l'avant-plan et à nationaliser des domaines importants de recherche et développement.

Le terme « recherche sensible » comprend maintenant une large gamme de domaines de recherche. Certaines technologies ciblées par des acteurs mal intentionnés pour le vol et l'appropriation illicite ne correspondent pas parfaitement aux définitions traditionnelles des technologies à « double usage ». Par exemple, certaines technologies sont sensibles, puisqu'elles sont essentielles au développement économique et à la compétitivité. En soi, il y a un besoin de développer un nouveau paradigme pour protéger ces types de technologies en tenant compte de leur importance.

Un accent a été mis sur le fait que les gouvernements et les établissements doivent réfléchir à une gamme d'outils pour améliorer la sécurité de la recherche. Un modèle qui a été adopté par plusieurs organismes de réglementation consiste à combiner des règlements, des exigences et des incitatifs pour inciter les personnes engagées dans la recherche à prendre des mesures préventives contre la divulgation non autorisée de recherches sensibles et de connaissances.

Pour être efficace, ce modèle exige une collaboration continue et un engagement dans l'ensemble des secteurs nationaux et internationaux. Cela peut se traduire par la diffusion d'analyses de risques et de meilleures pratiques tout en continuant de former et d'accompagner les spécialistes de la recherche dans la gestion des incertitudes.

RÉSUMÉS DES PANELS

La conférence a présenté sept panels sur deux jours, précédés par une brève présentation d'introduction afin de donner le ton pour les séances simultanées. Les résumés des discussions des panels sont présentés ci-dessous, mais ne constituent pas un rapport complet de tous les commentaires présentés lors de l'événement.

Panel no 1 : Perspective des organismes un an après l'adoption de la Politique sur la RTSAP

PRINCIPAUX ÉLÉMENTS À RETENIR

- Les chercheuses et chercheurs sont de plus en plus conscients des exigences administratives liées à la Politique sur la recherche en technologies sensibles et sur les affiliations préoccupantes (RTSAP) et aux Lignes directrices sur la sécurité nationale pour les partenariats de recherche (LDSNPR).
- L'année qui s'est écoulée depuis la mise en œuvre de la Politique sur la RTSAP et l'expansion des LDSNPR, les spécialistes et les gestionnaires de la recherche font preuve de moins d'évitement du risque et d'une conscience accrue des risques et des mesures correspondantes d'atténuation.
- Les organismes fédéraux de financement ont noté une diminution importante des demandes rejetées en raison de risques liés à la sécurité de la recherche non atténuables et une augmentation de la sensibilisation et de l'engagement des universités sur les sujets de sécurité de la recherche.

RÉSUMÉ

Ce panel comprenait des personnes qui représentaient la majorité des organismes fédéraux de financement de la recherche du Canada et des ministères qui travaillent directement sur des cadres de sécurité de la recherche. Les panélistes ont annoncé que les mises à jour attendues aux listes des ORN et des DRTS sont prévues pour l'automne 2025 et que les LDSNPR s'appliqueront dorénavant à des occasions de financement sélectionnées offertes par le Conseil de recherches en sciences humaines (CRSH). Il est à noter que les panélistes du gouvernement ont indiqué que les domaines de recherche liés aux sciences sociales peuvent être inclus dans de futures mises à jour de la liste des domaines de recherche en technologies sensibles.

Le panel a rapporté des améliorations importantes dans la qualité des plans d'atténuation des risques depuis le lancement des LDSNPR comme programme pilote en 2021. Une diminution dans le nombre de demandes soumises présentant les plus grands risques a été observée, avec seulement quatre ayant été rejetées pour raisons de sécurité nationale au cours de la dernière année (au moment de la conférence, un rapport public sur les résultats du programme était en préparation).

Au cours de la deuxième moitié de 2025, les LDSNPR devraient s'appliquer à un nombre croissant de subventions pour des partenariats et le CRSH a partagé sa définition de « partenaire du secteur privé » qui orientera sa mise en œuvre des LDSNPR. Les organismes de financement commenceront aussi à valider les formulaires d'attestation de la RTSAP en fonction des directives qu'ils auront publiées.

Les panélistes ont aussi noté que le financement de recherches liées aux infrastructures sur de plus longues périodes, comme celui de la Fondation canadienne pour l'innovation, exige une approche unique en matière de sécurité de la recherche. Par exemple, les équipes de projet pourraient rencontrer des défis dans l'identification

des affiliations potentielles avec des organismes de recherche nommés dans les cas où certaines personnes qui participent au projet n'ont pas de « rôles définis » dans le cadre de la demande de subvention. Ainsi, les équipes de projet pourraient devoir faire de la sensibilisation plus large sur la sécurité de la recherche au sein de l'équipe et adopter une posture plus holistique afin de soutenir l'atténuation efficace du risque.

La collaboration avec la communauté universitaire et les parties prenantes de Sécurité publique Canada et des ministères qui traitent de sécurité nationale joue un rôle essentiel dans l'écosystème de la sécurité de la recherche. Les menaces à la sécurité de la recherche ont évolué et ne ciblent pas principalement les établissements gouvernementaux et leurs représentants; les risques de sécurité incluent maintenant des menaces directes à des acteurs non étatiques qui peuvent inclure les spécialistes de la recherche et les établissements de recherche ainsi que les menaces émanant de ces acteurs. La mise en œuvre des dispositions incluses dans la loi C-70 du gouvernement du Canada, *Loi concernant la lutte contre l'ingérence étrangère*, permettra aux organismes nationaux de sécurité de partager des renseignements importants liés au risque avec des chercheuses et chercheurs et des établissements universitaires. Le gouvernement du Canada officialise actuellement un cadre de partage de renseignements fondé sur cette loi.

Panel no 2 : Perspective de spécialistes de la recherche dans des domaines de recherche en technologies sensibles

PRINCIPAUX ÉLÉMENTS À RETENIR

- Les chercheurs et chercheuses luttent avec certaines des conséquences des politiques et lignes directrices en matière de sécurité de la recherche, notamment en ce qui a trait à la mobilité étudiante, au recrutement international et aux collaborations internationales.
- Il est souhaité qu'il y ait une plus grande transparence dans les processus d'émission de visas d'immigration et de cotes de sécurité liés à la sécurité de la recherche.
- Les politiques de sécurité de la recherche peuvent avoir un impact disproportionné sur le corps professoral de recherche en début de carrière, car ce dernier dépend du recrutement prévisible et simple d'une population étudiante pour soutenir son travail.
- Les chercheurs et chercheuses optent souvent pour l'excès de prudence lors de la prise de décision concernant les collaborations, ce qui peut les mener à renoncer à des occasions de collaboration et de recrutement de talents qui ne seraient pas prohibés aux termes de la politique sur la RTSAP.

RÉSUMÉ

Trois spécialistes de la recherche affiliés à différents établissements ont exprimé leurs inquiétudes concernant les délais pour l'obtention des cotes de sécurité pour les étudiants et étudiantes qui travaillent sur des subventions financées par le fédéral et qui exigent de telles cotes. Selon leurs expériences, ces délais les empêchent de commencer leur travail jusqu'à ce que leur équipe de recherche complète ait sa cote et il semble y avoir un manque de transparence concernant les délais de traitement. Une incertitude semblable existe aussi concernant les délais dans le processus d'approbation de visas, ce qui peut décourager le recrutement de personnes étudiantes ou collaboratrices de certaines régions et de certains organismes de recherche.

