

Boîte à outils sur la sécurité des connaissances et la science ouverte

Annexe au rapport « [*Openness and Security: Two Pillars, One System*](#) »

Partenaires du projet :

Université de Berne, chef de projet

Center for Security Studies (ETH)

Haute école spécialisée de Suisse occidentale (HES-SO)

Avec le soutien de swissuniversities

Il s'agit d'une traduction automatique de [la version originale en anglais](#), réalisée à l'aide de DeepL Pro.

Sommaire

1.	Recommandation n° 1 : Élaborer une politique globale de sécurité des connaissances	5
2.	Recommandation n° 2 : Mettre en place des personnes responsables dédiées à la sécurité des connaissances ou des unités internes spécialisées	5
3.	Recommandation n° 3 : mettre en œuvre des programmes de formation et de sensibilisation à la sécurité des connaissances	8
4.	Recommandations 5, 6 et 7 : Mesures de sécurité des connaissances dans la science ouverte et la science ouverte en tant que mesure de sécurité des connaissances	9
5.	Mesures incitatives et harmonisation de l'évaluation	9
1.	Conseils complets ou évaluations des risques	11
2.	Contenu	11
2.1	Soumission aux contrôles à l'exportation	11
2.2	Listes des technologies critiques	12
2.3	Détermination du potentiel de double usage des projets de recherche	12
3.	Partenaires	14
3.1	Outils d'évaluation complets	14
3.2	Embargos et sanctions	14
3.3	Évaluation des réseaux d'institutions ou de chercheurs et chercheuses	15
3.4	Listes d'institutions critiques en raison de leur proximité avec le secteur militaire	16
3.5	Autres considérations	16
4.	Infrastructures	16
	Annexes	17

u^b

Cette boîte à outils est conçue pour aider les chercheurs et chercheuses et les institutions de recherche à s’y retrouver dans le paysage en constante évolution de la sécurité des connaissances, en particulier dans le contexte de la science ouverte (open science).¹ Elle s’appuie sur la conception commune exprimée dans les « Valeurs et principes communs du G7 en matière de sécurité et d’intégrité de la recherche », selon laquelle « l’ouverture et la sécurité ne sont pas contradictoires, mais complémentaires et se renforcent mutuellement ».

Dans son rapport, le groupe de travail national sur la sécurité des connaissances, piloté par swissuniversities, identifie des faiblesses dans le système suisse de gestion de la sécurité des connaissances, notamment un manque d’« expertise spécifique en matière d’évaluation de la sécurité des connaissances et de gestion des risques » : « Les administrateurs et administratrices universitaires traditionnels ne disposent pas nécessairement des connaissances spécialisées requises pour évaluer les implications complexes en matière de sécurité des projets de recherche ou des partenariats internationaux. Ce déficit de compétences représente un défi fondamental qui doit être relevé par le biais de formations, de recrutements ou de mécanismes de soutien externes. »²

Le rapport « *Openness and Security: Two Pillars, One System* »³ constitue un pas en avant pour combler cette lacune. Cette boîte à outils, qui complète le rapport plus général, fournit des conseils pratiques, des exemples et des outils opérationnels.

Elle s’adresse aux responsables universitaires, et seulement indirectement aux chercheurs et chercheuses. Les outils qu’elle contient peuvent être utilisés et adaptés au contexte spécifique de chaque établissement et à son cadre de gouvernance.

Elle vise à aider à identifier, évaluer et gérer les risques potentiels tout en préservant l’ouverture, la collaboration internationale et la liberté académique, qui sont fondamentales pour le progrès scientifique. Les mesures doivent rester proportionnées aux risques réels, éviter toute bureaucratie inutile et être appliquées de manière non discriminatoire.

La boîte à outils s’appuie sur cinq principes fondamentaux.

1. « Aussi ouvert que possible, aussi sécurisé que nécessaire » : les résultats de recherche, les méthodes et les collaborations doivent, par défaut, être ouverts, à moins que des risques légitimes n’exigent un accès contrôlé.
2. Proportionnalité : les contrôles de sécurité doivent être proportionnés au risque réel, en évitant toute bureaucratie excessive susceptible d’entraver la collaboration ou l’innovation.

¹ Pour une définition de la « science ouverte », veuillez vous reporter au rapport auquel se rattache cette boîte à outils : Université de Berne/Centre d’études sur la sécurité/Haute école spécialisée de Suisse occidentale : Ouverture et sécurité : deux piliers, un seul système, Berne : 2026. Nous suivons la définition de l’UNESCO et nous nous concentrons sur les deux dimensions que sont le libre accès et les données de recherche ouvertes.

² [swissuniversities – Sécurité des connaissances en Suisse : un cadre stratégique pour les établissements d’enseignement supérieur et les autorités](#), p. 8.

