Conseil de
l'Union européenne

Bruxelles, le 26 janvier 2024
(OR. en)

5788/24

Dossier interinstitutionnel:
2024/0012(NLE)

POLCOM 26
COMER 17
RELEX 97
DUAL USE 10
RECH 28
ENER 36
ENV 84

PROPOSITION

Origine:	Pour la secrétaire générale de la Commission européenne, Madame Martine DEPREZ, directrice
Date de réception:	25 janvier 2024
Destinataire:	Madame Thérèse BLANCHET, secrétaire générale du Conseil de l'Union européenne
N° doc. Cion:	COM(2024) 26 final
Objet:	Proposition de RECOMMANDATION DU CONSEIL sur le renforcement de la sécurité de la recherche

Les délégations trouveront ci-joint le document COM(2024) 26 final.

p.j.: COM(2024) 26 final

COMMISSION
EUROPÉENNE

Bruxelles, le 24.1.2024
COM(2024) 26 final

2024/0012 (NLE)

Proposition de

RECOMMANDATION DU CONSEIL

sur le renforcement de la sécurité de la recherche

EXPOSÉ DES MOTIFS

1. CONTEXTE DE LA PROPOSITION

• Justification et objectifs de la proposition

Comme indiqué dans la stratégie européenne en matière de sécurité économique, publiée en juin 2023[1], l'augmentation des tensions géopolitiques à l'échelle mondiale, les actions économiques hostiles, les cyberattaques et les attaques visant les infrastructures critiques, l'ingérence étrangère et la désinformation, ont mis en lumière, dans nos sociétés, nos économies et nos entreprises, des risques et des vulnérabilités. Dans certains cas, il est apparu clairement que l'Europe devait être mieux préparée face aux risques nouveaux, émergents et changeants, qui caractérisent ce contexte géopolitique désormais plus difficile.

Les technologies critiques et à double usage jouent un rôle central dans ce contexte, étant donné que certains de nos concurrents utilisent les technologies émergentes et de rupture pour renforcer leurs positions politiques, économiques et militaires. L'une des conséquences possibles serait que la recherche et l'innovation européennes subissent des influences malveillantes et fassent l'objet d'utilisations abusives nuisant à notre sécurité ou enfreignant nos normes éthiques.

Le secteur de la recherche et de l'innovation est particulièrement vulnérable en raison de son ouverture et de son internationalisation, qui font partie de son ADN. Pour renforcer la sécurité de la recherche dans le secteur de la recherche et de l'innovation dans toute l'Europe, il est donc nécessaire d'adopter une approche sur mesure fortement ancrée dans la liberté académique et l'autonomie institutionnelle, qui sont des principes fondamentaux de ce secteur.

Les établissements d'enseignement supérieur et les organismes exerçant des activités de recherche doivent naviguer dans un contexte international de plus en plus complexe et tendu. Il est du devoir de l'UE de les aider à évoluer dans cet environnement de manière responsable et sûre, dans le plein respect de la liberté académique et de l'autonomie institutionnelle.

La présente proposition de recommandation du Conseil offre, pour la première fois, une définition commune du problème et crée un sentiment d'urgence partagé. Elle fournit des orientations politiques sur ce que pourrait être une réponse politique efficace, tout en tenant compte du fait qu'une grande partie des travaux sur la sécurité de la recherche consiste à naviguer dans des «zones grises», dans lesquelles certaines formes de coopération internationale en matière de recherche et d'innovation ne peuvent pas être interdites, mais sont néanmoins indésirables parce qu'elles présentent des risques pour la sécurité de l'Union et de ses États membres ou qu'elles sont contraires à l'éthique.

• Cohérence avec les dispositions existantes dans le domaine d'action

La stratégie européenne en matière de sécurité économique repose sur une approche à trois piliers: promotion de la base économique et de la compétitivité de l'UE; protection contre les risques pesant sur la sécurité économique; et partenariat avec le plus large éventail possible de pays afin de répondre aux préoccupations communes et de défendre les intérêts communs. L'objectif de cette stratégie est de fournir un cadre pour une évaluation et une gestion solides des risques pour la sécurité économique au niveau de l'Union, au niveau national et au niveau des entreprises, tout en préservant et en renforçant notre dynamisme économique.

[1] Communication conjointe de la Commission et du haut représentant relative à la stratégie européenne en matière de sécurité économique, JOIN(2023)20 du 20.6.2023 (lien).

Dans sa communication relative à la stratégie, la Commission s'est engagée à «proposer des mesures destinées à améliorer la sécurité de la recherche, garantissant une application systématique et rigoureuse des outils susmentionnés et repérant et comblant les lacunes qui subsistent, tout en préservant l'ouverture de l'écosystème d'innovation.» La proposition de recommandation du Conseil répond à cet engagement en définissant des principes directeurs pour une internationalisation responsable et des actions stratégiques clés aux niveaux national et sectoriel pour renforcer la sécurité de la recherche et en recensant les initiatives prises au niveau de l'Union afin de soutenir les efforts des États membres et le secteur de la recherche.

La proposition de recommandation complète et s'appuie sur les travaux en cours depuis la publication par la Commission, en mai 2021, de sa communication sur l'approche mondiale de la recherche et de l'innovation[2]. Dans cette communication, la Commission a présenté une stratégie visant à préserver l'ouverture dans la coopération internationale en matière de recherche et d'innovation, tout en promouvant des conditions de concurrence équitables et de réciprocité reposant sur des valeurs fondamentales.

Dans ses conclusions de septembre 2021 sur l'approche mondiale, le Conseil a prévu un mandat pour les travaux visant à lutter contre les ingérences étrangères dans la recherche et l'innovation[3]. Sur cette base, d'importantes initiatives de suivi ont été prises, notamment l'adoption par la Commission, en janvier 2022, d'un document de travail de ses services sur la lutte contre les ingérences étrangères dans la R&I[4]. Ce document est utilisé par les États membres et les parties prenantes de la R&I comme base pour discuter de la sécurité de la recherche et comme source d'inspiration pour élaborer leurs propres lignes directrices et outils sur mesure. Le Parlement européen a salué ce document dans sa résolution du 6 avril 2022 sur l'approche mondiale[5]. La Commission a également facilité l'apprentissage par les pairs entre les États membres au moyen d'un exercice d'apprentissage mutuel et met actuellement en place un guichet unique en ligne qui rassemblera tous les documents, rapports et outils pertinents sur la sécurité de la recherche.

En outre, un débat d'orientation sur la sécurité des connaissances et l'internationalisation responsable s'est tenu au sein du Conseil «Compétitivité» de mai 2023 et a fourni des indications et des orientations précieuses pour la présente proposition.

- **Cohérence avec les autres politiques de l'Union**

La recommandation proposée relève d'un ensemble complet de mesures faisant suite à la stratégie européenne en matière de sécurité économique du 20 juin 2023. Ainsi, la proposition est l'un des éléments constitutifs d'une démarche globale visant à renforcer la sécurité économique globale de l'UE. Le 3 octobre 2023, la Commission a adopté une recommandation dans laquelle elle a identifié les domaines technologiques critiques pour la sécurité économique de l'UE en vue d'une évaluation approfondie des risques avec les États

---

2 Communication de la Commission intitulée «L'approche mondiale de la recherche et de l'innovation - La stratégie de coopération internationale de l'Europe dans un monde en mutation», COM(2021)252 du 18.5.2021 (lien).

3 Conclusions du Conseil sur l'approche mondiale de la R&I du 28.9.2021 (lien), notamment les points 3, 11 et 23.

4 Commission européenne, direction générale de la recherche et de l'innovation, *Tackling R&I foreign interference – Staff working document* (document de travail des services de la Commission sur la lutte contre les ingérences étrangères dans la R&I), Office des publications de l'Union européenne, 2022 (lien).

