

Éviter les dangers cachés: Besoin d'un modèle structuré de sécurité EN recherche à l'UQO

Didier Kabeya, Directeur Général et Fondateur, Rebintel

Agenda

- Mise en contexte
- Sécurité EN recherche & Régime Juridique
- Identification de risques & Responsabilités
- Cas d'études
- Mesures standards d'atténuation de risques
- Ressources



Mise en contexte

L'innovation est une source essentielle de puissance nationale. La capacité d'un pays à développer de nouveaux produits et de nouvelles méthodes de production lui permet de créer les biens désirés par d'autres. **L'innovation** crée de la richesse, **conduit au progrès technologique** et favorise le développement de produits dérivés.

L'un des moyens de mesurer l'innovation est la protection de la propriété intellectuelle (PI) sous la forme de brevets qui garantissent les droits exclusifs sur une invention.

La sécurité EN recherche est l'un des outils qui sert à protéger l'innovation et la commercialization de ses produits!

Chronologie de développement des mesures pour la sécurité En recherche au Canada





**Comment définir la
sécurité EN recherche?**



L'Approche Canadienne

La sécurité En recherche fait référence à la capacité d'identifier les risques pour vos recherches en cas d'accès indésirable, d'interférence ou de vols ainsi que les mesures qui minimisent ces risques et protègent les intrants, les processus et les produits qui font partie de la recherche et de la découverte scientifique.

Pourquoi la sécurité En recherche est-elle importante?

Expérience Hydro-Québec

- ❑ **YUESHENG** Wang, un employé d'Hydro-Québec, a été **arrêté**, par la GRC, **pour espionnage industriel** au profit de la Chine, en novembre 2022.
- ❑ Il aurait obtenu des secrets industriels pour le compte de la Chine, **agissant au détriment des intérêts économiques du Canada**.
- ❑ Il effectuait **des travaux de recherche liés aux matériaux de batterie**.
- ❑ Il a été **détecté** par des mécanismes internes de contrôle et **ses accès lui ont été retirés**.
- ❑ Depuis, il a fait l'objet des deux nouveaux chefs d'accusation d'actes préparatoires à des **activités d'espionnages économique** pour le compte de la Chine.

LA PRESSE

La Presse, samedi 23 novembre 2024

Montréal 6°C

ACTUALITÉS INTERNATIONAL DIALOGUE CONTEXTE AFFAIRES SPORTS AUTO ARTS CINÉMA SOCIÉTÉ GOURMETS

Chroniques Éditoriaux Caricatures Analyses National Politique Grand Montréal Régional Justice et faits divers Sa

JUSTICE ET FAITS DIVERS

Espionnage au profit de la Chine

Nouvelles accusations contre l'ex-employé d'Hydro-Québec



PHOTO TIRÉE DU PROFIL LINKEDIN DE YUESHENG WANG
Yuesheng Wang, accusé d'espionnage

De nouvelles accusations criminelles ont été portées mercredi contre l'ancien employé d'Hydro-Québec Yuesheng Wang, arrêté pour espionnage en novembre 2022. La poursuite de l'analyse du dossier a permis d'ajouter deux chefs d'accusation d'actes préparatoires à des activités d'espionnage économique pour le compte de la République populaire de Chine.

Publié le 7 février

↑ ↻

Expérience du Laboratoire National microbiologie de Winnipeg

- ❑ **XIANGGUO** Qiu et son mari **KEDING** Cheng travaillaient au seul laboratoire de virologie de niveau 4 du Canada (Winnipeg), avant leur congédiement en 2021.
- ❑ **Tous deux citoyens canadiens, ils étaient très enthousiastes quand aux collaborations scientifiques internationales.**
- ❑ **Les enquêtes** de l'Agence de la santé publique et du Service canadien du renseignement de sécurité (SCRS) **ont révélé plusieurs manquements aux règles** (y compris de sécurité En recherche?) de leur part:
 - KEDING aurait laissé un étudiant chinois circuler sans surveillance dans le laboratoire et aurait laissé un autre accéder au réseau informatique en utilisant son identifiant. Il aurait permis l'utilisation d'un compte Gmail et d'une clé USB pour faire sortir des données du laboratoire.
 - Le nom de Qiu serait apparu en Chine sur un brevet dans le même champ de recherche que ses travaux au Canada. Elle aussi aurait laissé deux chercheurs chinois liés à des institutions gouvernementales chinoises accéder au laboratoire de Winnipeg.
- ❑ **L'enquête du SCRS** a permis ensuite de **révéler des recherches conjointes** menées par le couple et des chercheurs liés à **l'Académie militaire des sciences médicales de Chine** qui relève de l'APC.

LA PRESSE La Presse, samedi 23 novembre 2024 Montréal 7°C Suivez-nous in @ f s x

ACTUALITÉS INTERNATIONAL DIALOGUE CONTEXTE AFFAIRES SPORTS AUTO ARTS CINÉMA SOCIÉTÉ GOURMAN

Chroniques Éditoriaux Caricatures Analyses National Politique Grand Montréal Régional Justice et faits divers San

ACTUALITÉS

Enquête sur un couple de chercheurs

Espionnage et Ebola au labo



IMAGE TIRÉE D'UNE VIDÉO DIFFUSÉE PAR RIDEAU HALL
Xiangguo Qiu et son mari Keding Cheng

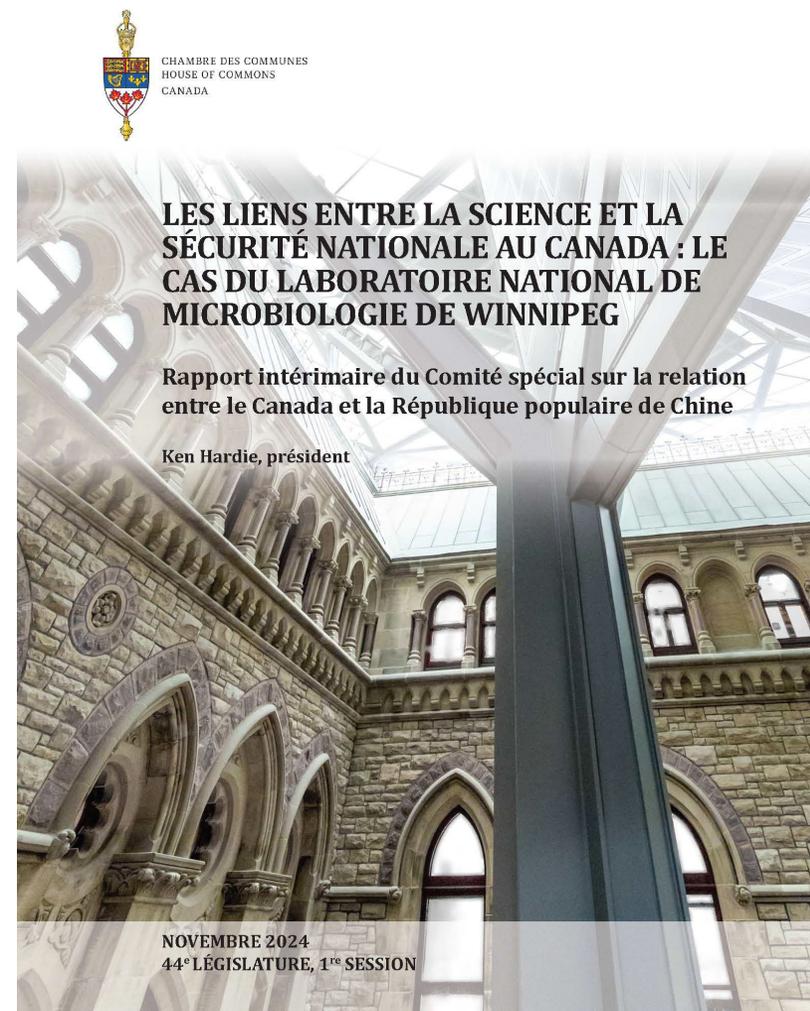
Après s'être fait tirer l'oreille pendant des années, le gouvernement Trudeau a rendu publics cette semaine des documents sur le congédiement d'un couple de scientifiques du Laboratoire national de microbiologie de Winnipeg en 2021. Les chercheurs, qui travaillaient avec les pathogènes les plus dangereux de la planète, entretenaient des liens avec l'armée chinoise. La femme a même livré des secrets à la Chine. Voici cinq faits saillants de l'enquête des services de renseignement canadiens à leur sujet.

Lecture de l'Expérience du laboratoire de Winnipeg par la chambre des communes |

Novembre 2024

Rapport intérimaire du comité spécial sur la relation Canada-Chine au gouvernement canadien | 12 recommandations.

- ❑ **La recommandation 3** suggère au gouvernement d'établir une liste de pays dignes de confiance pour l'échange de la recherche et de la propriété intellectuelle.
- ❑ **La recommandation 5** suggère au gouvernement de coopérer avec les provinces et le SCRS pour sensibiliser le milieu scientifique aux risques d'ingérence reliés à la coopération internationale.
- ❑ **La recommandation 7** suggère au gouvernement de mettre immédiatement fin à sa collaboration avec des entités et des personnes de la République populaire de Chine dans les domaines de recherche sur les technologies de nature délicate, comme les technologies de l'infrastructure numérique de pointe; (...) l'intelligence artificielle et la technologie des mégadonnées; (...) et la robotique et les systèmes autonomes.



