La sécurité de la recherche et la science ouverte au Canada

by **Caroline Winter** | 17 November 2023 | **French**, **Observations**, **Observations and Responses**

Read this in English

Cette observation a été écrite par Caroline Winter, avec des remerciements à Aaron Mauro et John Simpson pour leurs commentaires et contributions.

En bref :

Titre	La sécurité de la recherche et la science ouverte au Canada

Créateur	s.o.
Date de publication	s.o.
Mots clés	La sécurité de la recherche, les données ouvertes, la communication savante

La sécurité de la recherche, c'est-à-dire la capacité d'identifier les risques pour les processus et les produits de la recherche et de prendre des mesures pour les atténuer, est une préoccupation de longue date pour la communauté de la recherche et ses parties prenantes, y compris les individus et individues jusqu'aux gouvernements nationaux. Bien que l'ouverture et la collaboration soient essentielles pour faire avancer la recherche, une plus grande ouverture peut également entraîner de plus grands risques. Sécuriser les données et les connaissances numériques et d'autres extrants intangibles est particulièrement difficile. Cela a été mis en évidence pendant la pandémie de COVID-19, lorsque le pivot vers des environnements de travail virtuels et des niveaux sans précédent de collaboration mondiale et de partage de la recherche se sont accompagnés de menaces de sécurité accrues (voir « Science ouverte et COVID-19 »).

La sécurité de la recherche est une vaste question qui se rapporte à toutes les facettes de la recherche. Pour les chercheurs et chercheuses et les institutions individuelles, le vol de données et d'autres problèmes de sécurité peuvent entraver la recherche, menacer la propriété intellectuelle et affecter l'admissibilité au financement (voir « Les droits de propriété intellectuelle et la science ouverte en Europe »). La sécurité de la recherche est également une question de sécurité nationale puisque les données et les connaissances détournées peuvent être utilisées à des fins de renseignement national ou militaire néfastes. La sécurité est particulièrement préoccupante pour la recherche économiquement précieuse et à double usage – celle qui a des applications civiles et militaires potentielles – comme dans les domaines des infrastructures essentielles et de la recherche sur des sujets humains ainsi que de l'informatique quantique et de l'intelligence artificielle, qui sont tous deux des outils potentiels pour les cyberattaques ainsi que les domaines cibles actuels (Gouvernement du Canada 2023; OCDE 2022 ; Owens 2023a ; Science Canada 2021).

Le vol de données de recherche et/ou personnelles est une menace courante, car les données stockées sur les disques durs et les clés USB peuvent être volées ou égarées

et les cyberattaques peuvent causer des violations de données et endommager les systèmes informatiques. Les attaques d'hameçonnage ont tendance à cibler des chercheurs et chercheuses individuels pour qui la sécurité n'est peut-être pas une priorité (OCDE 2022).

La sécurité de la recherche est également menacée par les « acteurs malfaisants », qui peuvent être des collaborateurs, des chercheurs invités, des étudiants ou d'autres personnes qui visent à détourner ou à altérer la recherche pour leur propre profit (p. ex., dans le cas de concurrents commerciaux) ou pour le bénéfice d'autres personnes (p. ex. des états hostiles, des groupes du crime organisé, des organisations terroristes). Ces acteurs malfaisants peuvent agir par choix ou être forcés ou contraints (Science Canada 2021).

Étant donné que la sécurité de la recherche est une question de plus en plus urgente, l'élaboration de politiques dans ce domaine est très active. Le document politique de l'Organisation de coopération et de développement économiques (OCDE) *Intégrité et sécurité dans l'écosystème mondial de la recherche*, publié en juin 2022, traite d'un certain nombre de politiques et d'initiatives de sécurité de la recherche de l'Australie, du Japon, des Pays-Bas, du Royaume-Uni et des États-Unis, élaborées par des gouvernements nationaux, des organismes de financement, des établissements de recherche publics, des associations universitaires, des universités, des projets de recherche internationaux, et des organisations politiques internationales (p. ex., le G7, la Commission européenne, le Global Research Council). Bon nombre de ces politiques traitent de l'établissement d'évaluations des risques dans les processus existants (p. ex. l'évaluation des demandes de financement), de la détermination et de la gestion des menaces et des conflits d'intérêts, ainsi que des lignes directrices sur la diligence raisonnable.