³ Le rapport présente le cadre réglementaire relatif à la sécurité des connaissances et à la science ouverte à l’échelle internationale et en Suisse, identifie les risques réels pour la sécurité des connaissances dans le contexte spécifique de la science ouverte, explique quels facteurs entraînent ou augmentent ces risques et décrit comment les établissements en Europe et en Suisse gèrent actuellement les risques liés à la sécurité des connaissances dans le cadre de la science ouverte. Avant de conclure et de formuler des recommandations, nous nous permettons d’esquisser une perspective d’avenir pour la sécurité des connaissances et la science ouverte.

3. Accompagnement des chercheurs et chercheuses : les chercheurs et chercheuses ne doivent pas supporter seuls tout le poids de la mise en conformité. Les institutions doivent fournir l'infrastructure, la formation, les services de conseil et le soutien administratif nécessaires.
4. Transparence et responsabilité : les décisions en matière de sécurité des connaissances doivent être documentées, vérifiables et régies par des procédures institutionnelles claires.
5. Préservation de la collaboration internationale : l'objectif n'est pas la « déglobalisation » de la science, mais une collaboration résiliente, éthique et sécurisée.

u^b

La boîte à outils est structurée en deux sections : la section 1 répertorie les outils permettant d'aborder la sécurité des connaissances dans le contexte spécifique de la science ouverte. La section 2 est consacrée à d'autres outils d'évaluation et de classification des risques ainsi qu'à des recommandations qui ne sont pas spécifiques au contexte de la science ouverte, mais que les institutions pourraient juger utiles pour faire face aux risques liés à la sécurité des connaissances et pour renforcer leurs cadres de gestion des risques.

La plupart des outils référencés dans cette boîte à outils ont été développés dans le cadre du projet « swissuniversities » sur la sécurité des connaissances et la science ouverte (indiqués ci-dessous par la mention « Résultat du projet »). Nous avons également compilé des ressources existantes que nous avons jugées utiles. Lorsque les liens ne sont plus actifs, les utilisateurs et utilisatrices sont invités à rechercher le titre de la publication en ligne.

Les sections suivantes reprennent les recommandations du chapitre 6 du rapport « *Openness and Security: Two Pillars, One System* » et proposent des outils concrets et pratiques pour les mettre en œuvre.

u^b

1. **Recommandation n° 1 : Élaborer une politique globale de sécurité des connaissances**

La sécurité des connaissances doit être intégrée dans la stratégie institutionnelle, la gouvernance de la recherche et les cadres de gestion des risques. Les institutions doivent établir des politiques claires en matière de sécurité des connaissances, couvrant des domaines clés tels que les procédures de diligence raisonnable pour les collaborations internationales, les protocoles de transfert de technologie, les mesures de sécurité de l'information et les mécanismes de signalement des problèmes liés à la sécurité des connaissances. Ces politiques doivent être alignées sur les règles nationales et institutionnelles relatives au contrôle des exportations, à la protection des données et à la propriété intellectuelle.

Ces politiques doivent être élaborées en consultation avec la communauté des chercheurs et chercheuses afin de garantir qu'elles soient pratiques, proportionnées et transparentes. Parallèlement, elles doivent réduire au minimum les charges administratives inutiles tout en restant suffisamment souples pour s'adapter à l'évolution des risques et des exigences réglementaires.

La science ouverte doit être prise en compte de manière systématique dans cette politique et dans le cadre des activités opérationnelles. À titre de bonne pratique, les établissements devraient en outre adopter une politique spécifique relative à la sécurité des connaissances dans le cadre de la science ouverte, qui :

- définisse la tolérance au risque, tant au niveau national qu'au niveau de l'établissement, en matière d'ouverture par rapport à la restriction
- fournisse des orientations concrètes et spécifiques à l'établissement
- établisse une distinction entre les disciplines et les niveaux de risque (par exemple, les sciences humaines par rapport aux domaines des STIM à double usage).

Conformément aux recommandations 5, 6 et 7 du rapport « *Openness and Security: Two Pillars, One System* », nous recommandons qu'au niveau opérationnel, les pratiques de science ouverte soient considérées et utilisées comme des mesures de sécurité des connaissances, et que ces pratiques soient améliorées grâce à ces mesures.⁴ Cette approche garantit que les deux domaines se renforcent mutuellement, tout en réduisant le risque de créer une procédure administrative supplémentaire.

2. **Recommandation n° 2 : Mettre en place des personnes responsables dédiées à la sécurité des connaissances ou des unités internes spécialisées**

Afin d'élaborer et de mettre en œuvre correctement les politiques et procédures mentionnées ci-dessus au chapitre 1, section 1, les institutions doivent investir dans une structure d'appui couvrant

⁴ Un outil pratique est proposé au chapitre 1, section 4 de cette boîte à outils.

à la fois les aspects juridiques, de conformité et de sécurité, ainsi que la science ouverte. En raison du chevauchement entre la sécurité des connaissances et la science ouverte, les unités distinctes devraient respectivement recevoir une formation dans l'autre domaine.

Le portefeuille de services suivant est recommandé aux institutions :

1. Service d'assistance à la science ouverte : soutien à la publication et aux dépôts

Ce service constitue le point d'entrée pour les chercheurs et chercheuses qui souhaitent publier leurs résultats en libre accès tout en respectant les exigences des bailleurs de fonds ou de leur institution.