Un résultat souhaité, mais malheureux de la publication de la liste des ORN du Canada est que plusieurs collaborations ont dû être cessées et que des réseaux œuvrant depuis des décennies ont dû être restructurés. Les effets sur les réseaux s'étendent au-delà des affiliations actives, car les chercheuses et chercheurs sont inquiets d'être perçus comme contrevenant à la politique sur la RTSAP, même lorsqu'ils adhèrent aux lignes directrices de publication conjointe. Il a été mentionné que d'accepter des experts et expertes en visite peut être particulièrement difficile à gérer, puisque ces personnes peuvent cacher des affiliations actives avec des ORN.

Le panel a discuté de la perception d'un « effet paralysant » sur l'embauche de divers membres d'équipe en raison des craintes d'être en contravention avec la politique sur la RTSAP. Afin d'éviter toute conséquence potentielle sur leur financement, plusieurs personnes aimeraient mieux cesser ou éviter d'embaucher des étudiantes et étudiants du troisième cycle en provenance d'une ORN, même si cela favorisait une plus grande équité, diversité et inclusion dans leur équipe. Dans le contexte de la concurrence mondiale pour obtenir des talents dans les domaines de la science, de la technologie, de l'ingénierie et des mathématiques, les spécialistes de la recherche reçoivent régulièrement plusieurs demandes d'inscription de jeunes talentueux de pays tels que la RPC et l'Iran, des pays avec des établissements sur la liste des ORN où les éventuels étudiants et étudiantes peuvent avoir des affiliations. Cette compétition, particulièrement en ce qui a trait aux disciplines d'ingénierie et d'informatique, crée une fenêtre d'opportunité limitée pour offrir des invitations d'inscription. Le temps additionnel nécessaire pour assurer la conformité avec les politiques de sécurité de la recherche, combiné avec de longs délais dans le traitement des dossiers d'immigration après la pandémie, rétrécit considérablement cette fenêtre d'opportunité. Afin d'empêcher que des personnes de très grand talent évitent des occasions au Canada, les processus de confirmation du respect des politiques pertinentes des établissements et des ministères gouvernementaux doivent devenir plus efficaces.

Les panélistes ont aussi souligné le besoin de renforcer davantage la compréhension de ce qu'est la sécurité de la recherche et de la culture qui l'entoure à tous les niveaux des établissements postsecondaires, notamment au sein des facultés. Renforcer la culture de la sécurité de la recherche aidera aussi la prochaine génération de spécialistes de la recherche à comprendre les conséquences possibles de leurs décisions concernant leurs parcours et le développement de leurs réseaux, en plus de les aider à faire des choix prudents qui soutiennent les objectifs de sécurité de la recherche plus tôt dans leurs carrières.

Panel no 3 : Explorer les exigences provinciales en matière de sécurité de la recherche

PRINCIPAUX ÉLÉMENTS À RETENIR

- Chaque province tient compte de préoccupations uniques lors du développement et de la mise en œuvre de politiques de sécurité de la recherche, notamment : le nombre d'établissements d'enseignement supérieur, les types d'éducation post-secondaire, les niveaux de population et les taux de soutien financier.
- Les organismes de recherche ne devraient pas s'attendre à une harmonisation complète des exigences provinciales en matière de sécurité de la recherche, entre les provinces ou avec le gouvernement fédéral, même si les provinces s'engagent dans des discussions avec leurs homologues fédéraux.

- Les provinces qui évaluent actuellement la mise en œuvre de cadres de sécurité de la recherche essaient de réduire le fardeau pour les collaborations interprovinciales lorsque possible.

RÉSUMÉ

Ontario :

Le gouvernement de l'Ontario a établi un précédent en matière de politique de sécurité de la recherche au Canada avec son analyse de 2019 de l'éventail de projets du Fonds pour la recherche en Ontario. Le panel a discuté de l'évolution des efforts provinciaux : initialement, les demandeurs ne recevaient aucune rétroaction à savoir pourquoi leurs demandes étaient rejetées, y compris sur les risques qui pourraient ou ne pourraient pas être atténués. Plus récemment, une explication plus complète des risques est fournie.

Le gouvernement de l'Ontario exige une divulgation complète de l'implication des personnes responsables de la recherche et de celles qui y collaborent auprès d'entités étrangères lors de l'évaluation de la sécurité de la recherche. En vertu de sa *Loi de 2025 sur le soutien aux enfants, aux élèves et aux étudiants*, il est le premier gouvernement provincial à faire des politiques universitaires de sécurité de la recherche une exigence légale. Des établissements risquent de perdre du financement en cas de non-respect de cette législation. De plus, dans des scénarios précis, les établissements partenaires dans d'autres provinces sont aussi affectés par les exigences du gouvernement de l'Ontario.

La province ne fournit pas actuellement de financement additionnel pour aider les établissements à se conformer aux nouvelles exigences, et plusieurs personnes ont noté qu'il y a peu de chances que ça change. Durant la séance de questions et de réponses qui a suivi la présentation, il a été souligné que, même si les gens ne contestent pas l'idée que l'Ontario ait son propre cadre de sécurité de la recherche qui dépasse le cadre national, le manque de soutien financier direct de la province pour la sécurité de la recherche peut exercer une pression supplémentaire sur les établissements et entraîner une baisse de leur capacité à respecter les exigences en matière de sécurité de la recherche, tant en Ontario qu'à l'étranger.

Québec :

Le Québec a de nombreux petits établissements qui font face à des contraintes sévères en matière de ressources; ce qui met en péril leur capacité à mettre en œuvre des programmes de sécurité de la recherche. Les discussions liées à la sécurité de la recherche ont débuté en 2023 entre le ministère provincial qui finance les établissements postsecondaires et le ministère qui finance la recherche. Le gouvernement du Québec vise à modéliser ses politiques provinciales sur les lignes directrices fédérales tout en reconnaissant les préoccupations provinciales uniques.

Manitoba :

L'Université du Manitoba joue un rôle unique dans son écosystème de recherche provincial, puisque la majorité de la population de la province réside à Winnipeg, là où l'université est située. L'Université du Manitoba a approché la sécurité de la recherche avec l'intention de créer une culture de sensibilisation, d'éducation et de soutien à la sécurité de la recherche.

Alberta :

Les universités de l'Alberta ont formé une communauté de pratique composée de 19 membres, dirigée par les universités de Calgary et de l'Alberta, pour aider les établissements de toutes tailles à explorer les politiques de sécurité de la recherche provinciale et fédérale. Les quatre plus grandes universités de recherche de l'Alberta continuent d'intervenir auprès de leur gouvernement provincial pour mieux comprendre son approche « pause avec la Chine » pour toutes les activités de recherche, qui a mis en attente au printemps de 2021 tous les nouveaux partenariats de recherche avec des entités liées au gouvernement chinois et examiné les relations existantes. Le gouvernement de l'Alberta a ajusté son approche à la politique « pause avec la Chine » en 2023 pour permettre certaines collaborations à faible risque.

