

Bruxelles, le 3 décembre 2025
(OR. en)

16389/25

POLCOM 368
FDI 58
COMER 182
RECH 543
TELECOM 457
COMPET 1297
DUAL USE 58
RELEX 1623
ENER 647
ENV 1330
IND 580
INDEF 179
CYBER 364
PROCIV 176

NOTE DE TRANSMISSION

Origine:	Pour la secrétaire générale de la Commission européenne, Madame Martine DEPREZ, directrice
Date de réception:	3 décembre 2025
Destinataire:	Madame Thérèse BLANCHET, secrétaire générale du Conseil de l'Union européenne

Objet:	COMMUNICATION CONJOINTE AU PARLEMENT EUROPÉEN ET AU CONSEIL renforcer la sécurité économique de l'UE
--------	--

Les délégations trouveront ci-joint le document JOIN(2025) 977 final.

p.j.: JOIN(2025) 977 final



COMMISSION
EUROPÉENNE

LE HAUT REPRÉSENTANT DE
L'UNION POUR LES AFFAIRES
ÉTRANGÈRES ET LA
POLITIQUE DE SÉCURITÉ

Bruxelles, le 3.12.2025
JOIN(2025) 977 final

COMMUNICATION CONJOINTE AU PARLEMENT EUROPÉEN ET AU CONSEIL
renforcer la sécurité économique de l'UE

1. Introduction

L'usage de plus en plus fréquent et ciblé d'**outils économiques** pour atteindre des **objectifs stratégiques** est devenu un trait déterminant de notre paysage géopolitique. Droits de douane intempestifs, instrumentalisation des dépendances ou déploiement arbitraire de mesures de défense commerciale, les principaux acteurs utilisent les leviers économiques pour parvenir à leurs fins stratégiques et géopolitiques, malmenant ainsi l'économie, la compétitivité, la sécurité et l'ordre public de l'UE.

Les risques pour la sécurité économique de l'UE ne sont pas nouveaux, mais ils se sont récemment intensifiés: les vulnérabilités sont désormais plus visibles et plus urgentes, et il devient difficile de passer outre. Ces risques sont notamment les suivants:

- une **instabilité de l'environnement mondial du commerce et des investissements** s'aggravant au rythme des mesures commerciales et des restrictions à l'exportation prises en solution de continuité pour instrumentaliser les dépendances,
- une prolifération de **pratiques prédatrices** qui ciblent les chaînes d'approvisionnement et technologies critiques et sapent notre base industrielle, et dont certaines (telles que les surcapacités subventionnées par l'État) créent de nouvelles dépendances,
- la détérioration continue du contexte sécuritaire, au vu notamment de la poursuite de la **guerre d'agression menée par la Russie contre l'Ukraine** et de l'augmentation des attaques hybrides.

La **stratégie européenne en matière de sécurité économique** de 2023 a constitué une première réponse de l'UE à ces défis¹ grâce à une série d'actions — fondées sur des évaluations des risques — visant à renforcer la sécurité économique de l'UE par la **promotion** de sa compétitivité, la **protection** contre les risques et la **conclusion de partenariats** avec ceux qui partagent nos préoccupations. Ces trois piliers restent au cœur de notre stratégie de sécurité économique et la Commission, en collaboration avec les États membres, s'emploie à les intégrer dans toutes ses actions et politiques. En outre, la sécurité économique est essentielle pour que l'UE maintienne ses valeurs, ses principes et le bien-être de ses citoyens, et pour renforcer notre indépendance économique.

Depuis l'adoption de la stratégie de 2023, le besoin d'une Europe capable d'agir à l'unisson, avec audace et rapidité s'est cependant fait plus fort. La présente communication propose un usage plus stratégique et plus revendiqué des outils de l'Union, qui vient s'ajouter à leurs objectifs initiaux pour soutenir la sécurité économique de l'Europe, c'est-à-dire la capacité de l'Union, en sus de ses autres objectifs, d'assurer sa sécurité grâce à une économie forte, dynamique et résiliente, en anticipant les menaces potentielles ou réelles issues des relations économiques de l'UE avec le reste du monde, en les désamorçant et en les combattant. L'UE peut y parvenir, surtout si elle reste à l'avant-garde des technologies, industries et services critiques. La présente communication reflète un **changement de doctrine**, le passage d'une posture réactive à un déploiement proactif systématique de notre arsenal de mesures. Dans certains cas, il faudra en outre que l'UE, ses États membres et l'industrie se préparent

¹ JOIN(2023) 20 final.

inéluclablement à accepter le coût économique de cette réduction de nos vulnérabilités et du renforcement de la sécurité globale.

Le présent appel à l'action vise aussi à **améliorer** la collecte, le suivi et l'analyse de données, ainsi que la capacité à anticiper les menaces émergentes, à **dissuader** les pays tiers d'instrumentaliser les situations de dépendance de l'Union, à nous **désengager** de ces situations de dépendances envers des pays tiers susceptibles de les instrumentaliser et à nous **prémunir** des ripostes visant à contourner nos mesures de réduction des risques.

Le présent appel à l'action reconnaît avant tout la nécessité pour l'UE de **jouer de ses atouts**, notamment du poids sans équivalent de son marché unique, de ses capacités technologiques et industrielles et des financements provenant de ses Fonds et programmes. Pour ce faire, elle doit cartographier ses perspectives économiques et les domaines dans lesquels ce sont les autres qui dépendent d'elle. Dès lors, la présente communication plaide pour une **vision stratégique intégrée, transversale et tournée vers les entreprises**, une **meilleure gouvernance** et une **coopération encore plus étroite avec des partenaires partageant les mêmes valeurs, débouchant sur une action conjointe si la situation s'y prête**. Elle vient compléter la stratégie globale de l'UE pour une union de la préparation. La sécurité économique de l'UE repose sur celle de ses États membres, tout en étant intrinsèquement liée à ses relations plus larges avec le monde et, partant, à la politique étrangère et de sécurité commune, laquelle sera employée plus systématiquement pour soutenir les objectifs énoncés.

En partant de cette base et de ses analyses fondées sur les risques, la Commission se concentre sur six domaines à haut risque, énumérés à la section 3, pour leur appliquer les outils à notre disposition et souligner les possibilités de les améliorer.

2. Une démarche proactive en matière de sécurité économique

L'UE dispose d'un large éventail d'outils pour asseoir sa sécurité économique. Le renforcement de celle-ci exige qu'elle use désormais de ces outils **de manière plus stratégique, plus efficace et plus volontaire**. À l'origine, la plupart de ces outils n'avaient pas été conçus dans un souci de sécurité économique, mais ils sont très utiles pour contribuer aux objectifs de l'Union en la matière.

Une liste non exhaustive d'outils importants est présentée dans le *graphique 1*, et leur application coordonnée est expliquée plus en détail à la *section 3*.