Quel est le régime juridique applicable à la sécurité EN recherche?

Lignes directrices sur la sécurité nationale pour les partenariats de recherche

Objectif:

- ❑ Atténuer les risques liés aux partenariats avec le secteur privé et industriel

Politique sur la recherche en technologies sensibles et sur les affiliations préoccupantes

Objectif :

Atténuer les risques liés aux affiliations préoccupantes pour les projets faisant progresser un Domaine de Recherche en Techniques Sensibles.

Acteurs institutionnels de l'application des textes pour la sécurité EN recherche (LDSNPR & Politique RTSAP)

Les organismes subventionnaires fédéraux + la FCI ont le devoir d'appliquer les textes dans le traitement des demandes des subventions depuis le 1^{er} mai 2024

- ❑ CRSNG
researchsecurity@nserc-crsng.gc.ca
- ❑ IRSC
support-soutien@cihr-irsc.gc.ca
- ❑ CRSH
researchsecurity-securiterecherche@sshrc-crsh.gc.ca
- ❑ FCI
securite.recherche@innovation.ca

- ❑ Les ministères provinciaux et organismes provinciaux de financement peuvent choisir de s'aligner sur les textes fédéraux pour la sécurité EN recherche ou édicter leur propre réglementation comme l'a fait la province de l'Ontario.
- ❑ Les universités canadiennes qui font de la recherche intensive.



Il y a tout un monde

L'université de l'Outaouais et des Laurentides

Découvrez nos nouveaux programmes



Qu'en est il de l'UQO?

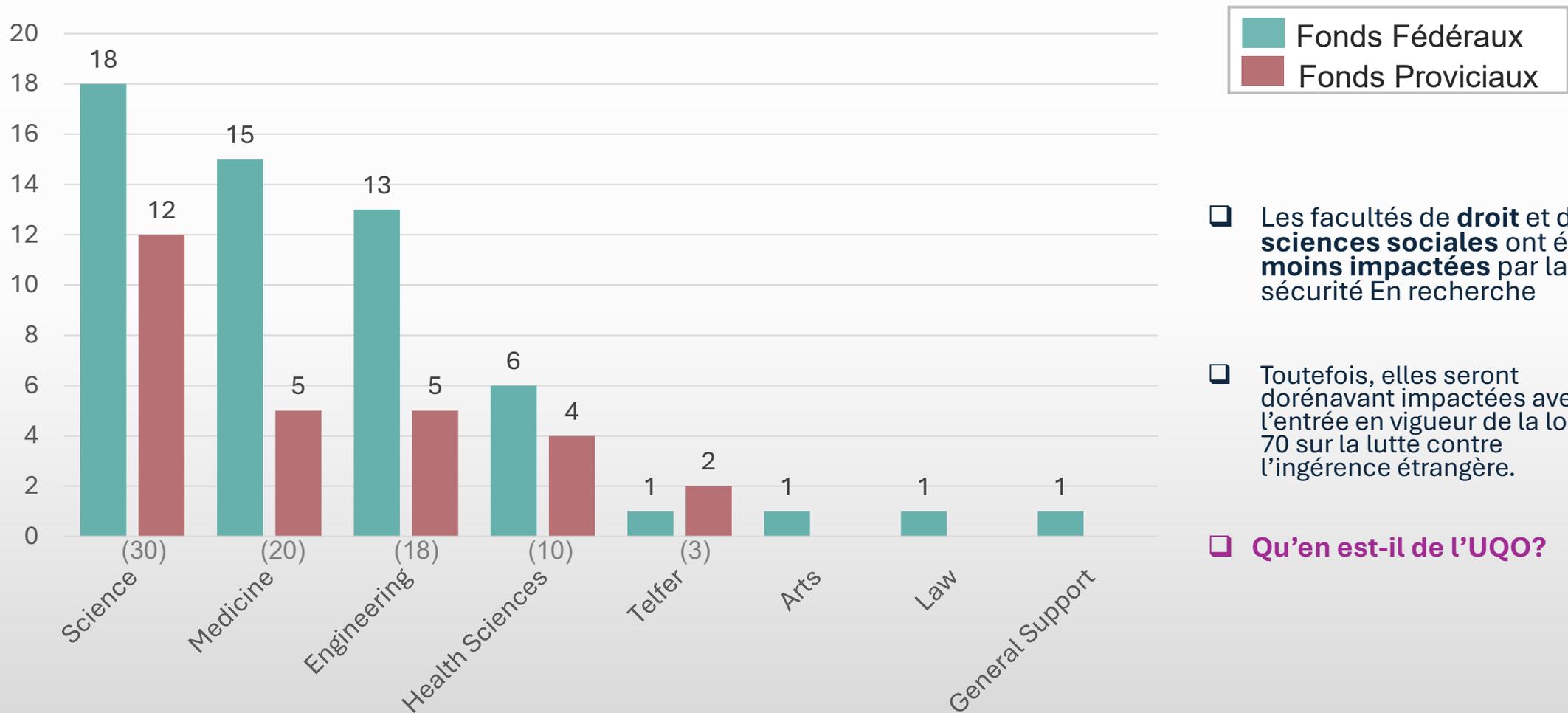
Quelles seraient les facultés ou
départements concernés?

Recherches intensives:

- Robotique et systèmes autonomes (LaRSA),
- Ingénierie des microsystèmes avancés (LIMA),
- Information et multimédia (LARIM),
- Intelligence Artificielle (LARIVIA),
- Sécurité informatique,
- Etc.



Exemple comparatif des facultés les plus touchées par la sécurité EN recherche: Cas d'une université canadienne



- Les facultés de **droit** et des **sciences sociales** ont été **moins impactées** par la sécurité En recherche
- Toutefois, elles seront dorénavant impactées avec l'entrée en vigueur de la loi C-70 sur la lutte contre l'ingérence étrangère.
- Qu'en est-il de l'UQO?**

Entités responsables de la sécurité EN recherche à l'UQO

☐ **Gouvernance | CA | Secrétariat**

- Adopter les **politiques et procédures** intégrant les LDSNPR à culture de recherche de l'UQO.

☐ **Décanat à la recherche et à la création | TI | Cyber-Sécurité**

- Mettre en place une stratégie de vulgarisation de la sécurité EN recherche, basée sur une planification stratégique.

☐ **Administrateurs | Gestionnaires des laboratoires | Chercheuses et chercheurs**

- Faire preuve de **Diligence Raisonnable** en utilisant les renseignements des sources ouvertes.
- Remplir le **Formulaire d'Évaluation de Risque (FER)**
- Écrire un **Plan d'Atténuation de Risque (PAR)** et le mettre en application dès l'obtention du financement.

☐ **Personnels des approvisionnements**

- Faire preuve de Diligence Raisonnable dans le processus des achats et acquisitions effectués avec des fonds de la recherche.

☐ **Personnels des finances**

- Faire preuve de Diligence Raisonnable pour tout paiement engageant des fonds de la recherche.