5 Résolution du Parlement européen sur l'approche mondiale de la recherche et de l'innovation, P9_TA(2022)0112 du 6.4.2022 (lien).

membres[6]. Les résultats de cette évaluation des risques pourraient servir de base à d'autres mesures visant à mettre en œuvre la stratégie européenne en matière de sécurité économique, y compris des mesures visant à renforcer la sécurité de la recherche. La consultation publique lancée par le livre blanc sur les investissements sortants sera examinée, en particulier en ce qui concerne les éléments pertinents pour la recherche et l'innovation.

En outre, la recommandation proposée complète de manière cohérente plusieurs autres initiatives de l'UE, notamment:

– les travaux réalisés en matière de lutte contre les menaces hybrides, dans le cadre de la stratégie de l'UE pour l'union de la sécurité[7] et de la boussole stratégique en matière de sécurité et de défense[8];

– les règles européennes applicables à l'exportation hors de l'UE de biens et technologies à double usage, telles que définies dans le règlement de l'UE sur le contrôle des exportations[9]. Afin d'aider les établissements d'enseignement supérieur et les organismes exerçant des activités de recherche, la Commission a publié en septembre 2021 une recommandation sur les programmes de conformité pour la recherche portant sur les biens à double usage[10].

– le train de mesures de défense de la démocratie, adopté par la Commission en décembre 2023 en amont des élections européennes de juin 2024. Ce train de mesures a pour objectif de lutter contre les menaces d'ingérences étrangères en renforçant la transparence des activités de représentation d'intérêts, tout en encourageant l'engagement civique et la participation des citoyens à nos démocraties[11].

2. BASE JURIDIQUE, SUBSIDIARITÉ ET PROPORTIONNALITÉ

• Base juridique

L'initiative relève du domaine politique «recherche et développement technologique» dans lequel l'Union et ses États membres partagent des compétences, conformément à l'article 4, paragraphe 3, du traité sur le fonctionnement de l'Union européenne (TFUE). La proposition de recommandation du Conseil repose sur l'article 182, paragraphe 5, du TFUE, en liaison avec l'article 292 de ce dernier.

L'article 182, paragraphe 5, du TFUE permet de compléter les actions prévues dans le programme-cadre pluriannuel en autorisant le Parlement européen et le Conseil, statuant conformément à la procédure législative ordinaire et après consultation du Comité

---

6 Recommandation de la Commission du 3.10.2023 relative aux domaines technologiques critiques pour la sécurité économique de l'UE en vue d'une évaluation approfondie des risques avec les États membres, C(2023) 6689 (lien).

7 Communication de la Commission relative à la stratégie de l'UE pour l'union de la sécurité, COM(2020) 605 du 24.7.2020 (lien).

8 Conseil de l'UE: Une boussole stratégique en matière de sécurité et de défense, ST 7371/22 du 21.3.2022 (lien).

9 Règlement (UE) 2021/821 instituant un régime de l'UE de contrôle des exportations, du courtage, de l'assistance technique, du transit et des transferts en ce qui concerne les biens à double usage (lien).

10 Recommandation de la Commission relative aux programmes internes de conformité pour les contrôles de la recherche portant sur les biens à double usage [...], 2021/1700 du 15.9.2021 (lien).

11 Communication de la Commission relative à la défense de la démocratie, COM(2023) 630 du 12.12.2023 (lien).

économique et social, à établir les mesures nécessaires à la mise en œuvre de l'espace européen de la recherche.

L'article 292 du TFUE constitue la base juridique permettant au Conseil d'adopter des recommandations sur proposition de la Commission.

L'initiative ne propose ni un renforcement du pouvoir réglementaire de l'Union ni des engagements contraignants pour les États membres. Ces derniers décideront, en fonction de leur situation nationale, de la manière de mettre en œuvre la présente recommandation du Conseil.

- **Subsidiarité (en cas de compétence non exclusive)**

La présente proposition est conforme au principe de subsidiarité prévu à l'article 5, paragraphe 3, du traité sur l'Union européenne (TUE).

Si les gouvernements nationaux sont les mieux placés pour nouer le dialogue avec leurs universités et autres organismes de recherche et les aider à prendre les mesures nécessaires, une coopération et une coordination au niveau de l'UE sont indispensables pour assurer le bon fonctionnement de l'Espace européen de la recherche et réduire les disparités dues aux différences entre les mesures nationales en matière de sécurité de la recherche.

À l'heure actuelle, le niveau de sensibilisation aux risques n'est pas uniforme dans l'ensemble de l'UE. Un nombre croissant d'États membres et d'acteurs de la R&I ont commencé à élaborer et à introduire des mesures de sauvegarde spécifiques, tandis que d'autres ne semblent guère conscients de cette nécessité, créant ainsi des vulnérabilités qui pourraient facilement être exploitées. Un niveau minimal de cohérence de l'approche dans l'ensemble de l'UE est donc essentiel.

- **Proportionnalité**

La présente proposition est conforme au principe de proportionnalité prévu à l'article 5, paragraphe 4, du TUE. Ni le contenu ni la forme de la présente proposition de recommandation du Conseil n'excèdent ce qui est nécessaire pour atteindre l'objectif consistant à atteindre un niveau minimal de cohérence de l'approche dans l'ensemble de l'UE.

Le statut juridique de cette initiative devrait garantir l'adhésion et l'engagement des États membres. Dans le même temps, elle devrait se fonder à titre prépondérant sur l'autonomie du secteur de la R&I, dans le respect de la liberté académique et de l'autonomie institutionnelle.

La proposition de recommandation aide les États membres et les organismes exerçant des activités de recherche à élaborer et à mettre en œuvre des politiques et des mesures à la fois efficaces et proportionnées. Elle met en exergue l'importance de la coopération et de l'ouverture internationales suivant le principe «aussi ouvert que possible, mais aussi fermé que nécessaire». Elle présente également les mesures de gestion de risques qui pourraient être introduites dans le plein respect de la liberté académique et de l'autonomie institutionnelle, en évitant la discrimination et la stigmatisation.

- **Choix de l'instrument**

La proposition de recommandation du Conseil fournit des orientations aux États membres sur la manière d'identifier et de faire face efficacement aux risques en matière de sécurité de la recherche. Elle recommande aux États membres de soutenir leur secteur de la recherche et de l'innovation, en prenant des mesures appropriées pour améliorer la sensibilisation et renforcer la résilience. Une recommandation du Conseil s'appuyant sur le document de travail des

services de la Commission sur la lutte contre les ingérences étrangères dans la R&I garantirait l'implication et l'engagement actifs des États membres au niveau politique.

Une recommandation ou une communication de la Commission pourrait également être envisagée. Sur le plan du contenu, elles pourraient en principe couvrir les mêmes questions qu'une recommandation du Conseil. Toutefois, ces instruments ont en commun qu'ils n'impliquent pas ou n'engagent pas activement les États membres. Rien ne garantit que les destinataires partagent l'approche proposée et le sentiment d'urgence.

Une initiative juridiquement contraignante, telle qu'une directive ou un règlement, qui réglementerait la coopération internationale en matière de recherche et d'innovation de manière à ce que les risques soient correctement identifiés et maîtrisés par les États membres, garantirait la cohérence juridique dans l'ensemble de l'Union. Toutefois, le principal inconvénient d'un instrument contraignant dans ce contexte spécifique est qu'il serait très difficile de le concevoir de telle manière que la répartition des compétences entre l'UE et les États membres, ainsi que les principes de liberté académique et d'autonomie institutionnelle, soient respectés.

Pour ces raisons, une proposition de recommandation du Conseil est considérée comme l'instrument d'intervention approprié pour résoudre les problèmes soulevés.

3. RÉSULTATS DES ÉVALUATIONS EX POST, DES CONSULTATIONS DES PARTIES INTÉRESSÉES ET DES ANALYSES D'IMPACT

• Évaluations ex post/bilans de qualité de la législation existante

Sans objet.