Graphique 1: Liste non exhaustive des outils contribuant à la sécurité économique



Pour améliorer la sécurité économique de l'UE, la Commission déploiera ces outils, en coordination avec les États membres, comme suit:

- Les **outils liés aux échanges et à la concurrence** serviront à réduire progressivement l'exposition de l'UE aux risques et à prémunir l'UE des ripostes visant à contourner ses mesures de réduction des risques. Cela passe par exemple par l'expansion des axes de diversification, et donc de la sécurité offerte par les accords commerciaux de l'UE, par un usage stratégique de l'arsenal douanier et par la lutte contre les distorsions causées par les subventions étrangères, tant au sein du marché unique que dans le cas des subventions ou des importations faisant l'objet d'un dumping.
- Les **outils liés à la résilience et la cybersécurité** serviront à nous préparer aux situations d'urgence et à les gérer, ainsi qu'à réduire l'exposition aux menaces extérieures, telles que les cybermenaces.
- Les **outils liés à la sécurité et à l'ordre public** serviront à réduire l'exposition excessive de l'UE aux risques pour garantir entre autres un fonctionnement normal de la société, tout en soutenant des actions visant à étoffer le rôle de l'UE dans les technologies et les industries critiques et à la prémunir des ripostes visant à contourner ses mesures de réduction des risques.
- Les **mesures anticoercitives et restrictives** viseront à décourager les pays tiers cherchant à exercer une coercition à l'encontre de l'UE, à gérer ce type de situations et à protéger les entreprises de l'UE contre les mesures extraterritoriales imposées par des pays tiers, le cas échéant en incitant le pays concerné à changer de comportement.

- Les **outils liés aux restrictions de financement** comme l'IVDCI (Global Gateway), Horizon Europe, NextGenerationEU, InvestEU, le programme pour une Europe numérique, le mécanisme pour l'interconnexion en Europe (MIE), les instruments d'aide de préadhésion (IAP), les plans de croissance pour les Balkans occidentaux et la Moldavie, ainsi que la facilité pour l'Ukraine, EU4Health et le futur Fonds européen pour la compétitivité, devraient renforcer la sécurité économique de l'UE ou, au minimum, ne pas l'affaiblir, dans le cadre des modalités de ces programmes.
- Les **initiatives sectorielles** serviront à renforcer les capacités propres et les savoir-faire stratégiques de l'UE dans les domaines à haut risque recensés au cours du processus d'évaluation des risques.

Il est plus important que jamais d'avoir une coopération et une coordination étroites avec les pays qui accordent la même importance à la sécurité économique et à un ordre mondial fondé sur des règles. L'UE s'emploiera à renforcer la **coopération internationale sur les questions de sécurité économique**, en particulier avec des **partenaires de confiance**, y compris au moyen de **dialogues ciblés sur la sécurité économique menés tant au niveau bilatéral que plurilatéral**. Cette coopération soutiendra une action commune sur des intérêts ou des problèmes communs de sécurité économique. Elle permettra aussi d'approfondir la compréhension collective des risques, d'anticiper les menaces, de concevoir des mesures d'atténuation qui **réduisent au minimum les externalités négatives**, de contribuer à la mise en place et au maintien de chaînes d'approvisionnement fiables et résilientes dans des secteurs stratégiques clés et d'éviter les incidences négatives sur nos partenaires internationaux partageant les mêmes valeurs.

La Commission s'efforcera de coopérer avec les pays tiers de manière bilatérale, par l'intermédiaire du G7 et dans des cadres tels que le partenariat transpacifique global et progressiste et autres enceintes appropriées. Elle collaborera avec ses partenaires à la conception et à l'adoption de normes de sécurité économique renforçant la résilience des chaînes d'approvisionnement. Le **déploiement coordonné des outils** peut participer de cette coopération plus étroite, tout comme la construction de coalitions avec des partenaires qui partagent des objectifs de sécurité économique semblables aux nôtres, ou qui sont confrontés à des défis du même ordre.

En outre, il conviendra de tenir compte de la pertinence et de l'incidence de la

politique de voisinage et d'élargissement de l'UE. La Commission prendra en considération

L'adoption de normes de sécurité économique

En s'appuyant sur les travaux menés au sein du G7 sur les échanges respectant des normes, la Commission encouragera la conception et l'adoption de normes de sécurité économique qui:

- soutiendront la diversification des chaînes d'approvisionnement critiques en créant des conditions favorisant l'accès au marché de nouveaux fournisseurs ou restreignant celui des fournisseurs dominants,
- suivront les principes de transparence, d'interopérabilité et de respect des règles internationales,
- seront conçues en fonction de chaque chaîne d'approvisionnement pour tenir compte de leurs risques spécifiques et de leurs incidences économiques et réalités sectorielles.

Ces travaux mettront l'accent en priorité sur les matières premières critiques et les chaînes d'approvisionnement en semi-conducteurs, tout en explorant l'opportunité de collaborer dans d'autres domaines.

les risques et potentialités pour la sécurité économique de l'UE quand elle mettra en œuvre les politiques et programmes destinés aux pays concernés. Les pays candidats suivent un parcours d'adhésion à l'UE et, pour en garantir la réussite, il est primordial qu'ils convergent avec la politique de sécurité économique et intègrent progressivement le marché unique, ce qui renforcera en parallèle la capacité de l'UE face aux risques existants et émergents. Il importe donc que les pays candidats suivent la stratégie européenne en matière de sécurité économique et, au besoin, s'alignent progressivement sur la législation de l'UE ayant trait aux objectifs de sécurité économique.

3. Améliorer la sécurité économique de l'Europe dans les domaines à haut risque

Dans le sillage de la stratégie de 2023 ont été commandées des évaluations des risques portant sur la résilience des chaînes d'approvisionnement et la sécurité énergétique, les infrastructures critiques, l'instrumentalisation des dépendances économiques, la sécurité technologique et les fuites de technologies. Quatre technologies critiques — l'IA, les technologies quantiques, les semi-conducteurs et les biotechnologies — ont déjà été évaluées. Au vu de ces travaux, la Commission a délimité six **domaines à haut risque** qui concentreront ses efforts dans un premier temps, en étroite coopération avec les États membres, l'industrie et nos partenaires de confiance. En parallèle, la Commission continuera de suivre l'évolution de la situation pour, le cas échéant, évaluer d'autres domaines à haut risque émergents et les intégrer dans son action.

Aperçu des six domaines à haut risque



3.1. Renforcer la résilience des chaînes d'approvisionnement et réduire les dépendances à

Indicateurs non cumulatifs d'une dépendance à haut risque:

- 60 % ou plus de l'approvisionnement de l'UE est contrôlé par un pays tiers, ou ses opérateurs économiques,
- des intrants/services ont une valeur systémique dans l'économie de l'UE en raison de leur rôle dans de multiples secteurs, à l'instar de matières premières critiques, des semi-conducteurs etc.,
- des intrants/services sont essentiels pour l'industrie ou les capacités stratégiques de défense de l'UE, ou pour certaines chaînes d'approvisionnement en technologies critiques, comme les technologies énergétiques propres,
- un pays tiers a déjà instrumentalisé les dépendances économiques à son égard, ou a menacé de le faire, par exemple au moyen de restrictions à l'exportation,
- il existe déjà une surcapacité non marchande ou elle est en cours de création.

haut risque en biens et services critiques

Le risque. Nos économies modernes sont profondément interconnectées et sont tributaires d'un large éventail d'intrants, de biens intermédiaires et de services essentiels fournis par des entreprises du monde entier. Dans certains cas, l'offre est

fortement concentrée, souvent dans des pays qui ne partagent pas les mêmes intérêts stratégiques et qui ont la capacité et le dessein de creuser et d'instrumentaliser ces dépendances. Ces risques pour les chaînes d'approvisionnement de l'UE sont particulièrement visibles dans notre dépendance aux **matières premières, transformées ou avancées critiques, composants de technologies propres et semi-conducteurs basiques**, ainsi que dans les domaines des **services financiers, des produits pharmaceutiques, de l'aéronautique, des technologies numériques et spatiales**. Elles sont aussi visibles dans le **secteur agroalimentaire**, où la «vision pour l'agriculture et l'alimentation»² souligne la nécessité de réduire les dépendances stratégiques, surtout lorsque l'UE dépend d'une poignée de pays fournisseurs pour les importations d'aliments pour animaux, d'additifs pour l'alimentation animale et d'engrais.