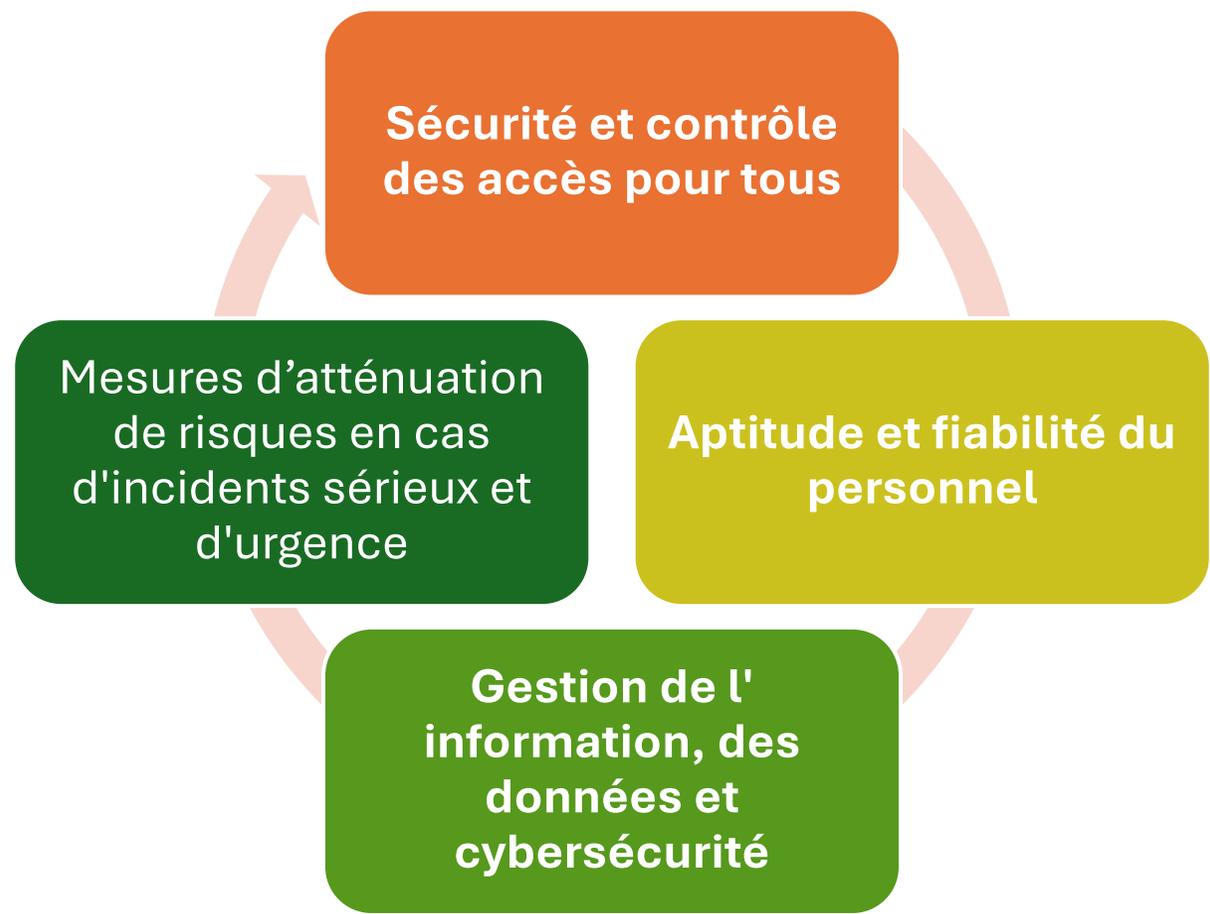
☐ **Personnels des Ressources humaines**

- Faire preuve de Diligence Raisonnable dans le processus de recrutement des personnels de recherche hautement qualifiés (PHQ) ?



Posture de la sécurité EN recherche à l'UQO

| Responsabilité partagée entre de nombreuses parties prenantes



(...), mais tout ceci ne peut mieux s'agencer qu'au travers une planification stratégique!

Regardons à présent chacun des textes gouvernant la sécurité En recherche au Canada





Lignes directrices sur la sécurité nationale pour les partenariats de recherche

Elles introduisent:

- La diligence raisonnable dans les partenariats de recherche.
- Le formulaire d'évaluation de risques.
- La formulation d'un plan d'atténuation de risques.

2024-12-04

Responsabilité des Administrateurs | Gestionnaires des laboratoires | Chercheurs face aux LDSNPR

Résumé – Utiliser les renseignements de sources ouvertes pour faire preuve de diligence raisonnable

Résumé – Utiliser les renseignements de sources ouvertes pour faire preuve de diligence raisonnable

Ce résumé est conçu pour aider les chercheurs à identifier, évaluer et gérer les risques liés à leurs recherches et leurs travaux – en particulier les risques découlant des partenariats. Ce document vous fournit des outils et des techniques pour l'utilisation des renseignements de sources ouvertes qui permettent de collecter et d'analyser les informations publiques afin d'identifier les risques de sécurité nationale liés aux partenariats de recherche.

Ce résumé est conçu pour aider les chercheurs à identifier, évaluer et gérer les risques liés à leurs recherches et leurs travaux – en particulier les risques découlant des partenariats. Ce document vous fournit des outils et des techniques pour l'utilisation des renseignements de sources ouvertes qui permettent de collecter et d'analyser les informations publiques afin d'identifier les risques de sécurité nationale liés aux partenariats de recherche.

En quoi consiste l'utilisation des renseignements de sources ouvertes pour faire preuve de diligence raisonnable?

Pourquoi devriez-vous utiliser cette méthode pour effectuer des recherches sur vos partenaires de recherche?

Les méthodes de diligence raisonnable en matière de sources ouvertes permettent de cibler et d'orienter la recherche et la découverte en ligne. Elles fournissent une approche structurée pour trouver et interpréter des renseignements en ligne afin de prendre des décisions importantes. Vous devez utiliser ces méthodes pour vérifier que vos partenaires sont bien ceux qu'ils prétendent être, pour confirmer que leurs relations et leurs motivations sont claires et pour vous assurer qu'il n'existe aucune source évidente de contrôle ou d'influence indésirable. Vous pourrez ainsi assurer la sécurité de vos recherches tout en poursuivant des partenariats ouverts et collaboratifs qui profitent au Canada.

Qu'est-ce que l'utilisation des renseignements de sources ouvertes devrait vous permettre de trouver?

Cette méthode vous permettra d'identifier les risques de sécurité nationale les plus importants concernant votre partenariat de recherche :

- le transfert des connaissances provenant de votre recherche à des gouvernements étrangers sans votre consentement.

- l'altération des résultats de votre recherche dans le but d'en minimiser la valeur, de nuire à votre réputation et à vos réalisations ou d'empêcher le Canada d'en bénéficier.

Les risques pour la sécurité nationale sont plus probables si votre partenaire de recherche a des intérêts conflictuels ou s'il est contrôlé ou influencé par un gouvernement étranger. En faisant preuve de diligence raisonnable, vous identifierez certains indicateurs de risque tels que :

- des structures organisationnelles ou des relations susceptibles de compromettre l'autonomie de votre partenaire.
- des indications de liens avec des gouvernements, des armées ou des services de sécurité étrangers sur des domaines de recherche sensibles.
- des informations qui montrent que votre partenaire opère dans des pays connus pour voler la propriété intellectuelle des chercheurs.
- toute information qui suggère un manque de transparence.

Rappelez-vous qu'en combinant l'information que vous avez accumulée à votre compréhension de la nature sensible de votre recherche, vous serez en mesure d'évaluer le niveau de risque.

© Sa Majesté la Reine du Chef du Canada, représentée par le ministre de l'Industrie, (2022).
N° de catalogue lu37-35/2022F-PDF
ISBN 978-0-660-45367-5

En quoi consiste l'utilisation des renseignements de sources ouvertes pour faire preuve de diligence raisonnable?

Pourquoi devriez-vous utiliser cette méthode pour effectuer des recherches sur vos partenaires de recherche?

Les méthodes de diligence raisonnable en matière de sources ouvertes permettent de cibler et d'orienter la recherche et la découverte en ligne. Elles fournissent une approche structurée pour trouver et interpréter des renseignements en ligne afin de prendre des décisions importantes. Vous devez utiliser ces méthodes pour vérifier que vos partenaires sont bien ceux qu'ils prétendent être, pour confirmer que leurs relations et leurs motivations sont claires et pour vous assurer qu'il n'existe aucune source évidente de contrôle ou d'influence indésirable. Vous pourrez ainsi assurer la sécurité de vos recherches tout en poursuivant des partenariats ouverts et collaboratifs qui profitent au Canada.

Qu'est-ce que l'utilisation des renseignements de sources ouvertes devrait vous permettre de trouver?

Cette méthode vous permettra d'identifier les risques de sécurité nationale les plus importants concernant votre partenariat de recherche :

- le transfert des connaissances provenant de votre recherche à des gouvernements étrangers sans votre consentement.

- l'altération des résultats de votre recherche dans le but d'en minimiser la valeur, de nuire à votre réputation et à vos réalisations ou d'empêcher le Canada d'en bénéficier.

Les risques pour la sécurité nationale sont plus probables si votre partenaire de recherche a des intérêts conflictuels ou s'il est contrôlé ou influencé par un gouvernement étranger. En faisant preuve de diligence raisonnable, vous identifierez certains indicateurs de risque tels que :

- des structures organisationnelles ou des relations susceptibles de compromettre l'autonomie de votre partenaire.
- des indications de liens avec des gouvernements, des armées ou des services de sécurité étrangers sur des domaines de recherche sensibles.
- des informations qui montrent que votre partenaire opère dans des pays connus pour voler la propriété intellectuelle des chercheurs.
- toute information qui suggère un manque de transparence.

Rappelez-vous qu'en combinant l'information que vous avez accumulée à votre compréhension de la nature sensible de votre recherche, vous serez en mesure d'évaluer le niveau de risque.

© Sa Majesté la Reine du Chef du Canada, représentée par le ministre de l'Industrie, (2022).
N° de catalogue lu37-35/2022F-PDF
ISBN 978-0-660-45367-5



**Lignes directrices sur la sécurité nationale pour les
partenariats de recherche
Formulaire d'évaluation des risques**

Sauvegarder Imprimer Réinitialiser

Nom de famille du demandeur :	Initiale(s) de tous les prénoms du demandeur :	Organisme qui administre la subvention :
-------------------------------	--	--

Introduction

Le Formulaire d'évaluation des risques est un outil qui permet d'identifier et d'évaluer les risques potentiels que les partenariats de recherche peuvent poser pour la sécurité nationale du Canada, tel que défini dans les [Lignes directrices sur la sécurité nationale pour les partenariats de recherche](#), et de développer des mesures d'atténuation efficaces.