Fonctions principales

- Assistance à la publication en libre accès : conseils sur les politiques des éditeurs, le financement des frais de publication (« APC »), les accords de transformation et la conservation des droits.
- Assistance aux dépôts : dépôt d'articles, de jeux de données, de logiciels, de thèses et d'autres productions dans des dépôts institutionnels ou disciplinaires.
- Métadonnées et visibilité : veiller à ce que les résultats soient correctement décrits, référencés (ORCID, DOI, identifiants de subventions) et indexés.
- Conseils en matière de licences : aider les chercheurs et chercheuses à choisir les licences appropriées (par exemple, Creative Commons).
- Contrôle de la conformité : vérification du respect des exigences des bailleurs de fonds et des politiques institutionnelles en matière de science ouverte.

2. « Data Stewardship » : gestion des données conforme aux principes FAIR et sécurisée, y compris les risques liés à la sécurité des connaissances dans le cadre de la science ouverte

Ce service garantit que les données de recherche sont à la fois réutilisables et protégées de manière appropriée.

Gestion des données selon les principes FAIR

- Facilement repérables : identifiants persistants et métadonnées riches
- Accessibles : mécanismes d'accès contrôlé ou libre
- Interopérables : utilisation de normes et de formats communs
- Réutilisables : documentation, provenance et licences

Fonctions de sécurité et de gouvernance

- Classification des données (publiques/internes/confidentielles/restreintes, ou : ouvertes/restreintes/classifiées/soumises à des contrôles à l'exportation, etc.)
- Stockage sécurisé et contrôles d'accès
- Politiques de chiffrement, de sauvegarde et de conservation
- Prise en charge des plans de gestion des données (DMP)

Rôle de la sécurité des connaissances dans la science ouverte

Une unité moderne de gestion des données évalue également si la mise à disposition ouverte des données pourrait créer des risques pour la sécurité des connaissances. Citons par exemple les données de recherche à double usage, les informations sensibles sur les infrastructures, les technologies stratégiques ou les données soumises à des restrictions contractuelles ou nationales.

Le gestionnaire (data-steward) effectue ou coordonne, en collaboration avec les responsables de la conformité en matière de sécurité des connaissances (voir ci-dessous), les tâches suivantes :

- Identification des risques
- Évaluation des risques (probabilité et impact)
- Atténuation des risques (divulgaration partielle, embargos, accès contrôlé, anonymisation)
- Consignation des décisions

3. Responsable de la conformité en matière de sécurité des connaissances (Knowledge Security compliance officer)

Les établissements doivent nommer des responsables de la sécurité des connaissances et/ou mettre en place un comité de sécurité des connaissances afin de soutenir la mise en œuvre et la prise de décision.⁵ Ces responsables conseillent les chercheurs et chercheuses et la direction, coordonnent les évaluations des risques, examinent les cas complexes ou à haut risque, prévoient des procédures d'escalade claires pour les décisions difficiles et veillent à l'application cohérente et proportionnée des politiques au sein de l'établissement, ainsi qu'à l'intégration efficace et harmonisée de la sécurité des connaissances dans les autres services de l'établissement (par exemple, les bureaux chargés de la science ouverte ou des affaires internationales, etc.).

Principales responsabilités⁶

- Évaluations des collaborations internationales : identifier les partenaires, les sources de financement, les juridictions et les domaines technologiques stratégiques ; évaluer les risques de transfert indésirable de connaissances, de technologies, de données ou d'expertise.
- Vérification des candidatures lors du recrutement : examiner les nominations dans des domaines de recherche sensibles ; identifier les conflits d'intérêts, les affiliations non divulguées ou les problèmes liés à des sanctions.
- Vérification des étudiants et étudiantes (lorsque la loi l'autorise et que l'établissement l'a adoptée) : évaluer l'accès aux installations, ensembles de données ou technologies hautement sensibles ; appliquer des mesures proportionnées et fondées sur les risques.
- Gestion des risques liés à la science ouverte : vérifier si les publications, prépublications, lancements de logiciels ou partages de données prévus sont susceptibles de soulever des problèmes de sécurité des connaissances ; coordonner les mesures d'atténuation avant leur diffusion.
- Formation et sensibilisation : fournir des conseils aux chercheurs et chercheuses, aux superviseurs et superviseuses, aux administrateurs et administratrices et aux dirigeants et dirigeantes

Ce rôle ne doit pas s'apparenter à un contrôle général de la collaboration internationale. Les bonnes pratiques sont fondées sur les risques, proportionnées et transparentes, et concilient la liberté académique et les obligations en matière de sécurité.

Service juridique et de contrôle à l'exportation : assistance pour les questions réglementaires Ce service fournit l'interprétation juridique et réglementaire officielle qui sous-tend les autres fonctions.

⁵ Voir également la recommandation du groupe de travail national ici : [swissuniversities – Sécurité des connaissances en Suisse : un cadre stratégique pour les établissements d'enseignement supérieur et les autorités](#), section 4.1, ainsi que la recommandation n° 2 du rapport « Ouverture et sécurité : deux piliers, un système ».

