Public Safety Canada | Sécurité publique Canada

Canada

Février 2022

Le point sur la sécurité de la recherche

EN BREF

Développements notables en matière de sécurité de la recherche

Septembre 2021 : Le groupe de travail sur la sécurité économique de Sécurité publique Canada a terminé des consultations sur les menaces économiques à la sécurité nationale qui incluent la sécurité de la recherche comme sujet clé. Les résultats de ces consultations sont en cours d'être analysés et alimenteront l'élaboration possible d'options politiques pour la sécurité de la recherche dans le contexte de la sécurité économique.

12 juillet 2021 : Le Ministre de la Sécurité publique et de la Protection civile; le ministre de l'Innovation, des Sciences et de l'Industrie; et le ministre de la Santé a publié les Lignes directrices sur la sécurité nationale pour les partenariats de recherche. Ces lignes directrices incluent des considérations de sécurité nationale dans l'évaluation et le financement des partenariats de recherche et aideront les chercheurs, les organismes de recherche et le gouvernement fédéral à appliquer des évaluations de diligence raisonnable améliorées et fondées sur les risques des demandes de recherche.

Juin 2021 : Le gouvernement du Canada a collaboré avec ses homologues du Groupe des Sept (G7) pour avancer les priorités du Canada en matière de sécurité de la recherche à l'échelle internationale. L'inclusion de la sécurité de la recherche dans le Communiqué des dirigeants du G7 et dans le Pacte pour la recherche du G7 renforce la protection de la recherche en tant que priorité partagée par les plus proches alliés et partenaires du Canada. Innovation, Sciences et Développement économique Canada va continuer d'avancer ces conversations dans son rôle de coprésident du Groupe de travail du G7 sur la sécurité et l'intégrité de l'écosystème de recherche mondial.

Mai 2021 : Le 20 mai 2021, le gouvernement de l'Alberta a demandé aux quatre universités de la province de suspendre tout nouveau partenariat avec des liens avec le gouvernement chinois, de revoir ses relations existantes et de soumettre un rapport au gouvernement. Quelques jours plus tard, l'Alberta a noté que des règles de sécurité nationale pour les universitaires étaient nécessaires pour empêcher le transfert de propriété intellectuelle vers la Chine. Cet article donne un aperçu des mesures prises par le gouvernement fédéral pour résoudre ce problème et souligne les efforts mis en œuvre par nos partenaires, y compris le traqueur des universités chinoises de défense.

Mai 2021 : Le traqueur des universités chinoises de défense a été mis à jour. Le traqueur est une base de données des institutions chinoises engagées dans la recherche scientifique et technologique militaire ou liée à la sécurité créée par le Centre international de cyberpolitique de l'ASPI (Australian Strategic Policy Institute).

Avril 2021 : Au cours de la conférence ministérielle virtuelle des cinq pays, les ministres du Canada, des États-Unis, de l'Australie, du Royaume-Uni et de la Nouvelle-Zélande ont accepté de coopérer sur les inquiétudes de la sécurité de la recherche. Le communiqué indique que les pays du Groupe des cinq sont « engagés à travailler ensemble, avec des pays aux vues similaires à travers des forums multilatéraux, pour partager leurs expériences et rendre compte de nos progrès pour renforcer la résilience collective dans les secteurs universitaire, de la recherche et du développement contre l'ingérence étrangère et le transfert indésirable de la connaissance. »

Étude de cas vedette

Les institutions canadiennes sont à la fine pointe de l'innovation, de la recherche et du développement dans plusieurs domaines. Le scénario suivant est un exemple concret qui démontre pourquoi il est nécessaire de faire preuve de vigilence et de prendre des mesures pour atténuer les menaces provenant d'acteurs hostiles.

Une université canadienne était l'hôte d'une conférence scientifique internationale sur un domaine ayant un double usage. Pendant l'une des pauses entre les présentations, une personne non identifiée s'est rendue sur la tribune et a inséré une clé USB dans l'ordinateur portable servant aux présentations. Les organisateurs et les participants ont vu un déplacement de fichiers sur l'écran, mais n'y ont pas prêté attention, car il pouvait s'agir du prochain conférencier qui téléchargeait la dernière version de sa présentation.

Cette personne n'a participé à aucune des séances et a ensuite été surprise en train de photographier les communications affichées, ce qui enfreignait le règlement de la conférence. Les organisateurs ont abordé la personne, qui a affirmé qu'elle n'avait rien fait de mal, est devenue agressive en essayant d'éluder les questions et a tenté de quitter les lieux.

Il s'agissait d'un universitaire étranger qui visitait l'université canadienne afin de profiter d'une possibilité de perfectionnement à court terme, mais dans un domaine sans lien avec celui de la conférence. Une enquête plus approfondie a révélé qu'il avait en fait copié illicitement un certain nombre de présentations de la conférence sur sa clé USB lorsqu'il se trouvait sur le podium. Il a également été déterminé que l'universitaire étranger n'avait même pas été invité à participer à la conférence, qu'il ne s'était pas inscrit et qu'il n'avait pas payé les frais d'inscription. Heureusement, cette violation flagrante de l'étiquette universitaire et ce vol potentiel de propriété intellectuelle ont été signalés aux responsables de la conférence. On ignore ce que l'universitaire étranger avait l'intention de faire des renseignements volés, mais les intérêts du Canada en matière de sécurité auraient pu être compromis s'il avait réussi son vol.