Panel no 4 : Approches internationales envers la protection de la recherche

PRINCIPAUX ÉLÉMENTS À RETENIR

- La sécurité de la recherche, bien qu'une préoccupation relativement nouvelle pour plusieurs pays et qui n'a pas de définition commune, gagne énormément d'attention au niveau politique de la part des gouvernements autour du monde.
- À l'échelle mondiale, les gouvernements commencent à établir des cadres, des politiques et des procédures qui ciblent l'amélioration des capacités en matière de sécurité de la recherche tout en réalisant de la recherche collaborative et innovante.
- Plusieurs pays se sont inspirés de la politique du Canada sur la RTSAP et des listes qui y sont liées lors de la conception de leurs approches.

RÉSUMÉ

États-Unis d'Amérique :

La National Science Foundation (NSF) a commencé à utiliser des formulaires de déclaration harmonisés en février 2024 et a publié un cadre de révision du risque plus tard cette année-là afin d'aider les universités à faire preuve de diligence raisonnable en matière de sécurité de la recherche. Les établissements qui reçoivent plus de 50 millions de dollars US en financement fédéral de recherche doivent certifier à l'organisme de financement que l'établissement a établi et utilise un programme de sécurité de la recherche. Sensibiliser est important pour l'approche de la NSF par rapport à la sécurité de la recherche; les risques de la recherche ne seront jamais nuls.

La NSF souhaite trouver un équilibre entre le financement de la science ouverte et la réduction des risques de sécurité, dans la mesure du possible. À cette fin, elle a soutenu la création du programme Safeguarding the Entire Community of the U.S. Research Ecosystem (SECURE) (par l'entremise d'un investissement de 67 millions de dollars US sur cinq ans). Le programme SECURE a deux composantes : un Centre SECURE mené par l'Université de Washington et une équipe SECURE Analytics menée par l'Université Texas A&M. Le centre aidera à créer un « environnement virtuel partagé » afin que les spécialistes de la recherche, les responsables et les leaders puissent identifier conjointement les défis de sécurité de la recherche et

les aborder. L'équipe d'analytique, de son côté, développera les outils et les technologies pour le recueil d'information, la compilation de données, le remisage et l'analyse liés au domaine de la sécurité de la recherche et à divers types d'incidents de sécurité. Le groupe d'analytique fournira aussi de la formation et du soutien et aidera à développer les cadres d'évaluation des risques et les rapports sur les risques de sécurité de la recherche.

Japon :

Au Japon, les conversations portant sur les meilleures façons de protéger la recherche ont commencé en 2024 et étaient axées sur l'intégrité de la recherche. En 2025, en portant une attention accrue sur la sécurité de la recherche, le gouvernement a publié des lignes directrices de sécurité de la recherche plus détaillées, fondées sur les cadres de contrôle d'exportation du pays, et a établi l'Inter-University Cooperation Scheme (URSIC).

En juin 2025, URSIC compte parmi ses membres onze universités sur les 800 que compte le Japon, et incite activement d'autres établissements à soumettre leur candidature. URSIC fonctionne de façon similaire à la communauté de pratique informelle du Canada, connue sous le nom de « Team Canada », mais est organisée de façon plus centralisée et comprend des rôles précis pour ses membres, comme de soutenir les membres pour faire preuve de diligence raisonnable. URSIC aide aussi à sensibiliser en matière de sécurité de la recherche, à développer des ressources humaines, à soutenir les plus petits établissements et à communiquer avec le gouvernement du Japon et les partenaires internationaux.

Le ministère de l'Éducation du Japon (MEXT) et l'organisme de science et de technologie du Japon (JST) ont commencé à faire l'essai d'exigences en matière de sécurité de la recherche et à superviser des subventions précises, en plus de publier des ressources de formation en 2025. Ces ressources comprennent le développement et le partage d'études de cas instructives pour le personnel administratif et de recherche des universités.

Allemagne :

Le gouvernement fédéral d'Allemagne n'a pas encore publié de stratégie nationale ou de cadre pour la sécurité de la recherche, mais il participe à des discussions sur la sécurité de la recherche depuis environ cinq ans. La liberté universitaire est protégée comme un droit fondamental selon l'article 5 de la Constitution de l'Allemagne, ce qui encadre donc plusieurs conversations sur la sécurité de la recherche. Le gouvernement allemand a publié un exposé de position sur la sécurité de la recherche en mars 2024 et en mai 2025, le German Science and Humanities Council a aussi publié un rapport intitulé « *Science and security in times of global political upheaval* » (La science et la sécurité en période de bouleversements politiques mondiaux). De nombreux organismes de financement et établissements gouvernementaux ont commencé à élaborer ou à mettre en œuvre des lignes directrices et des conseils sur les partenariats internationaux de recherche. Il y a aussi un débat actif en Allemagne sur le rôle des établissements allemands dans la recherche militaire nationale; ce débat est lié à la sécurité de la recherche vu la nature de la recherche en défense.

Au début de 2024, l'association Helmoltz, qui représente 18 établissements de recherche à travers l'Allemagne, a réaligné ses politiques liées à la sécurité de la recherche. Helmholtz adopte une approche agnostique relativement aux pays en matière de financement de recherche et cible la diminution du risque plutôt que le découplage de collaborations avec des partenaires internationaux. À cette fin, les centres Helmoltz sont responsables de mettre en œuvre « des mesures de sécurité individuelles adéquates » au niveau local. Les centres sont encouragés à examiner de façon holistique les risques liés à la recherche et au partenariat plutôt que d'interdire à tous les établissements d'avoir certaines collaborations. Divers centres ont pris leurs propres approches; par exemple, Forschungszentrum Jülich (FZJ) a mis en place un service de soutien administratif intitulé « Due Diligence in Science » pour aider l'établissement à évaluer les opportunités et les risques associés aux collaborations proposées.

Australie :

La Commonwealth Scientific and Industrial Research Organisation (CSIRO) de l'Australie finance la recherche dans l'espace, l'IA, le calcul de haute performance et d'autres domaines pour résoudre des défis mondiaux par l'entremise de l'innovation, de la science et de la technologie. Elle a 51 sites de recherche, 87 pays partenaires et reçoit 40 pour cent de son financement des gouvernements fédéral et territoriaux de l'Australie.

La CSIRO aborde la sécurité de la recherche à l'aide de trois principes : 1) diligence raisonnable et gouvernance éclairées; 2) sensibilisation et collaboration; 3) révision et audit continus. La CSIRO vise à donner aux chercheurs et chercheuses les renseignements et les outils pour prendre des décisions axées sur la sécurité, par exemple, à l'aide de l'outil « Research Engagement Sensitivities Tool 2.0 » (Sensibilités de la participation à la recherche). L'organisation a aussi ludifié la formation en créant le jeu « Security Quest » (Quête de sécurité) pour sensibiliser et éduquer les chercheurs et chercheuses par rapport aux risques de la recherche. La CSIRO examine régulièrement l'efficacité de ces initiatives (entre autres) et les raffine.

La CSIRO a récemment lancé un programme de formation obligatoire sur les moyens de contrer l'interférence étrangère et prend une approche structurée similaire face à la formation plus large en matière de sécurité de la recherche. Ceci inclut des évaluations de diligence raisonnable, l'éducation sur des thèmes liés à la sécurité de la recherche, et des examens réguliers des projets et des audits des programmes de la CSIRO. L'objectif de la CSIRO est de créer un écosystème pour répondre à de potentielles menaces à la sécurité.