⁶ Voir également la recommandation du groupe de travail national ici : [swissuniversities – Sécurité des connaissances en Suisse : un cadre stratégique pour les établissements d'enseignement supérieur et les autorités](#), section 4.2 et annexe 3.

Responsabilités types

- Classification des exportations et vérification des sanctions
- Examen des contrats
- Conseils en matière de propriété intellectuelle
- Conformité en matière de protection des données et de confidentialité
- Tenue des registres et assistance aux audits
- Relations avec les autorités nationales

4. Comment ces quatre services s'articulent entre eux

Service d'assistance « Open Science » → Gestion des données (Data Stewardship) → Responsable de la sécurité des connaissances → Questions juridiques et contrôles à l'exportation

Par exemple :

- Un chercheur ou une chercheuse souhaite publier un article et mettre à disposition un ensemble de données.
- Le service d'assistance à la science ouverte l'aide à déposer ses données dans un référentiel et à gérer les licences.
- La gestion des données vérifie la conformité aux principes FAIR, la confidentialité et les éventuels risques liés à la sécurité.
- Si le projet implique des données sensibles, le responsable de la sécurité des connaissances intervient dans l'évaluation et la gestion des risques.
- Si des questions relatives aux technologies contrôlées ou aux sanctions se posent, le service juridique/contrôles à l'exportation détermine les exigences légales applicables.
- Le chercheur ou la chercheuse bénéficie ainsi d'un parcours décisionnel coordonné, plutôt que de conseils contradictoires émanant de plusieurs services.

3. **Recommandation n° 3 : mettre en œuvre des programmes de formation et de sensibilisation à la sécurité des connaissances**

La condition préalable à la mise en œuvre réussie des mesures de sécurité des connaissances dans le fonctionnement des institutions est la sensibilisation et l'adhésion de la communauté des chercheurs et chercheuses. Lancer un mouvement ascendant, plutôt que d'imposer des exigences descendantes, s'avérera plus efficace et durable. Les outils suivants ont pour but d'aider les institutions à sensibiliser et à informer sur la sécurité des connaissances (dans le cadre de la science ouverte).

- **Livrable du projet** : Ce qu'il faut faire et ne pas faire en matière de sécurité des connaissances dans le cadre de la science ouverte (annexe 1)

Contenu : Outil concis de réflexion et d'orientation, destiné à sensibiliser le grand public

Destinataires : chercheurs et chercheuses

Quand : outil intemporel

- **Livrable du projet** : diapositives sur « Introduction à la sécurité des connaissances dans la science ouverte » (annexe 2)

Contenu : diapositives présentant la sécurité des connaissances dans la science ouverte, à adapter en fonction des besoins et des priorités de chaque établissement.

*Destinataires: l'administration universitaire, chargée de sensibiliser les chercheurs et chercheuses.
Quand : outil intemporel ; peut être partagé lors de l'intégration des nouveaux collaborateurs et collaboratrices et/ou lors de formations régulières.*

u^b

4. Recommandations 5, 6 et 7 : Mesures de sécurité des connaissances dans la science ouverte et la science ouverte en tant que mesure de sécurité des connaissances

Les outils suivants ont pour objectif d'aider les institutions à intégrer la sécurité des connaissances dans les pratiques de la science ouverte et à utiliser ces dernières comme des outils de sécurité des connaissances.

- **Livrable du projet :** Plan de gestion de la sécurité des connaissances (pour la science ouverte), KSMP (Knowledge Security Management Plan) (annexe 3)

Contenu : proposition d'un questionnaire complet pouvant servir d'outil d'évaluation des risques liés à la sécurité des connaissances lors de la mise en œuvre de la science ouverte. Il s'agit d'un outil permettant de mettre en évidence certains risques et de sensibiliser les acteurs et actrices concernés.

Destinataires : chercheurs et chercheuses en collaboration avec les gestionnaires de données (data-stewards) et les responsables de la sécurité des connaissances.

Quand : le plus tôt possible dans le processus de recherche, mais au plus tard avant la publication des données.

- **Livrable du projet :** Arbre de décision sur le partage des données (sécurité des connaissances dans le cadre de la science ouverte) (annexe 4)

Contenu : Un arbre de décision pratique qui complète et rend opérationnel le plan de gestion de la sécurité des connaissances (pour la science ouverte). Le plan de gestion de la sécurité des connaissances (KSMP) peut clarifier ou fournir des indications sur la manière de répondre aux questions posées dans l'arbre de décision.

Destinataires : chercheurs et chercheuses, éventuellement en collaboration avec les gestionnaires de données (data-stewards) et les responsables de la sécurité des connaissances.

Quand : dès que possible au cours du processus de recherche, mais au plus tard avant la publication des données.

