COMMISSION
EUROPÉENNE

Strasbourg, le 15.2.2022
COM(2022) 61 final

COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPÉEN, AU CONSEIL, AU COMITÉ ÉCONOMIQUE ET SOCIAL EUROPÉEN ET AU COMITÉ DES RÉGIONS

Feuille de route sur les technologies critiques pour la sécurité et la défense

1. Introduction

Rester à la pointe du développement technologique est essentiel pour garantir la prospérité et la sécurité de l'Europe, et le mode de vie européen. Jamais auparavant les nouvelles technologies n'ont transformé aussi rapidement les secteurs de la sécurité et de la défense, et elles estompent la frontière entre le domaine civil et le domaine militaire. Les technologies numériques, en particulier, ont une incidence sur les rapports de force à l'œuvre au niveau mondial en matière de sécurité. Il est donc crucial de veiller à ce que les secteurs de la sécurité et de la défense en Europe restent technologiquement adaptés aux objectifs qui sont les leurs.

De plus en plus, nombre de technologies critiques en matière de sécurité et de défense prennent leur source dans le domaine civil et utilisent des composants critiques à double usage. Pour accélérer l'innovation dans tous les domaines et favoriser la souveraineté technologique dans les secteurs de la sécurité et de la défense, il est nécessaire d'améliorer les échanges entre les communautés de la recherche et de l'innovation des secteurs civils et de la défense. Compte tenu de son expertise de longue date en matière de développement technologique civil et de ses nouveaux instruments de coopération en matière de défense[1], l'UE est bien placée pour jouer un rôle moteur. Toutefois, cela nécessitera une utilisation plus efficiente des ressources et une volonté d'explorer les possibilités offertes en ce qui concerne les éléments à double usage, dans le respect des valeurs fondamentales de l'UE. Cela signifie par ailleurs qu'il convient de réduire les dépendances stratégiques et les vulnérabilités des chaînes de valeur et d'approvisionnement associées à ces technologies.

La fragmentation des capacités européennes en matière de sécurité et de défense a entraîné une inefficacité économique, une réduction des capacités opérationnelles et une augmentation des dépendances stratégiques. La révolution en cours dans le domaine des technologies de sécurité et de défense et les nouveaux instruments de coopération de l'Union en matière de défense offrent à l'UE l'occasion d'éviter de répéter les erreurs du passé, de s'appuyer sur ses capacités existantes et de préserver sa prospérité économique et sa sécurité. **Le futur paysage européen en matière de technologies et d'innovation dans les secteurs de la sécurité et de la défense devrait s'ancrer d'emblée dans les cadres de coopération de l'UE.**

Dans son discours sur l'état de l'Union de 2021[2], la présidente von der Leyen a reconnu que si les travaux concernant le développement d'un écosystème européen de la défense avaient démarré, une Union européenne de la défense était encore nécessaire. La boussole stratégique de l'UE pour la sécurité et la défense (la «boussole stratégique»), qui doit être adoptée par les États membres en mars 2022, présentera une vision stratégique commune pour la prochaine décennie et définira la manière dont l'Union renforcera sa capacité à agir et à faire face à différents types de défis et de crises; à sauvegarder ses intérêts et à protéger ses citoyens; à investir et à innover pour développer conjointement les capacités et les technologies nécessaires; et à approfondir les partenariats fondés sur les valeurs et les intérêts de l'UE.

---

[1] Fonds européen de la défense (FED), examen annuel coordonné en matière de défense (EACD) et coopération structurée permanente (PESCO) en matière de défense.