• Consultation des parties intéressées

La proposition de recommandation du Conseil s'appuie sur le document de travail des services de la Commission de janvier 2022 sur la lutte contre les ingérences étrangères dans la R&I. Tout au long de l'année 2023 a eu lieu un exercice d'apprentissage mutuel sur la lutte contre les ingérences étrangères dans la R&I dans le cadre duquel des experts de 13 États membres ont échangé leur expérience et leur expertise nationales. En outre, trois réunions consacrées à la sécurité de la recherche avec des experts des États membres ont eu lieu dans le cadre du réseau européen de connaissances sur la Chine.

L'élaboration de la proposition a également été étayée par un appel à contributions, qui a été ouvert pour une consultation publique sur la page web «Donnez votre avis» du 6 décembre 2023 au 3 janvier 2024. La Commission a reçu 56 contributions, dont près de 40 % provenaient d'établissements universitaires ou de recherche. Outre l'appel à contributions, une réunion de consultation ciblée a eu lieu le 15 décembre 2023, avec la participation de représentants des principales organisations de parties prenantes au niveau de l'UE dans le domaine de la recherche et de l'innovation.

• Obtention et utilisation d'expertise

Outre les contributions reçues au cours du processus de consultation, la proposition s'appuie sur de nombreux éléments probants, rapports et études collectés ces dernières années. Les principales sources d'éléments probants comprennent un ensemble important et constamment élargi de documents d'orientation sur la sécurité de la recherche élaborés par les États

membres et les organisations sectorielles[12], ainsi que des rapports sur cette problématique établis par des groupes de réflexion, des organisations de parties prenantes et des conseils consultatifs.

Une attention particulière a également été accordée aux politiques en matière de sécurité de la recherche que certains de nos partenaires internationaux ont mises en œuvre ces dernières années, ainsi qu'aux connaissances et à l'expérience qu'ils en ont retirées. Il s'agit notamment des politiques menées par des pays tels que les États-Unis, le Royaume-Uni, l'Australie et le Canada[13]. Dans le cadre du dialogue multilatéral sur les valeurs et les principes[14], un atelier sur la sécurité de la recherche a eu lieu en décembre 2023, auquel ont activement participé les partenaires internationaux.

- **Analyse d'impact**

Aucune analyse d'impact n'a été réalisée, compte tenu de la complémentarité des activités avec les initiatives des États membres et du caractère non contraignant et volontaire des activités proposées.

L'impact de la recommandation dépend dans une large mesure de l'engagement et de la volonté d'agir des États membres et des organisations sectorielles et est donc impossible à anticiper. La proposition, si le Conseil l'adopte et que les États membres s'engagent à mettre en œuvre ses recommandations avec l'appui du secteur, a le pouvoir de renforcer la recherche par l'amélioration du niveau de sensibilisation et le renforcement de la résilience dans toute l'Europe.

- **Réglementation affûtée et simplification**

La proposition n'est pas liée au programme de simplification législative REFIT de la Commission. Néanmoins, tout est mis en œuvre pour assurer l'utilisation efficiente de ressources limitées, notamment par le recours aux structures de gouvernance existantes de l'espace européen de la recherche et aux structures existantes en matière de communication d'informations. En outre, il est souligné dans la recommandation proposée qu'il convient d'éviter toute charge administrative inutile pour le secteur lors de l'introduction de mesures de sauvegarde et que, dans le cadre du financement de la recherche, le délai d'octroi des financements ne devrait pas être inutilement prolongé.

- **Droits fondamentaux**

L'un des principaux objectifs de la proposition est d'aider les États membres et les organismes de recherche à veiller à ce que la coopération internationale en matière de recherche et d'innovation ne viole pas les valeurs fondamentales et les droits de l'homme. La protection des valeurs académiques fondamentales, notamment la liberté académique et l'intégrité de la recherche, occupe une place centrale dans la recommandation.

4. INCIDENCE BUDGÉTAIRE

[12] Voir, par exemple, le recueil annoté d'orientations pour une coopération sûre et fructueuse en matière de R&I («Annotated collection of guidance for secure and successful R&I cooperation») (2022), établi par DLR-PT à la demande de la Commission (lien).

[13] De plus amples informations sont disponibles, par exemple, sur les sites web suivants: pour les États-Unis (lien), pour le Royaume-Uni (lien), pour l'Australie (lien) et pour le Canada (lien).

[14] De plus amples informations concernant le dialogue multilatéral sur les valeurs et les principes peuvent être consultées à l'adresse suivante: lien.

Bien que cette initiative ne nécessite pas de ressources supplémentaires provenant du budget de l'Union, les mesures prévues dans la présente recommandation mobiliseront des sources de financement au niveau de l'Union, au niveau national et au niveau sectoriel.

En ce qui concerne le «centre européen d'expertise en matière de sécurité de la recherche» que la Commission prévoit de créer, c'est le budget actuel d'Horizon Europe qui serait mobilisé. Sur le plan de la structure organisationnelle, plusieurs pistes sont envisagées, dont la Commission poursuivra l'examen en tenant compte des préférences des États membres et des parties prenantes quant à ses fonctionnalités.

5. AUTRES ÉLÉMENTS

- **Plans de mise en œuvre et modalités de suivi, d'évaluation et d'information**

Afin de soutenir les États membres et les parties prenantes dans la mise en œuvre de la recommandation, les structures de gouvernance existantes de l'espace européen de la recherche seront pleinement exploitées. La sécurité de la recherche devrait figurer dans le prochain programme stratégique de l'espace européen de la recherche pour la période 2025-2027, actuellement élaboré en concertation avec les États membres et les parties prenantes.

Les rapports de la Commission s'appuieront sur les rapports bisannuels déjà prévus dans le cadre de l'approche mondiale de la recherche et de l'innovation. Le prochain rapport est prévu pour la mi-2025. Les États membres sont invités à présenter des plans d'action nationaux sur la manière dont ils entendent mettre en œuvre la recommandation dans un délai de 9 mois à compter de son adoption.

- **Documents explicatifs (pour les directives)**

Sans objet.

- **Explication détaillée de certaines dispositions de la proposition**

L'objectif général de l'initiative est d'aider les États membres, les établissements d'enseignement supérieur et les organismes, tant publics que privés, exerçant des activités de recherche à faire face aux risques en matière de sécurité de la recherche. Il s'agit d'empêcher que les activités de recherche, d'innovation et d'enseignement supérieur ne soient détournées ou mises à profit au détriment de la sécurité de l'UE et de ses États membres ou ne soient contraires à l'éthique. À cette fin, la proposition de recommandation du Conseil s'articule comme suit.

– L'exposé de la problématique et du contexte politique de la proposition figurant dans les considérants est suivi d'une explication de son champ d'application. Une définition de la notion de «sécurité de la recherche» est proposée, qui se fonde sur les principaux éléments empruntés aux différentes définitions utilisées au niveau international. Il est également précisé quels organismes et parties prenantes sont les principaux destinataires de la recommandation.

– Ensuite, des principes en matière d'internationalisation responsable sont proposés. Ces principes se veulent propres à l'élaboration et à la conception d'une politique répondant au problème de la sécurité de la recherche à tous les niveaux (UE, États membres ou organismes de recherche). Ils s'appuient sur les approches adoptées dans les orientations nationales et sectorielles en matière d'internationalisation responsable. Il ressort des réactions à l'appel à contributions que la communauté des parties prenantes adhère clairement à ces principes.

– La section suivante contient les recommandations proprement dites adressées aux États membres. Elle se divise en quatre sous-sections. La première sous-section contient des recommandations aux pouvoirs publics pour soutenir le secteur de la recherche et de l'innovation en créant une structure d'appui et en fournissant des orientations. La deuxième sous-section porte sur le rôle central que jouent les organismes de financement nationaux pour renforcer la sécurité de la recherche. La troisième sous-section expose des recommandations aux États membres pour soutenir les établissements d'enseignement supérieur et les organismes de recherche lorsqu'ils instaurent des politiques et des mesures de sauvegarde.