- **Livrable du projet :** Risques liés à la sécurité des connaissances dans la science ouverte : mesures d'atténuation des risques (annexe 5)

Contenu : Compilation de mesures visant à atténuer les risques identifiés dans le Plan de gestion de la sécurité des connaissances. Peut être utilisé comme outil de suivi du KSMP ou de l'arbre de décision, une fois que les risques ont été identifiés et/ou qu'une décision a été prise concernant le niveau de restriction d'un ensemble de données.

Destinataires : chercheurs et chercheuses, en collaboration avec les gestionnaires de données (data-stewards) et les responsables de la sécurité des connaissances.

Quand : dès que les risques sont identifiés, mais au plus tard avant la publication des données.

5. Mesures incitatives et harmonisation de l'évaluation

La sécurité des connaissances et la science ouverte peuvent toutes deux être renforcées par des mesures incitatives et une harmonisation du système d'évaluation d'une institution, en complément

des éventuelles normes CoARA. L’objectif est de récompenser les chercheurs et chercheuses pour leur ouverture responsable et la conduite sécurisée de leurs recherches.

Par exemple, les éléments suivants peuvent être intégrés dans un cadre existant de critères de promotion :

Domaine	Exemple d’indicateur
Accès libre	Pourcentage de publications librement accessibles
Données ouvertes	Ensembles de données conformes aux principes FAIR déposés
Reproductibilité	Code FAIR, flux de travail, protocoles
Engagement du public	Science citoyenne et impact sociétal
Collaboration responsable	Achèvement des procédures de diligence raisonnable
Pratiques sécurisées en matière de données	Traitement approprié des données sensibles

De la même manière, des prix institutionnels pourraient être décernés pour ces mêmes activités et les subventions internes pourraient prendre en compte les critères de la science ouverte et de la sécurité des connaissances.

u^b

Chapitre 2

Autres outils et recommandations en matière d'évaluation et de classification des risques (indépendamment de la science ouverte)

u^b

Dans le chapitre 3 du rapport « Openness and Security: Two Pillars, One System », nous analysons les facteurs qui engendrent ou accentuent les risques liés à la sécurité des connaissances. Les outils suivants aident les institutions à évaluer la probabilité de risques juridiques et de sécurité au-delà de la science ouverte, en fonction de ces facteurs (contenu de la recherche (résultats), partenaires et infrastructure).

1. Conseils complets ou évaluations des risques

Les deux outils suivants couvrent plusieurs risques juridiques et de sécurité et ne s'inscrivent donc pas dans l'une des catégories (contenu, partenaires, infrastructure).

- Gouvernement des Pays-Bas (2022) : [Lignes directrices nationales en matière de sécurité des connaissances](#)
Contenu : Conseils sur l'évaluation des menaces, le cadre juridique, l'évaluation des risques, la gestion des risques, les partenariats internationaux, le recrutement et la cybersécurité
Destinataires : les établissements d'enseignement supérieur et leurs dirigeants et dirigeantes
Quand : Avant ou pendant la mise en place des structures de gouvernance institutionnelle
- DLR Projektträger/Safeguarding Science (2024) : [Due Diligence in Science](#)
Contenu : Conseils portant principalement sur les risques liés aux recrutements et aux collaborations internationales
Destinataires : les établissements d'enseignement supérieur et leurs dirigeants et dirigeantes
Quand : Avant ou pendant la mise en place des structures de gouvernance institutionnelle

2. Contenu

2.1 Soumission aux contrôles à l'exportation

- Listes suisses de contrôle à l'exportation
 - [Loi sur le contrôle des biens](#)
 - [Ordonnance sur le contrôle des biens](#)
 - [Loi sur le matériel de guerre](#)
 - [Ordonnance sur le matériel de guerre](#)
 - Ordonnance sur le contrôle des produits chimiques (en [allemand](#), [français](#) ou [italien](#))
 - Ordonnance sur l'exportation et le courtage de biens destinés à la surveillance des communications par Internet et par téléphonie mobile (en [allemand](#), [français](#) ou [italien](#))
 - Annexes répertoriant les biens soumis à un contrôle à l'exportation (en [allemand](#), [français](#) ou [italien](#))
 - Réglementations étrangères à portée extraterritoriale Les réglementations américaines en matière de sanctions, d'embargos et de contrôles à l'exportation ont

un caractère extraterritorial. Elles s'appliquent dans le monde entier si certains critères de rattachement sont remplis :