En répondant aux questions du Formulaire d'évaluation des risques, vous fournirez, au meilleur de vos connaissances, des renseignements spécifiques à votre domaine de recherche proposé et aux éventuels organismes de recherche partenaires. Ces renseignements seront utilisés pour évaluer les risques pour la sécurité nationale dans les cas où le partenariat de recherche proposé pourrait exposer le projet de recherche à de l'ingérence étrangère, de l'espionnage ou du vol de la part de gouvernements, des organisations militaires et d'autres organisations étrangers. Ces renseignements seront aussi utilisés pour évaluer les risques dans les cas où le partenariat de recherche pourrait poser des risques potentiels pour le secteur canadien de la recherche dans son ensemble.

Aux fins des Lignes directrices sur la sécurité nationale pour les partenariats de recherche, le terme « organisme partenaire » désigne tout organisme qui joue un rôle actif dans le projet et/ou qui appuie un partenariat de recherche au moyen de contributions en argent et/ou en nature. Les organismes partenaires peuvent jouer les rôles suivants :

- partager le leadership intellectuel ou fournir une expertise;
- participer activement aux activités de recherche; et/ou
- appliquer les résultats de la recherche, et/ou participer activement au transfert ou à la mobilisation des connaissances produites pour contribuer à atteindre les résultats attendus pour le projet.

Les risques pour la sécurité nationale peuvent être définis comme, sans s'y limiter, des circonstances dans lesquelles pourraient survenir des cas potentiels d'ingérence étrangère, d'espionnage, de vol de propriété intellectuelle ou de transfert de connaissances non autorisé qui :

- contribuent à l'avancement des capacités militaires, en matière de sécurité et de renseignement d'États ou de groupes qui posent une menace pour le Canada; et/ou
- perturbent le développement de la recherche et de l'innovation canadiennes, diminuant la résilience des infrastructures essentielles ou compromettent la protection de données sensibles des Canadiens.

Les renseignements recueillis dans le formulaire ne seront pas utilisés pour établir votre conformité à toute exigence législative ou réglementaire pouvant s'appliquer à votre projet de recherche proposé. La collecte de ces renseignements servira à évaluer le profil de risque global de votre projet de recherche.

Qui doit remplir le Formulaire d'évaluation des risques?

Tout le monde peut utiliser le Formulaire d'évaluation des risques pour faire preuve de diligence raisonnable lors de l'établissement ou de la poursuite de partenariats avec des partenaires nationaux, internationaux et multinationaux.

Ce formulaire peut être requis pour des possibilités spécifiques de financement fédéral de la recherche. Vous devriez consulter la littérature de programme appropriée et associée à la possibilité de financement pour laquelle vous présentez une demande afin de déterminer si vous devez inclure un Formulaire d'évaluation des risques avec votre demande de subvention.

Selon la possibilité de financement, le « demandeur » peut être un individu, au nom de tout codemandeurs, ou peut être une institution postsecondaire ou de recherche.

Quels outils et ressources peuvent vous être utiles?

Nous vous encourageons à effectuer une recherche à partir de sources ouvertes pour compléter le Formulaire d'évaluation des risques et à consulter votre ou vos organismes partenaires pour valider les renseignements au besoin. Pour obtenir davantage de renseignements, consultez le guide détaillé [Faire preuve de diligence raisonnable en matière de sources ouvertes pour protéger les partenariats de recherche](#).

Des orientations et des ressources supplémentaires, notamment les [ateliers Science en sécurité](#) de Sécurité publique Canada ainsi que la [séance d'information sur les menaces et la Liste de contrôle](#) du Service canadien du renseignement de sécurité, qui peuvent vous aider à compléter ce formulaire sont accessibles sur le portail [Protégez votre recherche](#).

Section 4 : Plan d'atténuation des risques

L'objectif de cette section est de présenter votre **plan d'atténuation des risques**. Ce plan vous permettra d'identifier les mesures d'atténuation appropriées pour réduire la probabilité qu'un risque pour la sécurité ne se concrétise, et/ou pour en atténuer les répercussions dans l'éventualité où ce risque se matérialiserait.

Lors de l'élaboration de votre plan d'atténuation des risques, vous devez prendre en considération tous les facteurs de risque que vous avez identifiés en répondant « Oui » ou « Incertain » aux questions des sections **Connaissez votre recherche** et **Connaissez votre organismes partenaire**.

Votre plan d'atténuation des risques doit être élaboré **avec votre institution**. Vous pouvez aussi faire appel aux services de soutien à la gestion de votre institution (p. ex. services de TI, de sécurité, juridiques) afin de confirmer la viabilité et la faisabilité des mesures proposées.

Les mesures d'atténuation doivent être adaptées au projet de recherche et proportionnelles aux risques relevés tout en tenant compte des principes de la science ouverte. Par exemple, votre plan d'atténuation des risques pourrait couvrir les domaines suivants, sans s'y limiter :

- réviser tout autre processus de révision pertinent auquel le projet a été soumis (p. ex. une révision par un comité d'éthique de la recherche) en tenant compte de la façon dont les données personnelles recueillies dans le cadre du projet de recherche seront protégées)
- accroître la sensibilisation à la sécurité de la recherche et renforcer les capacités au sein de votre équipe de recherche
- assurer que les objectifs de votre ou vos organismes partenaires s'harmonisent aux objectifs du partenariat
- garantir le recours à de saines pratiques de gestion de la cybersécurité et des données
- convenir de l'utilisation prévue des conclusions de la recherche

Pour chacune des mesures d'atténuation que vous proposez, vous devez aussi fournir un **échecancier** pour sa mise en œuvre et décrire **la manière dont vous et votre institution allez surveiller son efficacité**.

Il n'est pas suffisant de faire référence aux politiques et pratiques actuelles ou futures de votre institution. Si vous faites référence à une politique ou à une pratique, vous devez aussi décrire **ce qu'implique** cette politique ou cette pratique et **la manière** dont elle sera appliquée pour atténuer les risques identifiés.

Les Lignes directrices sur la sécurité nationale pour les partenariats de recherche ne ciblent aucun pays et entreprise puisque les risques peuvent évoluer et provenir de n'importe qui et de n'importe quel endroit dans le monde. Conformément aux principes des Lignes directrices, les mesures d'atténuation des risques ne doivent jamais entraîner la discrimination ou le profilage d'un membre de la communauté de recherche. Par conséquent, empêcher toute personne de participer au projet de recherche proposé en raison de sa citoyenneté ou de son pays de résidence **ne constitue pas** une mesure acceptable d'atténuation des risques.

Des renseignements supplémentaires sur l'atténuation des risques sont disponibles sur le portail [Protégez votre recherche](#).

Présentez votre plan d'atténuation des risques dans la zone de texte à la page 7.

Formulaire d'évaluation des risques:

Section 1 – Connaissez votre recherche

1.6. Est-ce à double usage?

Section 2 – Connaissez votre organisme partenaire

2.1 Est-ce sous l'influence ou au contrôle d'un gouvernement étranger?

Section 3 – Identification des risques

Des trouvailles sur votre partenaire?

Section 4 – Plan d'atténuation des risques

Quelles mesures seront mises en œuvre pour éviter les résultats de vos recherches