– La dernière sous-section décrit un certain nombre d'actions et d'initiatives de soutien de la Commission qui nécessitent la facilitation des États membres.

– La section finale précise les modalités de facilitation et de contrôle du suivi de la recommandation.

2024/0012 (NLE)

Proposition de

RECOMMANDATION DU CONSEIL

sur le renforcement de la sécurité de la recherche

LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 292, première et deuxième phrases, en liaison avec son article 182, paragraphe 5,

vu la proposition de la Commission européenne,

considérant ce qui suit:

(1) L'ouverture, la coopération internationale et la liberté académique occupent une place centrale dans la recherche et l'innovation d'envergure mondiale. Or, compte tenu des tensions internationales croissantes et du poids géopolitique grandissant de la recherche et de l'innovation, nos chercheurs et universitaires sont de plus en plus exposés à des risques en matière de sécurité de la recherche lorsqu'ils coopèrent au niveau international, de sorte que la recherche et l'innovation européennes subissent des influences malveillantes et font l'objet d'utilisations abusives nuisant à notre sécurité ou enfreignant nos normes éthiques. Il est donc essentiel que les établissements d'enseignement supérieur et les organismes de recherche publics et privés européens bénéficient du soutien et des moyens nécessaires pour faire face à ces risques. Des mesures de sauvegarde précises et proportionnées s'imposent pour préserver une coopération internationale ouverte et sûre.

(2) La science ouverte garantit une accessibilité maximale de la science dans l'intérêt de la science elle-même, de l'économie et de la société dans son ensemble, tandis que la coopération internationale contribue à relever efficacement les défis mondiaux. La liberté académique implique que les chercheurs sont libres de mener leurs recherches et de choisir des méthodes de recherche et des partenaires de recherche dans le monde entier, tandis que la mobilité internationale des talents de la recherche enrichit les travaux scientifiques et est essentielle pour favoriser l'innovation et réaliser des avancées scientifiques.

(3) La concurrence stratégique croissante et le retour à la politique des rapports de force conduisent à des relations de plus en plus transactionnelles entre les États. Cette évolution crée des menaces plus diversifiées, imprévisibles et souvent hybrides[1]. Compte tenu du rôle central de la technologie pour la prééminence politique, économique et militaire, certains concurrents de l'UE cherchent à acquérir une primauté mondiale dans le domaine des technologies émergentes et de rupture afin de renforcer leurs capacités militaires et de renseignement tout en menant activement des stratégies de fusion entre le civil et le militaire.

[1] Par menaces hybrides, on entend des situations dans lesquelles des acteurs étatiques ou non étatiques s'efforcent d'exploiter les vulnérabilités de l'UE à leur profit en utilisant d'une manière coordonnée une combinaison de mesures (diplomatiques, militaires, économiques, technologiques) sans que le seuil d'une guerre déclarée officiellement ne soit dépassé (lien).

(4) Les menaces hybrides peuvent toucher tous les secteurs présentant un intérêt à cet égard, mais en raison de ses caractéristiques d'ouverture, de liberté académique, d'autonomie institutionnelle et de collaboration à l'échelle mondiale, le secteur de la recherche et de l'innovation est particulièrement vulnérable. Les chercheurs et innovateurs travaillant dans l'UE sont visés afin de pouvoir intercepter les connaissances et les technologies les plus récentes, en usant parfois de méthodes trompeuses et dissimulées ou en pratiquant le vol pur et simple, mais plus souvent en exploitant une coopération universitaire internationale en apparence loyale. Outre la mise en péril de notre sécurité, ces menaces hybrides pourraient porter atteinte à la liberté académique en Europe.

(5) Les établissements d'enseignement supérieur et autres organismes exerçant des activités de recherche se meuvent, dès lors, dans un contexte international de plus en plus difficile, marqué par des risques de transfert indésirable de connaissances et de technologies critiques vers des pays suscitant des préoccupations, où elles peuvent être utilisées pour renforcer les capacités des forces militaires ou servir à des fins contraires aux valeurs fondamentales. Bien qu'elles ne soient pas toujours illicites, ces collaborations ne sont pas souhaitables car elles suscitent d'importantes préoccupations en matière de sécurité et d'éthique.

(6) Dans le droit fil de l'autonomie institutionnelle et de la liberté académique, les établissements d'enseignement supérieur et autres organismes de recherche sont responsables au premier chef du développement et de la gestion de leur coopération internationale. Les pouvoirs publics à tous les niveaux devraient leur apporter assistance et soutien, en leur donnant les moyens de prendre des décisions éclairées et de gérer les risques qui s'ensuivent pour la sécurité de la recherche, de telle manière que la coopération internationale dans le domaine de la recherche, de l'innovation et de l'enseignement supérieur reste à la fois ouverte et sûre.

(7) Depuis quelques années, des discussions ont lieu au niveau de l'UE sur le renforcement de la sécurité de la recherche, plusieurs initiatives ayant également vu le jour:

– En mai 2021, la Commission a publié sa communication sur l'approche mondiale de la recherche et de l'innovation[2], traçant les grandes lignes d'une nouvelle stratégie européenne pour la politique internationale en matière de recherche et d'innovation. En septembre 2021, le Conseil y a donné suite en adoptant des conclusions[3] prévoyant un mandat politique pour travailler en commun à la sécurité de la recherche.

– Plusieurs mesures de sauvegarde ont été introduites dans Horizon Europe, le programme-cadre de l'UE pour la recherche et l'innovation 2021-2027[4], au

[2] Communication intitulée «L'approche mondiale de la recherche et de l'innovation - La stratégie de coopération internationale de l'Europe dans un monde en mutation», COM(2021) 252 du 18.5.2021 (lien).

[3] Conclusions du Conseil sur l'approche mondiale de la R&I du 28.9.2021 (lien), notamment les points 3, 11 et 23.

[4] Le règlement «Horizon Europe» [règlement (UE) 2021/695 du 28.4.2021] (lien), prévoit notamment une évaluation de la sécurité de tous les projets sélectionnés en vue d'un financement (article 20), la possibilité d'exclure de certains appels les entités établies dans des pays tiers ou contrôlées par des pays tiers (article 22, paragraphe 5), ainsi que d'ajouter des critères d'éligibilité à ceux définis aux paragraphes 2 à 5 afin de tenir compte d'impératifs stratégiques spécifiques ou de la nature et des objectifs de l'action (article 22, paragraphe 6), et le droit, pour la Commission ou l'organisme de financement concerné, de s'opposer à un transfert de propriété des résultats, ou à la concession d'une licence exclusive sur les résultats (article 40, paragraphe 4). Des dispositions similaires sont prévues dans le Fonds européen de la défense et le programme spatial européen.

titre de la responsabilité particulière qui incombe à l'UE dans la mesure où elle compte parmi les principaux bailleurs de fonds de la recherche en Europe.

– En novembre 2021, le Conseil a adopté le programme stratégique de l'EER 2022-2024 dans le cadre de ses conclusions sur la future gouvernance de l'espace européen de la recherche (EER)[5], dont les actions prioritaires comprennent la lutte contre les ingérences étrangères.

– En janvier 2022, donnant suite à ses engagements résultant à la fois de l'approche mondiale et du programme stratégique de l'EER, la Commission a publié son document de travail sur la lutte contre les ingérences étrangères dans la R&I[6]. En outre, afin de faciliter l'apprentissage par les pairs entre les États membres, un exercice d'apprentissage mutuel s'est déroulé tout au long de l'année 2023.