Les dépendances à haut risque peuvent: i) être **instrumentalisées** à des fins de coercition (matières premières critiques, semi-conducteurs basiques, matériaux avancés, produits énergétiques, menaces de désactivation de certains services etc.); ii) créer une **vulnérabilité économique systémique** ou un risque systémique pour l'ordre public et la santé publique en cas de crise (équipements de protection individuelle, approvisionnement en médicaments critiques, fournitures alimentaires etc.); iii) poser le risque de perturbations intersectorielles à grande échelle (intrusion dans les réseaux de télécommunications, dépendance à un fournisseur unique de services en nuage, arrêt brutal de services numériques etc.); iv) **compromettre la compétitivité de l'Union en ralentissant les transitions écologique et numérique** en cas de rupture d'approvisionnement (batteries, aimants permanents, produits et composants de technologies propres, matériaux avancés etc.); v) porter atteinte à l'autonomie des États membres en matière de développement et de mobilisation de leurs **capacités militaires**; vi) menacer la souveraineté alimentaire de l'UE.

Exemple d'application: les semi-conducteurs basiques

Le risque. La dépendance structurelle envers un seul fournisseur non européen pour la fabrication de puces basiques, à faibles marges, représente un risque pour plusieurs industries européennes. Ces semi-conducteurs sont un maillon essentiel de plusieurs chaînes d'approvisionnement.

Utilisation des outils: la Commission collaborera avec des partenaires de confiance pour diversifier les sources d'approvisionnement et travaillera à développer la production de l'UE. La révision à venir du règlement sur les puces contiendra des mesures d'atténuation des risques efficaces. La cybersécurité des semi-conducteurs basiques importés utilisés dans des applications liées à la sécurité devrait faire l'objet d'une évaluation approfondie au titre du règlement sur la cyberrésilience.

Objectif. La Commission et les États membres tâcheront de **réduire au minimum le risque de perturbations à court terme** tout en mettant en œuvre des mesures visant à **résorber progressivement les dépendances à haut risque que connaît actuellement le marché unique** et à **combattre les tentatives d'en créer de nouvelles**. La Commission utilisera ses outils pour surveiller la chaîne d'approvisionnement, créer un cadre favorable à la

² COM/2025/75 du 19 février 2025.

diversification de l'approvisionnement et prévenir le sapement des efforts de l'UE en remédiant aux distorsions de concurrence dans le marché unique. Les mesures en faveur de l'économie circulaire joueront aussi un rôle important.

La Commission prendra les mesures nécessaires pour protéger ces chaînes d'approvisionnement supplétives du dumping et de la manipulation des prix.

La Commission aidera les États membres à déployer pleinement et efficacement les outils existants, notamment les critères de résilience que les États membres devront faire jouer dès janvier 2026 dans leurs marchés publics, enchères et régimes d'aide publique en vertu du règlement pour une industrie «zéro net».

La Commission prendra aussi des mesures pour développer les **capacités internes de l'UE** et diversifier l'approvisionnement **grâce à la coopération avec ses partenaires, notamment en s'appuyant sur son vaste réseau d'accords commerciaux et d'autres formes de coopération bilatérale et plurilatérale**. Ainsi, elle envisagera la production de certains produits critiques dans les pays candidats, ou les pays partenaires de l'UE, au Moyen-Orient et en Afrique du Nord par exemple. Des chaînes d'approvisionnement diversifiées renforceront la résilience de l'UE et ouvriront de nouvelles perspectives à ses entreprises. La Commission continuera de détecter et de surveiller en permanence les vulnérabilités des chaînes d'approvisionnement et les **dépendances à haut risque** dans le cadre de son processus d'évaluation des risques et de ses échanges avec les États membres et l'industrie. .

3.2. Attirer dans l'UE des investissements à forte valeur ajoutée qui renforcent sa sécurité économique

Le risque. Les investissements entrants stimulent la résilience et la compétitivité de l'UE en créant des emplois, en développant les capacités industrielles, en faisant jouer les effets de levier et d'échelle et en favorisant l'innovation et le transfert de technologies. Toutefois, certaines formes d'investissements entrants peuvent présenter des risques. Ces risques sont notamment les suivants: i) les risques pour **la sécurité et l'ordre public**, concernant notamment l'accès aux données sensibles (géolocalisation, données biométriques, secrets d'affaires etc.), l'accès aux infrastructures critiques, l'accès aux technologies à double usage et à d'autres technologies critiques; ii) les risques pour **la résilience économique**, comme les dépendances sévères ou les situations où un seul maillon faible d'une chaîne d'approvisionnement critique, contrôlé par des entités à haut risque ou des pays tiers, menace notre sécurité économique (batteries, matières premières critiques, logiciels et composants etc.), en rendant l'UE vulnérable à des ruptures d'approvisionnement ou à une instrumentalisation; iii) les risques pour **la compétitivité**, comme l'absence de transfert technologique, un apport de valeur ajoutée limité (chaînes d'assemblage uniquement par exemple), ou le recours à des travailleurs venant du pays de l'investisseur avec les conséquences que cela entraîne sur le marché du travail local.

Objectif. La Commission s'attachera en priorité à ce que l'UE reste ouverte et attrayante pour les investissements étrangers, en trouvant un équilibre, lorsque la sécurité économique de l'UE le requiert, entre cette ouverture et l'impératif d'éviter que des

dépendances ne se creusent ou ne se créent. Par ailleurs, il est crucial de préserver la capacité des entreprises de l'UE à innover, par exemple en achetant à l'étranger les droits de propriété intellectuelle clés d'acteurs de pointe émergents, et de garantir la sécurité de l'approvisionnement et la continuité de l'activité. La Commission fera appel à ses instruments et initiatives pour concevoir et appliquer des mesures ciblées, qui soumettraient par exemple les investissements entrants à des conditions favorables au transfert de technologies pour les entités provenant de pays qui attaquent délibérément notre sécurité économique.

3.3. Soutenir le dynamisme de la base industrielle de la défense et de l'espace, tout comme d'autres secteurs industriels à haut risque

Le risque. La guerre d'agression menée par la Russie contre l'Ukraine, la montée des tensions géopolitiques et l'instrumentalisation des liens de dépendance commerciale à des fins

Exemple: véhicules électriques à accumulateur

Le risque. La position dominante de certains fabricants de véhicules électriques et le contrôle jaloux des technologies que nécessite cette production risquent de faire perdre au secteur automobile son rôle clé dans l'économie de l'Union, alors que ces fabricants tirent profit du marché de l'UE. Les véhicules connectés présentent aussi des risques inhérents de cybersécurité.