Le document politique de l'OCDE reconnaît que le sujet de la sécurité de la recherche peut être difficile à discuter, controversé et polarisant, mais souligne qu'il est essentiel de le considérer néanmoins. Il offre sept recommandations de haut niveau pour la communauté de la recherche :

1. Souligner l'importance de la liberté de la recherche scientifique et de la collaboration internationale en tant qu'élément clé de l'écosystème mondial de la recherche
2. Intégrer les considérations relatives à la sécurité de la recherche dans les cadres nationaux et institutionnels pour l'intégrité de la recherche

3. Promouvoir une approche proportionnée et systématique de la gestion des risques dans la recherche
4. Promouvoir l'ouverture et la transparence en matière de conflits d'intérêts ou d'engagement
5. Mettre au point des directives claires, rationaliser les procédures et limiter la bureaucratie inutile
6. Mobiliser l'ensemble des secteurs et des institutions pour élaborer des politiques plus intégrées et efficaces
7. Améliorer le partage d'informations sur l'intégrité et la sécurité de la recherche à l'échelle internationale (10)

Le Canada a également élaboré des politiques sur la sécurité de la recherche. En décembre 2019, le U15 Regroupement des universités de recherche du Canada et Universités Canada ont publié *Atténuer les risques économiques et géopolitiques associés aux projets de recherche sensibles : Guide à l'intention des chercheurs universitaires*. Le guide traite de divers types de risques en plus de l'appropriation illicite de données. Par exemple, il souligne que, comme tous les chercheurs ne jouissent pas du même degré de liberté académique, la publication de certains résultats pourrait mettre en danger les partenaires internationaux et que les risques pour les droits humains doivent être évalués dans le cadre des plans de voyage des chercheurs (10).

Le gouvernement du Canada a également publié un groupe d'énoncés de politique connexes sur la sécurité de la recherche :

Déclaration du CSE et SCRS, le 14 mai 2020 : Cette déclaration du Centre de la sécurité des télécommunications (CST) et du Service canadien du renseignement de sécurité (SCRS) répond aux préoccupations accrues au sujet de la recherche et de la sécurité nationale liées à l'incertitude générée par la COVID-19. Il met en garde contre les menaces à la propriété intellectuelle ainsi qu'aux renseignements personnels, citant une alerte du Centre canadien pour la cybersécurité et une déclaration d'Affaires mondiales Canada sur l'augmentation des cybermenaces pour le secteur de la santé.

Énoncé de politique sur la sécurité de la recherche et la COVID-19, le 14 septembre 2020 : Cet énoncé d'Innovation, Sciences et Développement économique Canada (ISDE) réaffirme l'engagement du gouvernement du Canada à l'égard de la science ouverte et rappelle à la communauté de la recherche de demeurer vigilant et

d'examiner ses politiques et pratiques en matière de cybersécurité face aux menaces à la sécurité continues.

Énoncé de politique sur la sécurité de la recherche – Printemps 2021, le 24 mars 2021 : Cet énoncé d'ISDE fait état d'une augmentation des niveaux de menace pour la recherche et la sécurité nationale et rappelle à la communauté de la recherche l'énoncé de politique de septembre 2020. Il note également qu'il a demandé au Groupe de travail mixte du gouvernement du Canada et des universités d'élaborer des lignes directrices sur les risques pour guider les chercheurs dans l'examen des questions de sécurité nationale liées à leurs recherches. Ces Lignes directrices sur la sécurité nationale pour les partenariats de recherche ont été publiées en juillet 2021.

Déclaration des ministres Champagne, Duclos et Mendicino sur la protection de la recherche canadienne, le 14 février 2023 : Cette déclaration d'ISDE des Ministères de l'Innovation, des Sciences et de l'Industrie ; Santé ; et la Sécurité publique note encore une fois un niveau accru de menaces et annonce un changement dans la politique de financement pour les trois organismes : « Une demande de subvention de recherche dans un domaine sensible sera refusée si l'un des chercheurs travaillant sur le projet est affilié à une université, un institut de recherche ou un laboratoire rattaché à une organisation militaire ou à un organisme de défense nationale ou de sécurité d'un acteur étatique étranger qui représente un risque pour notre sécurité nationale » (ISDE 2023).

De plus, le budget fédéral de 2022 du Canada a instauré un financement de 125 millions de dollars pour le Fonds de soutien à la recherche pour aider les établissements postsecondaires à renforcer leur capacité en matière de sécurité de la recherche, ainsi que 34,6 millions de dollars sur cinq ans et un financement permanent de 8,4 millions de dollars pour établir un centre de la sécurité de la recherche pour conseiller les établissements de recherche.