Panel no 5 : Études de cas et leçons apprises

PRINCIPAUX ÉLÉMENTS À RETENIR

- Dans des circonstances précises, les questions de sécurité de recherche peuvent s'étendre au-delà de la conformité administrative à des politiques fédérales. Les établissements universitaires peuvent faire face à des risques émanant de sources non liées au financement, comme des délégations en visite, des partenariats avec le secteur privé et des personnes qui pourraient agir au nom de gouvernements

étrangers.

- La diligence raisonnable entreprise par les équipes de sécurité de la recherche peut aider à atténuer de façon importante les risques dans ces contextes par l'identification de source ouverte d'enjeux potentiels et l'adoption des mesures requises pour aborder les défis.
- Dans certains cas, des politiques et processus institutionnels ont été changés en raison d'efforts pour améliorer les mesures d'atténuation des risques liés à la sécurité de la recherche.

RÉSUMÉ

Une étude de cas a impliqué une personne spécialisée en ingénierie d'une université aux États-Unis qui a été trouvée coupable de 36 chefs d'accusation de fausses divulgations pour des subventions après qu'une enquête ait révélé qu'elle faisait partie du Programme des mille talents[1] de la RPC. L'université en question a travaillé avec le FBI (Federal Bureau of Investigation) des États-Unis pour comprendre pourquoi cette information n'a pas été identifiée par l'université ou divulguée avant l'enquête. Ce cas a entraîné la mise à jour des politiques d'emploi de l'université et le développement de nouveaux mécanismes de licenciement de spécialistes en recherche pour prévenir les futures violations de politiques et les impacts réputationnels. De plus, l'université a augmenté la diligence raisonnable liée au recrutement de personnes en provenance de ce qui a été défini comme des « pays préoccupants ».

Une autre étude de cas impliquait une importante délégation en visite qui a demandé à visiter un laboratoire de recherche sensible au Canada à l'extérieur des heures d'ouverture normales. Le projet du laboratoire était très décentralisé et comprenait du travail avec des biomatériaux avancés. Les visiteurs étaient des représentants connus de diverses entreprises du secteur privé ayant certaines affiliations universitaires vaguement liées aux ORN et des relations étroites avec un gouvernement étranger.

Le groupe de sécurité de la recherche de l'université canadienne a fourni son évaluation des risques à son personnel de recherche qui a décidé de permettre à la délégation de faire la visite. L'équipe de sécurité de la recherche a mis en place des mesures d'atténuation strictes pour réduire le risque, comme ne permettre qu'à de petits groupes de la délégation à la fois de participer à des visites pleinement supervisées, et faire la gestion d'appareils électroniques pendant que les groupes étaient dans l'espace du laboratoire. L'université a depuis mis à jour ses politiques opérationnelles pour les délégations en visite.

Une autre université canadienne a parlé d'une étude de cas concernant une compagnie privée enregistrée dans la province de la Colombie-Britannique qui souhaitait visiter des laboratoires et des installations qui réalisent des recherches sur les matériaux avancés. La compagnie avait contacté l'équipe de partenariats de l'université pour organiser une visite. Elle avait aussi des opérations en RPC liées aux composants de semiconducteurs et de capteurs. En raison de la nature obscure de la compagnie, de leurs intentions de devenir partenaires dans un domaine de recherche sensible et d'autres divergences qui incluent des liens personnels avec une compagnie séparée de fournitures militaires, l'équipe des partenariats n'a pas poursuivi la collaboration.

---

[1] Le Programme des mille talents (PMT) est l'un des nombreux programmes de plans de talent de la Chine. En vertu du PMT, le gouvernement de la RPC cherche à recruter des ressortissants étrangers pour faire de la recherche dans des établissements chinois. Le gouvernement peut alors extraire et exploiter des résultats de recherche afin de faire progresser des intérêts nationaux. Pour d'autres renseignements, consultez la description du FBI des plans de talents chinois (en anglais), le rapport du comité du Sénat des É.-U. « Threats to the U.S. Research Enterprise: China's Talent Recruitment Plans » (Menaces à la recherche des États-Unis : les plans de recrutement chinois), ou la déclaration de Sécurité publique Canada sur le PMT.

Une dernière étude de cas canadienne impliquait un membre du personnel enseignant qui a reçu une demande d'un spécialiste qui a exprimé l'intérêt de visiter un établissement canadien pour assister à des cours afin d'améliorer ses capacités d'enseignement, mais dont la demande ultime était d'obtenir une invitation dans un laboratoire de recherche. L'analyse de diligence raisonnable a déterminé les risques par rapport à la recherche et au partenaire de recherche, incluant des publications de recherche, des brevets et des soumissions au Traité de coopération en matière de brevets pour des applications à double usage : civiles et militaires. Lorsque ces renseignements ont été présentés, le membre du personnel enseignant a déterminé que le risque l'emportait sur les avantages, et a décidé de ne pas inviter officiellement le spécialiste. L'université a depuis changé son processus pour inclure un examen de protection de la recherche avant de signer une lettre d'invitation pour les spécialistes en visite.

Panel no 6 : Adopter l'approche humaine : assurer l'accès, la diversité et la non-discrimination

PRINCIPAUX ÉLÉMENTS À RETENIR

- Il est essentiel d'être sensible au potentiel de pratiques discriminatoires qui peuvent résulter de la mise en œuvre de politiques de sécurité de la recherche.
- Un enjeu important pour les personnes présentes était le potentiel de discrimination en raison de la perception que certaines politiques s'appliquent à des pays entiers ou à leurs citoyens, et qu'une telle discrimination doit être évitée.
- Les panélistes ont proposé différentes stratégies pour minimiser les effets discriminatoires potentiels découlant de l'application des règles. Il a par exemple été suggéré de prendre le temps d'expliquer en détail les subtilités des règles, ainsi que d'investir dans la création de liens durables avec la communauté scientifique.

RÉSUMÉ

La politique sur la RTSAP a eu des conséquences inattendues par rapport à la création de réseaux et de collaborations pour les chercheuses et chercheurs. Il y a un équilibre à trouver, surtout pour les personnes débutant leur carrière universitaire, entre le développement de réseaux mondiaux avec des établissements et des spécialistes de renom et le risque de limiter leurs propres opportunités en raison d'une aversion excessive au risque. Pour plusieurs personnes qui examinent les politiques, le chemin de la moindre résistance est souvent la réponse par défaut. Elles pourraient même renoncer à des collaborations avec des pays précis ou dans certains domaines de recherche pour simplifier le respect des politiques de sécurité de la recherche. C'est surtout le cas si les équipes de recherche et les établissements émettent des suppositions sur les organismes qui peuvent être ajoutés à de prochaines versions de la liste des ORN du Canada.

Une personne a parlé des pratiques exemplaires sur ce sujet, soit d'incorporer une approche non discriminatoire et fondée sur les droits de la personne lors de la prestation de conseils en sécurité de la recherche aux équipes. D'autres pratiques exemplaires incluent de rencontrer les spécialistes en recherche en personne pour établir de meilleures relations, de prendre beaucoup de temps lors de l'introduction des politiques pour confirmer leur compréhension générale et leur logique (même si cela peut vouloir dire des

réunions plus longues et répétées), d'évaluer leurs propres biais à titre de praticiens de sécurité de la recherche et de discuter des décisions en fonction de l'équilibre entre compromis et avantages. Il est important de reconnaître les conséquences graves qui peuvent survenir lors de décisions hâtives faites pour accélérer des approbations de financement : éviter d'embaucher ou de collaborer avec tout le talent d'une certaine région peut encourager la discrimination et amener à renoncer à l'opportunité de travailler avec des personnes hautement qualifiées.