Que feriez-vous dans cette situation?

Voici ce qu'il est important de faire :

- être attentif aux possibilités de double usage de vos recherches, et mettre en place des mesures efficaces pour protéger vos recherches;
- comprendre que les auteurs de menace n'ont pas les mêmes valeurs ni la même éthique ni ne suivent les mêmes politiques de recherche que vous;
- si possible de le faire en toute sécurité, interpeller les personnes qui se trouvent où elles ne devraient pas être, poser des questions pour vérifier ce qu'elles font là (p. ex., « Puis-je vous aider à trouver quelque chose? »; « Êtes-vous ici avec quelqu'un? »);
- mettre en place des contrôles et des protocoles pour établir la crédibilité des personnes susceptibles de visiter votre établissement et vos laboratoires ou de participer à des événements, comme des conférences, que vous organisez;
- signaler tout comportement suspect ou criminel à la police locale;
- en cas de questions sans réponse, signaler toute préoccupation aux autorités compétentes (la Gendarmerie royale du Canada; le Service canadien du renseignement de sécurité – voir les coordonnées ci-après).

Aperçu de la sécurité matérielle

Il est non seulement important de s'assurer que son institution a une bonne cybersécurité, mais aussi de porter attention aux mesures de sécurité matérielle. Le gouvernement du Canada définit la sécurité matérielle comme la mise en œuvre de mesures de protection matérielle pour empêcher et retarder un accès non autorisé aux biens, à l'information, aux personnes et aux services, détecter un accès non autorisé ou une tentative en ce sens et déclencher une intervention appropriée. Les mesures de sécurité matérielle peuvent servir à assurer la sécurité générale des édifices et celle des laboratoires et des bureaux.

Éléments de mesures de sécurité efficaces pour un laboratoire de recherche

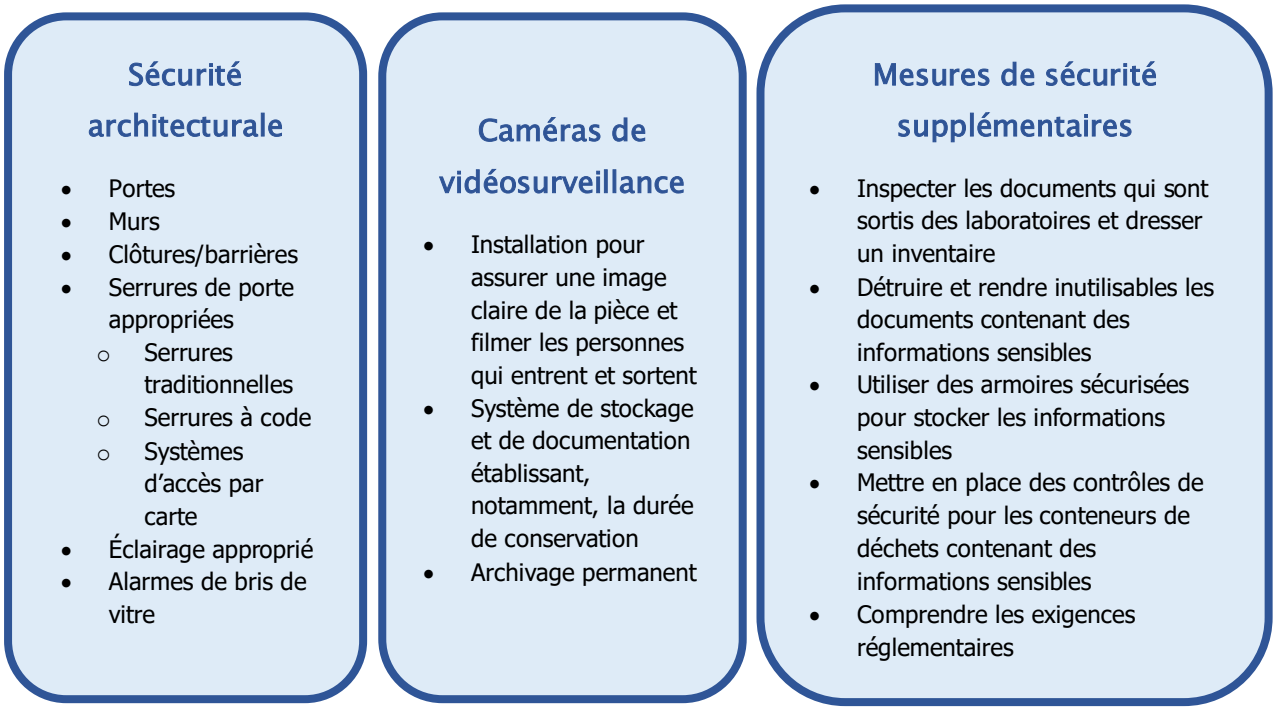

Figure 1 : Éléments de mesures de sécurité efficaces pour un laboratoire de recherche