[2] Discours sur l'état de l'Union 2021 de la présidente von der Leyen

La présente feuille de route sur les technologies critiques pour la sécurité et la défense répond à une demande du Conseil européen des 25 et 26 février 2021[3] visant à tracer la voie à suivre pour stimuler la recherche, le développement technologique et l'innovation (RDTI) et réduire les dépendances stratégiques de l'UE à l'égard des technologies et des chaînes de valeur critiques pour la sécurité et la défense. La feuille de route sera présentée lors du sommet informel qui se tiendra à Paris les 10 et 11 mars 2022, et elle alimentera la boussole stratégique. La feuille de route propose plusieurs étapes pour permettre à l'UE et aux États membres d'atteindre conjointement l'objectif susmentionné, notamment par les actions suivantes:

- recenser les technologies critiques pour la sécurité et la défense de l'UE, en les stimulant au moyen de programmes (RDTI) européens;
- veiller à ce que les considérations liées à la défense soient mieux prises en compte dans les programmes RDTI civils européens et dans les politiques industrielles et commerciales, le cas échéant, tout en veillant à ce que les possibles utilisations des technologies dans le domaine civil soient également mieux prises en considération dans les programmes RDTI de la défense;
- favoriser d'emblée une approche stratégique et coordonnée à l'échelle de l'UE en ce qui concerne les technologies critiques pour la sécurité et la défense, afin de tirer le meilleur parti possible des programmes RDTI de l'UE et des États membres, de créer des synergies entre les communautés RDTI des domaines civils et de la défense, et d'atténuer les dépendances stratégiques à l'égard de sources extérieures; et
- veiller à la coordination la plus étroite possible avec d'autres partenaires partageant les mêmes valeurs, tels que les États-Unis et l'Organisation du traité de l'Atlantique Nord (OTAN), dans des conditions mutuellement avantageuses.

2. Technologies critiques et dépendances stratégiques en matière de sécurité et de défense

Il ressort de la communication intitulée «Mise à jour de la nouvelle stratégie industrielle de 2020: construire un marché unique plus solide pour soutenir la reprise en Europe» («stratégie industrielle actualisée»)[4] de mai 2021 que le fait de jouer un rôle de premier plan dans le domaine des technologies demeure un moteur essentiel de compétitivité et d'innovation pour l'UE, notamment en ce qui concerne les technologies dites critiques[5]. Il y est également souligné qu'il importe de repérer et d'atténuer les dépendances stratégiques dans les «écosystèmes sensibles», notamment dans l'écosystème «Économie sociale et de proximité et Sécurité civile», et dans l'écosystème «Aérospatiale et défense», afin de garantir la résilience de l'UE.

[3] Déclaration commune des membres du Conseil européen, 26 février 2021

[4] COM(2021) 350 final

[5] Dans le cadre de ses travaux sur l'observatoire des technologies critiques, la Commission s'emploie à définir la «criticité» pour les besoins des secteurs de l'espace et de la défense et des secteurs civils connexes (notamment la sécurité).

Le plan d'action de la Commission sur les synergies entre les industries civile, spatiale et de la défense (ci-après le «plan d'action sur les synergies»)[6] de février 2021 reconnaît l'importance croissante, pour l'avenir de l'Europe en matière de sécurité et de défense, des technologies de rupture et des technologies génériques prenant leur source dans le domaine civil, et la nécessité de favoriser les synergies entre les technologies du secteur civil et de celui de la défense, et l'enrichissement mutuel entre ces industries. Le plan définit plusieurs actions clés visant à encourager l'échange d'informations et la coopération entre les communautés civiles et celles de la défense en utilisant les programmes et instruments RDTI de l'UE comme point de départ.

2.1. Les spécificités des secteurs de la sécurité et de la défense

L'industrie de la défense de l'UE compte des structures diverses, de grandes multinationales et des acteurs de petite taille et de taille moyenne. La demande émane presque exclusivement des gouvernements nationaux, qui contrôlent par ailleurs toutes les acquisitions de technologies et de produits liés à la défense, ainsi que leurs exportations. La diversité d'exigences, de dépenses et d'investissements publics nationaux continue de fragmenter le marché de la défense de l'Union avec le risque, parfois, d'entraver l'interopérabilité entre les forces armées nationales des États membres. Le secteur de la défense ne suit donc pas les règles habituelles ni les modèles économiques habituels régissant des marchés plus traditionnels, et il dispose dès lors d'une marge de manœuvre limitée pour exercer une influence sur les investissements et les choix du marché qui y sont liés. Il est donc difficile pour l'industrie de lancer de grands projets RDTI autofinancés dans le domaine de la défense.