Panel no 7 : Les répercussions des politiques de sécurité de la recherche dans divers contextes

PRINCIPAUX ÉLÉMENTS À RETENIR

- Il n'y a aucune solution passe-partout pour les universités ou les établissements de recherche qui souhaitent établir un programme de sécurité de la recherche.
- Une option est de commencer par l'identification des cultures et des politiques existantes de leur établissement et de travailler à l'intérieur de celles-ci pour développer des approches à la sécurité de la recherche efficaces.
- Des politiques institutionnelles existantes qui peuvent être des mesures efficaces d'atténuation des risques incluent celles qui touchent les conflits d'intérêts, les conflits de loyauté et les examens internes des subventions et des approbations.

RÉSUMÉ

Les discussions portaient sur la création d'équipes de sécurité de la recherche dans de grands établissements, en mettant l'accent sur les avantages et les défis à surmonter pour implanter une telle pratique dans des organismes bien établis, dont le personnel de recherche n'a pas l'habitude d'intégrer des considérations liées à la sécurité nationale dans son travail et ses processus.

Un défi particulier soulevé dans l'ensemble du panel est les structures très décentralisées des universités. Cette structure peut poser des difficultés pour la sensibilisation face aux politiques et aux pratiques en matière de sécurité de la recherche. La sensibilisation générale, les introductions progressives et la création de relations personnelles ont recueilli les résultats les plus positifs pour les équipes de sécurité de la recherche lors de la collaboration et des contacts avec les nombreux départements et facultés dans leurs établissements respectifs.

Les environnements universitaires fournissent aussi une occasion unique de contribuer à des approches de sécurité de la recherche ayant plus d'impact, en tirant profit de prises de décision fondées sur des données probantes, et en répondant à des événements d'actualité urgents et à des enjeux géopolitiques préoccupants. Pourvoir les équipes de sécurité de la recherche en personnel provenant d'une grande variété de milieux et de compétences (p. ex., la recherche, le gouvernement, la gestion du changement, etc.) peut donner aux établissements une approche mieux équilibrée pour encourager efficacement la protection de la recherche en prenant en compte la liberté académique et la collaboration ouverte.

RÉSUMÉS DES SÉANCES SIMULTANÉS

Jour 1, séance no 1 : Universités de petite et moyenne taille

PRINCIPAUX ÉLÉMENTS À RETENIR

- Les plus petits établissements n'ont souvent pas les ressources pour créer des équipes ou des bureaux uniquement dédiés à la sécurité de la recherche. Ce contexte, combiné avec du financement fédéral dédié limité (ou, dans certains cas, nul) à la sécurité de la recherche, crée des défis uniques pour établir des programmes de sécurité de la recherche robustes.
- « Universités de taille petite à moyenne » est une catégorie large, et il est important de reconnaître qu'une approche mur-à-mur ne peut être appliquée à chaque établissement de cette catégorie.
- Les établissements devraient tirer profit de toutes les ressources disponibles pour des directives et du soutien, incluant des conseillers de Sécurité publique Canada (SPC) et des communautés de pratique provinciales ou nationales.

RÉSUMÉ

Plusieurs universités de petite et moyenne taille au Canada n'ont pas de gestionnaires responsables de la recherche et de l'innovation, et certains professionnels de la sécurité de la recherche dans ces établissements relèvent directement des doyens. Les professionnels assignés à des responsabilités liées à la sécurité de la recherche dans de plus petits établissements gèrent souvent de nombreux dossiers; ce qui a un impact négatif sur leur capacité de fournir du soutien uniforme et dédié à la sécurité de la recherche. Du soutien plus faible à la sécurité de la recherche par l'entremise du Fonds de soutien à la recherche (FSR) aggrave ces défis.

Il n'y a aucune définition claire d'un établissement « de taille petite à moyenne » dans un contexte de sécurité de la recherche, et plusieurs organismes qui pourraient être considérés comme faisant partie de cette catégorie ont des programmes de recherche robustes et en croissance. La diversité de ces établissements nécessite donc des approches uniques à la sécurité de la recherche qui sont créées sur mesure pour les besoins précis d'un établissement. Une analyse plus approfondie est nécessaire pour mieux comprendre où les défis et les opportunités existent au sein de ces environnements.

Les établissements plus petits peuvent aussi avoir certains avantages, tels qu'une plus grande capacité d'influencer le changement de culture des spécialistes de la recherche et des leaders. Le fait d'expliquer le raisonnement qui sous-tend les politiques de sécurité de la recherche a contribué à favoriser le respect de ces politiques, plutôt que de se concentrer uniquement sur l'obligation de remplir les formulaires requis.

Les conseils généraux pour les établissements de petite et moyenne taille afin d'accéder à des ressources de sécurité de la recherche comprennent :

- contacter le conseiller régional de sécurité de la recherche de Sécurité publique Canada, qui peut fournir du soutien et potentiellement alléger certaines contraintes en matière de ressources;
- tirer profit des communautés de pratique nationales : des établissements membres plus grands et avec plus de ressources peuvent fournir des conseils et des directives sur les enjeux complexes auxquels ils peuvent avoir fait face;

- s'impliquer auprès des communautés de pratique provinciales ou régionales; des groupes précis pour les régions Pacifique, Alberta, Québec et d'autres régions créent des forums supplémentaires afin de partager des pratiques exemplaires et obtenir des rétroactions régionales;
- tirer profit des ressources du gouvernement du Canada, incluant les ateliers sur la protection de la science, les cours de formation, etc.;
- explorer les prix de groupe pour les outils de diligence raisonnable en matière de sécurité de la recherche et mettre en commun des ressources limitées avec d'autres établissements de petite et moyenne taille pour y accéder;
- tirer profit d'Universités Canada, qui fait des revendications auprès du gouvernement fédéral au nom de toutes les universités, peu importe leur taille.

Jour 1, séance no 2 : U15 et les grandes universités

PRINCIPAUX ÉLÉMENTS À RETENIR

- La structure décentralisée des établissements d'enseignement supérieur pose des défis importants pour la sensibilisation et la mise en place des pratiques exemplaires et des protocoles de sécurité de la recherche.
- Les équipes de sécurité de la recherche et leurs établissements respectifs ont un besoin de ressources, de capacités et de soutiens supplémentaires.

RÉSUMÉ

La discussion était centrée sur trois thèmes ayant pour but de fournir un forum pour aborder les défis uniques aux grands établissements lors de la prestation de services de sécurité de la recherche.

Gains

Cette discussion a encouragé les personnes présentes à partager les réussites de leur établissement en matière de sécurité de la recherche et la façon dont elles ont été communiquées. Les personnes ont exprimé que d'incorporer la sécurité de la recherche dans des programmes de formation obligatoire pour le personnel et le corps professoral a réussi comme forme d'atténuation du risque et pour accroître la familiarité avec des concepts de sécurité de la recherche. Certains établissements ont cité l'adoption de cours de formation fédéraux comme étant un succès. Toutefois, certains établissements ont affirmé qu'ils ont eu de la difficulté à rendre la formation en matière de sécurité de la recherche obligatoire. Les mêmes personnes ont noté que plus de soutien de la part du leadership des établissements est nécessaire pour rendre la formation obligatoire.