- Personnes américaines : tous les citoyens et citoyennes américains, toutes les personnes résidant aux États-Unis et les personnes titulaires d'un titre de séjour américain (par exemple, une « green card »), quel que soit leur lieu de résidence ; toutes les personnes physiques et morales résidant ou domiciliées aux États-Unis ; et toutes les entreprises domiciliées aux États-Unis ainsi que leurs succursales étrangères.
- Produits américains, y compris les produits composés d'au moins 10 % ou 25 % de composants d'origine américaine (par exemple, un drone utilisant un logiciel américain pour son pilotage).
- Régimes de contrôle des exportations américains :
 - Export Administration Regulation (EAR) : biens à double usage ([Commerce Control List](#))
 - [International Traffic in Arms Regulations \(ITAR\)](#) : biens militaires
- Aide à la recherche dans les listes de biens :
 - Les listes de biens ne sont disponibles qu'en allemand, en français ou en italien. Si vous avez besoin de ces listes dans une autre langue, vous pouvez consulter la liste des biens à double usage de l'UE (annexe 1 du [règlement \(UE\) 2021/821](#)), disponible dans toutes les langues de l'UE. Elle n'est pas identique à 100 % à la liste suisse ; veuillez donc à vérifier si l'entrée que vous avez trouvée correspond bien à celle de la liste suisse.
 - Index par mots-clés permettant de déterminer si un bien, une technologie ou un logiciel donné est soumis à des contrôles à l'exportation
 - Office fédéral de l'économie et du contrôle des exportations (BAFA) : [glossaire commun et non contraignant pour la partie I de la liste des exportations et l'annexe I du règlement de l'UE sur les biens à double usage](#) (en allemand). Cet index par mots-clés se base sur la liste des biens à double usage de l'UE ; vous devez donc vérifier si l'entrée que vous avez trouvée est identique dans la liste suisse.
 - Bureau de l'industrie et de la sécurité (BIS) : [Liste interactive des contrôles commerciaux](#). Il s'agit de la liste américaine des biens à double usage, qui peut faire l'objet d'une recherche par mots-clés. Là encore, la liste suisse n'étant pas identique à 100 % à la liste américaine, vous devez vérifier si l'entrée que vous avez trouvée figure également dans la liste suisse.

2.2 Listes des technologies critiques

- DLR Projektträger/Safeguarding Science (2026) : [Listes des technologies critiques et sensibles – champ d'application, objectif et public visé](#) (cette publication présente les listes élaborées par différents acteurs et pays)
- [Liste européenne des technologies critiques](#)
- Liste américaine des technologies critiques et émergentes ([janvier 2026](#))
- [Liste canadienne des technologies sensibles](#)
- Liste des technologies critiques de l'ETH (mentionnée dans cet article : « [Double usage et sanctions : ces applications nécessitent un contrôle de sécurité](#) » – Staffnet | ETH Zurich)

2.3 Détermination du potentiel de double usage des projets de recherche

- **Livrable du projet** : Questionnaire sur le potentiel de double usage (annexe 6)

Contenu : Questionnaire complet visant à déterminer le potentiel de double usage d'un projet de recherche donné dans les domaines de l'intelligence artificielle/de l'apprentissage automatique, de la biotechnologie, de la chimie, de la robotique, de la cybersécurité, de la science des matériaux, des systèmes énergétiques, des technologies quantiques, de l'aérospatiale, de la biologie synthétique ou des neurosciences. Un outil de sensibilisation permettant d'identifier les risques, de définir des stratégies d'atténuation ou de déterminer les besoins en matière de surveillance institutionnelle ou gouvernementale.

Destinataires : chercheurs et chercheuses.

Quand : Tout au long du cycle de vie de la recherche : lors de la planification du projet, chaque fois qu'un projet entre dans une nouvelle phase ou produit des résultats inattendus, avant de transférer des résultats ou du matériel à des collaborateurs et collaboratrices, et avant la publication ou toute autre diffusion des résultats de la recherche.

- Institut Robert Koch (2013) : [Potentiel de double usage de la recherche en sciences de la vie](#) (section 3)

Contenu : Le Code de conduite de l'Institut Robert Koch pour l'évaluation et l'atténuation des risques établit des principes et des procédures visant à identifier, évaluer et atténuer le potentiel de double usage de la recherche dans les sciences de la vie, de la santé et médicales.

Destinataires : Principalement aux chercheurs et chercheuses, responsables de projet, en particulier celles et ceux qui mènent des recherches en sciences de la vie impliquant des agents pathogènes, des toxines ou d'autres recherches présentant des implications potentielles de double usage.

Quand : Tout au long du cycle de vie de la recherche : lors de la planification du projet, chaque fois qu'un projet entre dans une nouvelle phase ou produit des résultats inattendus, avant de transférer des résultats ou du matériel à des collaborateurs et collaboratrices, et avant la publication ou toute autre diffusion des résultats de la recherche.

- Bureau néerlandais de biosécurité (2021) : « [Dual-use Quickscan](#) »

Contenu : Le « Dual-Use Quickscan » est un outil d'auto-évaluation en ligne qui aide les chercheurs et chercheuses en sciences de la vie à identifier les aspects potentiels de double usage de leurs travaux grâce à un questionnaire structuré, et qui les sensibilise aux risques liés à la biosécurité.

Destinataires : chercheurs et chercheuses travaillant sur des micro-organismes ou sur des connaissances et technologies biologiques connexes.

Quand : À n'importe quelle étape du cycle de vie de la recherche, de la conception du projet à la publication.