Le secteur européen de la sécurité est confronté à des défis similaires, étant donné que les marchés y sont aussi essentiellement nationaux, mais encore plus fragmentés. Ses clients sont divers (forces de police, agences de sécurité intérieure, services douaniers, autorités frontalières, services privés de sécurité), les activités se déroulent à différents niveaux (local, régional, national), et l'organisation varie d'un État membre à l'autre. **La Commission présentera, en 2022, une étude sur le marché de la sécurité de l'UE et fournira de plus amples informations sur ce secteur complexe**. En outre, au premier semestre 2022, les services de la Commission feront la synthèse des propositions visant à encourager l'adoption d'approches axées sur les capacités dans l'ensemble des secteurs de la sécurité. Ces propositions renforceront le recensement précoce et prospectif des besoins et des solutions en matière de sécurité et de répression.

Les secteurs spatial et cyber sont des «catalyseurs» stratégiques pour les secteurs de la sécurité et de la défense. Le secteur spatial partage un grand nombre de leurs caractéristiques spécifiques, avec de faibles volumes de marché et un effet de levier limité sur le marché privé des composants. La résilience des programmes spatiaux et des chaînes de valeur spatiales est essentielle pour les objectifs de l'UE en matière de sécurité et de défense. Le secteur cyber joue également un rôle de plus en plus important dans l'ensemble des capacités de défense et requiert de l'attention et des investissements. Compte tenu de la multiplication rapide des cyberattaques ciblant les moyens et les réseaux tant civils que du secteur de la défense, et du rôle croissant du

[6] COM(2021) 70 final

secteur civil dans l'innovation et la normalisation dans le secteur cyber, il est nécessaire de resserrer les liens entre la cybersécurité et la cyberdéfense. La contribution de la Commission à la défense européenne dans le contexte de la boussole stratégique («communication sur la défense»), qui fait partie du présent train de mesures dans le domaine de la défense, expose d'autres mesures pour ces deux secteurs.

2.2. Cartographie des technologies critiques et des dépendances stratégiques en matière de sécurité et de défense

La stratégie industrielle actualisée fournit une cartographie et une analyse reposant sur une large assise des dépendances et des capacités stratégiques de l'UE, sur la base d'une première série d'examens approfondis des écosystèmes sensibles[7]. Si ces travaux ont servi de base à l'action stratégique en faveur d'une meilleure résilience de l'UE, il y est par ailleurs reconnu que des efforts supplémentaires sont nécessaires pour améliorer encore notre compréhension des dépendances stratégiques de l'UE et de la manière dont elles peuvent s'accentuer et conduire à de nouvelles vulnérabilités. Ces travaux incluent une deuxième série d'examens approfondis des écosystèmes sensibles et prévoient un système de suivi par l'intermédiaire de l'observatoire des technologies critiques (l'«observatoire»), voir section 2.3.

Les services de la Commission ont commencé à procéder à des examens approfondis dans les domaines des technologies en matière de défense et de sécurité, notamment dans le domaine de la cybersécurité, afin de soutenir la stratégie industrielle actualisée et le développement de l'observatoire. À ce jour, deux études de cas préliminaires ont été réalisées sur les domaines des technologies de défense des systèmes autonomes et des semi-conducteurs, qui ont été considérés comme constituant des échantillons représentatifs en raison de leur importance transversale pour les capacités militaires dans différents domaines (voir encadré 1). L'objectif était de repérer des éléments communs entre ces domaines des technologies de la défense, notamment en ce qui concerne les causes des dépendances et les risques qui y sont associés, ainsi que d'esquisser des premières pistes pour les atténuer.