Utilisation des outils: la Commission étudie les moyens d'encourager les investissements à valeur ajoutée, y compris par des ajustements de sa politique commerciale et de concurrence. Elle continuera de surveiller les flux commerciaux et d'appliquer des mesures d'atténuation pour réduire les risques dus aux véhicules connectés, de soutenir les investissements dans la prochaine génération des technologies des véhicules électriques pour que l'Europe reste résiliente et compétitive et, le cas échéant, de limiter l'exposition à des entités à haut risque dans le domaine des composants connectés des véhicules électriques. Elle encouragera aussi le partage des technologies et savoir-faire susceptibles de renforcer les objectifs de sécurité économique de l'UE.

politiques soulignent l'importance d'investir dans une base industrielle européenne dynamique, notamment dans les secteurs de la défense et de l'espace et dans les secteurs stratégiques à double usage, tels que les transports (aviation, aéronautique, construction navale, ports etc.), qui nourrit toute l'économie de l'UE et soutient son autonomie stratégique. Les risques pour une telle base industrielle sont notamment les suivants: i) des investissements (internes) insuffisants; ii) de faibles volumes de production combinés à un recours insuffisant en technologies internes pour les infrastructures institutionnelles; iii) des politiques et des pratiques des pays tiers contraires aux règles du marché, qui entraînent des distorsions sur les marchés mondiaux et régionaux; iv) des contrôles à l'exportation injustifiés ou disproportionnés des produits et technologies européens menés par des pays tiers (extraterritorialité des régimes d'exportation des pays tiers); v) une aliénation et une perte de contrôle causées par les acquisitions étrangères, comme les acquisitions de portefeuilles d'actifs dans certains cas; vi) un cadre réglementaire rigide et des marchés des capitaux fragmentés qui ne facilitent pas les flux de fonds et ne favorisent pas l'essor de technologies à double usage, à haut risque ou à haut rendement.

Exemple d'application: les composants essentiels des drones et systèmes antidrones

Le risque. La dépendance à l'égard des fournisseurs de pays tiers pour les composants essentiels des drones, des batteries et des systèmes antidrones présente un risque, dans un domaine où l'expérience montre que l'efficacité opérationnelle des drones sur le champ de bataille dépend d'un cycle d'innovation extrêmement court (se comptant en mois voire en semaines).

Utilisation des outils: la Commission utilisera les outils de ses programmes consacrés à l'industrie de la défense pour sanctuariser les capacités de production de l'UE et raccourcir les cycles d'innovation des technologies des drones, au regard de l'expérience sur le terrain. Elle continuera de renforcer la coopération et l'échange d'informations gracieux entre organismes compétents (agences nationales et organisations internationales de passation de marchés — OCCAR, AED, OTAN etc.) et dans le cadre des instruments/actions des programmes européens de soutien à l'industrie de la défense. Pour garantir la résilience de la chaîne d'approvisionnement, elle établira une cartographie ciblée des chaînes d'approvisionnement de certains produits et équipements, dont des biens à double usage, et soutiendra leur production par des cofinancements.

Dans des secteurs critiques tels que la défense, certains composants proviennent d'entités à haut risque qui pourraient, en période de tension géopolitique, entraver l'accès et le recours à certains **équipements de défense, technologies à double usage et moyens de mobilité militaire**. Par ailleurs, il est crucial que l'UE conserve une main-d'œuvre hautement qualifiée et se maintienne dans la course à l'innovation caractérisant les technologies utiles aux secteurs stratégiques. S'agissant des capacités militaires et de défense dans l'UE, il est essentiel d'atténuer efficacement les risques en mobilisant rapidement des outils ciblés et efficaces.

Objectif. La Commission utilisera ses outils pour maintenir et développer les capacités de production stratégiques de l'UE, notamment: i) en favorisant les **investissements** publics et privés et, au besoin, en réduisant les risques qu'ils présentent; ii) en **soutenant la**

demande (mesures incitatives), y compris par l'agrégation de la demande et les achats communs; iii) en **empêchant la délocalisation** des capacités de production et secteurs

stratégiques; iv) en **se désengageant progressivement vis-à-vis des acteurs potentiellement hostiles** de la défense et d'autres chaînes d'approvisionnement critiques, par exemple en limitant l'acquisition hors l'Union de technologies critiques restreintes dans les domaines de la défense et de l'espace; v) en atténuant **les menaces que représentent les investissements directs étrangers** dans des entreprises fournissant des produits ou des technologies critiques; vi) en **soutenant le développement de technologies, de composants et de matériaux critiques** dans l'UE selon des objectifs à long terme et les besoins en fournisseurs internes de ces produits pour les infrastructures institutionnelles; vii) en veillant à ce que les entreprises de l'UE, et surtout les **jeunes entreprises** disposent des conditions nécessaires pour se développer, par exemple au moyen d'un financement adéquat et d'un traitement tarifaire temporaire favorable de certains intrants, ainsi que d'un écosystème favorable en ce qui concerne les capitaux.

La priorité sera de soutenir la **base industrielle de la défense et de l'espace**. L'accent sera mis tout d'abord sur les situations spécifiques à haut risque que le processus d'évaluation des risques a détectées, mais la Commission suivra de près la sécurité économique de tous les secteurs clés tels que les technologies propres, l'énergie et les industries circulaires et à forte

Exemple d'application: technologies quantiques

Risque: Des entités soutenues par des États étrangers et des entités à haut risque cherchent à accéder au savoir-faire et aux infrastructures de l'UE dans les domaines de l'informatique, de la communication et de la détection quantiques au moyen d'investissements, d'acquisitions ou de partenariats de R&D, accélérant les usages sensibles à des fins militaires et de renseignement à l'étranger et érodant la souveraineté technologique de l'UE.

Utilisation des outils: la Commission continuera de recenser les principaux acteurs/infrastructures quantiques de l'UE et de suivre les investissements étrangers, les partenariats et les flux de PI, afin d'alimenter le filtrage des IDE, le contrôle des exportations et les évaluations des risques en matière de sécurité de la recherche. Elle utilisera ses outils pour enquêter sur les investissements qui présentent des risques et pour collaborer avec les États membres afin d'apporter une réponse coordonnée et rapide aux tentatives d'acquisitions hostiles ou aux cas de fuite. Afin de soutenir les objectifs de sécurité économique, elle donnera la priorité aux financements et aux fournisseurs de composants et de services quantiques critiques de l'UE/partageant les mêmes valeurs, et limitera la dépendance à l'égard des fournisseurs quantiques ou des fournisseurs de services en nuage présentant un risque élevé dans des secteurs sensibles. Elle s'efforcera en outre de veiller à ce que les entités sous influence étrangère induite ne puissent pas accéder à des projets quantiques sensibles.

intensité énergétique, l'agroalimentaire, le numérique et l'électronique, l'aviation (y compris l'aéronautique), la construction navale, l'automobile et la santé.