Bien que la sécurité de la recherche soit une question complexe, les chercheurs peuvent prendre des mesures pour se protéger et protéger leur travail. Le portail Protégez votre recherche du gouvernement du Canada comprend de l'information sur la sécurité de la recherche ainsi que des outils et des lignes directrices à l'intention des chercheurs et des établissements. Les outils Évaluez votre profil de risque et Atténuez les risques liés à la sécurité de la recherche fournissent des conseils pratiques précis pour aider les chercheurs à évaluer et à gérer les risques propres à leurs projets. Les

ressources partagées par l'entremise de ce portail sont celles du Groupe de travail sur les universités, qui travaille à la science ouverte, collaborative et sécurisée au Canada.

La sécurité de la recherche dans la presse

L'une des questions abordées dans la presse universitaire et populaire était un programme pilote élaboré en réponse à l'énoncé de politique de mars 2021 dans lequel les demandes de financement pour les Subventions Alliance du CRSNG ont été examinées par le SCRS et le CST. Des articles dans *Affaires universitaires*, *CBC News*, le *Globe and Mail* (annonçant le projet pilote en 2021 et ses résultats en 2023) et *ScienceBusiness* rapportent que, sur les quelque 1000 demandes de financement reçues par le CRSNG, 48 ont été signalées pcomme ayant besoin d'être examinéesur examen et 32 d'entre elles se sont vu refuser le financement pour des raisons de sécurité.

À la suite de ce programme pilote, des examens de sécurité sont prévus pour toutes les demandes de financement des trois organismes. Cependant, certains chercheurs ont critiqué le programme pour son manque de transparence et de clarté (Owens 2023b). L'examen préalable ne peut pas mettre fin aux projets potentiellement risqués, puisque les projets qui se voient refuser du financement du CRSNG peuvent obtenir un financement équivalent auprès de leurs partenaires internationaux, et les projets qui ne cherchent pas à obtenir le financement fédéral ne seront pas examinés (Fife et Chase 2021). En mai 2023, le *Toronto Star* a rapporté que l'ISDE était en train d'élaborer une politique énumérant des domaines de recherche et des établissements de préoccupation spécifiques pour relever certains de ces défis.

Une autre question abordée dans la presse est la menace spécifique à la sécurité de la recherche de la part de l'État chinois. Écrivant au sujet du programme pilote de dépistage, Brian Owens note que « [b]ien qu'on n'y nomme aucune organisation ni aucun pays explicitement » dans la Déclaration sur la protection de la recherche canadienne de février 2023, « il est généralement admis que les laboratoires et les entreprises chinoises présentent un risque particulier en raison de leurs liens étroits et souvent nébuleux avec les forces armées ainsi que des allégations d'usage abusif des droits de propriété intellectuelle » (Owens 2023b). La Chine a été largement discutée comme une menace pour la sécurité de la recherche dans la presse internationale, y compris des articles dans *Global News*, *Science* et *Times Higher Education*.

Bien que la plupart des politiques (y compris la politique s'inclus le d'OCDE) aient adopté une approche agnostique par pays, des préoccupations ont été soulevées – comme dans des articles pour l'*Atlantic,* la *Chronicle of Higher Education*, *Policy Options* et *ScienceBusiness*, et *Affaires universitaires* – au sujet de l'accent implicite mis sur les menaces de la Chine. David Robinson décrit ces risques dans un article pour le bulletin de l'Association canadienne des professeurs d'université (ACPPU) :

> La recherche universitaire peut présenter des risques légitimes pour la sécurité nationale, mais nous devons, en tant que communauté, nous garder de tout excès. Nous devons veiller à ce que les universitaires ne soient pas ciblés en raison de leur origine ethnique et à ce que les règles ne soient pas si larges qu'elles restreignent la recherche et l'érudition légitimes. La loi sur l'influence étrangère ne doit pas non plus être utilisée à mauvais escient pour cibler les universitaires qui critiquent la politique militaire ou étrangère du Canada. (Robinson 2023)

Comme le fait remarquer Robinson, l'accent mis sur les menaces de la Chine a conduit à un climat de peur de collaborer avec des chercheurs et chercheuses chinois qui entrave la recherche et les relations de collaboration et met les chercheurs et chercheuses individuels en danger.