Décentralisation

La deuxième discussion portait sur les impacts de la décentralisation sur la gestion des exigences de sécurité de la recherche; plusieurs personnes ont identifié la décentralisation comme l'un des plus importants défis auxquels leurs équipes de sécurité de la recherche font face. Certaines personnes étaient inquiètes par rapport

à la capacité de promouvoir l'impact de leurs programmes dans le cas d'un examen des efforts de sécurité de la recherche de leur établissement. Les équipes de sécurité de la recherche savent généralement comment partager et promouvoir les meilleures pratiques en matière de sécurité de la recherche. Cependant, il n'existe aucune procédure formelle (comme des évaluations de programmes) pour évaluer l'efficacité de ces efforts et mesurer les compétences des parties prenantes en matière de sécurité de la recherche. Une personne a parlé de la façon dont son équipe aborde la nature décentralisée de son établissement en assignant à chaque membre de l'équipe la responsabilité d'une faculté de recherche. Chaque membre de l'équipe peut alors créer des relations avec les facultés qui lui sont assignées pour intégrer des considérations et des conversations portant sur la sécurité de la recherche au sein des processus et des cycles de demandes de subvention et à l'extérieur de ceux-ci. Cette personne a aussi noté que l'équipe a une redondance intrinsèque, par l'entremise d'une boîte courriel partagée, afin de s'assurer qu'il y a toujours un point de contact accessible pour les spécialistes de la recherche et le personnel qui explore les questions de sécurité de la recherche.

Étendue des travaux

La troisième invite a suscité une discussion sur la façon dont, malgré le financement relativement important des grandes universités, les équipes de sécurité de la recherche sont limitées dans leur capacité. Cette discussion a aussi permis de soulever la question du champ d'application des équipes. Plusieurs personnes ont partagé leur besoin de ressources supplémentaires et la capacité de bien aborder tout ce qui leur est soumis. Une personne a souligné l'importance de dresser des limites afin d'éviter les dérives d'extension de leur champ d'application. Éviter les dérives d'extension de leur champ d'application est aussi essentiel pour s'assurer que les exigences relatives à des politiques précises soient respectées avec soin et selon les normes les plus élevées. Le potentiel d'utiliser de l'intelligence artificielle (IA) pour aider à automatiser les processus et accroître l'efficacité a été brièvement soulevé. Il est nécessaire de développer des méthodes de validation solides avant de pouvoir utiliser couramment des outils d'IA.

Jour 1, séance no 3 : Hôpitaux, établissements et OSBL de recherche

PRINCIPAUX ÉLÉMENTS À RETENIR

- Les hôpitaux, établissements et organismes sans but lucratif axés sur la recherche font face aux défis continus de promotion de la sécurité de la recherche auprès des spécialistes de la recherche et d'explication de l'importance de la sécurité de la recherche.
- Ils font aussi face aux défis du manque de ressources liés à la prestation de formation, à l'achat d'outils de diligence raisonnable et à l'embauche de personnel qualifié.
- Le souhait d'équilibrer les considérations de sécurité nationale (y compris la sécurité de la recherche) tout en établissant un cadre qui fonctionne sans freiner l'innovation a été exprimé.

RÉSUMÉ

La discussion a porté sur les approches adoptées par diverses organisations pour adapter les considérations de sécurité de la recherche à leur contexte, en tenant compte des différences entre celles-ci et les établissements d'enseignement. En effet, ces organisations portent peut-être moins d'attention au financement fédéral pour la recherche. Ainsi, les structures de soutien disponibles peuvent varier grandement. Certaines organisations ont des chercheurs et chercheuses qui ont des postes dans des universités et qui peuvent donc soumettre des demandes de subvention par l'entremise de leur établissement postsecondaire. De telles organisations s'en remettent donc aux universités pour mettre en œuvre des politiques liées à la sécurité de la recherche.

Les organisations qui ont des contextes spéciaux qui orientent leur positionnement face à la sécurité, comme les laboratoires qui travaillent avec les maladies infectieuses, portent une attention supplémentaire aux aspects de la sécurité physique et de la cybersécurité pour la sécurité de la recherche. L'objectif pour ces organisations est d'adopter une approche plus holistique face à la sécurité en général, ce qui prend aussi en compte des considérations liées spécifiquement à la recherche dans les partenariats et les collaborations.

Certaines organisations ont adopté des processus de sélection du personnel en créant des relations avec des équipes qui les appuient dans leur processus d'embauche de personnel de recherche. Créer des relations fortes avec ces autres équipes administratives aide à la sensibilisation par rapport aux exigences de sécurité de la recherche et à l'utilisation de pratiques de sélection appropriées.

Certaines organisations qui fonctionnent également à titre d'organismes de financement ont de petites équipes pour mettre en œuvre des plans de sécurité de la recherche afin de répondre aux exigences du gouvernement fédéral. Ces organisations ont développé de solides relations avec des paires, y compris avec des organismes de financement fédéraux pour partager les apprentissages et les approches dans la mise en place efficace des politiques gouvernementales. Certaines approches incluent l'adaptation des directives existantes des trois organismes pour créer des directives sur mesure pour leur organisation. Les organisations ont aussi discuté du défi de valider les évaluations des risques qu'elles reçoivent, puisqu'il y a un manque de directives du gouvernement sur la façon de valider l'information d'une perspective de la sécurité de la recherche.

Jour 1, séance no 4 : Pratiques exemplaires et perspectives comportementales du Royaume-Uni

PRINCIPAUX ÉLÉMENTS À RETENIR

- Le Royaume-Uni (R.-U.) aborde la sécurité de la recherche d'une perspective de confiance en recherche et innovation pour évaluer tous les partenariats et toutes les activités de collaboration.
- La Research Collaboration Advice Team (Équipe conseil en matière de collaboration de recherche — RCAT) du R.-U. soutient et conseille les établissements relativement aux risques de sécurité nationale et les aide à créer de la capacité.

RÉSUMÉ

Pour contextualiser la discussion, la séance a commencé avec un aperçu du système de recherche du R.-U. et des approches en sécurité de la recherche. Le secteur postsecondaire est considéré comme une composante essentielle de l'économie nationale du R.-U. et soutient environ 250 000 emplois. La capacité du R.-U. à collaborer à l'échelle internationale est le fondement de son succès à titre de chef de file mondiale en recherche-développement.

Ensuite, les divers ministères ainsi que les mesures législatives et non législatives qui abordent la sécurité de la recherche ont été discutés. Il a été souligné que ces mesures sont conçues pour être précises et proportionnelles afin de réduire le risque de conséquences inattendues, incluant un effet de frein sur des collaborations internationales légitimes et importantes. Ces mesures incluent les contrôles d'exportation, les campagnes de sensibilisation et les modifications aux subventions. De plus, les questions posées aux demandeurs ainsi que le cadre d'évaluation des risques ont été présentés.

La séance a ensuite examiné trois études de cas : une demande de présentation scientifique à l'étranger, incluant l'approche d'un pays étranger pour une consultation; une entreprise issue d'une université qui cherche à commercialiser sa percée technologique; et l'influence de la supervision institutionnelle sur les collaborations informelles, surtout lorsque les résultats sont publiés. Chaque étude de cas a été présentée avec quelques questions de réflexion pour les personnes présentes, suivie de discussion en petits groupes et de réflexion en plénière.