3.4. Étoffer et conserver un rôle de premier plan dans le domaine des technologies critiques

Le risque. Certains pays tiers et certaines entreprises ont dévoilé une stratégie de prise de contrôle de technologies et de savoir-faire, encore en incubation ou déjà avancés, de l'UE. Dans certains cas, ces actions visaient à compromettre la capacité de l'Union à rester compétitive sur le plan technologique, et ce par tous les procédés: acquisitions, coopération R&D, rétro-ingénierie ou espionnage industriel. Ils arrivent parfois à leurs fins en privant artificiellement des sociétés innovantes de parts de marché pour diminuer les revenus que celles-ci peuvent réinvestir dans la R&D. À long terme, le positionnement géopolitique de l'UE, sa sécurité et sa bonne santé

économique dépendront du maintien et du développement de ses atouts technologiques. Préserver les capacités de l'UE dans l'ensemble de ces technologies, en renforçant les outils de financement de l'UE alloués à ce but et en s'attachant à préserver la sécurité de nos technologies et à en empêcher les fuites, relève d'une importance stratégique. Dans le même temps, il convient d'accorder une attention particulière à la mise en œuvre et à l'application de plus en plus fragmentées des contrôles des exportations de biens à double usage.

Objectif La Commission utilisera ses outils pour soutenir un environnement propice au développement de technologies critiques dans l'UE et prévenir toute action qui saperait les efforts de l'UE en remédiant aux distorsions. Elle suivra l'évolution du marché et apportera un soutien supplémentaire à la recherche et à l'innovation menées dans l'UE par les start-up et scale-up, les entreprises établies, les organismes de recherche et d'innovation et le monde universitaire. Elle s'attachera à assurer le déploiement industriel et la valorisation des réalisations en matière de RDI dans la base industrielle du marché unique. Le 28^e régime, qui fournit aux entreprises un ensemble unique et harmonisé de règles à l'échelle de l'UE en matière de constitution d'entreprises, de gouvernance, de mobilité et d'accès au financement, renforcera la résilience économique de l'UE en permettant des opérations transfrontières plus sûres et des chaînes d'approvisionnement plus solides et diversifiées.

La Commission fera progresser la sécurité de la recherche et de l'innovation et prendra les mesures d'accompagnement nécessaires pour atténuer le risque de fuite de technologie ou de savoir-faire, passant par exemple par les acquisitions prédatrices, la coopération en matière de R&D et d'investissements sur les marchés stratégiques et émergents de l'UE dans des destinations ou des secteurs sensibles, tout en continuant à promouvoir des partenariats internationaux de recherche et d'innovation fiables qui sont essentiels pour les objectifs de l'Union en matière de sécurité économique. Elle étudiera comment faire en sorte que les entreprises et les organismes de recherche et d'innovation de l'UE puissent se développer et éviter les acquisitions/transferts de propriété dus exclusivement à des possibilités insuffisantes de financement provenant de sources fiables. Dans le même temps, la Commission s'efforcera d'empêcher les entités à haut risque d'accéder aux actions soutenues par l'Union dans le domaine des technologies critiques, susceptibles d'être instrumentalisées contre l'UE.

3.5. Empêcher l'accès à des informations et données sensibles susceptibles de compromettre la sécurité économique de l'UE

Le risque. Les pays tiers ont accès aux informations/données sensibles de l'UE ou de ses États membres, par le biais de l'espionnage industriel, de la fourniture de matériel ou de logiciels utilisés dans certains produits (par exemple, véhicules connectés, systèmes 5G/autres systèmes de télécommunications, infrastructures de réseaux électriques, plateformes de séquençage de l'ADN), ou par le biais des liens de propriété et de contrôle de certaines entreprises détenant des informations/données sensibles (par exemple, les opérateurs portuaires, aéroportuaires et de trafic, les réseaux financiers, les modèles d'IA, les portails de données, les télécommunications, les données à caractère personnel ou les informations sensibles relatives à un marché). Il existe des implications évidentes sur la sécurité et l'ordre public, encore aggravées par des incidences économiques potentielles, par exemple liées à la fragmentation des chaînes d'approvisionnement. Dans le secteur de l'énergie, par exemple, ce risque s'étend à l'acquisition, par des investisseurs de pays tiers, d'entreprises de l'UE qui détiennent des technologies avancées pour la surveillance et le traitement des données opérationnelles provenant d'infrastructures énergétiques critiques.

Objectif Réduire et, si possible, éliminer le risque d'accès des entités à haut risque et des entités liées aux informations/données sensibles de l'UE ou de ses États membres et limiter ainsi les incidences négatives potentielles sur l'économie et la sécurité de l'UE. Une attention particulière sera également accordée au risque que peuvent représenter les travailleurs étrangers dans les secteurs stratégiques et les étudiants étrangers de l'enseignement supérieur, y compris dans les domaines des sciences, de la technologie, de l'ingénierie et des mathématiques (STIM), conformément aux procédures applicables.

3.6. Prévenir et atténuer les perturbations des infrastructures critiques de l'UE affectant l'économie de l'UE

Exemple: équipements de détection aux frontières de l'UE (ports, aéroports, frontières terrestres, etc.)

Risque: absence de pratique commune dans l'ensemble de l'UE, dépendance à l'égard d'un seul fournisseur ou d'un nombre limité de fournisseurs, accès non autorisé (y compris par des canaux autorisés, par exemple la maintenance) ayant une incidence sur les performances des équipements de détection et sur l'intégrité et/ou la confidentialité des informations sensibles connexes, vulnérabilité aux logiciels malveillants susceptibles de compromettre ou de fausser les informations/systèmes/réseaux connexes via les équipements

Utilisation des outils: sur la base de l'évaluation des risques de cybersécurité au titre de la directive SRI 2, la Commission s'efforcera d'atténuer les risques recensés en identifiant les fournisseurs à haut risque, en utilisant des schémas de certification de cybersécurité, en renforçant les normes de cybersécurité et en intégrant des exigences de sécurité dans les appels d'offres. La Commission évaluera le rôle potentiel des subventions étrangères dans l'octroi d'un avantage concurrentiel à certains fournisseurs.

Le risque. Les infrastructures critiques de l'UE — y compris les infrastructures critiques dans les domaines des transports, des systèmes spatiaux, de l'énergie et des communications, en particulier celles qui sont considérées comme stratégiques pour la mobilité militaire — pourraient être perturbées par des acteurs étrangers, ce qui pourrait avoir des effets en cascade sur l'économie européenne. L'accent sera mis sur la stabilité des services fournis. Ces perturbations pourraient survenir à la suite d'attaques physiques, informatiques ou hybrides, y compris le sabotage d'installations entières ou de certains de leurs composants/éléments. Elles pourraient également affecter les chaînes d'approvisionnement des TIC, qui sous-tendent des éléments ou services critiques pour les infrastructures essentielles. En outre, il existe un risque de prépositionnement de pays tiers et d'opérateurs à haut risque dans les infrastructures critiques de l'UE en vue d'acquérir la capacité de les perturber (le cas échéant). Par ailleurs, un risque pèse sur la réputation et la crédibilité de certaines infrastructures, si elles étaient menacées ou effectivement touchées. Enfin, il existe un risque que des pays tiers jouent un rôle de premier plan dans l'établissement de normes internationales, ce qui pourrait avoir une incidence sur les infrastructures critiques.

Exemple: onduleurs solaires

Risque: dépendance croissante à l'égard d'un seul fournisseur; cyberrisques — manipulation des paramètres de production d'électricité, prévention de la production d'électricité, accès aux données opérationnelles, infiltration des acteurs de la chaîne d'approvisionnement.