Cette figure illustre les éléments de mesures de sécurité efficaces pour un laboratoire de recherche. Ces éléments peuvent servir de liste de contrôle pour s'assurer que vos informations sont protégées contre les acteurs de la menace. Le premier élément porte sur la sécurité architecturale, le deuxième sur les caméras de vidéosurveillance et le troisième sur les mesures de sécurité supplémentaires qui peuvent être mises en œuvre, comme le déchiquetage des documents contenant des éléments sensibles, l'inspection et l'inventaire des documents, la mise en place de contrôles de sécurité pour les conteneurs à déchets et la sécurisation des armoires.

Ressources pour évaluer la sécurité matérielle

Le Programme d'évaluation de la résilience régionale (PERR) est un programme d'évaluation de la vulnérabilité et des dépendances destiné aux propriétaires et aux exploitants d'infrastructures essentielles au Canada. Ce programme prévoit, entre autres, des évaluations de sites visant à aider les organisations à mesurer et à accroître leur résilience à tous les risques au Canada, comme les menaces cybernétiques, les événements accidentels ou intentionnels d'origine humaine et les catastrophes naturelles. Ces évaluations de sites sont volontaires, non réglementaires, gratuites et confidentielles. Le volet sécurité matérielle du PERR comporte deux outils :

- Outil d'évaluation de la résilience des infrastructures essentielles (OERIE) (durée : une journée)
    - L'OERIE est un outil d'évaluation sur le terrain qui mesure la résilience et le niveau de protection d'une installation. Les résultats comprennent un rapport et des tableaux de bord interactifs qui présentent des notes et des comparaisons avec des installations de pairs, et mettent en évidence les dépendances et les options d'amélioration ayant trait à la résilience, à la sécurité matérielle et à la cybersécurité.

- Outil multimédia pour les infrastructures essentielles (OMIE) (durée : une demi-journée à une journée)
    - L'OMIE est une représentation virtuelle d'une installation selon les plans d'étage. Il présente des photos panoramiques de l'intérieur et de l'extérieur des parties importantes de l'installation. L'outil peut être communiqué aux premiers intervenants ou utilisé dans le cadre d'exercices. Bien que l'utilisation de l'OMIE demeure à la discrétion de l'organisation, nous encourageons fortement la communication de l'outil aux premiers

- intervenants de manière à ce qu'il soit utilisé pour les mesures de préparation aux urgences et d'intervention, le cas échéant.

Les propriétaires et exploitants d'infrastructures essentielles peuvent écrire à ps.rrap-perr.sp@ps-sp.gc.ca pour soulever la possibilité de faire évaluer leurs installations. Des membres sont prêts à donner une présentation interactive pour expliquer plus en profondeur le programme et les produits fournis.

Vous voulez en savoir plus?

Avez-vous des questions ou avez-vous besoin d'aide? Vous voulez rester au courant et en savoir plus sur tous les aspects de la sécurité de la recherche? Veuillez nous envoyer un courriel à safeguardingscience-scienceensecurite@ps-sp.gc.ca ou visitez notre page Web Science en sécurité.

Sécurité publique Canada vise à publier continuellement de l'information utile à la communauté de recherche canadienne sur des questions pertinentes reliées à la sécurité de la recherche. N'hésitez pas à nous faire part de vos commentaires. Y a-t-il des produits, des outils ou des renseignements particuliers que vous aimeriez recevoir (par exemple, sur les risques et les menaces émergents, les études de cas de recherche sur la sécurité, les statistiques, les conseils sur les principaux enjeux, les pratiques exemplaires en matière de sécurité, etc.)? Veuillez nous faire part de vos suggestions par l'entremise du courriel de Science en sécurité ci-dessus.

Comment signaler un incident

GRC – Réseau info-sécurité nationale (RISN)
Pour signaler la présence d'inconnus ou des incidents ou activités informatiques suspects.

N° de téléphone : 1-800-420-5805	Courriel : NSIN_RISN@rcmp-grc.gc.ca

Service canadien du renseignement de sécurité (SCRS)
Pour signaler des menaces à la sécurité nationale ou des activités suspectes potentielles non urgentes.

N° de téléphone : 1-800-267-7685	Site Web : https://www.canada.ca/fr/service-renseignement-securite/organisation/signaler-des-informations-relatives-a-la-securite-nationale.html

Centre canadien pour la cybersécurité (CCC)
Le Centre de contact du CCC est le guichet unique pour les questions sur la cybersécurité.

N° de téléphone : 1-833-CYBER-88	Courriel : contact@cyber.gc.ca

Veuillez noter qu'il n'y a pas de calendrier de publication prévu pour Le point sur la sécurité de la recherche. Sécurité publique Canada fournira de l'information à notre public à mesure qu'elle se présente ou devient disponible.

ISSN: 2564-1476
Cat. No.: PS7-2F-PDF