Troisièmement, la séance a permis de discuter de la manière de mettre en œuvre des changements comportementaux favorisant la sécurité de la recherche. Le temps et l'attention limités des chercheuses et chercheurs en raison de demandes concurrentielles, ainsi que le fait que la sécurité de la recherche exige une vigilance constante et peut avoir un impact négatif sur la mise en œuvre d'efforts pour soutenir les changements comportementaux. Pour soutenir la gestion du changement, le R.-U. recommande un cadre « EAST » pour easy (facile), attractive (attirant), social (social) et timely (opportun).

Jour 2, séance no 1 : Approches manuelles de renseignement d'origine sources ouvertes

PRINCIPAUX ÉLÉMENTS À RETENIR

- Le renseignement d'origine sources ouvertes est fondé sur les méthodes traditionnelles de recherche, utilisant le contexte et l'expérience de cas précédents pour orienter une approche sensible au risque.
- Avec des ressources limitées, les professionnels de la sécurité de la recherche doivent équilibrer leurs efforts avec les exigences des cas, en fonction de leur jugement initial du cas, à partir de leur expérience et de l'identification d'informations clés à évaluer.

RÉSUMÉ

Pour commencer l'atelier, les personnes présentes ont défini leurs enjeux communs dans la collecte du renseignement d'origine sources ouvertes (ROSO). Les personnes présentes se sont demandé où commencer leur recherche, et ont soulevé des questions sur la traçabilité des individus ou des établissements dans les

recherches, et sur les informations verrouillées par un accès payant; des barrières liées à la traduction de matériel documentaire dans des langues étrangères ont aussi été mises de l'avant.

Les discussions ont inclus des pratiques exemplaires potentielles pour le ROSO, telles que l'utilisation de services payants et la protection de l'identité de la personne lors de la réalisation de travaux de diligence raisonnable. Il a été reconnu que les données sur l'appareil et le navigateur communiquées aux sites Web peuvent fournir des renseignements importants sur l'utilisateur et le système de l'utilisateur et l'accent a été mis sur les pratiques pour prévenir le transfert de ces données.

La méthodologie du ROSO est basée sur des méthodes de recherche conventionnelles, en utilisant le contexte et l'expérience de cas précédents pour orienter une approche sensible au risque. Vu que plusieurs équipes de sécurité de la recherche travaillent avec des ressources limitées, il a été affirmé qu'il est nécessaire d'équilibrer l'effort et l'exhaustivité de l'évaluation selon les besoins du cas. L'accent a été mis sur les approches de recherche orientées par le contexte. Tout au long de la séance, plusieurs ressources ont été mentionnées, notamment Silo, Wayback Machine, l'Organized Crime and Corruption Reporting Project (OCCRP), Aleph, ainsi que le portail Internet OpenCorporates. Ces outils peuvent aider pendant la réalisation de recherches tout en protégeant l'identité de l'utilisateur et la propriété intellectuelle.

Jour 2, séance no 2 : Plateformes payantes : avantages, désavantages et considérations

PRINCIPAUX ÉLÉMENTS À RETENIR

- Les outils de sécurité de la recherche peuvent économiser du temps, mais les utiliser n'est pas absolument nécessaire pour recueillir ou analyser efficacement des renseignements d'origine source ouverte (ROSO) de bonne qualité.
- Il y a de la valeur à « démontrer votre travail » lors de discussions sur les risques avec des chercheurs et chercheuses. Des outils peuvent fournir un accès à des données ou des rapports qui peuvent être partagés pendant des conversations sur les risques.
- Les outils sont dispendieux et certains établissements peuvent plutôt opter pour embaucher et former des personnes à réaliser la diligence raisonnable de source ouverte, en fonction de leurs besoins.
- Les plateformes payantes ne fournissent pas « toute la vérité », vérifier les faits et faire des suivis sont souvent nécessaires. Bien que ces outils puissent être utiles pour fournir un point de départ pour les analyses, les professionnels de la sécurité de la recherche doivent également être en mesure de comprendre comment analyser et contextualiser les renseignements fournis par l'outil.

Les organismes subventionnaires et les ministères gouvernementaux peuvent utiliser des outils pour filtrer les demandes en fonction des enjeux. De ce fait, certaines personnes sont d'avis qu'elles doivent acquérir des outils pour mieux conceptualiser les inquiétudes identifiées par le gouvernement ou l'organisme subventionnaire.

RÉSUMÉ

L'objectif de cette séance était de discuter des considérations liées à l'acquisition et à l'utilisation d'outils de diligence raisonnable ou liés à la sécurité de recherche (p. ex., logiciels, plateformes de recherche, etc.) disponibles commercialement. Plusieurs des personnes qui ont participé à cette discussion représentaient des établissements de petite et moyenne taille et des organisations de parties tierces qui évaluent actuellement des plateformes payantes qui pourraient améliorer leur capacité en matière de sécurité de la recherche.

De plus, plusieurs établissements qui utilisent actuellement des plateformes payantes étaient présents. Ils ont partagé leur expérience, notamment leurs commentaires sur le service à la clientèle, la fiabilité des données, les enjeux liés à la protection des renseignements personnels ainsi que la valeur de ces plateformes. Les discussions ont fourni des aperçus utiles sur les plateformes payantes qui permettront aux abonnés potentiels de prendre des décisions éclairées dans le contexte de budgets et de ressources limités.

Les avantages et désavantages des plateformes payantes ont été discutés à partir de scénarios pour lesquels les outils peuvent être utiles. Il a été dit que des outils peuvent aider à réduire le temps consacré à des recherches complexes de sources ouvertes, notamment lorsque certaines recherches exigent la révision de plusieurs documents, sites Web ou ressources. De plus, certaines personnes ont noté que des outils peuvent aider à recueillir et à analyser des données en langues autres qu'en anglais, agissant donc comme « multiplicateur de force » pour les usagers qui ont un temps limité pour réaliser des analyses approfondies de certains sujets.

La facilité d'utilisation de certaines plateformes ainsi que la confiance dans les données sont des considérations importantes lors de la décision d'utiliser un outil. Les erreurs dans les données générées par certains outils ou la confusion causée par la façon dont les données sont présentées aux usagers ont été mises en lumière. Des inquiétudes concernant le temps additionnel nécessaire pour vérifier les résultats d'outils de sécurité de la recherche dans le contexte d'échéances courtes et des ressources limitées des équipes ont été soulignées. Une personne a souligné des inquiétudes sur l'utilisation croissante de grands modèles de langage pour collecter et structurer des données qui sont téléchargées sur des plateformes sans vérification ou révision humaine adéquate.

La vie privée était une considération supplémentaire pour certaines personnes. Plus précisément, certaines personnes étaient inquiètes que certains outils puissent conserver des données de recherche ou d'autres renseignements sur la plateforme. Selon l'endroit à partir duquel une personne utilise l'outil, la collecte de données sur l'usager peut créer des enjeux liés à la vie privée qui doivent être traités par le vendeur de l'outil.

Jour 2, séance no 3 : Étude de cas et atelier sur la sécurité publique

PRINCIPAUX ÉLÉMENTS À RETENIR :

- Les personnes participantes ont pris connaissance des « drapeaux rouges » à prendre en considération lors de l'évaluation des risques internes, ainsi que de la façon dont les politiques institutionnelles existantes peuvent renforcer la sécurité de la recherche, telles que les politiques portant sur la gestion de la propriété intellectuelle, le conflit de loyauté, les contrôles à l'exportation, etc.