Les études de cas confirment que le secteur de la défense est confronté dans une large mesure aux mêmes dépendances et vulnérabilités stratégiques que d'autres écosystèmes sensibles, notamment en ce qui concerne les lacunes technologiques, les matières premières (critiques), les compétences, les faibles investissements dans la RDTI et les réglementations extraterritoriales des pays tiers. Il en ressort également que les vulnérabilités du secteur sont généralement exacerbées par le caractère stratégique et sensible de ses activités (par exemple, des normes plus élevées en matière de sécurité de l'information et de sécurité de l'approvisionnement), ainsi que par la taille tout aussi marginale de son marché.

Les études de cas montrent en outre que certains des concurrents mondiaux de l'UE prennent davantage de mesures offensives et défensives pour promouvoir les technologies critiques et s'attaquer aux dépendances stratégiques que ne l'a fait l'UE jusqu'à présent. Par exemple, ils associent plus systématiquement les considérations nationales en matière de défense au

[7] SWD(2021) 352 final

développement technologique dans le domaine civil, investissent massivement dans leurs capacités RDTI et industrielles locales, attirent des investisseurs extérieurs et, parfois, déploient des stratégies d'achat agressives dans des pays tiers. Par ailleurs, ils protègent leurs propres expertises et influences industrielles en tirant parti d'interdépendances ou en appliquant des réglementations extraterritoriales strictes pour limiter l'accès de pays tiers aux technologies.

Si l'UE dispose de ses propres outils pour renforcer sa capacité industrielle conformément aux règles de l'Union, elle est freinée par la demande encore largement fragmentée du marché de la défense de l'UE, la séparation historiquement stricte entre RDTI civile et RDTI de la défense au niveau de l'Union et les investissements comparativement insuffisants des États membres dans la base industrielle et technologique de défense européenne (BITDE). En effet, les dépenses collectives consacrées à l'innovation en matière de défense par les États membres (2,5 milliards d'euros, soit 1,2 % des dépenses dans ce domaine) demeurent en retrait par rapport à l'objectif de 2 % fixé par l'AED il y a 15 ans.

Si les forces du marché ont conduit à une situation dans laquelle aucun pays ne peut, seul, parvenir à une entière souveraineté technologique dans un domaine de technologies, il y a une course mondiale à la primauté technologique et aux avantages économiques et militaires qui y sont associés. Si l'UE ne réagit pas, cela pourrait aggraver ses dépendances stratégiques actuelles et en créer de nouvelles. Une approche structurée est nécessaire pour que l'UE reste à la pointe des technologies critiques et pour recenser et atténuer les dépendances stratégiques dans le domaine de la sécurité et de la défense. La présente feuille de route vise à fournir une telle approche, à intégrer dans la boussole stratégique de l'UE.

Encadré n° 1: Études de cas – Systèmes autonomes et semi-conducteurs pour la défense

Les travaux d'analyse réalisés par la Commission sur les systèmes autonomes dans le domaine de la défense, avec une attention particulière portée sur l'intelligence artificielle (IA) et l'apprentissage automatique, ont permis de recenser les technologies critiques pertinentes et quatre domaines d'action où l'UE est à la traîne, à savoir les compétences, les données, le matériel informatique et les essais. Les mesures possibles pour remédier aux lacunes recensées s'appuieraient sur la stratégie existante de l'UE en matière d'IA[8] et les initiatives stratégiques connexes, ainsi que sur les stratégies nationales des États membres en matière d'IA. Il s'agit notamment des activités de RDTI (par exemple, disponibilité accrue des données et entraînement des systèmes d'IA, lien avec l'initiative relative à un processeur européen), des infrastructures (par exemple, capacités en matière d'informatique en nuage à des fins de défense, installations d'essai nationales) et de la protection des actifs critiques existants (par exemple, le filtrage des investissements directs étrangers).