RESUMÉ –

Responsabilité de la communauté de recherche à l'UQO face aux LDSNPR

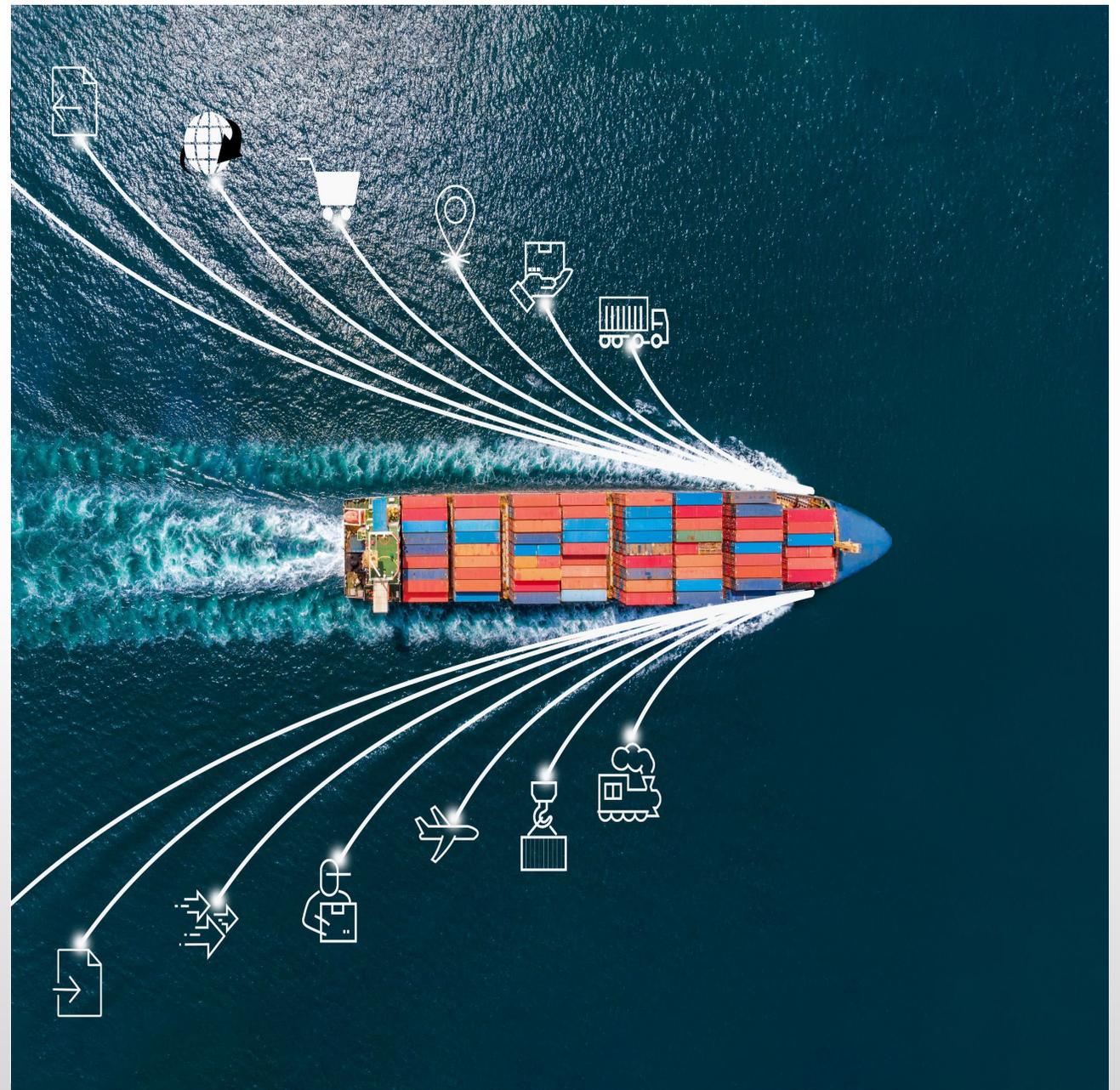
- Conduire une **diligence raisonnable!**
- Remplir un **formulaire d'évaluation de risques**, si un partenaire du secteur privé et industriel collabore à la recherche!
- Formuler un **plan d'atténuation de risques**.

Est-ce que d'autres partagent cette responsabilité à l'OQO?

- Qu'en est-il du département **des approvisionnements?**
- Qu'en est-il des **ressources humaines?**
- Qu'en est-il du département **des finances?**

Quelles sont les meilleures pratiques de diligence raisonnable avant une demande de subvention aux trois organismes et la FCI?

- Un document de procédure de 10 pages a été développé et sera partagé avec la communauté de recherche de l'UQO.





Janvier 2024

Politique sur la recherche en technologies sensibles et sur les affiliations préoccupantes

- ❑ Elle remet en question le financement de tout projet dans un domaine sensible si l'un des chercheurs a des affiliations préoccupantes.
- ❑ Elle exige aux chercheurs de remplir une attestation de conformité à la politique.
- ❑ Elle introduit la liste des DRTS.
- ❑ Elle introduit la liste des ORN.



Remise en question du financement de projets dans un DRTS et besoin d'attestation

Énoncé de la Politique RTSAP –

Toute demande de subvention (...) qui porte sur des projets visant à faire progresser un domaine figurant sur la liste des **Domaine de Recherche en Technologies Sensibles (DRTS)** ne sera pas financé si l'un des membres de l'équipe de recherche (...) est actuellement affiliée à l'une des organisations figurant dans la liste des organisations de recherche nommées (ORN) ou reçois du financement ou une contribution en nature d'une ORN.

D'où l'exigence de remplir l'attestation (ci-contre) pour refuter toute affiliation à une ORN!

Attestation relative à la recherche visant à faire progresser les domaines de recherche en technologies sensibles

Date de l'attestation (aaaa-mm-jj)

Instructions

- Pour confirmer que vous respectez les exigences de la Politique sur la recherche en technologies sensibles et sur les affiliations préoccupantes, remplissez le présent formulaire et enregistrez-le en lecture seule. Pour enregistrer le fichier en lecture seule, vous pouvez, entre autres, l'imprimer en format PDF. Conservez une copie du formulaire dûment rempli dans vos dossiers.
- La personne candidate principale doit recueillir le formulaire d'attestation de chaque membre de l'équipe de recherche ayant un rôle défini dans la demande de subvention. Elle doit ensuite regrouper les formulaires en un seul fichier PDF en utilisant le logiciel de confiance fourni ou recommandé par son établissement.
- Ce fichier doit ensuite être téléversé dans le module Formulaire d'attestation du système de gestion des subventions.

PARTIE 1 – RENSEIGNEMENTS SUR LA CHERCHEUSE OU LE CHERCHEUR		
Nom	Prénom	Principale affiliation
Adresse courriel		
Lien menant au profil public de la chercheuse ou du chercheur (facultatif) – aux fins d'identification		
Vous pouvez présenter n'importe quel profil public, par exemple celui qui figure dans ORCID, Google Scholar, ResearchGate ou LinkedIn ou, encore, dans votre page Web personnelle ou dans le site de votre établissement.		
PARTIE 2 – ATTESTATION		
En date de la présente attestation, je, [nom figurant à la partie 1], confirme, en remplissant le présent formulaire, que j'ai lu la Politique sur la recherche en technologies sensibles et sur les affiliations préoccupantes (RTSAP), que je la comprends et que je m'y conforme.		
En vertu de cette politique, toute demande de subvention présentée par une université ou un établissement de recherche affilié à une université aux organismes subventionnaires fédéraux ou à la Fondation canadienne pour l'innovation qui porte sur des projets visant à faire progresser un domaine figurant sur la liste des Domaines de recherche en technologies sensibles ne sera pas financée si l'un des membres de l'équipe de recherche participant aux activités financées par la subvention est actuellement affilié à l'une des organisations figurant dans la liste des Organisations de recherche nommées ou reçoit du financement ou une contribution en nature de l'une de ces organisations.		
Pour en savoir plus, y compris sur les définitions des termes en caractères gras, consultez les modalités d'application de la politique .		
Je soussignée ou soussigné, [nom figurant à la partie 1], atteste avoir lu et compris ce qui suit :		
<ol style="list-style-type: none">1. Je dois présenter le formulaire, puisque la personne candidate principale a déclaré, au nom de l'équipe de recherche, que les travaux décrits dans la demande de subvention visent à faire progresser un domaine figurant sur la liste des Domaines de recherche en technologies sensibles.2. En remplissant le formulaire, j'assume l'entière responsabilité de l'exactitude de l'information fournie dans la présente attestation.3. Tous les renseignements fournis dans le formulaire seront conservés de façon sécuritaire par l'organisme subventionnaire concerné, et ce, conformément à la <i>Loi sur la protection des renseignements personnels</i>. Ces renseignements pourront, à tout moment, être communiqués aux ministères et organismes fédéraux concernés aux fins de l'évaluation de la sécurité nationale qui permettra de valider la conformité à la Politique.4. Si la subvention demandée est accordée, la Politique sur la RTSAP, telle qu'elle est formulée au moment de la présentation de la demande, devra être respectée pendant toute la période de validité de la subvention, et ce, conformément aux modalités de la subvention.5. Tel qu'il est énoncé dans les modalités d'application de la politique, si des modifications sont apportées à la nature des travaux décrits dans la demande ou à la composition de l'équipe de recherche, l'organisme subventionnaire concerné pourrait exiger des mesures supplémentaires.6. Le non-respect de la Politique sur la RTSAP pourrait constituer une violation au titre du Cadre de recherche des trois organismes sur la conduite responsable de la recherche.		
Pour en savoir plus		
Consultez les Orientations des trois organismes concernant la Politique sur la RTSAP , la Politique sur la RTSAP , la Foire aux questions ainsi que la liste des domaines de recherche en technologies sensibles et la liste des organisations de recherche nommées .		
Déclaration		
<input type="checkbox"/> En date de la présente attestation, je [nom figurant à la partie 1], atteste en cochant la case ci-contre n'avoir, à ma connaissance, aucune affiliation à l'une des organisations figurant dans la liste d'organisations de recherche nommées et ne recevoir aucun financement ni aucune contribution en nature de l'une d'entre elles. En outre, je confirme avoir pris connaissance du fait que les membres de l'équipe de recherche participant aux activités visées par la subvention sont tenus de respecter la Politique sur la recherche en technologies sensibles et sur les affiliations préoccupantes , telle qu'elle est formulée au moment de la présentation de la demande, et ce, pendant toute la période de validité de la subvention.		

(06-2024)

PROTÉGÉ B LORSQUE REMPLI

This form is available in English.