Réponses de la communauté INKE

Les recherches d'Aaron Mauro, membre du partenariat INKE, se concentrent actuellement sur la cybersécurité de la recherche. Son livre de 2022 *Hacking in the Humanities : Cybersecurity, Speculative Fiction, and Navigating a Digital Future* (2022) traite d'une approche de recherche qui prioritise la sécurité. Son discours du même nom au Dahlem Humanities Center en 2022 soutient que les projets d'humanités numériques doivent adopter les meilleures pratiques de sécurité dans la façon dont nous planifions, menons et communiquons la recherche et que les humanistes numériques sont bien placés pour poser les questions critiques nécessaires.

Mauro a donné une conférence au Digital Humanities Summer Institute (DHSI) 2021intitulée « Human Exploits : Cybersecurity and the Humanities », et enseigne un cours DHSI sur la cybersécurité pour les humanistes.

Parmi d'autres écrits liés à la cybersécurité, Mauro a écrit plusieurs articles pour *The Conversation.* Dans « Working from Home during the Coronovirus Pandemic Creates New Cybersecurity Threats », il décrit comment les menaces telles que l'hameçonnage et le ransomware sont devenues de plus en plus courantes pendant la pandémie et le besoin d'une infrastructure plus sécurisée et de meilleures habitudes de sécurité par les utilisateurs. Dans « Ukrainian Cultural Artifacts are at Risk during the Russian Invasion, but Digitizing Them my Offer Some Protection », il décrit comment les cyberattaques et la rhétorique russes menacent le patrimoine culturel ukrainien ainsi que sa sécurité nationale. Bien que la numérisation puisse créer des sauvegardes de documents du patrimoine culturel, note-t-il, elle dépend des infrastructures qui sont également menacées (pour plus sur la numérisation des documents du patrimoine culturel, voir « La Stratégie canadienne de numérisation du patrimoine documentaire »).

La sécurité de la recherche et la communauté universitaire élargie

De nombreuses initiatives dans l'ensemble de la communauté universitaire canadien portent sur des questions de sécurité de la recherche. À l'échelle nationale, par exemple, l'Alliance de recherche numérique du Canada (l'Alliance) a lancé en décembre 2022 un ensemble de normes et de politiques de cybersécurité liées à l'infrastructure nationale, abordant la classification des données, la gestion des données, la gestion des vulnérabilités et la gestion des risques liés à la cybersécurité. L'Alliance souligne également le Mois de la sensibilisation à la cybersécurité 2023 avec une série d'ateliers en ligne tenus tout au long du mois d'octobre, chacun portant sur une question liée à la sécurité de la recherche numérique.

Toujours à l'échelle nationale, le Canadian Shared Security Operations Centre (CanSSOC), une collaboration entre CANARIE et le Réseau national de la recherche et de l'éducation (RNRE), coordonne les services de cybersécurité locaux, régionaux et nationaux partout au Canada.

Les institutions et les organisations prennent également des mesures. Par exemple, en septembre 2021, le U15 a publié une Déclaration du U15 sur la protection des valeurs canadiennes et de la recherche canadienne qui souligne la nécessité que les politiques de sécurité soient claires, transparentes et prises en compte, reconnaissant que

> la liberté académique et l'autonomie institutionnelle font partie des principes fondamentaux qui font que nos institutions sont à l'abri de toute ingérence politique, peuvent parler en toute franchise aux autorités et sont en mesure de répondre aux besoins sociaux, culturels et économiques des Canadiens. (Regroupement 2021)

En février 2023, l'Université de Waterloo a organisé une conférence sur la sécurité de la recherche afin de sensibiliser les gens à des questions clés et d'encourager la discussion, y compris sur le potentiel de discrimination raciale en raison des mesures de sécurité. Il a également abordé l'évolution du rôle des bureaux des services de recherche, car de nombreux établissements ont maintenant des divisions, des bureaux et / ou du financement dédié à la sécurité de la recherche.

Et, bien qu'il n'est pas spécifiquement une politique de sécurité de la recherche, Les principes de PCAP® des Premières Nations du Centre de gouvernance de l'information des Premières Nations traitent de la propriété, du contrôle, de l'accès et de la possession, qui ont tous trait à l'intégrité et à la sécurité des données.

Sécurité de la recherche et la science ouverte

Un défi clé pour la science ouverte et sécurisée est que l'ouverture, la collaboration et le partage qui sont à la base des mouvements ouverts sont précisément ce que les acteurs malfaisants exploitent pour saper la sécurité de la recherche. Similairement, les infrastructures numériques et les technologies de communication en ligne qui rendent possible la science ouverte sont également particulièrement vulnérables aux attaques.