Les travaux d'analyse sur les semi-conducteurs destinés au domaine de la défense ont mis en évidence l'omniprésence des semi-conducteurs dans les équipements de défense, ainsi que les dépendances actuelles et futures dues, notamment, au manque de capacités propres de l'UE (fonderies) pour les nœuds les plus avancés. La Commission a inclus des mesures d'atténuation dans le paquet législatif sur les semi-conducteurs adopté le 8 février 2022[9], qui

8 COM(2018) 237 final
9 COM(2022) 45 final

vise à créer un écosystème européen des semi-conducteurs à la pointe du progrès afin d'améliorer les capacités de l'UE dans ce domaine et, partant, à répondre aussi aux besoins dans le domaine de la défense.

2.3. L'observatoire des technologies critiques

Le manque de perspective sur l'importance future des technologies est en partie imputable à certaines des dépendances stratégiques existantes de l'UE vis-à-vis des pays tiers (par exemple, en ce qui concerne les systèmes pilotés à distance ou les semi-conducteurs). L'UE a besoin d'une vision et d'une réflexion stratégique plus structurées sur les technologies critiques pour la sécurité et la défense, qui lui permettent de recenser les domaines qui sont prioritaires pour stimuler la recherche et l'innovation, réduire les dépendances stratégiques existantes et éviter l'apparition de nouvelles dépendances.

L'observatoire des technologies critiques, actuellement mis en place par la Commission conformément au plan d'action sur les synergies (action n° 4), contribuera à cette réflexion. Ses méthodes de travail prendront en considération d'autres initiatives similaires[10] afin d'éviter les doubles emplois. Cela permettra d'affiner la liste des technologies critiques mentionnées dans le plan d'action sur les synergies afin de tenir compte de l'évolution du paysage technologique et des besoins en matière de capacités.

L'observatoire recensera, surveillera et évaluera les technologies critiques pour les secteurs de l'espace, de la défense et les secteurs civils connexes, leurs applications potentielles et les chaînes de valeur et d'approvisionnement qui y sont liées. Par ailleurs, il recensera, surveillera et analysera les lacunes technologiques existantes et prévisibles, et les causes profondes des dépendances et des vulnérabilités stratégiques.

Il sera essentiel de convenir avec les États membres du niveau de détail approprié pour discuter de ces questions au niveau de l'UE, et de la nécessité d'un partage des données pertinentes entre les différents États membres et avec la Commission. Un mécanisme sera mis en place au sein de l'observatoire, sous la forme d'un groupe d'experts ad hoc, pour échanger et discuter avec les États membres dans un environnement sécurisé. Il s'agira notamment de discuter de l'émergence de nouvelles technologies de rupture afin d'éviter de nouvelles dépendances pour les industries de la sécurité, de la défense et de l'espace. Le haut représentant et ses services seront associés à ce processus.

La Commission, sur la base des données de l'observatoire, présentera aux États membres un rapport classifié sur les technologies critiques et les risques associés aux dépendances stratégiques affectant la sécurité, l'espace et la défense d'ici la fin de 2022, puis tous les deux ans. La Commission élaborera des feuilles de route technologiques sur la base de ces rapports,

[10] Par exemple, le soutien et les outils des technologies de pointe pour l'industrie (ATI), le suivi des technologies spatiales critiques, l'agenda de recherche stratégique général (OSRA), les modules technologiques (TBB) et les principales activités stratégiques (KSA) de l'Agence européenne de défense (AED).

qui comprendront des mesures d'atténuation visant à stimuler la RDTI et à réduire les dépendances stratégiques en matière de sécurité et de défense.

Une fois les activités de l'observatoire bien établies, le champ d'application de ses travaux pourrait être étendu à d'autres industries, comme indiqué dans la stratégie industrielle actualisée.

