Journal officiel
de l'Union européenne

FR
Série L

2023/2113

11.10.2023

RECOMMANDATION (UE) 2023/2113 DE LA COMMISSION

du 3 octobre 2023

relative aux domaines technologiques critiques pour la sécurité économique de l'Union en vue d'une évaluation approfondie des risques avec les États membres

LA COMMISSION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 292,

considérant ce qui suit:

(1) La Commission et le haut représentant ont reconnu qu'avec les tensions géopolitiques croissantes, l'approfondissement de l'intégration économique et l'accélération du développement technologique, certains flux et activités économiques peuvent présenter un risque pour notre sécurité économique et ont adopté une communication conjointe relative à la stratégie européenne en matière de sécurité économique ([1]) afin de mettre en place une approche stratégique globale de la sécurité économique.

(2) 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'Union, protection contre les risques et partenariat avec le plus large éventail possible de pays afin de répondre aux préoccupations et aux intérêts communs.

(3) Dans ce cadre et compte tenu des risques que peuvent présenter certaines dépendances économiques et évolutions techniques, l'Union a besoin d'une vision claire des risques pour sa sécurité économique et de leur évolution dans le temps.

(4) Ces risques devraient être identifiés et évalués avec les États membres de l'Union, moyennant des contributions des acteurs privés dans le cadre d'un processus dynamique et continu.

(5) La stratégie européenne en matière de sécurité économique a recensé quatre catégories générales et non exhaustives de risque qui doivent faire l'objet d'une évaluation approfondie: la résilience des chaînes d'approvisionnement, y compris la sécurité énergétique; la sécurité physique et la cybersécurité des infrastructures critiques; la sécurité des technologies et les fuites de technologies; l'instrumentalisation des dépendances économiques et la coercition économique.

(6) Dans sa communication conjointe, la Commission s'est engagée à évaluer les risques liés à la sécurité des technologies et aux fuites de technologies sur la base d'une liste de technologies stratégiques critiques pour la sécurité économique et, en ce qui concerne les risques les plus sensibles, à proposer une liste de technologies critiques en vue d'une évaluation des risques à mener conjointement avec les États membres d'ici la fin de 2023.

(7) La communication conjointe a recensé les trois critères de sélection des technologies présentant les risques les plus sensibles, définis de manière précise et prospective, qui doivent faire l'objet d'une évaluation approfondie: la faculté de la technologie à être détournée ou à servir de précurseur, le risque de fusion entre usage civil et militaire et le risque d'utilisation abusive de la technologie à des fins relevant de la violation des droits de l'homme.

(8) Le critère relatif à la faculté de la technologie à être détournée ou à servir de précurseur examine le potentiel et la pertinence de la technologie pour entraîner des augmentations significatives des performances et de l'efficacité et/ou des changements radicaux pour les secteurs, les capacités, etc.

(9) Le critère relatif au risque de fusion entre usage civil et militaire examine la pertinence de la technologie tant pour le secteur civil que pour le secteur militaire et sa capacité à générer des progrès dans ces deux domaines, ainsi que le risque d'utilisation de certaines technologies pour nuire à la paix et à la sécurité.

([1]) JOIN(2023) 20 final.

(10) Le risque d'utilisation abusive de la technologie à des fins relevant de la violation des droits de l'homme examine l'utilisation abusive potentielle de la technologie en violation des droits de l'homme, y compris la restriction des libertés fondamentales.

(11) À la suite d'une première analyse interne, la Commission a dressé une liste de 10 domaines technologiques critiques pour la sécurité économique de l'Union. Cette liste de domaines technologiques tient compte des travaux réalisés dans le cadre du plan d'action sur les synergies entre les industries civile, spatiale et de la défense ([2]). Il s'agit d'un document évolutif qui pourrait faire l'objet de nouvelles modifications reflétant les évolutions technologiques dans le cadre d'un exercice en cours.

(12) Sur la base des trois critères précis et prospectifs pour la sélection des technologies devant faire l'objet d'une évaluation approfondie, la présente recommandation recense 4 domaines technologiques considérés comme hautement susceptibles de présenter les risques les plus sensibles et les plus immédiats liés à la sécurité des technologies et aux fuites de technologies, à savoir les semi-conducteurs avancés, l'intelligence artificielle, les technologies quantiques et les biotechnologies. Ces domaines technologiques devraient, en priorité absolue, faire l'objet d'une évaluation collective des risques avec les États membres d'ici la fin de l'année. Sous réserve d'un travail exploratoire avec les États membres, cette évaluation collective peut se concentrer sur des sous-ensembles de technologies relevant de ces quatre domaines technologiques.