Un défi de sécurité connexe qui est aussi particulièrement pertinent pour la science ouverte est que plus les informations sont partagées ouvertement, plus le risque qu'elles soient utilisées à des fins néfastes est grand, comme Grace Browne s'explique dans un article pour *Wired*. La recherche sur la COVID-19 pourrait être utilisée pour développer des bioarmes, par exemple, et le code d'intelligence générale artificielle génératif pourrait être utilisé pour diffuser de la désinformation. L'essor des serveurs de préimpression ouverts, en particulier pour la recherche à double usage, est particulièrement préoccupante parce que cette recherche n'est pas encore évaluée par les pairs et peut contenir des erreurs ou poser des risques potentiels pour la sécurité qui n'ont pas été identifiés. Notant que l'ouverture amplifie le risque déjà existant que la recherche soit utilisée de manière non intentionnelle et nuisible, Browne

soutient qu'il est temps que la science ouverte réponde à ses risques, avant que le pire ne se réalise (Browne 2022).

En plus des efforts canadiens décrits ci-dessus, des efforts sont en cours dans le monde entier pour développer une culture de recherche axée sur la sécurité, souvent liée à des questions qui recoupent la science ouverte. Par exemple, les TRUST Principles for Digital Repositories (transparence, responsabilité, accent mis sur l'utilisateur, durabilité, technologie), qui reconnaissent que les infrastructures numériques que les chercheurs utilisent pour déposer et sourcer des données doivent être sécurisées et fiables (voir « Les principes TRUST pour les dépôts numériques »). Dans leur approbation conjointe des principes, l'Association des bibliothèques de recherche du Canada (ABRC) et Portage (2020) ont noté que la technologie comprend « la capacité d'identifier immédiatement des menaces de sécurité et d'y répondre de manière efficace ».

Educause a un guide de sécurité et de confidentialité contenant des informations et des ressources pour soutenir l'élaboration de politiques et les programmes d'éducation pour la communauté de l'enseignement supérieur. En janvier 2022, la Commission européenne a publié *Tackling R&I Foreign Interference*, un document de travail contenant des lignes directrices spécifiques pour les organismes de recherche afin d'atténuer les risques de sécurité tout en faisant progresser la science ouverte.

Ce ne sont là que quelques exemples d'initiatives en cours dans le monde pour s'attaquer à la question complexe de la sécurité de la recherche. Ils reflètent le consensus parmi les intervenants en matière de sécurité de la recherche selon lequel l'ouverture doit être équilibrée avec la sécurité tout en respectant les libertés académiques : une reconnaissance des avantages de travailler ouvertement et en collaboration au-delà des frontières nationales et des risques légitimes pour la sécurité encourus.

Ouvrages cités

ABRC (Association des bibliothèques de recherche du Canada). 2020. « L'ABRC et Portage adhérent aux principes TRUST pour les dépôts numériques. » Le 31 juillet 2020. https://www.carl-abrc.ca/news/trust-principles-for-digital-repositories/.

Browne, Grace. 2022. « Making Science More Open is Good for Research––But Bad for Security. » *Wired*, le 22 avril 2022. https://www.wired.com/story/making-science-more-open-good-research-bad-security/.

Fife, Robert, et Steven Chase. 2021. « Ottawa Imposes National-Security Risk Assessments for University Researchers Seeking Federal Funds ». *The Globe and Mail*, le 12 juillet 2021. https://www.theglobeandmail.com/politics/article-ottawa-imposes-national-security-risk-assessments-for-university/.

Gouvernement du Canada. 2021. « Qui constitue une menace? » Le 11 juillet 2021. https://science.gc.ca/site/science/fr/protegez-votre-recherche/renseignements-generaux-securite-recherche/qui-constitue-menace.

Gouvernement du Canada. 2023. « Pourquoi devriez-vous protéger votre recherche? » Le 31 mars 2023. https://science.gc.ca/site/science/fr/protegez-votre-recherche/renseignements-generaux-securite-recherche/pourquoi-devriez-vous-proteger-votre-recherche.

ISDE (Innovation, Sciences et Développement Économique Canada). 2023. “Déclaration des ministres Champagne, Duclos et Mendicino sur la protection de la recherche canadienne.” Gouvernement du Canada. February 14, 2023. https://www.canada.ca/fr/innovation-sciences-developpement-economique/nouvelles/2023/02/declaration-des-ministres-champagne-duclos-et-mendicino-sur-la-protection-de-la-recherche-canadienne.html.