- Centre commun de recherche et Université de Liège : [plateforme web TIM Dual-Use](#) (projet STRIKE, unités G.II.7 et T.5)

Contenu : TIM Dual-Use est une plateforme web d'exploration de textes qui recense les publications scientifiques, les brevets et les projets de recherche financés par l'UE afin d'identifier les travaux de recherche présentant un intérêt potentiel en matière de double usage, sur la base de la liste de contrôle des biens à double usage de l'UE et des technologies émergentes. Elle favorise la sensibilisation, l'analyse des tendances et la conformité institutionnelle en aidant les utilisateurs et utilisatrices à identifier les résultats de recherche potentiellement sensibles. Elle peut être utilisée pour détecter rétrospectivement (c'est-à-dire après publication) les recherches à double usage ou celles impliquant des biens soumis à des contrôles à l'exportation.

Destinataires : instituts de recherche, universités, décideurs et décideuses politiques et les personnes professionnelles du contrôle des exportations.

Quand : Pour passer au crible les résultats de recherche existants et surveiller les technologies à double usage à des fins de sensibilisation, de conformité et d'analyse stratégique.

3. Partenaires

3.1 Outils d'évaluation complets

- **Livrable du projet** : auto-évaluation de la sécurité des connaissances destinée aux chercheurs et chercheuses et grille d'évaluation destinée à la direction de l'établissement (annexe 7)

Contenu : Une auto-évaluation destinée aux chercheurs et chercheuses souhaitant s'engager dans des collaborations internationales, qui analyse et sensibilise aux risques liés à la sécurité des connaissances. La matrice d'accompagnement (facultative) permet à la direction de l'université d'évaluer l'auto-évaluation à l'aide d'un système de feux tricolores.

Destinataires : L'auto-évaluation s'adresse aux chercheurs et chercheuses qui entament une nouvelle collaboration internationale. La matrice d'évaluation est un outil destiné à la direction de l'université qui facilite la prise de décision.

Quand : Avant la conclusion d'une collaboration internationale.

- Service allemand d'échanges universitaires/Kiwi (2025) : [La liste de contrôle KIWi sur la sécurité des connaissances](#) (en allemand)

Contenu : La liste de contrôle KIWi sur la sécurité des connaissances est un outil pratique d'auto-évaluation qui aide à identifier et à analyser les risques liés à la sécurité des connaissances dans le cadre de collaborations de recherche internationales, grâce à une série structurée de questions portant sur les partenaires, le financement, les contrôles à l'exportation, la propriété intellectuelle et l'éthique de la recherche.

Destinataires : chercheurs et chercheuses individuels, la direction ou l'administration des établissements lors de la mise en œuvre de processus institutionnels.

Quand : Avant ou pendant la mise en place de collaborations de recherche internationales, dans le cadre d'une première évaluation des risques.

- Commission européenne (2024) : [Sécurité de la recherche – Éléments constitutifs de l'évaluation des risques](#)

Contenu : Les « Éléments constitutifs de l'évaluation des risques » de la Commission européenne fournissent un cadre pour évaluer les risques liés à la sécurité de la recherche dans les collaborations internationales en matière de recherche et d'innovation. Ils proposent une évaluation structurée et adaptée au contexte, couvrant le domaine de recherche, les partenaires, le contexte national et les facteurs spécifiques au projet, afin de favoriser une prise de décision éclairée plutôt que de restreindre la collaboration.

Destinataires : les organismes de recherche, les organismes de financement de la recherche et aux établissements d'enseignement supérieur.

Quand : Avant de mettre en place des partenariats de recherche internationaux ou d'octroyer des financements à la recherche.

3.2 Embargos et sanctions

- Suisse :
 - CH-SECO : [Moteur de recherche permettant d'identifier les personnes ou entités faisant l'objet de sanctions](#)

u^b

- CH-SECO : [Mesures de sanctions suisses](#) (contenu disponible en allemand, français ou italien)
- Dispositions étrangères à application extraterritoriale
(Les sanctions et embargos américains s'appliquent à tous les citoyens américains et aux titulaires d'une carte verte, quel que soit leur lieu de résidence. Les sanctions de l'UE doivent être respectées par tous les citoyens de l'UE et toutes les personnes morales constituées ou enregistrées en vertu du droit d'un État membre de l'UE, quel que soit leur pays de résidence ou de domicile. Il en va de même pour les citoyens britanniques et les personnes morales en ce qui concerne les sanctions britanniques)
 - Office américain du contrôle des avoirs étrangers (OFAC) : [programmes de sanctions et informations par pays](#)
 - OFAC (États-Unis) : [Recherche dans la liste des sanctions](#)
 - Sanctions et embargos de l'UE : [carte des sanctions](#)
 - Sanctions et embargos britanniques : [sanctions commerciales, embargos sur les armes et autres restrictions commerciales – GOV.UK](#)

3.3 Évaluation des réseaux d'institutions ou de chercheurs et chercheuses

Les outils suivants sont des outils commerciaux assez coûteux et leur intégration dans les processus de diligence raisonnable d'une institution peut créer des dépendances. La plupart des outils présentés sont axés sur la détection de réseaux impliquant des partenaires sanctionnés ou militaires.

La Commission européenne travaille actuellement (2026) au développement d'une plateforme publique de diligence raisonnable.