Utilisation des outils: la Commission continuera d'évaluer les cyberrisques au moyen d'une évaluation coordonnée dans le cadre de la directive SRI 2 (qui doit être achevée en 2026). Sur cette base, elle déploiera des mesures d'atténuation axées à la fois sur le renforcement de la préparation (par exemple, le règlement sur la préparation aux risques dans le secteur de l'électricité, la directive sur la résilience des entités critiques) et sur la lutte contre les vulnérabilités recensées, par exemple: la certification et la normalisation au titre du règlement sur la cyberrésilience et les critères autres que le prix au titre du règlement pour une industrie «zéro net». La Commission suivra l'évolution du marché et s'efforcera de prévenir ou d'atténuer les investissements à haut risque. La Commission continuera d'évaluer le rôle des subventions étrangères susceptibles de fausser les conditions de concurrence sur les marchés de l'énergie solaire, notamment au moyen d'importations faisant l'objet de subventions.

Objectif. Faire appliquer, conformément aux stratégies pertinentes de l'UE en matière de défense, de sécurité intérieure et de préparation, les règles existantes afin de réduire le risque de fuite/espionnage de données et de perturbation physique et informatique, et notamment: i) **limiter la propriété/le contrôle/l'exploitation des infrastructures critiques européennes par des entités à haut risque;** ii) **renforcer les mesures de protection physique;** iii) **limiter les cybervulnérabilités;** et iv) **limiter les dépendances à l'égard de fournisseurs uniques ou de fournisseurs à haut risque,** ainsi que les vulnérabilités dissimulées, les portes dérobées ou les éventuelles ruptures systémiques de l'approvisionnement en TIC, en particulier en cas de verrouillage technologique ou de dépendance à l'égard de fournisseurs; v) **réserver**

des capacités de production critiques de l'Union susceptibles de se déployer en période de

perturbations de la chaîne d’approvisionnement mondiale ou de crises sanitaires; vi) la Commission **empêchera les entités à haut risque de prendre part aux actions soutenues par l’Union**, y compris les actions soutenues par des institutions et instruments financiers publics; ; vii) soutenir le **développement de fournisseurs fiables de sous-composants critiques** dans l’Union et dans les pays tiers de confiance, afin qu’il existe des solutions de remplacement viables; viii) soutenir les **initiatives phares** dans le domaine de la défense et les domaines connexes (surveillance du flanc oriental, initiative de défense antidrones européenne).

4. Actions visant à renforcer la sécurité économique de l’UE

L’accès à des informations de qualité et leur analyse approfondie constituent le point de départ d’une politique et d’un processus décisionnel de l’UE efficaces et bien informés en matière de sécurité économique. Le système d’évaluation des risques lancé par la stratégie Europe 2023 restera au cœur de ces efforts. Les évaluations existantes seront mises à jour, approfondies et complétées par de nouvelles évaluations pour l’ensemble des technologies et chaînes d’approvisionnement critiques.

La Commission continuera à développer sa capacité de collecte d’informations sur la sécurité économique. Elle accélérera le **processus de cartographie des dépendances stratégiques en matière de chaînes de valeur qui entraînent des vulnérabilités pour l’économie de l’Union** et elle renforcera le **suivi et l’anticipation des actions de pays tiers** visant à créer ou à maintenir des dépendances.

En outre, le succès de la politique de sécurité économique de l’UE dépendra d’une **meilleure coordination tant au niveau de l’UE qu’avec les États membres**. Il s’agit notamment de parvenir à une compréhension commune des menaces pesant sur la sécurité économique, de recenser les risques concrets et d’élaborer des mesures d’atténuation. Ce travail devrait être étayé par de meilleurs flux d’informations, une compréhension complète des coûts et des avantages des actions de l’UE et une volonté d’agir conjointement si nécessaire, mettant ainsi l’UE en position de force. La Commission a pris les mesures organisationnelles internes nécessaires. Toutefois, ces efforts appellent également de nouvelles modalités de coopération avec les États membres et – dans des proportions croissantes – entre les États membres, et au sein de ceux-ci, notamment en ce qui concerne des domaines d’action de plus en plus stratégiques, mais traditionnellement décentralisés, tels que la recherche et l’innovation.

L’UE continuera de dialoguer étroitement avec les entreprises du secteur de l’**industrie**, en garantissant un échange d’informations sécurisé et un engagement plus structuré. L’industrie est en première ligne de la sécurité économique de l’UE. Les entreprises doivent devenir plus résilientes et diversifier leurs chaînes d’approvisionnement critiques, notamment en éliminant toute dépendance à l’égard d’un seul fournisseur à haut risque. Il est également essentiel d’intégrer dans leurs modèles économiques les coûts induits par une plus grande diversification, au vu des avantages qu’apporte la résilience aux risques géopolitiques. Il doit s’agir d’un **processus à double sens et d’une responsabilité qui doit être partagée entre le secteur public et le secteur privé**, afin de permettre aux décideurs politiques d’améliorer les capacités de l’UE en matière d’évaluation des menaces et de renseignement commercial et de

les doter des moyens d'action nécessaires, tout en aidant l'industrie à mettre en œuvre des mesures d'atténuation au niveau des entreprises.

La Commission, soutenue par la haute représentante, va:

- améliorer sa capacité de **collecte et d'analyse d'informations** en faisant progresser plus rapidement les évaluations des risques concernant des chaînes d'approvisionnement critiques, des infrastructures critiques et des technologies critiques spécifiques, et en lançant régulièrement des **appels à contributions** afin d'obtenir de la part de l'industrie et des parties prenantes des éléments sur les vulnérabilités de la chaîne d'approvisionnement et l'exposition à des pressions extérieures;
- promouvoir une **coordination et un échange d'informations accrus par l'intermédiaire de son réseau de sécurité économique avec les États membres**. La Commission utilisera le réseau pour favoriser l'élaboration de scénarios, harmoniser la compréhension des menaces, des risques et des possibilités d'atténuation, faciliter l'échange d'informations et soutenir la mise en œuvre, en particulier dans l'utilisation des outils relevant de la responsabilité des États membres. Dans ce contexte, la Commission veillera à ce que des systèmes d'information appropriés soient disponibles pour favoriser **l'échange rapide et sécurisé d'informations classifiées entre et avec les États membres** sur les questions de sécurité économique, y compris les évaluations des risques, les entités critiques et à haut risque et les transactions potentiellement préoccupantes. Cela complètera les travaux du réseau de constitution de stocks à l'échelle de l'UE, qui met l'accent sur la garantie de l'approvisionnement en biens essentiels dans les situations de crise;
- créer un **pôle d'information sur la sécurité économique**, avec le soutien du SEAE, de l'INTCEN/SIAC³, du réseau des délégations de l'UE et des États membres, ainsi que des outils existants de suivi économique du marché unique tels que la notification d'alerte de la chaîne d'approvisionnement (SCAN); il recensera et consolidera les informations disponibles dans le cadre des mécanismes publics et privés existants et coordonnera la collecte d'informations supplémentaires pertinentes pour la sécurité économique. Il s'agira notamment de mettre en place un **mécanisme de surveillance du marché** afin de recueillir des informations sur l'évolution de la situation dans les zones à haut risque, y compris des informations rapides sur les flux commerciaux dans les secteurs faisant l'objet d'une diversification, afin de veiller à ce que l'action de l'UE ne soit pas compromise. Le pôle d'information sur la sécurité économique consolidera également les informations sur les **entités à haut risque** afin de soutenir le processus d'évaluation de l'éligibilité à un financement de l'UE et de participation à un processus d'investissement ou de passation de marchés de l'UE. En outre, l'Autorité douanière européenne et la plateforme des données douanières de l'UE **permettraient de soutenir et de faire**