RÉSUMÉ

Le contexte a été établi par l'entremise d'une discussion où les participants et participantes ont partagé les types d'évaluation du risque qui existent dans leurs organisations et le type de politiques qui traitent des relations acceptables entre des collègues. Les personnes présentes représentaient des universités de petite et moyenne taille, des organisations publiques et des organisations privées.

Le groupe a par la suite été guidé à travers une étude de cas hypothétique où des informations étaient progressivement dévoilées. Les risques à l'établissement devaient être évalués alors que les comportements d'un chercheur et d'un stagiaire postdoctoral devenaient de plus en plus erratiques et inappropriés. À la fin de l'exercice, plusieurs indicateurs d'alerte et conséquences potentielles des comportements des sujets avaient été identifiés; des discussions ont aussi eu lieu sur des mécanismes qui auraient pu prévenir la situation.

La séance a permis une discussion productive sur les approches de diverses organisations face à la sécurité de la recherche et l'atténuation des risques, en plus d'offrir une occasion d'appliquer des connaissances en matière de pratiques de sécurité de la recherche à une étude de cas.

Jour 2, séance no 4 : Considérations face aux chaînes d'approvisionnement et à l'approvisionnement

PRINCIPAUX ÉLÉMENTS À RETENIR

- La cybercriminalité est la principale menace aux chaînes d'approvisionnement et aux processus d'approvisionnement, surtout en ce qui a trait aux « services de cybercriminalité (CaaS) » ayant des motivations financières, et aux menaces de la RPC, de la Russie, d'Iran, d'Inde et de la République populaire démocratique de Corée.
- Pour atténuer les risques visant les chaînes d'approvisionnement, il est essentiel d'incorporer des considérations de sécurité à chaque étape du processus d'approvisionnement.

RÉSUMÉ

Cette séance a permis de discuter des auteurs des menaces et de leurs motivations, des menaces aux chaînes d'approvisionnement et de la façon de les évaluer, et de comment créer de la sécurité dans le processus d'approvisionnement.

Auteurs des menaces et leurs motivations

Les états adversaires du Canada utilisent des campagnes de désinformation ciblées pour perturber et diviser les opinions politiques de la population votante. Les principaux adversaires sont la RPC, la Russie et l'Iran, suivi par la République populaire démocratique de Corée et l'Inde. Les rançongiciels représentent la principale

menace de cybersécurité pour les infrastructures canadiennes. Il y a eu une augmentation des services de cybercriminalité (CaaS), où des personnes ou des firmes sont embauchées pour commettre des cybercrimes contre d'autres personnes ou organisations. Ce type de cybercrime motivé par les gains financiers est la cybermenace la plus susceptible d'affecter la population canadienne, les résidents et les organisations.

Menaces aux chaînes d'approvisionnement

Les menaces aux chaînes d'approvisionnement sont plus complexes que les compromissions directes à la sécurité de la recherche d'un établissement et sont susceptibles de demeurer un outil pour les auteurs de menaces et les cybercriminels avancés. Les menaces aux chaînes d'approvisionnement incluent l'exploitation indirecte de cibles par l'entremise de vulnérabilités dans les chaînes d'approvisionnement et l'infrastructure internet. Cette sorte de menace devient de plus en plus commune alors que les logiciels et l'infrastructure infonuagique deviennent omniprésents. Il y a trois types de compromission des chaînes d'approvisionnement : le logiciel, le matériel et l'utilisation de réseaux de tierces parties pour obtenir l'accès. Pour gérer les menaces aux chaînes d'approvisionnement, les établissements de recherche doivent définir, évaluer, atténuer et surveiller leurs enjeux en matière de risque.

Créer de la sécurité dans le processus d'approvisionnement

Certains principes essentiels vers lesquels tendre sont les suivants : mettre en œuvre la sécurité à toutes les étapes du processus d'approvisionnement; faire confiance aux attestations, mais s'efforcer de les vérifier; établir une évaluation rigoureuse des risques et des procédures d'atténuation; et instaurer une bonne gouvernance, notamment un engagement précoce et un suivi continu.

CONCLUSION ET REGARD VERS L'AVENIR

La *Conférence sur la sécurité de la recherche 2025* s'est tenue à un point de jonction important pour la communauté de sécurité de la recherche. En tenant compte de la vitesse à laquelle la communauté canadienne de professionnels dédiés à la sécurité de la recherche a crû, c'était la première occasion pour plusieurs collègues de se rencontrer en personne. Les façons de soutenir au mieux les chercheurs et chercheuses pour faire la promotion de la sécurité et l'ouverture dans leur travail au sein d'une gamme de cadres de sécurité de la recherche régionaux, nationaux et internationaux ont été discutées.

L'événement a établi que la sécurité de la recherche au Canada a beaucoup évolué dans une période très courte et que les investissements fédéraux dans les établissements canadiens pour soutenir leurs efforts de sécurité de la recherche ont donné des résultats importants.

Les communautés de pratique, comme le réseau de sécurité de la recherche Team Canada, ont été identifiées à plusieurs reprises comme des mécanismes importants pour créer une résilience partagée et des compétences. Alors que des homologues internationaux continuent de développer leurs cadres pour la sécurité de la recherche, il sera important de chercher des occasions d'aligner ces nouveaux paradigmes lorsque possible.

À la fin de l'événement, il était clair qu'en plus de protéger adéquatement la recherche, les parties prenantes doivent aussi appuyer et investir dans la recherche qu'elles essaient de protéger. Les conséquences de la surcompensation et le potentiel de perte de talents ou de limiter le risque de partenariats ne doivent pas être sous-estimés. Les professionnels de la sécurité de la recherche doivent être conscients des impacts humains de l'application excessivement stricte ou erronée des cadres de sécurité de la recherche. Il sera crucial que les entités gouvernementales qui développent et appliquent des exigences continuent de communiquer ouvertement et de dialoguer avec les personnes qui effectuent et facilitent la recherche. Facilité par du soutien gouvernemental essentiel, l'engagement continu auprès des établissements d'éducation supérieure est essentiel pour créer un écosystème de recherche canadien ouvert.

Regard vers l'avenir : Conférence sur la sécurité de la recherche 2026

La conférence sur la sécurité de la recherche 2026 sera organisée conjointement par l'Université du Manitoba et l'Université Toronto Metropolitan, à Winnipeg (Manitoba). La conférence est provisoirement prévue pour le milieu de 2026.

L'équipe de l'Université de la Colombie-Britannique est heureuse d'avoir accueilli la Conférence sur la sécurité de la recherche en 2025 et tient à remercier celles et ceux qui ont rendu cette conférence possible à Vancouver.

Nous avons hâte à la conférence de l'an prochain et continuons de collaborer afin d'appuyer un écosystème canadien de la recherche qui demeure aussi ouvert que possible et aussi sécuritaire que nécessaire.

L'Université de la Colombie-Britannique reconnaît le rôle du Fonds de soutien à la recherche du gouvernement du Canada dans l'amélioration et la promotion de la sécurité de la recherche ainsi que relativement au développement et au soutien offert pour la création d'un environnement afin de soutenir la recherche et l'excellence universitaire.