- [China Defence Universities Tracker](#)

Un outil accessible par abonnement qui surveille plus de 180 entités chinoises liées à la défense, au renseignement et à la recherche technologique. Il permet aux utilisateurs et utilisatrices d'explorer les capacités potentielles à double usage, de consulter les listes de sanctions pertinentes et d'évaluer les risques liés à la collaboration internationale. Le Tracker est conçu comme une ressource analytique ciblée permettant de comprendre les relations institutionnelles. Il ne s'agit ni d'un outil de profilage des individus, ni d'une base justifiant des restrictions générales, et il ne doit pas être interprété comme une liste noire. Son objectif est plutôt de favoriser une prise de décision éclairée et proportionnée. Bien que très complet, le Tracker n'est pas exhaustif. Les institutions qui n'y figurent pas peuvent néanmoins présenter des risques, et les entrées de la base de données peuvent ne pas refléter l'étendue ou la nature complète des liens d'une institution avec les secteurs de la défense et de la sécurité.

- [Strider Technologies](#)

Strider est un outil accessible par abonnement qui offre une vue d'ensemble externe et open source du paysage mondial de la recherche. Il identifie les divergences entre l'expérience déclarée d'un individu et les archives publiques, en tenant compte des publications antérieures, de l'engagement institutionnel et de la présence professionnelle à long terme. Il propose également une vue d'ensemble unifiée des organisations, du personnel et des unités de recherche, ainsi qu'un suivi continu des risques liés aux États-nations.

- [Kharon](#)

Kharon est une plateforme de veille des risques qui facilite la conformité aux sanctions, la diligence raisonnable en matière de contrôle des exportations, la gestion des risques liés à la chaîne

d'approvisionnement et la vérification des tiers. Elle utilise des informations issues de sources ouvertes, l'analyse de réseaux et l'analyse de données pour identifier les relations cachées entre des individus, des organisations, des structures de propriété et des acteurs et actrices soumis à des restrictions ou présentant un risque élevé.

- [Xapien](#)

Xapien est une plateforme d'évaluation des risques liés aux tiers et de diligence raisonnable alimentée par l'IA. Elle automatise les recherches d'antécédents sur les personnes et les organisations en combinant des informations issues du Web ouvert, des sources d'actualité, des registres du commerce, des listes de sanctions et de surveillance, ainsi que d'autres ensembles de données commerciales, pour les regrouper dans un rapport unique étayé par des sources fiables.

- [Dimensions Research Security](#)

Cet outil accessible par abonnement cartographie les affiliations internationales, les collaborations et les flux de financement. Il permet d'identifier les doubles mandats, la participation à des programmes de recrutement de talents étrangers et les liens potentiels avec des entités sanctionnées, aidant ainsi les institutions à mieux évaluer et gérer les risques liés à la collaboration.

3.4 Listes d'institutions critiques en raison de leur proximité avec le secteur militaire

- Gouvernement du Canada : [Liste des organismes de recherche désignés](#)
- [Entités identifiées comme des entreprises militaires chinoises opérant aux États-Unis](#)
- [Liste japonaise des utilisateurs finaux](#)
- Institut australien de politique stratégique : [outil de suivi des universités chinoises spécialisées dans la défense](#)

3.5 Autres considérations

- [Indice de l'État de droit du World Justice Project](#)
- [Indice de démocratie](#)
- [Indice des droits de l'homme 2025 : classement des meilleurs et des pires pays](#)
- [Indice de liberté humaine](#)
- [Indice de Freedom House](#)
- [Indice de la liberté académique](#)
- [Indice de perception de la corruption](#)

4. Infrastructures

Les risques liés à la sécurité des connaissances en matière d'infrastructures peuvent être évalués à l'aide du plan de gestion de la sécurité des connaissances proposé au chapitre 1, section 4.

Annexes

Click to download annexes in English:

1. [Do's and Don'ts for Knowledge Security in Open Science](#)
2. [Slides on "Introduction to Knowledge Security in Open Science"](#)
3. [Knowledge Security Management Plan \(for Open Science\)](#)
4. [Decision tree on data sharing \(Knowledge Security in Open Science\)](#)
5. [Knowledge Security risks in Open Science: mitigation measures](#)
6. [Questionnaire on Dual-use potential](#)
7. [Checklist for researchers and evaluation matrix for institutional management for international collaborations](#)

Traductions en français:

1. [À faire et à ne pas faire en matière de sécurité des connaissances dans le cadre de la science ouverte](#)
2. [Diapositives sur « Introduction à la sécurité des connaissances dans le cadre de la science ouverte »](#)
3. [Plan de gestion de la sécurité des connaissances \(pour la science ouverte\)](#)
4. [Arbre de décision sur le partage des données \(sécurité des connaissances dans la science ouverte\)](#)
5. [Risques liés à la sécurité des connaissances dans la science ouverte : mesures d'atténuation](#)
6. [Questionnaire sur le potentiel de double usage](#)
7. [Liste de contrôle à l'intention des chercheurs et chercheuses et matrice d'évaluation destinée à la direction des établissements dans le cadre des collaborations internationales](#)

u^b