– Dans sa communication sur une stratégie européenne en faveur des universités[7], la Commission rappelle que les établissements d'enseignement supérieur occupent une position unique au carrefour de l'éducation, de la recherche et de l'innovation et jouent ainsi un rôle essentiel dans la réalisation de l'espace européen de l'éducation[8] et de l'espace européen de la recherche, qu'elle considère l'ingérence étrangère dans les établissements d'enseignement supérieur comme une menace et qu'elle soutient la mise en œuvre des lignes directrices sur l'ingérence étrangère. Le rôle des établissements d'enseignement supérieur dans la protection des valeurs démocratiques européennes est au cœur de la stratégie.

– Le 9 mars 2022, le Parlement européen a adopté une résolution sur l'ingérence étrangère dans l'ensemble des processus démocratiques de l'Union européenne, y compris la désinformation, dans laquelle il demande le renforcement de la liberté académique, l'amélioration de la transparence des financements étrangers ainsi que la cartographie et le suivi de l'ingérence étrangère dans les sphères culturelle, universitaire et religieuse[9].

– Du point de vue plus large de la sécurité et de la défense, des travaux sont en cours dans le cadre de la stratégie de l'UE pour l'union de la sécurité[10] ainsi que de la boussole stratégique en matière de sécurité et de défense[11], en vue d'une évaluation commune des menaces et des défis et d'une plus grande cohérence des actions dans le domaine de la sécurité et de la défense, y compris au moyen de différents instruments dans une boîte à outils hybride de l'UE permettant de détecter les menaces hybrides et d'y répondre.

---

5 Conclusions du Conseil sur la future gouvernance de l'espace européen de la recherche (EER) du 26.11.2021 (lien).

6 Commission européenne, direction générale de la recherche et de l'innovation, *Tackling R&I foreign interference – Staff working document* (document de travail des services de la Commission sur la lutte contre les ingérences étrangères dans la R&I), Office des publications de l'Union européenne, 2022 (lien).

7 Communication de la Commission sur une stratégie européenne en faveur des universités, COM(2022) 16 du 18.1.2022 (lien).

8 Communication de la Commission relative à la réalisation d'un espace européen de l'éducation d'ici à 2025, COM(2020) 625 du 30.9.2020 (lien).

9 Résolution du Parlement européen sur l'ingérence étrangère dans l'ensemble des processus démocratiques de l'Union européenne, y compris la désinformation, P9_TA(2022)0064 du 9.3.2022 (lien).

10 Communication de la Commission relative à la stratégie de l'UE pour l'union de la sécurité, COM(2020) 605 du 24.7.2020 (lien).

11 Conseil de l'Union européenne: Une boussole stratégique en matière de sécurité et de défense, ST 7371/22 du 21.3.2022 (lien).

– Dans le domaine des règles de l'UE en matière de contrôle des exportations de biens et technologies à double usage, le règlement de l'UE sur le contrôle des exportations[12] revêt une importance considérable pour la sécurité de la recherche. Afin d'aider les établissements d'enseignement supérieur et les organismes exerçant des activités de recherche, la Commission a publié en septembre 2021 une recommandation sur les programmes de conformité pour la recherche portant sur les biens à double usage[13].

(8) La Commission et le haut représentant ont adopté une communication conjointe relative à la «stratégie européenne en matière de sécurité économique»[14], qui vise à faire en sorte que l'Union continue de bénéficier de l'ouverture économique, tout en réduisant au minimum les risques pour sa sécurité économique. La stratégie propose une approche à trois piliers: promotion de la base économique et de la compétitivité de l'UE; protection contre les risques; et partenariat avec le plus large éventail possible de pays afin de répondre aux préoccupations et aux intérêts communs. Dans chacun des piliers, la recherche et l'innovation ont un rôle essentiel à jouer.

(9) Dans le prolongement de cette communication conjointe, la Commission a recensé des domaines technologiques critiques pour la sécurité économique de l'UE en vue d'une évaluation plus approfondie des risques avec les États membres dans sa recommandation du 3 octobre 2023[15]. Des évaluations des risques ont déjà été lancées en priorité dans quatre des dix domaines technologiques critiques recensés, à savoir les semi-conducteurs avancés, l'intelligence artificielle, les technologies quantiques et les biotechnologies. Les résultats des évaluations des risques, une fois finalisés, pourraient servir de base à d'autres mesures visant à mettre en œuvre la stratégie européenne de sécurité économique, y compris des mesures visant à renforcer la sécurité de la recherche.

(10) Dans la communication conjointe sur la stratégie européenne en matière de sécurité économique, la Commission a en outre annoncé vouloir proposer des mesures visant à renforcer la sécurité de la recherche en garantissant l'utilisation des outils existants ainsi qu'en recensant et en comblant les lacunes restantes, tout en préservant l'ouverture de l'écosystème de recherche et d'innovation.

(11) En ce qui concerne le recensement des lacunes mentionné au point précédent, les discussions avec les États membres et les organisations de parties prenantes montrent que les décideurs politiques et les professionnels ont un besoin urgent de clarté conceptuelle et d'une compréhension commune des questions en jeu ainsi que de ce qui constitue une réponse politique à la fois proportionnée et efficace.

(12) Un nombre croissant d'États membres ont élaboré ou sont en train d'élaborer des politiques visant à renforcer la sécurité de la recherche. Si ces efforts contribuent généralement à la sensibilisation et au renforcement de la résilience, une multiplication non coordonnée de mesures nationales se traduirait par une mosaïque de politiques nationales, des disparités entre les États membres et, partant, une fragmentation de

[12] Règlement (UE) 2021/821 instituant un régime de l'Union de contrôle des exportations, du courtage, de l'assistance technique, du transit et des transferts en ce qui concerne les biens à double usage (lien).

[13] Recommandation de la Commission relative aux programmes internes de conformité pour les contrôles de la recherche portant sur les biens à double usage [...], 2021/1700 du 15.9.2021 (lien).

[14] Communication conjointe relative à la «stratégie européenne en matière de sécurité économique», JOIN(2023) 20 du 20.6.2023 (lien).

[15] Recommandation de la Commission du 3 octobre 2023 relative aux domaines technologiques critiques pour la sécurité économique de l'UE en vue d'une évaluation approfondie des risques avec les États membres, C(2023) 6689 du 3.10.2023 (lien).

l'espace européen de la recherche. Une coordination au niveau de l'UE est donc nécessaire pour garantir des conditions de concurrence équitables et protéger l'intégrité de l'espace européen de la recherche.

(13) Il convient de souligner que les garanties en matière de sécurité de la recherche ne peuvent être réellement efficaces que si elles sont appliquées de manière cohérente à tous les niveaux, y compris aux niveaux européen, national, régional et au niveau des organismes de recherche publics et privés, de manière à éviter les failles et les contournements.

(14) Dans certains cas spécifiques, le respect de la législation et de la réglementation pertinentes de l'UE pourrait bénéficier d'orientations interprétatives. Cela vaut en particulier pour les règles de contrôle des exportations, notamment le transfert immatériel de technologie, les exigences en matière de visas pour les chercheurs étrangers[16], ainsi que l'interprétation de certaines exigences en matière de science ouverte et de gestion des actifs intellectuels du point de vue de la sécurité de la recherche.

(15) Il importe que les menaces hybrides qui affectent l'écosystème de recherche et d'innovation fassent l'objet d'une évaluation structurelle, afin d'améliorer la connaissance de la situation parmi les décideurs politiques en s'appuyant sur la capacité unique d'analyse du renseignement (SIAC), en particulier la cellule de fusion contre les menaces hybrides, les travaux du Centre européen d'excellence pour la lutte contre les menaces hybrides[17] ainsi que l'ENISA en ce qui concerne les menaces en matière de cybersécurité[18].