Prochaines étapes:

- En 2022, la Commission mettra en place un groupe d'experts afin de faciliter les échanges avec les États membres en ce qui concerne les technologies critiques, les chaînes de valeur et les chaînes d'approvisionnement. Ce groupe d'experts fera partie de l'Observatoire des technologies critiques pour le secteur de la défense, le secteur spatial et les industries civiles connexes, l'objectif étant de:
  - consulter régulièrement les autorités des États membres en vue de l'élaboration du rapport classifié; et de
  - garantir un traitement approprié des informations sensibles et classifiées susceptibles d'être échangées dans le cadre de l'Observatoire des technologies critiques, de rapports connexes et de feuilles de route.
- D'ici à la mi-2022, la Commission présentera une étude relative au marché européen de la sécurité, qui permettra de mieux comprendre les caractéristiques spécifiques du marché de la sécurité civile, d'encourager le recensement des technologies critiques et des dépendances stratégiques, ainsi que de soutenir la nouvelle approche axée sur les capacités pour la sécurité et d'autres activités de RTDI.
- D'ici à la mi-2022, les services de la Commission élaboreront un document synthétisant les propositions visant à encourager l'adoption d'approches axées sur les capacités applicables dans tous les domaines de la sécurité.

3. Promouvoir la RTDI relative aux technologies critiques pour la sécurité et la défense

Les feuilles de route technologiques que la Commission élaborera sur la base des évaluations fournies par l'Observatoire constitueront le fondement d'activités allant de la programmation de la RTDI relative aux technologies critiques au développement d'initiatives phares de plus grande envergure, qui contribueront au renforcement de la compétitivité et de la résilience de l'UE dans les secteurs de la sécurité et de la défense. Pour que ces objectifs puissent être atteints, les ressources financières disponibles devront être utilisées plus efficacement, grâce à une meilleure coordination des programmes et instruments existants en matière de RTDI à l'échelle européenne et nationale.

3.1. Combler le fossé entre les RTDI européennes à des fins civiles et à des fins de défense

Conformément à son plan d'action sur les synergies (action nº 2), la Commission s'est engagée à renforcer, d'ici à 2022, la coordination interne entre les programmes et les instruments de l'UE (voir encadré nº 2), de façon à tirer parti des avantages considérables que présentent les synergies entre la RTDI à des fins civiles et celle à des fins de défense pour la croissance économique, le marché unique et la sécurité des citoyens européens.

Bien qu'il soit possible de poursuivre la réalisation de cet objectif également en 2023 (par exemple, en améliorant la planification et la synchronisation, en fournissant des orientations aux autorités de gestion des États membres, etc.), certains obstacles seront plus difficiles à surmonter à court et moyen terme et pourraient nécessiter la participation d'autres parties prenantes. Tel est le cas, notamment, lorsque les dispositions juridiques des actes de base des programmes et instruments de l'UE imposent des contraintes pratiques. Ainsi, par exemple, bien que des activités à double usage puissent être financées au titre du mécanisme pour l'interconnexion en Europe (MIE) et des Fonds structurels et d'investissement européens (Fonds ESI), les activités menées dans le cadre d'Horizon Europe[11] mettent l'accent sur des applications civiles; il n'existe pas de cadre permettant de soutenir directement de telles activités au titre de programmes et d'instruments de RTDI. De même, la stratégie de la Banque européenne d'investissement en matière d'octroi de prêts comporte toujours des restrictions concernant le secteur de la défense.

Afin de faciliter les échanges entre la communauté civile et la communauté de la défense, en particulier dans le domaine des technologies critiques, la Commission élaborera en 2023 une approche visant à encourager la pleine mise en œuvre de la RTDI à double usage au niveau de l'UE, à moyen et long terme, au titre des différents programmes et instruments européens. Ces travaux alimenteront également l'évaluation à mi-parcours des programmes sectoriels pertinents, tels que les fonds octroyés au titre du règlement portant dispositions communes, et notamment les fonds consacrés à la préparation en cas d'urgence sanitaire.