(13) La structuration de la liste reflète l'évaluation par la Commission des domaines technologiques les plus susceptibles de présenter les risques les plus sensibles et les plus immédiats liés à la sécurité des technologies et aux fuites de technologies. Ce travail peut aider à la prise de décisions concernant la marche à suivre. La Commission engagera un dialogue ouvert avec les États membres sur le calendrier et la portée appropriés de nouvelles évaluations des risques, compte tenu notamment de la contribution du facteur temps à l'évolution des risques. La Commission souhaiterait que le Conseil procède en temps utile à un échange de vues sur cet aspect de la stratégie en matière de sécurité économique, dans le cadre de ses délibérations politiques générales et de ses orientations en réponse à la communication conjointe. La Commission peut présenter d'autres initiatives à cet égard au plus tard au printemps 2024, à la lumière de ce dialogue et de la première expérience acquise dans le cadre des évaluations collectives initiales, ainsi que d'autres contributions susceptibles d'être reçues pour les domaines technologiques énumérés. Lorsqu'elle statuera sur des propositions de nouvelles évaluations collectives des risques avec les États membres sur un ou plusieurs des domaines technologiques supplémentaires énumérés, ou sur des sous-ensembles de ceux-ci, la Commission tiendra compte des actions en cours ou prévues visant à promouvoir le domaine technologique considéré ou à établir des partenariats dans ce domaine. Plus généralement, la Commission gardera à l'esprit que les mesures prises pour renforcer la compétitivité de l'Union dans les domaines concernés peuvent contribuer à réduire certains risques pour les technologies.

(14) L'évaluation des risques devrait avoir pour objectif de recenser et d'analyser les vulnérabilités de nature systémique en fonction de leur incidence potentielle sur la sécurité économique de l'Union et du degré de probabilité que l'incidence négative se concrétise. Afin de structurer l'exercice d'évaluation des risques à venir avec les États membres, la Commission a défini certains principes directeurs.

(15) La présente recommandation ne préjuge pas du résultat de l'évaluation des risques. Seuls les résultats de l'évaluation collective détaillée du niveau et de la nature des risques présentés peuvent servir de base à une discussion approfondie sur la nécessité de prendre des mesures précises et proportionnées pour promouvoir ou protéger l'un quelconque de ces domaines technologiques, ou tout sous-ensemble de ceux-ci, ou pour y établir des partenariats. Les États membres et la Commission peuvent utiliser ces informations pour concevoir de futures actions stratégiques, y compris des mesures de promotion, de partenariat ou de protection au niveau national, de l'Union ou international, qui devraient être proportionnelles au niveau de risque traité et avoir un champ d'application précis. À ce stade préalable à l'évaluation, on ne peut donc tirer aucune conclusion quant au recours à un instrument particulier figurant dans les boîtes à outils de l'Union ou des États membres pour promouvoir, protéger ou établir des partenariats avec d'autres en vue de renforcer la sécurité économique.

(16) Toute mesure susceptible d'être prise sera proportionnée et ciblée avec précision par rapport aux risques évalués pour chaque domaine technologique critique ou pour une technologie pertinente. Toute mesure mise en œuvre visera à cimenter la position de force de l'Union dans ces domaines et sera conçue de manière à réduire au minimum tout effet d'entraînement négatif sur le marché et l'économie. En particulier, ces évaluations contribueront à l'élaboration de politiques de l'Union en faveur de l'innovation et du développement industriel au profit des technologies recensées, y compris au moyen d'initiatives internationales,

([2]) 70 final

A ADOPTÉ LA PRÉSENTE RECOMMANDATION:

1. Sur la liste des 10 domaines technologiques critiques figurant à l'annexe, il est recommandé, dans un premier temps, que les États membres et la Commission évaluent, d'ici la fin de 2023, les 4 technologies ci-après ayant la plus forte probabilité de présenter les risques les plus sensibles et les plus immédiats liés à la sécurité des technologies et aux fuites de technologies:

   a) Technologies avancées des semi-conducteurs

      Les semi-conducteurs, la microélectronique et la photonique sont des composants essentiels des dispositifs électroniques dans des domaines critiques tels que les systèmes et applications des communications, de l'informatique, de l'énergie, de la santé, des transports ainsi que de la défense et de l'espace. En raison de l'énorme faculté de ces technologies à être détournées ou à servir de précurseur et de leur utilisation à des fins civiles et militaires, il est essentiel, pour la sécurité économique, de rester à la pointe de la construction et du développement de ces technologies.

   b) Technologies liées à l'intelligence artificielle

      L'IA (et ses logiciels), le calcul à haute performance, l'informatique en nuage et l'informatique de périphérie, de même que l'analyse de données, présentent un large éventail d'applications à double usage et sont essentiels en particulier pour le traitement de grandes quantités de données et pour la prise de décisions ou la formulation de prévisions reposant sur cette analyse fondée sur les données. Ces technologies recèlent un énorme potentiel précurseur à cet égard.

   c) Technologies quantiques

      Les technologies quantiques recèlent un vaste potentiel pour transformer de multiples secteurs, civils et militaires, en permettant de nouvelles technologies et de nouveaux systèmes qui utilisent les propriétés de la mécanique quantique. Il n'est pas encore possible de qualifier pleinement l'impact total des technologies quantiques qui sont ou seront développées.

   d) Biotechnologies

      Les biotechnologies ont une grande faculté à être détournées ou à servir de précurseur dans des domaines tels que l'agriculture, l'environnement, les soins de santé, les sciences de la vie, les chaînes alimentaires ou la production de produits biologiques. Certaines biotechnologies, telles que le génie génétique appliqué à des agents pathogènes ou à des composés nocifs issus de la modification génétique de micro-organismes, peuvent avoir une dimension sécuritaire/militaire, en particulier lorsqu'elles sont utilisées à mauvais escient.

2. La Commission invite les États membres à engager un dialogue ouvert sur un calendrier et la portée appropriés de l'évaluation collective des risques liés aux autres domaines technologiques énumérés en annexe, compte tenu de l'évolution rapide de l'environnement géopolitique et des différents degrés de probabilité que les technologies énumérées présentent les risques les plus sensibles et les plus immédiats liés à la sécurité des technologies et aux fuites de technologies.

3. Pour structurer l'exercice collectif d'évaluation des risques, les principes directeurs suivants ont été définis:

   a) identifier et analyser les vulnérabilités en fonction de leur incidence potentielle sur la sécurité économique de l'Union et du degré de probabilité que l'incidence négative se concrétise. L'analyse devrait recenser les principaux types de menaces et d'acteurs de la menace et tenir compte, le cas échéant, des facteurs géopolitiques pour évaluer la probabilité d'incidences négatives. Elle devrait également tenir compte, entre autres, de la chaîne de valeur des technologies, de l'évolution des risques ainsi que des évolutions technologiques pertinentes, y compris les éventuels goulets d'étranglement et les futurs goulets d'étranglement attendus, d'une cartographie de la position relative de l'Union dans chaque technologie, y compris les acteurs clés et les éléments de l'avance comparative de l'Union; l'interconnexion mondiale de l'écosystème de la technologie, y compris dans la recherche et la chaîne d'approvisionnement de la technologie;

   b) lors de la phase de définition de l'évaluation collective, il convient d'examiner si l'évaluation détaillée se concentrera sur certains sous-ensembles de technologies les plus pertinents;

   c) l'évaluation des risques ne sera pas propre à chaque pays;

d) donner la priorité aux risques susceptibles d'avoir des effets sur l'ensemble de l'Union;

e) assurer des synergies et des complémentarités avec les analyses existantes au niveau de l'Union et des États membres, afin d'alimenter le processus d'évaluation des risques;

f) tenir compte des contributions du secteur privé;

4. l'évaluation collective des risques devrait garantir la confidentialité, sur demande, des contributions reçues des États membres ou du secteur privé. Le document final issu de l'évaluation collective des risques sera dûment classifié;

5. les États membres et la Commission devraient effectuer l'évaluation en recourant aux instances existantes ou, le cas échéant, à de nouvelles instances, afin d'inclure des experts, en fonction de chaque technologie critique;

6. en outre, la Commission continuera de suivre l'évolution technologique et, si nécessaire, complétera la présente recommandation en proposant des technologies supplémentaires en vue d'une évaluation approfondie.