³ le Centre de situation et du renseignement de l'UE (INTCEN) du Service européen pour l'action extérieure fait partie de la capacité unique d'analyse du renseignement (SIAC) de l'UE et est le centre civil de renseignement de l'UE. Il fournit des analyses approfondies aux décideurs de l'ensemble des institutions de l'UE.

respecter efficacement la mise en œuvre des initiatives connexes de l'UE en matière de sécurité économique, en facilitant également l'échange d'informations pertinentes;

- intensifier **l'engagement structuré des délégations de l'UE**, en liaison avec les missions des États membres, d'autres organes de l'UE et les milieux d'affaires de l'UE présents dans les pays tiers; garantir des contributions efficaces à l'évaluation, au suivi et à l'atténuation des risques en ce qui concerne la sécurité économique, notamment en facilitant les échanges entre entreprises ainsi qu'entre entreprises et administrations publiques;
- évaluer, d'ici au troisième trimestre de 2026, dans quelle mesure le règlement sur les situations d'urgence et la résilience du marché intérieur (SURMI) permet de recueillir des informations sur la chaîne d'approvisionnement au niveau des entreprises auprès des sociétés opérant dans les secteurs à haut risque. À la lumière de cette analyse, la Commission évaluera la nécessité de nouvelles mesures;
- recommander aux États membres de nommer des **conseillers nationaux de haut niveau** pour la sécurité économique, chargés de la coordination intergouvernementale de l'évaluation et de l'atténuation des risques en matière de sécurité économique. La Commission encouragera une meilleure coordination des politiques et des actions conjointes **en réunissant régulièrement ces conseillers**. Elle invite également le Conseil de l'UE à envisager de convoquer régulièrement les formations compétentes du Conseil pour des discussions au niveau politique;
- créer un **groupe de conseillers de confiance, composé de représentants des entreprises de l'UE**, chargé, entre autres, de donner des conseils sur les risques spécifiques et les réponses potentielles et d'examiner les stratégies de réduction des risques. La Commission invitera régulièrement des représentants du secteur de l'industrie à participer aux discussions sectorielles du réseau pour la sécurité économique et, le cas échéant, à rendre compte aux commissaires européens;
- mettre en place un **portail d'information sur la résilience du commerce** afin de fournir aux entreprises de l'UE des informations actualisées, dans le cadre du portail «Accès aux marchés» (A2M), sur les restrictions à l'exportation et les autres mesures restrictives imposées par des pays tiers, ainsi que sur les risques potentiels liés à la nécessité de renforcer la résilience de l'UE;
- élargir l'**observatoire des technologies critiques** afin de recenser, de suivre et d'analyser l'industrie spatiale et de la défense et les chaînes d'approvisionnement connexes, de couvrir les technologies émergentes et de soutenir la mise en œuvre, au niveau de l'UE et au niveau national, des feuilles de route technologiques de l'UE qui en résultent;
- utiliser le futur **centre d'expertise en matière de sécurité de la recherche** pour promouvoir la sécurité de la recherche et accroître la résilience de la communauté des chercheurs, notamment en mettant en place une plateforme de diligence raisonnable pour aider les universités à choisir leurs partenaires internationaux;
- étudier les moyens d'aligner et d'**intégrer les pays candidats sur notre approche en**

matière de sécurité économique, en particulier dans les domaines où leurs vulnérabilités en matière de sécurité économique peuvent présenter un risque pour la sécurité de l'UE.

En s'appuyant sur une analyse et une gouvernance renforcées, l'UE peut mieux poursuivre ses objectifs en matière de sécurité économique: i) en clarifiant et en améliorant le déploiement des outils existants et ii) en mettant au point de nouveaux outils si nécessaire.

Premièrement, la **Commission adaptera la manière dont elle utilise certains de ses outils** pour les rendre plus efficaces dans la gestion des risques en matière de sécurité économique et s'efforcera d'améliorer la coordination entre ces outils.

La Commission prendra les mesures suivantes pour améliorer l'utilisation des outils:

→ Financements européens:

- À l'avenir, la Commission **encouragera, dans ses activités de financement, les projets qui soutiennent la sécurité économique de l'UE.**
- En particulier, elle devrait mobiliser un niveau de financement suffisant pour réduire les dépendances à l'égard des technologies, composants et matériaux critiques, en particulier dans des secteurs stratégiques tels que l'espace et la défense, y compris pour mettre pleinement en œuvre les feuilles de route technologiques de l'Observatoire des technologies critiques (OTC).
- La Commission, les États membres et les partenaires chargés de la mise en œuvre devraient s'efforcer d'empêcher les entités à haut risque de prendre part aux actions sensibles soutenues par l'Union. L'article 136 du règlement financier fournit une base juridique horizontale pour protéger la sécurité et l'ordre public de l'UE lorsque la Commission et les partenaires chargés de la mise en œuvre exécutent le budget de l'UE. Cela permet d'empêcher les entités à haut risque de bénéficier de fonds de l'UE et de restreindre l'accès aux fonds de l'UE dans les secteurs et domaines stratégiques des technologies et infrastructures critiques pour les entités provenant de pays tiers qui portent atteinte aux intérêts de l'UE en matière de sécurité économique. Pour éviter toute ambiguïté, les partenaires chargés de la mise en œuvre devraient s'abstenir de soutenir des projets qui contredisent ce qui précède, y compris dans le cadre d'opérations à leurs propres risques. À cette fin, et afin de garantir un meilleur alignement des politiques entre les programmes de l'UE et les objectifs en matière de sécurité économique, des orientations seront disponibles au premier trimestre de 2026, favorisant ainsi l'élaboration d'une approche plus cohérente et plus efficace. En outre, la Commission encouragera les États membres, le **groupe BEI et d'autres IFI/banques et institutions nationales de développement qui mettent en œuvre des budgets nationaux ou de l'UE à accorder la priorité au soutien aux entreprises de l'UE** qui réduisent les dépendances vis-à-vis de l'étranger dans des secteurs critiques, en particulier pour des projets spécifiques, des technologies critiques et des infrastructures critiques recensés comme étant à haut risque. De même, les fournisseurs de pays tiers à haut risque devraient être empêchés

d'accéder aux financements nationaux et aux financements de l'Union lorsque ces pays tiers, sur la base de critères spécifiques, sont identifiés comme portant atteinte aux intérêts de l'Union en matière de sécurité économique.

→ Filtrage des IDE:

- Élaborer des **lignes directrices** s'appuyant sur l'expérience acquise dans la mise en œuvre de l'actuel règlement sur le filtrage des IDE afin de garantir que les autorités nationales de filtrage abordent ce processus de manière cohérente, y compris dans les secteurs stratégiques. Les lignes directrices indiqueraient également comment tenir compte du risque cumulé potentiel d'investissements multiples. À cela s'ajouteront des orientations sur l'interaction entre les éventuelles exigences au niveau de l'UE et l'application des mécanismes nationaux de filtrage dans le secteur financier.