Gouvernement du Canada

Government of Canada

Canada

REB INTEL

DRTS & ORN | Responsabilité des chercheurs et gestionnaires des laboratoires

DRTS = 11 Domaines



1. Technologies de l'infrastructure numérique de pointe



2. Technologies énergétiques de pointe



3. Matériaux et fabrication de pointe



4. Technologies de détection et de surveillance avancées



5. Armes de pointe



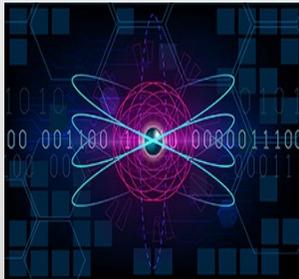
6. Technologies aérospatiales, spatiales et satellitaires



7. Intelligence artificielle et technologie des mégadonnées



9. Technologies des sciences de la vie



10. Science et technologie quantiques



11. Robotique et systèmes autonomes



8. Intégration personne-machine

ORN = 103 organizations



85 instituts en Chine
(Environ 82,5 % des ORN)



- ❑ Centre de recherche en sciences informatiques de Beijing.
- ❑ Laboratoire principal d'ingénierie des systèmes d'information.
- ❑ Université des relations internationales.



12 instituts en Iran
(Environ 11,6 % des ORN)



- ❑ Centre de recherche sur les technologies d'explosion et d'impact.
- ❑ Institut de physique appliquée.
- ❑ Organisation iranienne de recherche pour la science et la technologie.



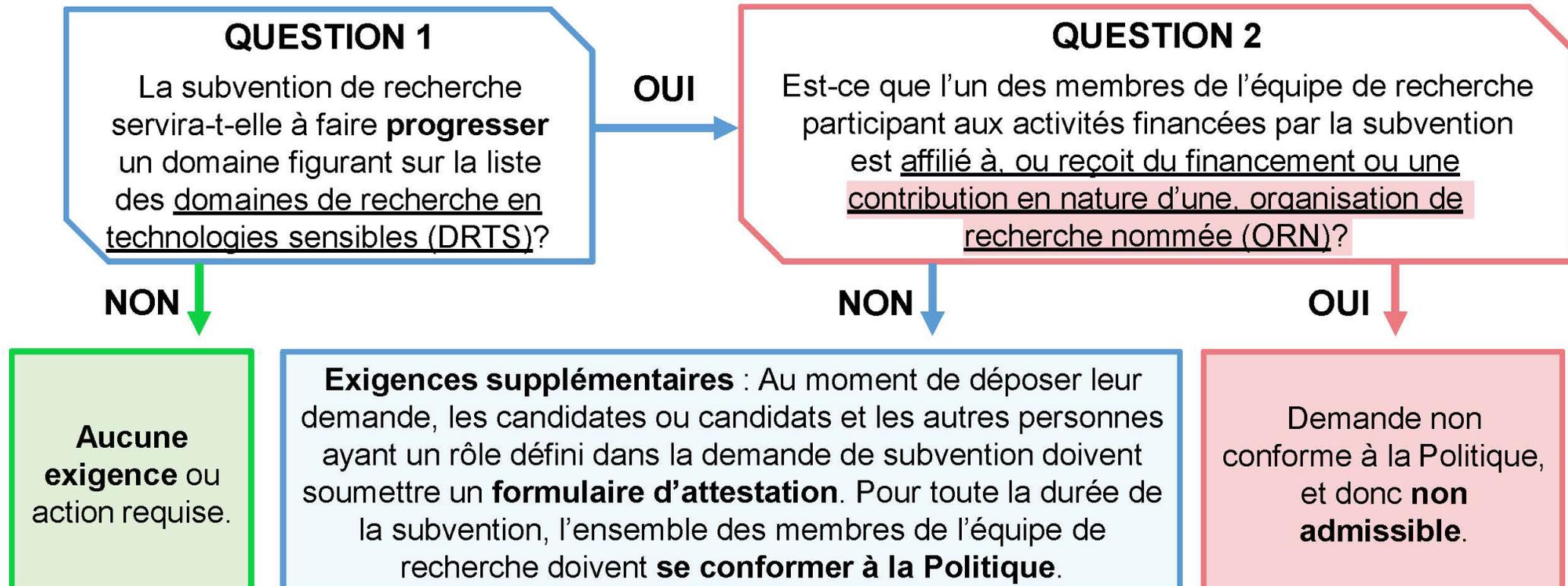
6 instituts en Russie
(Environ 5,8 % des ORN)



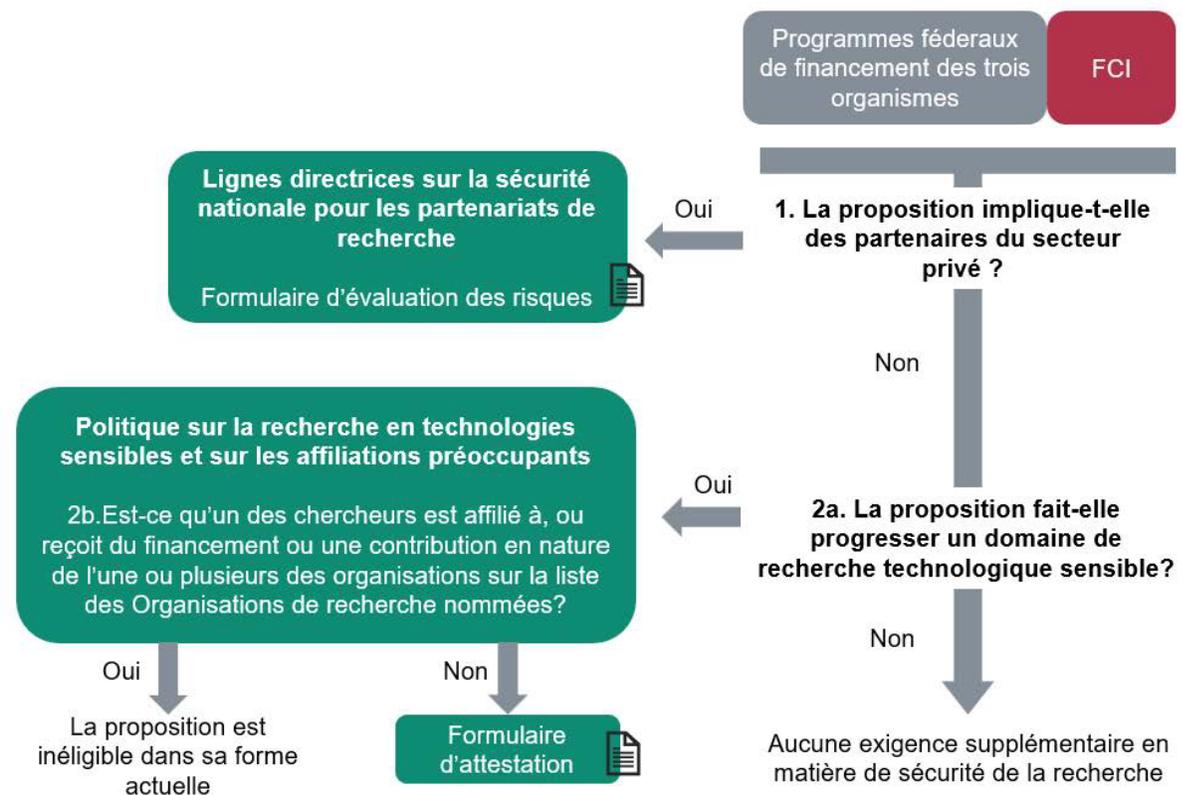
- ❑ Institut A.A. Kharkevich pour les problèmes de transmission de l'information, Académie des sciences de Russie.
- ❑ 33^{ème} Institut de recherche et d'essais scientifiques.

Conformité à la RTSAP pour chercheuses | chercheurs | gestionnaires des laboratoires?

Avant de présenter une demande de subvention pour un projet visé par la Politique, les personnes candidates doivent poser se **deux questions** pour savoir quelles exigences s'appliquent :



Applications CONJOINTE des TEXTES par la communauté de recherche.



Comment s'assurer de
l'application des textes
gouvernant la sécurité EN
recherche par les universités ?

Rapport du Comité permanent de la science et de la recherche sur la sécurité des partenariats de recherche

Dans son deuxième rapport, le comité permanent fait **huit (8) recommandations** au gouvernement canadien, notamment de:

- ❑ **Recommandation 4** – envisager l’adoption de mesures contraignantes pour s’assurer que les universités suivent les LDSNPR et la Politique RTSAP pour être éligibles à recevoir du financement fédéral.
- ❑ **Recommandation 5** – revoir les modalités d’attribution des fonds pour la sécurité de la recherche versés aux universités au titre du FSR, afin que les plus petits établissements ne soient pas laissés pour compte.
- ❑ **Recommandation 8** – prendre des mesures pour s’assurer que les politiques liées à la sécurité EN recherche n’aient pas involontairement pour effet d’exacerber les préjugés et la discrimination à l’encontre des étudiants et chercheurs d’origine asiatique sur les campus et dans la manière dont le financement de la recherche est distribué.



CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

LA SÉCURITÉ DES PARTENARIATS DE RECHERCHE DES UNIVERSITÉS ET DES ÉTABLISSEMENTS DE RECHERCHE CANADIENS AVEC DES ENTITÉS LIÉES À LA RÉPUBLIQUE POPULAIRE DE CHINE

Rapport du Comité permanent de la science et de la recherche

Lloyd Longfield, président

MAI 2024
44^e LÉGISLATURE, 1^{re} SESSION

L'éducation à travers des études de cas: Exemple 1

Scénario : Dr. X, chercheuse à l'UQO, est actuellement affiliée à un institut de recherche figurant sur la liste des organisations de recherche désignées (ORD) de la RTSAP et souhaite faire une demande de subvention auprès des trois organismes. Son objectif est de faire progresser une recherche en technologies sensibles (RTS) répertoriée au cours de ses recherches.

Application : Selon la RTSAP, les affiliations actuelles avec les ORD empêchent les chercheurs de recevoir des financements fédéraux en raison des préoccupations liées au transfert de technologies sensibles.

Actions :

- ❑ **Évaluer l'impact de l'affiliation** : Le Dr N. évalue l'impact de son affiliation actuelle à une ORD sur son éligibilité aux prochaines subventions fédérales. Elle se réfère aux lignes directrices [des trois organismes](#) et aux FAQ [de la politique RTSAP](#) pour plus de clarté.
- ❑ **Consulter l'équipe de sécurité EN recherche de l'UQO** : Elle consulte ensuite le coordinateur de la sécurité EN recherche de l'université pour vérifier les implications de son affiliation sur les demandes de subventions.
- ❑ **Cesser l'affiliation** : Si elle décide d'obtenir un financement fédéral, Mme N. prend des mesures pour mettre fin officiellement à son affiliation à l'ORN afin de retrouver son éligibilité.
- ❑ **Modifications des documents** : Tous les changements et toutes les communications concernant la cessation de son affiliation sont documentés par elle à des fins de transparence et de référence future.

Cas d'étude 2 – Évaluation des affiliations antérieures en vertu des exigences de l'Ontario en matière de sécurité EN recherche

Scénario :

- ❑ Le Dr H fait une demande de subvention provinciale et a des affiliations passées avec des organisations présentant des risques accrus au regard des exigences de l'Ontario en matière de sécurité EN recherche, qui prévoient un examen minutieux des affiliations passées avec des entités susceptibles de présenter des risques pour la sécurité nationale | provinciale.

Application :

- ❑ Contrairement à la politique de la RTSAP qui prévoit une liste précise des ORN **et qui se concentre sur les affiliations actuelles**, les exigences de l'Ontario en matière de sécurité EN recherche nécessitent la divulgation des affiliations passées | présentes afin d'évaluer les risques de sécurité associés au financement provincial avec des institutions très diverses qui ne se limitent pas aux ORN.

Mesures à prendre :

- ❑ **Examiner les affiliations passées** : Le Dr H. passe en revue ses engagements professionnels antérieurs afin d'identifier toute collaboration susceptible de tomber sous le coup des exigences de l'Ontario en matière de [sécurité de la recherche](#).
- ❑ **Divulgarion et documentation** : Il divulgue toutes les affiliations passées pertinentes dans sa demande de subvention en utilisant le formulaire de divulgation fourni par son université, en fournissant des informations détaillées sur la nature et la durée de chacune d'entre elles.
- ❑ **Consulter les conseils en matière de conformité** : Il demande conseil au coordinateur de la sécurité EN recherche de l'université pour s'assurer que toutes les divulgations répondent aux exigences provinciales.
- ❑ **Se préparer aux audits** : Organiser et préparer toute la documentation et les preuves à l'appui de ses divulgations en vue d'audits éventuels ou de demandes de renseignements supplémentaires.



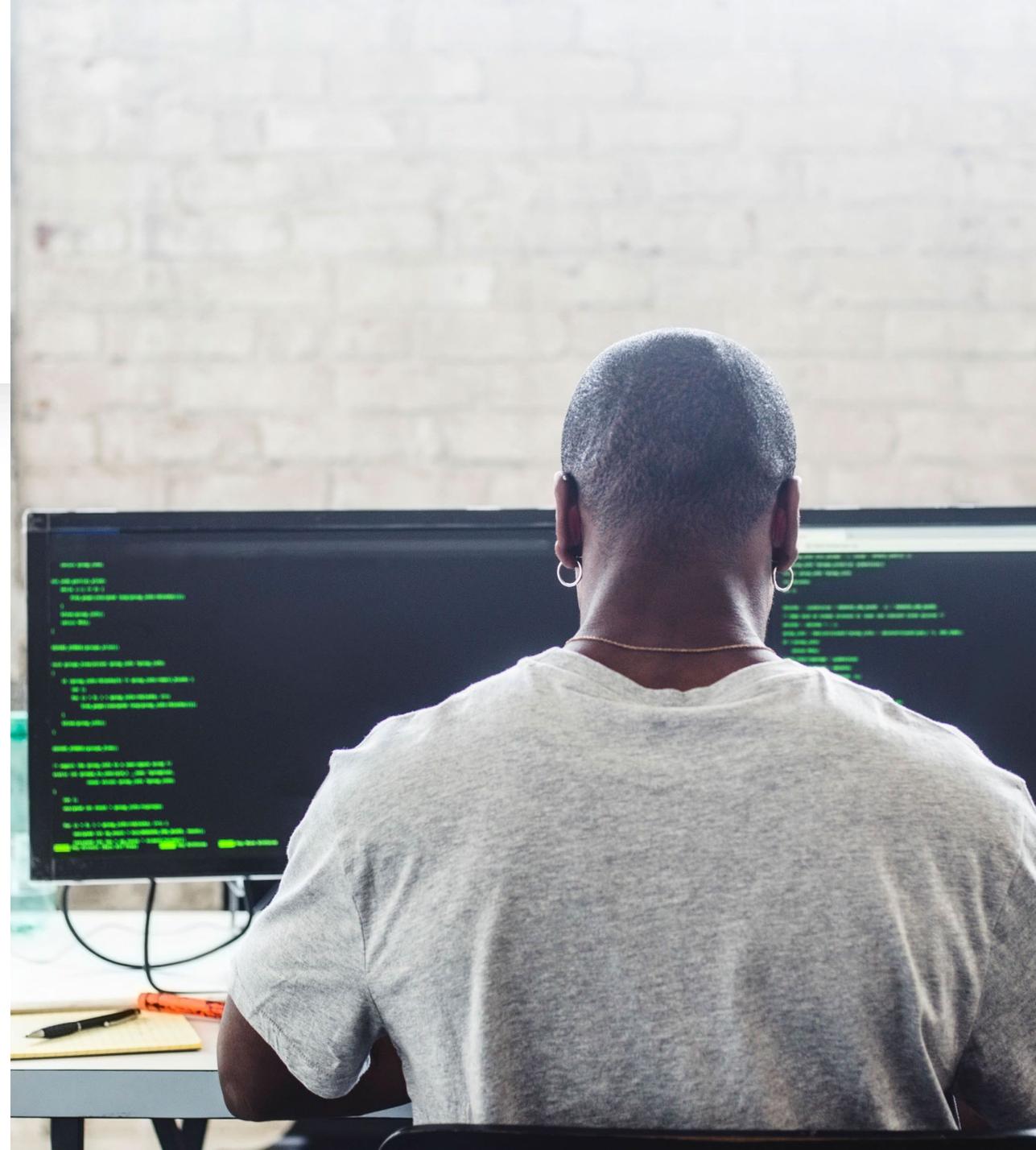
Mesures d'atténuation de risques standards pour la sécurité EN recherche

- Gestion du Contrôle des Accès (GCA)
- Gestion des Données de Recherche (GDR)
- Gestion de la Propriété Intellectuelle (GPI)
- Meilleures Pratiques en Technologies de l'information et Cybersécurité (MPTIC)

Gestion du Contrôle des Accès: Responsabilité institutionnelle

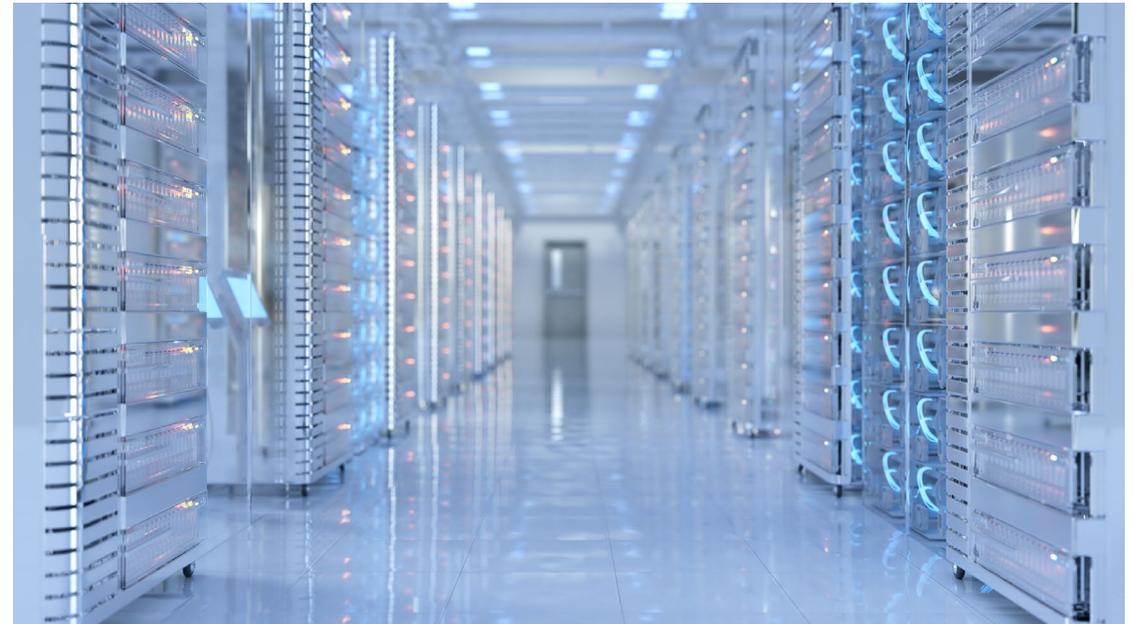
(Gouvernance, TI, Cyber, Service de terrains et des bâtiments)