Fait à Strasbourg, le 3 octobre 2023.

Par la Commission
Thierry BRETON
Membre de la Commission

ANNEXE

Liste des 10 domaines technologiques critiques pour la sécurité économique de l'Union

	Domaine technologique	Technologies* * *Les technologies citées dans chaque domaine sont susceptibles de constituer un élément central de l'évaluation des risques, mais leur liste n'est pas exhaustive*
1.	TECHNOLOGIES AVANCÉES DES SEMI-CONDUCTEURS	— Microélectronique, y compris les processeurs — Technologies photoniques (y compris le laser à haute énergie) — Puces à haute fréquence — Équipements de fabrication des semi-conducteurs à des tailles de nœud très avancées
2.	TECHNOLOGIES D'INTELLIGENCE ARTIFICIELLE	— Calcul à haute performance — Informatique en nuage et de périphérie — Technologies d'analyse des données — Vision par ordinateur, traitement linguistique, reconnaissance des objets
3.	TECHNOLOGIES QUANTIQUES	— Informatique quantique — Cryptographie quantique — Communications quantiques — Détection et radar quantiques
4.	BIOTECHNOLOGIES	— Techniques de modification génétique — Nouvelles techniques génomiques — Forçage génétique — Biologie synthétique
5.	TECHNOLOGIES AVANCÉES DE CONNECTIVITÉ, DE NAVIGATION ET NUMÉRIQUES	— Communications et connectivité numériques sécurisées, telles que le RAN et le RAN ouvert (réseau d'accès radio) et la 6G — Technologies de cybersécurité, dont la cybersurveillance, les systèmes de sécurité et d'intrusion, criminalistique numérique — Internet des objets et réalité virtuelle — Technologies des registres distribués et de l'identité numérique — Technologies de guidage, de navigation et de contrôle, y compris l'avionique et le positionnement marin
6.	TECHNOLOGIES AVANCÉES DE DÉTECTION	— Détection électro-optique, radar, chimique, biologique, radiologique et distribuée — Magnétomètres, gradiomètres magnétiques — Capteurs de champ électrique sous-marin — Gravimètres et gradiomètres
7.	TECHNOLOGIES SPATIALES ET DE PROPULSION	— Technologies spécialisées axées sur l'espace, allant du niveau des composants au niveau des systèmes — Technologies de surveillance de l'espace et d'observation de la Terre — Positionnement, navigation et synchronisation (PNS) dans l'espace — Communications sécurisées, y compris connectivité en orbite terrestre basse (LEO) — Technologies de propulsion, y compris aérodynamique hypersonique et composants à usage militaire

	Domaine technologique	Technologies* * *Les technologies citées dans chaque domaine sont susceptibles de constituer un élément central de l'évaluation des risques, mais leur liste n'est pas exhaustive*
8.	TECHNOLOGIES ÉNERGÉTIQUES	— Technologies de fusion nucléaire, réacteurs et production d'électricité, technologies de conversion radiologique/d'enrichissement/de recyclage — Hydrogène et nouveaux carburants — Technologies à zéro émission nette, y compris l'énergie photovoltaïque — Réseaux intelligents et stockage de l'énergie, batteries
9.	ROBOTIQUE ET SYSTÈMES AUTONOMES	— Drones et véhicules (aériens, terrestres, de surface et sous-marins) — Robots et systèmes de précision à commande robotisée — Exosquelettes — Systèmes fondés sur l'IA
10.	TECHNOLOGIES AVANCÉES DE MATÉRIAUX, DE FABRICATION ET DE RECYCLAGE	— Technologies de nanomatériaux, de matériaux intelligents, de matériaux céramiques avancés, de matériaux solides, de matériaux sûrs et durables dès la conception — Fabrication additive, y compris sur le terrain — Fabrication de microprécision à commande numérique et usinage/soudage au laser à petite échelle — Technologies d'extraction, de traitement et de recyclage des matières premières critiques (y compris l'extraction hydrométallurgique, la biolixiviation, la filtration par nanotechnologie, le traitement électrochimique et la masse noire)