(16) Étant donné qu'une part importante de la recherche et de l'innovation a lieu dans le secteur privé, il est essentiel de mettre au point des orientations et des outils ciblés pour les entreprises, notamment les start-up et les petites et moyennes entreprises à forte intensité de recherche. Si les risques auxquels les entreprises sont exposées peuvent être similaires, leur situation diffère de celle des établissements d'enseignement supérieur et des organismes de recherche. En conséquence, il convient d'attirer l'attention sur les règles existantes, y compris celles relatives au contrôle des exportations de biens à double usage, sur le filtrage des investissements étrangers ainsi que sur les travaux en cours concernant le suivi des investissements sortants.

(17) Lors de l'élaboration de la présente recommandation, une attention particulière a été accordée à l'expérience des États membres et des partenaires de l'UE, tant dans le cadre bilatéral que multilatéral. Elle tient compte des enseignements des principaux partenaires, tout en soulignant qu'il convient de formuler une approche adaptée à la spécificité du contexte européen. Des efforts continus sont déployés avec nos partenaires pour échanger des informations et des expériences, partager les bonnes pratiques et chercher des moyens d'aligner les mesures de sauvegarde, y compris par le dialogue multilatéral sur les valeurs et les principes, dans le cadre des négociations d'association et des réunions conjointes du comité de pilotage S&T au titre d'accords internationaux dans le domaine des sciences et des technologies, ainsi que dans des

[16] Directive (UE) 2016/801 du 11 mai 2016 relative aux conditions d'entrée et de séjour des ressortissants de pays tiers à des fins de recherche, d'études, de formation, de volontariat et de programmes d'échange d'élèves ou de projets éducatifs et de travail au pair (lien).

[17] Le Centre d'excellence pour la lutte contre les menaces hybrides est une organisation internationale autonome de lutte contre les menaces hybrides fondée sur des réseaux, créée en 2017 et basée à Helsinki (lien).

[18] L'Agence de l'Union européenne pour la cybersécurité (ENISA) est l'agence de l'Union ayant pour but de parvenir à un niveau commun élevé de cybersécurité dans l'ensemble de l'Europe (lien).

enceintes multilatérales telles que le G7, l'OCDE et l'OTAN, et dans le contexte d'accords multilatéraux pertinents en matière de contrôle des exportations.

(18) La sécurité de la recherche est une préoccupation qui suscite de plus en plus d'attention et le débat en cours sur les risques encourus et la meilleure manière de les gérer s'intensifie. Par conséquent, il convient de sensibiliser davantage, de faciliter l'apprentissage par les pairs entre les États membres et les organisations de parties prenantes concernées, et de contribuer à une approche d'apprentissage à la fois souple et agile.

CHAMP D'APPLICATION

1. Aux fins de la présente recommandation, on entend par «sécurité de la recherche» la gestion des risques liés:

   a) au transfert indésirable de connaissances, de savoir-faire et de technologies critiques susceptible d'affecter la sécurité de l'UE et de ses États membres, par exemple s'ils sont acheminés à des fins militaires dans des pays tiers;

   b) à l'influence malveillante sur la recherche, celle-ci pouvant être instrumentalisée par ou depuis des pays tiers afin de diffuser certains discours ou d'inciter les étudiants et les chercheurs à s'autocensurer, en violation de la liberté académique et de l'intégrité de la recherche dans l'Union;

   c) aux atteintes à l'éthique ou à l'intégrité, les connaissances et les technologies étant utilisées pour faire supprimer ou saper des valeurs fondamentales, que ce soit dans l'UE ou ailleurs.

2. Aux fins de la présente recommandation, on entend par «coopération internationale» la coopération entre, d'une part, des organismes de recherche publics et privés et des établissements d'enseignement supérieur et, d'autre part, des entreprises et des organismes de recherche et d'innovation établis en dehors de l'UE. Les entreprises et organismes de recherche et d'innovation établis dans l'UE mais détenus ou contrôlés depuis l'extérieur de l'UE devraient faire l'objet d'une évaluation des risques.

3. Aux fins de la présente recommandation, on entend par «évaluation des risques» un processus lié à la coopération internationale en matière de recherche et d'innovation dans le cadre duquel une combinaison des principaux facteurs de risque est prise en considération. La combinaison de ces facteurs détermine le niveau de risque. Les principaux éléments à évaluer peuvent être regroupés en quatre catégories:

   – le profil de risque de l'organisation établie dans l'UE qui participe à la coopération internationale: prendre en considération les points forts et les vulnérabilités de l'organisation, y compris ses dépendances financières, en rapport avec le projet de recherche;

   – le domaine de la recherche et de l'innovation dans lequel la coopération internationale doit avoir lieu: déterminer si le projet se concentre sur un domaine de recherche, par exemple un domaine technologique critique, ou s'il implique une méthodologie ou une infrastructure de recherche considérée comme particulièrement sensible du point de vue de la sécurité ou de l'éthique/des droits de l'homme;

   – le profil de risque du pays tiers dans lequel le partenaire international est établi ou à partir duquel il est détenu ou contrôlé (par exemple: le pays fait l'objet de sanctions ou a des antécédents négatifs en matière d'état de droit ou de

protection des droits de l'homme, mène une stratégie agressive de fusion civilo-militaire ou dispose d'une liberté académique limitée);

– le profil de risque de l'organisation internationale partenaire: faire preuve de vigilance à l'égard de l'organisation avec laquelle vous envisagez de coopérer pour déterminer si elle a des liens avec le gouvernement ou l'armée et quelles sont les affiliations des chercheurs/membres du personnel concernés ainsi que les intentions du partenaire en ce qui concerne l'utilisation finale ou l'application des résultats de la recherche.

4. Aux fins de la présente recommandation, le «secteur de la recherche et de l'innovation» couvre tous les organismes exerçant des activités de recherche et les établissements d'enseignement supérieur dans l'ensemble de l'Union, qu'ils soient publics ou privés. Compte tenu de l'importance d'autres parties prenantes, telles que les bureaux de transfert de technologie, les agences d'internationalisation, les chambres de commerce et les entreprises à forte intensité de recherche, la présente recommandation peut tout aussi bien s'appliquer aux autres acteurs de l'écosystème de recherche et d'innovation de l'UE. Le cas échéant, des activités de coopération internationale liées à l'éducation pourraient également être envisagées.

PRINCIPES D'INTERNATIONALISATION RESPONSABLE

1. Continuer à promouvoir et à défendre la liberté académique et l'autonomie institutionnelle, en tenant compte du fait que la responsabilité de la coopération internationale en matière de recherche et d'innovation incombe principalement aux établissements d'enseignement supérieur et aux autres organismes exerçant des activités de recherche.

2. Continuer à promouvoir et à encourager une coopération internationale à la fois ouverte et sûre en matière de recherche et d'innovation avec les partenaires des pays tiers, conformément au principe «aussi ouverte que possible, aussi fermée que nécessaire», en veillant à ce que les résultats de la recherche soient faciles à trouver, accessibles, interopérables et réutilisables (principes «FAIR»), en tenant dûment compte des restrictions applicables, y compris les préoccupations en matière de sécurité.

3. Garantir la proportionnalité des mesures: lorsque des garanties sont introduites, celles-ci ne devraient pas aller au-delà de ce qui est strictement nécessaire pour atténuer les risques en jeu et devraient éviter une charge administrative inutile. L'objectif est la réduction des risques, non le découplage.

4. Orienter les mesures de sécurité dans le domaine de la recherche afin de préserver la sécurité économique, y compris la sécurité de l'Union et la sécurité nationale, et de défendre des valeurs communes, y compris la liberté académique, tout en évitant le protectionnisme et l'instrumentalisation politique injustifiée de la recherche et de l'innovation.

5. Promouvoir l'autogouvernance au sein du secteur, en donnant aux chercheurs et aux innovateurs les moyens de prendre des décisions éclairées, en soulignant la responsabilité sociétale des établissements d'enseignement supérieur et des autres organismes exerçant des activités de recherche dans le droit fil du principe selon lequel «la liberté académique implique une responsabilité académique».