→ Contrôles à l'exportation des biens à double usage:

- Procéder à une **évaluation globale** du règlement relatif au contrôle des exportations de biens à double usage. Dans le cadre de cette évaluation, la Commission évaluera si le règlement atteint ses objectifs dans le contexte des nouvelles réalités géopolitiques et géoéconomiques, y compris l'incidence du recours accru aux contrôles unilatéraux qui peuvent également avoir un impact sur le marché unique. Elle continuera d'étudier avec les États membres les moyens d'adopter efficacement des contrôles européens dans les domaines technologiques émergents dans ce nouveau contexte. Durant le processus d'évaluation, la Commission assurera une sensibilisation active des parties prenantes parmi les États membres, les entreprises du secteur de l'industrie, les instituts de recherche et le monde universitaire.

→ Instruments de défense commerciale:

- Lorsqu'une affaire présente un intérêt pour la sécurité économique de l'UE, **il sera tenu compte de la sécurité économique de l'UE dans la conduite de l'enquête et dans la conception d'éventuelles mesures.**

→ Outils relatifs au marché intérieur, aux douanes et à la concurrence:

- Tirer pleinement parti du **règlement relatif aux subventions étrangères** pour maintenir une concurrence loyale dans les domaines où les subventions étrangères entraînent des distorsions qui présentent des risques pour la sécurité économique.
- Encourager les États membres à tirer pleinement parti des possibilités existantes en matière d'aides d'État, telles que l'encadrement des aides d'État pour une industrie propre, les lignes directrices concernant les aides d'État à finalité régionale, l'encadrement des aides d'État à la recherche, au développement et à l'innovation, le règlement général d'exemption par catégorie et les projets importants d'intérêt européen commun en tant qu'instruments visant à renforcer la résilience.
- **Réexaminer l'utilisation d'instruments douaniers stratégiques (suspensions**

tarifaires, contingents autonomes) pour les intrants clés en vue de soutenir la compétitivité des entreprises de l'Union.

Deuxièmement, la Commission **élaborera de nouvelles mesures** pour améliorer la sécurité économique de l'UE.

La Commission:

- Étudiera la possibilité de mettre en place un **mécanisme pilote de suivi des start-up au niveau de l'UE visant à recenser les start-up dans des domaines technologiques critiques qui sont vulnérables au risque d'acquisitions étrangères hostiles**, en les réorientant vers d'autres solutions d'investissement de l'UE et d'autres formes de soutien (par exemple, conseil, renforcement des capacités, mise en relation avec les investisseurs). Le mécanisme fonctionnerait en phase avec les initiatives existantes, telles que la stratégie de l'UE en faveur des start-up et des scale-up.
- Collaborera avec les autorités compétentes pour surveiller les **investissements de portefeuille** (qui ne relèvent pas du champ d'application du mécanisme de coordination des IDE) dans les domaines recensés comme étant à haut risque à des fins de sécurité économique.
- Introduira un volet sécurité économique des secteurs stratégiques clés dans le prochain **outil de coordination de la compétitivité**.
- Renforcera la base industrielle et la résilience des chaînes d'approvisionnement de l'UE au moyen de l'**acte législatif pour l'accélération de l'activité industrielle**.
- Poursuivra, comme indiqué dans ResourceEU, le développement des **marchés secondaires** des matières premières critiques, y compris au moyen de l'acte législatif sur l'économie circulaire, afin de faciliter le financement de projets stratégiques de matières premières critiques dans les domaines recensés comme étant à haut risque à des fins de sécurité économique.
- Évaluera, d'ici au troisième trimestre de 2026, les moyens de **renforcer la protection de l'industrie contre les politiques commerciales déloyales et les évolutions négatives du marché mondial, telles que les surcapacités**. À cet égard, la Commission évaluera l'efficacité et l'adéquation des outils existants et examinera la nécessité d'éventuelles nouvelles mesures.
- Réexaminera la **loi de blocage** afin de simplifier son application, de réduire les coûts de mise en conformité pour les personnes et les entreprises de l'UE et de créer un effet dissuasif crédible contre l'application extraterritoriale des sanctions de pays tiers. Cela renforcera la sécurité économique européenne en protégeant mieux les opérateurs de l'UE contre les mesures contradictoires prises par des pays tiers et en garantissant un cadre plus prévisible, plus efficace et plus ferme.
- Étudiera les modalités visant à encourager les entreprises de certains secteurs à haut risque à **veiller à ce que les approvisionnements proviennent d'au moins deux fournisseurs différents** et à limiter l'exposition à un seul fournisseur dominant.

- Étudiera la possibilité d'apporter un **soutien financier aux entreprises faisant l'objet de décisions de filtrage des IDE** dans des situations où leur viabilité financière pourrait être menacée en l'absence d'investissement, sans préjudice des règles en matière d'aides d'État.
- Proposera, dans le cadre de la révision des directives sur les marchés publics, **des critères de préférence européenne dans des secteurs stratégiques spécifiques** dans lesquels nos marchés publics stimulent la demande pour l'industrie européenne de pointe, augmentent notre résilience et atténuent les risques pour la sécurité.
- Encouragera les entreprises à **réduire leurs dépendances dans les domaines technologiques émergents** dans le cadre du futur règlement sur les puces 2.0, de l'acte législatif sur les technologies quantiques, de l'acte législatif sur le développement de l'informatique en nuage et de l'IA et de la stratégie de la Commission en matière de logiciels libres.
- Utilisera la prochaine révision du **règlement sur la cybersécurité** pour mettre en œuvre, au niveau de l'UE, des restrictions à l'accès des fournisseurs à haut risque aux infrastructures critiques.

5. Conclusion

L'UE reste fermement attachée à un commerce ouvert et fondé sur des règles, à des relations propices aux investissements et à la coopération internationale. Elle continuera donc de soutenir les échanges commerciaux et les investissements ouverts avec des partenaires du monde entier et à en tirer parti. Dans le même temps, compte tenu de l'environnement géopolitique actuel, il est impératif de préserver la sécurité économique de l'UE. Faire face aux risques qui découlent de l'ouverture est essentiel pour préserver cette dernière, de même que notre sécurité au sens large et la compétitivité de notre industrie.

L'UE dispose déjà de nombreux outils pour atteindre cet objectif. Ces instruments doivent désormais être utilisés de manière stratégique et, le cas échéant, être encore renforcés, à la fois pour décourager de manière crédible les menaces qui pèsent sur la sécurité économique de l'UE avant qu'elles ne se concrétisent et pour réagir efficacement lorsqu'elles se produisent. Pour y parvenir, la Commission, le Parlement européen et les États membres doivent travailler de concert et coopérer étroitement avec l'industrie, en vue d'une prise de décision efficace et éclairée.

L'UE est déterminée à faire un usage plus proactif, stratégique et coordonné de tous les outils disponibles pour construire une économie forte, sûre et résiliente à long terme et pour opérer efficacement dans les nouvelles conditions géopolitiques et géoéconomiques qui façonnent le commerce mondial.