Mauro, Aaron. 2022. « Hacking in the Humanities : Cybersecurity, Speculative Fiction, and Navigating a Digital Future ». Dahlem Humanities Center (DHC). Le 7 juin 2022. https://www.fu-berlin.de/en/sites/dhc/videothek/Videothek/908-DHCL-Mauro/index.html.

OCDE (Organisation de coopération et de développement économiques). 2022. « Intégrité et sécurité dans l’écosystème mondial de la recherche ». OECD Science, Technology and Industry Policy Papers, no. 130. https://doi.org/10.1787/39ee9438-fr.

Owens, Brian. 2023a. « La sécurité nationale et la recherche font-ils bon ménage? ». *Affaires universitaires*, le 14 juin 2023. https://www.affairesuniversitaires.ca/articles-de-fond/article/la-securite-nationale-et-la-recherche-font-ils-bon-menage/.

Owens, Brian. 2023b. “Le manque de clarté lors des évaluations de risque pour la sécurité nationale est dénoncé.” *Affaires universitaires*, le 23 mars 2023.

https://www.affairesuniversitaires.ca/actualites/actualites-article/le-manque-de-clarte-lors-des-evaluations-de-risque-pour-la-securite-nationale-est-denonce/.

Robinson, David. 2023. « Liberté académique et sécurité nationale ». *Bulletin de l'ACPPU*, le juin 2023. https://www.caut.ca/fr/bulletin/2023/05/le-coin-du-directeur-general-liberte-academique-et-securite-nationale.

Regroupement des universités de recherche canadiennes U15. 2021. « Déclaration du U15 sur la protection des valeurs canadiennes et de la recherche canadienne ». Groupe U15 des universités de recherche canadiennes. Le 28 septembre 2021. https://u15.ca/fr/publications/statements-releases/declaration-du-u15-sur-la-protection-des-valeurs-canadiennes-et-de-la-recherche-canadienne/.

Regroupement des universités de recherche canadiennes et universités du Canada U15. 2019. « Atténuer les risques économiques et géopolitiques associés aux projets de recherche sensibles : guide à l'intention des chercheurs universitaires ». https://www.univcan.ca/wp-content/uploads/2020/08/attenuer-les-risques-economiques-et-geopolitiques-associes-aux-projets-de-recherche-sensibles-dec-2019.pdf.

Science Canada. 2021. « CSIS Research Security Briefing ». Le 9 juillet 2021. https://www.youtube.com/watch?v=LSu5ObwzM8c.

Search

Archives

Select Year

Categories

Community News

English

French

Observations

Observations and Responses

Policies

Responses

Uncategorized

Tags

Berlin Declaration / Déclaration de Berlin Bethesda Statement / Déclaration de Bethesda bibliodiversity / bibliodiversité Budapest Statement / Déclaration de Budapest Canada Canadiana.org Canadian government/le gouvernement du Canada CAPOS CARL / ABRC collaboration Compute Canada / calcul Canada copyright / droits d'auteurs CRKN / RCDR data management / gestion des données digital scholarship / version numérique en français / French english English / en anglais Federation for the HSS / Fédération des sciences humaines funding agencies / organismes de financement identity management / gestion de l'identité implementation / mise en oeuvre INKE international policy / politique internationale Naylor Report / le rapport Naylor open access / libre accès open data / données ouvertes open education / éducation ouverte open government / gouvernement ouvert open infrastructure / infrastructure ouverte open scien open science / science ouverte open source software / les logicels libres ORCID peer review / critique des pairs PKP Plan S Plan S update / mise à jour du Plan S policy / politique promotion et titularisation publishing / édition RDC / DRC RDM RECODE recommendations / recommandations reports / les rapports repositories / les dépôts research evaluation / l'évaluation de la recherche research evaluation / évaluation de la recherche

research libraries / les bibliothèques de recherche

research output / les résultats de la recherche research security / sécurité de la recherche

RPT / révision scholarly communication / la communication savante

SFU Library / Bibliothèque social media / les medias sociaux

Tri-Agency / des trois organismes UK UK / Royaume-Uni UNESCO UVic Libraries

Érudit

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

INKE
IMPLEMENTING NEW KNOWLEDGE ENVIRONMENTS