6. Adopter une approche pangouvernementale, qui rassemble l'expertise et les compétences pertinentes, garantit une approche globale de la sécurité de la recherche et favorise la cohérence des actions gouvernementales et des messages à l'égard du

secteur de la recherche et de l'innovation, y compris des mesures concrètes visant à perfectionner et à reconvertir la main-d'œuvre concernée.

7. Tout en appliquant une approche fondée sur les risques, adopter des politiques qui soient neutres en matière de pays, recensent et traitent les risques pour la sécurité de la recherche, quelle que soit leur origine, car il s'agit de la meilleure garantie qu'une approche équilibrée des possibilités et des risques dans le cadre de la coopération en matière de recherche et d'innovation est maintenue et que l'évolution du panorama de la menace, y compris l'émergence de nouveaux acteurs de la menace, n'est pas négligée.

8. Veiller à ce que tout soit mis en œuvre pour éviter toutes les formes de discrimination et de stigmatisation, directes ou indirectes, qui pourraient se produire comme des effets secondaires involontaires des mesures de sauvegarde et garantir le plein respect des droits fondamentaux et des valeurs partagées.

9. Reconnaître la nature dynamique de la sécurité de la recherche façonnée par l'évolution des risques, les nouvelles connaissances et les contextes géopolitiques, ce qui nécessite une approche d'apprentissage avec des bilans périodiques visant à garantir que les politiques de sécurité de la recherche restent à jour, efficaces et proportionnées.

RECOMMANDE AUX ÉTATS MEMBRES

tout en respectant strictement l'autonomie institutionnelle et la liberté académique, et compte tenu des situations nationales et de la responsabilité de garantir la sécurité nationale:

1. de travailler à la définition et à la mise en œuvre d'un ensemble cohérent de mesures stratégiques visant à renforcer la sécurité de la recherche, en s'appuyant au maximum sur les éléments recensés dans la présente partie, et en tenant compte des principes susmentionnés en matière d'internationalisation responsable;

2. d'entretenir un dialogue avec les parties prenantes de la recherche et de l'innovation afin de définir les responsabilités et les rôles, et d'élaborer un plan d'action national, formulant, le cas échéant, des lignes directrices nationales, et recensant les mesures et initiatives à même de renforcer la sécurité de la recherche, avec un calendrier de mise en œuvre;

3. de créer une structure de soutien, par exemple une plateforme de conseil sur la sécurité de la recherche, afin d'aider les chercheurs et les innovateurs à faire face aux risques liés à la coopération internationale dans le domaine de la recherche et de l'innovation. Une telle structure devrait, tout en rassemblant l'expertise et les compétences transsectorielles, informer et conseiller les organismes de recherche de manière à leur permettre de prendre des décisions éclairées sur la base d'une évaluation des opportunités et des risques découlant des activités de coopération internationale envisagées et d'autres services essentiels pour le secteur de la recherche et de l'innovation, tels que des activités de sensibilisation et de formation;

4. d'enrichir le socle des données validées aux fins de l'élaboration des politiques en matière de sécurité de la recherche, en s'appuyant sur l'analyse du panorama de la menace, y compris du point de vue de la cybersécurité, ainsi que par la réalisation ou la commande de travaux de recherche pertinents pour les politiques;

5. d'accorder une attention particulière aux technologiques critiques énumérées dans la recommandation de la Commission relative aux domaines technologiques critiques pour la sécurité économique de l'UE en vue d'une évaluation approfondie des

risques avec les États membres[19], et aux résultats de ces évaluations conjointes des risques;

6. de renforcer la coopération intersectorielle au sein des pouvoirs publics, notamment en réunissant les responsables des politiques de l'enseignement supérieur, de la recherche et de l'innovation, des affaires étrangères, ainsi que du renseignement et de la sécurité;

7. de faciliter l'échange d'informations avec les organismes de recherche publics et privés au sujet des activités d'analyse et de recherche susmentionnées, y compris en s'appuyant sur des notes d'information classifiées et non classifiées ou en faisant appel à des officiers de liaison spécialisés;

8. de récolter des éléments d'appréciation sur la résilience du secteur ainsi que sur l'efficacité et la proportionnalité des politiques applicables en matière de sécurité de la recherche, y compris, le cas échéant, en procédant sur une base régulière à des tests de résilience et à des simulations d'incidents;

9. afin d'assurer le respect des règles applicables de l'UE en matière de contrôles des exportations des biens à double usage et des sanctions adoptées en vertu de l'article 29 du TUE et de l'article 215 du TFUE, de prendre des mesures au niveau national, notamment, d'une part, en ce qui concerne le transfert immatériel de technologies et, d'autre part, dans le but de renforcer la mise en œuvre et l'application des régimes de sanctions touchant à la recherche et à l'innovation, notamment les interdictions de transférer certaines technologies;

10. de contribuer de manière proactive à la plateforme à guichet unique destinée à la lutte contre l'ingérence étrangère dans la R&I, en partageant les instruments et les ressources déployés grâce à des fonds publics dans le but de faciliter leur pénétration transfrontière et de les mettre en œuvre d'une manière conviviale et accessible;

11. de préparer, en collaboration avec le secteur privé, des informations et des orientations ciblées à l'intention des entreprises actives dans la recherche et l'innovation privées, y compris pour les start-up et les petites et moyennes entreprises à forte intensité de recherche;

12. d'envisager, le cas échéant, et sur la base d'une évaluation des risques, l'application des mesures contenues dans la présente recommandation aux activités de coopération internationale menées dans l'enseignement supérieur, y compris les activités de mobilité des étudiants et du personnel.

Rôle des organismes de financement de la recherche

13. de dialoguer avec les organismes de financement de la recherche afin de faire en sorte que:

    a) la sécurité de la recherche fasse partie intégrante de la procédure de candidature et prenne en compte les différents facteurs qui, ensemble, définissent le profil de risque du projet. L'objectif est d'inciter les bénéficiaires à considérer le contexte dans lequel s'inscrit la coopération en matière de R&I et à analyser quelles motivations et quels objectifs (dissimulés) pourraient jouer un rôle, de façon à assurer l'identification en amont des risques et des menaces potentiels et, partant, d'éviter les problèmes éventuels à un stade ultérieur;

[19] Recommandation de la Commission du 3.10.2023 relative aux domaines technologiques critiques pour la sécurité économique de l'UE en vue d'une évaluation approfondie des risques avec les États membres (lien).

b) les projets de recherche sélectionnés en vue d'un financement qui suscitent des préoccupations («signaux d'alerte») soient soumis à une évaluation des risques proportionnée à leur profil de risque, de façon à pouvoir convenir de mesures de sauvegarde appropriées face aux risques recensés, tout en veillant à ce que le délai d'octroi ne soit pas indûment retardé et à ne pas créer de charge administrative inutile;

c) l'application des mesures de sauvegarde dans les programmes de financement nationaux prenne en compte celles appliquées dans les programmes de financement pertinents de l'UE;

d) les candidats cherchent à s'assurer auprès des partenaires susceptibles de participer à des projets présentant un profil de risque élevé, par exemple en concluant un accord de partenariat, que les résultats de la recherche seront utilisés d'une manière conforme aux valeurs fondamentales, y compris le respect des droits de l'homme;

e) l'organisme de financement dispose d'une expertise et de compétences adéquates qui lui permettent de répondre aux préoccupations en matière de sécurité de la recherche et de disposer de mesures de suivi et d'évaluation appropriées pour superviser les projets à différents stades, y compris le suivi des incidents et l'application de mesures crédibles en cas de non-conformité.