- ❑ **Mise en place d'une politique de gestion centralisée des accès** aux sites sensibles de gouvernance et de recherche est une mesure efficace d'atténuation de risques en sécurité EN recherche.
- ❑ **Disponibilisation des cartes nominatives** (et balayables), y compris pour les visiteurs, afin d'accéder aux sites sensibles de recherche (notamment aux laboratoires) dans les universités.
- ❑ **Mise en place des règles strictes de visite** au sein des laboratoires à recherche intensive et sensible.



Gestion des Données de Recherche (GDR) : Responsabilité Institutionnelle Partagée (?)!

- ❑ La politique des trois organismes en matière de gestion des données de recherche (CRSNG, CRSH, IRSC) exige que les candidat(e)s à certaines occasions de financement soumettent des plans de GDR avec leurs demandes.
- ❑ **Les universités canadiennes s'alignent aux nouvelles recommandations.** C'est l'exemple, tout récemment, de l'uOttawa qui s'est dotée d'un centre de GDR (Centre de gestion des données de recherche (GDR) | Recherche et innovation).
- ❑ **L'assistant PGD** (<https://dmp-pgd.ca/>) est une ressource clé pour se doter d'un plan de GDR.
- ❑ **Les parties prenantes nécessaires** à une mise en place d'un PGD **seraient**: La gouvernance (Rectorat & Secrétariat Général), le Décanat de la recherche et de la création, les chercheurs, la bibliothèque, les administrateurs de recherche et gestionnaires des laboratoires, les TI, la gestion de l'information et le département de cybersécurité.



Gestion de la Propriété Intellectuelle, comme mesure d'atténuation de risques

- ❑ La **GPI** est une mesure phare **de la sécurité EN recherche**, car elle permet de protéger l'innovation et ses produits avant qu'ils n'atteignent le stade de brevettage et de commercialization.
- ❑ **Une politique claire et des procédures structurées de gestion de la GPI** sont essentielles à tout établissement menant des recherches intensives. Elles se veulent être un rampart contre tout accès non autorisé des acteurs malveillant à la PI des établissements de recherche.



Problématique de l'appropriation des produits de la PI des établissements de recherche par des entreprises étrangères

De plus en plus, **les industries des secteurs du numérique**, de l'agriculture, des mines et de l'énergie **collaborent avec** les institutions de recherche (centre de recherche, **universités**, incubateurs, accélérateurs d'entreprises, etc.) **pour obtenir des droits exclusifs** | non exclusifs d'exploitation **de la propriété intellectuelle à travers des licences.**

Il est important que les universités et le gouvernement fédéral se coordonnent pour assurer l'adoption ainsi que l'application des directives de sécurité dans la GPI.

Les universités sont encouragées à mettre en place des mécanismes pour analyser les risques soulevés par des partenariats avec des entreprises étrangères, notamment les risques en matière de sécurité nationale. Car, il est souvent difficile de savoir si les entreprises partenaires font partie de sociétés mères plus importantes ou ont des attaches avec des gouvernements étrangers pouvant représenter une menace pour la recherche et la sécurité EN recherche.



CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

SOUTIEN À LA COMMERCIALISATION DE LA PROPRIÉTÉ INTELLECTUELLE

Rapport du Comité permanent de la science et de la recherche

Lloyd Longfield, président

NOVEMBRE 2023
44^e LÉGISLATURE, 1^{re} SESSION

Problématique de l'appropriation des produits de la PI des établissements de recherche – Cas d'études

Une réalité récente démontre que les entreprises étrangères ayant une présence au Canada ont bénéficié des brevets produits par les universités canadiennes en défaveur desdites universités. **Par exemple :**

- ❑ **L'université de Calgary** a déclaré qu'elle **avait transféré un seul brevet** à des entreprises **en Chine** au cours des cinq dernières années, qu'elle avait trois projets en cours avec Huawei et qu'elle refuserait de nouveaux projets en partenariats avec Huawei à l'avenir.
- ❑ **L'université de la Colombie britannique** a affirmé **avoir cédé huit familles de brevets à Huawei entre mai 2014 et octobre 2018**, avant de se fixer un modèle de propriété intellectuelle conjointe entre octobre 2018 et décembre 2022. **Ce modèle a donné lieu à une seule famille de brevets et à un modèle de partenariats selon lequel l'UCB était propriétaire de la technologie créée en collaboration avec Huawei. Depuis, tous les partenariats** entre l'UCB et Huawei **font l'objet d'un audit de sécurité** avant d'être mis en œuvre.



CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

SOUTIEN À LA COMMERCIALISATION DE LA PROPRIÉTÉ INTELLECTUELLE

Rapport du Comité permanent de la science et de la recherche

Lloyd Longfield, président

NOVEMBRE 2023
44^e LÉGISLATURE, 1^{re} SESSION



Meilleures Pratiques en Technologies de l'information et Cybersécurité (MPTIC) pour renforcer la sécurité EN recherche | Une responsabilité institutionnelle (!?)

Recommandations avant l'adoption d'une politique institutionnelle:

- Un programme de cybersécurité doit identifier tous les fournisseurs** qui collectent, utilisent et stockent des données sensibles.
- En créant un programme, **l'organisation doit également négocier et rédiger un contrat** qui établit les obligations et les attentes de chaque partie en matière de traitement des données sensibles ;
- Un contrat bien rédigé avec des clauses spécifiques visant à atténuer les cyber-risques peut contribuer grandement à prévenir et à atténuer les cybermenaces.**



Meilleures Pratiques en Technologies de l'information et Cybersécurité (MPTIC) pour renforcer la sécurité EN recherche | Une responsabilité de la contractualisation.

Principales considérations pour la rédaction de dispositions relatives à la cybersécurité dans un contrat de fournisseur.

Contexte de la gestion des fournisseurs :

- ❑ Comprendre le programme de sélection et de gestion des fournisseurs de l'acheteur (UQO) à la lumière de ses besoins et objectifs commerciaux.

Approche rédactionnelle et objectifs du contrat :

- ❑ Les dispositions relatives à la cybersécurité dans un contrat avec un fournisseur **doivent être rédigées de manière à rester efficaces dans le temps tout en exprimant correctement les attentes de base.**
- ❑ Les objectifs de toutes les parties en matière de cybersécurité **doivent être clairement** définis et les coûts liés à ces objectifs doivent être équilibrés.



Principaux points à retenir de la formation



- ❑ Les préoccupations relatives à l'espionnage et au vol des données scientifiques (y compris la propriété intellectuelle) sont réelles.
- ❑ La recherche, les données et les résultats de la recherche sont à la fois précieux et très vulnérables.
- ❑ Il est important de tenir compte des risques et des considérations liés à la sécurité au moment de soumettre les demandes des subventions.
- ❑ Bref, il s'agit d'en être conscient et de poser des questions pour trouver des réponses adéquates.

Message clé –

“La science doit rester aussi ouverte que possible et protégée dans la mesure du nécessaire”



Ressources

- **Le Centre de la sécurité de la recherche du Canada, sous l'égide de Sécurité publique Canada:**
 - Courriel: researchsecurity-securiteenrecherche@ps-sp.gc.ca
 - [Prendre contact avec un conseiller régional ou une conseillère régionale](#)
 - [Science en sécurité – Renseignements sur les ateliers](#)
- **Portail [Protégez votre recherche](#):**
 - [Guide à l'intention des organismes de recherche et de financement et des universités \(science.gc.ca\)](#)
 - [Faire preuve de diligence raisonnable en utilisant des renseignements de sources ouvertes \(science.gc.ca\)](#)
 - [Cours de formation sur la sécurité de la recherche \(science.gc.ca\)](#)
 - [Atténuez les risques liés à la sécurité de la recherche \(science.gc.ca\)](#)
- **Autres ressources offertes par Universités Canada et U15Canada:**
 - [Protéger la recherche au Canada : Guide des politiques et des pratiques universitaires.](#)