Soutien aux établissements d'enseignement supérieur et aux autres organismes de recherche

14. d'encourager et de soutenir les établissements d'enseignement supérieur et les autres organismes de recherche aux fins suivantes:

a) créer une plateforme sectorielle des parties prenantes afin de faciliter l'échange d'informations, l'apprentissage par les pairs, la création d'instruments et l'élaboration de lignes directrices, ainsi que la notification des incidents; envisager la mise en commun des ressources afin de compenser de manière optimale la rareté et la dispersion des ressources et de l'expertise;

b) mettre en œuvre des procédures internes de gestion des risques dans le cadre d'une approche structurelle, y compris l'évaluation des risques, une vigilance appropriée à l'égard des partenaires potentiels et la sollicitation des niveaux plus élevés de prise de décision interne lorsque des éléments suscitent des préoccupations («signaux d'alerte») et ce, sans charge administrative inutile;

c) insister systématiquement, lorsque des accords de partenariat dans le domaine de la recherche sont conclus avec des entités étrangères, y compris les protocoles d'accord, sur l'inclusion de conditions-cadres essentielles, telles que le respect des valeurs fondamentales, de la liberté académique, de la réciprocité et des modalités en matière de gestion des actifs intellectuels, y compris la diffusion et la valorisation des résultats, la couverture des résultats par des licences ou le transfert de résultats et l'essaimage, et veiller à ce qu'une stratégie de sortie soit prévue en cas de non-respect des conditions de ces accords;

d) évaluer les risques liés aux programmes de soutien aux talents financés par les pouvoirs publics étrangers dans l'enseignement supérieur et la recherche, notamment en mettant l'accent sur toute obligation indésirable imposée à leurs

bénéficiaires, et veiller à ce que les prestataires de cours et de formations soutenus par les pouvoirs publics étrangers et accueillis sur les campus universitaires respectent la mission et les règles de l'établissement d'accueil;

e) investir dans l'expertise et les compétences spécifiques internes dans le domaine de la recherche en matière de sécurité, attribuer la responsabilité en matière de sécurité de la recherche aux niveaux organisationnels appropriés, et investir dans l'hygiène informatique et dans l'instauration d'une culture assurant l'équilibre entre ouverture et sécurité;

f) établir des programmes de formation, y compris des cours en ligne, à l'intention des professionnels déjà en poste et des nouveaux membres du personnel dans le cadre de leur intégration, ainsi que des programmes de formation destinés à la prochaine génération de conseillers et de décideurs dans le domaine de la sécurité; former les recruteurs pour qu'ils soient capables, en application d'un processus de vérification structurelle, d'analyser et de détecter les éléments qui suscitent des préoccupations («signaux d'alerte») dans les candidatures à des postes de recherche, en particulier dans les domaines critiques;

g) assurer, dans les publications scientifiques et dans toutes les autres formes de diffusion des résultats de la recherche, une transparence totale des sources de financement et des affiliations du personnel de recherche, de manière à éviter que des situations de dépendance à l'égard de pays étrangers et des conflits d'intérêts ou d'engagement n'affectent la qualité et le contenu de la recherche;

h) introduire un cloisonnement, à la fois physique et virtuel, qui garantisse que, d'une part pour les espaces physiques, tels que les laboratoires et les infrastructures de recherche, et d'autre part pour les données et systèmes particulièrement sensibles, l'accès soit accordé sur la base du strict besoin d'en connaître, et que, pour les systèmes en ligne, des mesures robustes de cybersécurité soient en place;

i) veiller à ce que toutes les formes de discrimination et de stigmatisation, à la fois directes et indirectes, soient évitées, à ce que soit garantie la sécurité individuelle, en s'intéressant en particulier aux tactiques de coercition appliquées par l'État d'origine sur la diaspora et à d'autres formes d'influence malveillante qui pourraient aboutir à l'autocensure et avoir des incidences en matière de sécurité pour les chercheurs, doctorants et étudiants étrangers concernés, et à ce que les incidents soient signalés.

Actions de soutien au niveau de l'Union

15. de coopérer pleinement en vue de faciliter les mesures que la Commission a prises ou compte prendre pour soutenir la mise en œuvre de la présente recommandation, et, notamment:

a) l'exploitation optimale de la méthode ouverte de coordination, notamment les structures de gouvernance de l'EER, pour sensibiliser, faciliter l'apprentissage par les pairs et favoriser la cohérence des politiques;

b) l'établissement d'un centre européen d'expertise en matière de sécurité de la recherche en tant que point focal, lié à la plateforme à guichet unique de la Commission destinée à la lutte contre l'ingérence étrangère dans la R&I, de manière à contribuer à la création d'une communauté de pratique à l'échelle de l'UE et au maintien d'un dialogue structurel avec les organisations de parties

prenantes, ainsi qu'à des activités de recherche pertinentes pour les politiques en matière de sécurité de la recherche et à l'analyse des tendances et des modèles dans l'ensemble de l'Union;

c) l'amélioration, en coopération avec le haut représentant, du niveau de sensibilisation à la situation parmi les décideurs politiques, en s'appuyant sur l'évaluation, au niveau structurel, des menaces hybrides qui visent l'écosystème de la recherche et de l'innovation;

d) l'élaboration d'une méthodologie de test de la résilience utilisable au niveau national sur une base volontaire par les établissements d'enseignement supérieur et les organismes publics et privés exerçant des activités de recherche;

e) la poursuite de ses travaux, en collaboration avec les États membres et avec la participation des parties prenantes, sur l'évaluation des risques liés aux technologies critiques[20], et l'instauration d'un dialogue visant à assurer le partage d'informations et la cohérence des approches en matière d'évaluation des risques et de garanties en matière de sécurité de la recherche, d'une part, dans les programmes de financement nationaux et, d'autre part, dans les programmes de financement pertinents de l'UE;

f) la création d'outils et la constitution de ressources, par pays ou indépendamment, afin d'aider les établissements d'enseignement supérieur et les organismes publics et privés exerçant des activités de recherche à faire preuve d'une vigilance appropriée à l'égard des partenaires potentiels; et l'organisation, en collaboration avec les organisations de parties prenantes au niveau de l'UE, d'un forum bisannuel des parties prenantes sur la sécurité de la recherche;

g) l'élaboration d'orientations interprétatives, le cas échéant, sur la formulation des procédures d'évaluation des risques et sur l'application de la législation pertinente de l'UE;

h) le dialogue avec le secteur de la recherche et de l'innovation afin de déterminer la meilleure manière d'accroître la transparence des sources de financement de la recherche et des affiliations des chercheurs;

i) le renforcement du dialogue avec les partenaires internationaux sur la sécurité de la recherche et la prise d'initiatives visant à faire en sorte que l'UE s'exprime d'une même voix sur ce sujet dans les enceintes multilatérales.

COMMUNICATION D'INFORMATIONS

1. Il est recommandé aux États membres de mettre la présente recommandation en œuvre dès que possible. Les États membres sont invités à partager avec la Commission, au plus tard le [*insérer la date: 9 mois après l'adoption par le Conseil*], leur plan d'action (visé au point 2 des recommandations destinées aux États membres) exposant les mesures correspondantes à prendre pour renforcer la sécurité de la recherche, compte tenu des situations de départ respectives.

[20] Recommandation de la Commission du 3 octobre 2023 relative aux domaines technologiques critiques pour la sécurité économique de l'UE en vue d'une évaluation approfondie des risques avec les États membres (lien).

2. Les progrès réalisés dans la mise en œuvre de la présente recommandation feront l'objet d'un suivi par la Commission à l'aide des cadres de gouvernance, de suivi et de déclaration de l'EER, en coopération avec les États membres et après consultation des parties prenantes concernées, et seront présentés dans un rapport au Conseil tous les deux ans, dans le cadre du rapport bisannuel sur l'approche mondiale de la recherche et de l'innovation. Sur la base d'une évaluation approfondie et selon l'évolution de la situation géopolitique, d'autres démarches et mesures pourront être proposées.

Fait à Bruxelles, le

Par le Conseil
Le Président