Encadré nº 2: Programmes et instruments européens de soutien à la RTDI relative aux technologies critiques pertinentes pour la sécurité et la défense, ainsi que du déploiement de leurs infrastructures au titre du programme financier pluriannuel (2021-2027)

- Le FED consacre 8 milliards d'euros à la recherche et au développement dans le domaine de la défense. 4 à 8 % du budget du FED alloué à la recherche et au développement, soit 100 millions d'euros au maximum par an, concerneront les technologies de rupture.
- Horizon Europe alloue, au titre du pilier II intitulé «Problématiques mondiales et compétitivité industrielle européenne», 1,6 milliard d'euros à la recherche et à l'innovation en matière de sécurité civile au titre du pôle «Sécurité civile pour la société», tandis que les technologies critiques bénéficient d'un soutien au titre des pôles «Numérique, industrie et espace», «Climat, énergie et mobilité» et «Alimentation, bioéconomie, ressources naturelles, agriculture et environnement». Des activités complémentaires sont financées au titre du pilier I intitulé «Science d'excellence» et par le Conseil européen de l'innovation (CEI) et l'Institut européen d'innovation et de technologie (EIT) au titre du pilier III intitulé «Europe plus innovante», ainsi que par des partenariats européens, qui mettent en commun et mobilisent des ressources afin de garantir l'avance technologique de l'UE ainsi qu'une autonomie stratégique ouverte dans des domaines critiques;
- le programme pour une Europe numérique encouragera les activités de déploiement pertinentes pour les technologies critiques dans les domaines prioritaires de la cybersécurité, de l'IA et du calcul à haute performance;

[11] Dans le présent document, les termes «Horizon Europe» désignent le programme d'exécution spécifique d'Horizon Europe et l'Institut européen d'innovation et de technologie, dont les activités portent exclusivement sur des applications civiles.

- le Centre de compétences pour l'industrie, les technologies et la recherche en matière de cybersécurité et le Réseau de centres de coordination adopteront en 2022 un programme stratégique relatif aux cyberinvestissements alimentant Horizon Europe et le programme pour une Europe numérique. Les synergies entre les technologies civiles et de la défense et les applications à double usage pourraient être examinées en liaison avec le FED, conformément aux règles applicables;
- les Fonds ESI [et notamment le Fonds européen de développement régional et le Fonds social européen plus (FSE+)] peuvent être utilisés afin de soutenir la BITDE;
- parmi les autres programmes, fonds et instruments pertinents de l'UE figurent le programme spatial, le MIE, le programme InvestEU, la facilité pour la reprise et la résilience (FRR), le programme LIFE, des partenariats public-privé, ainsi que des mécanismes de mixage.

3.2. Établir des liens entre les programmes et les instruments européens et nationaux de soutien à la RTDI en ce qui concerne les technologies critiques pour la sécurité et la défense

Si les programmes et les instruments de l'UE allouent des fonds importants aux activités de RTDI relatives à la sécurité et à la défense dans l'UE, la majeure partie du financement de ces activités incombe toujours aux États membres, et la fragmentation des marchés de la sécurité et de la défense reste un problème grave. Une coordination à l'échelle de l'UE sera donc nécessaire pour parvenir à la souveraineté technologique dans certains domaines technologiques critiques et atténuer les dépendances stratégiques dans d'autres domaines.

Les États membres sont invités à s'engager, dans le cadre de la boussole stratégique, à élaborer d'emblée, conjointement avec la Commission, une approche stratégique coordonnée à l'échelle de l'UE pour les technologies critiques pertinentes pour la sécurité et la défense, qui tienne pleinement compte de la diversité et de la complexité de la gouvernance des programmes et des instruments européens et nationaux. Cette approche devrait également prendre en considération d'autres structures de coordination, telles que le nouveau pôle d'innovation de l'UE pour la sécurité intérieure, présidé par le comité permanent de coopération opérationnelle en matière de sécurité intérieure (COSI), et le nouveau pôle d'innovation de l'UE dans le domaine de la défense, qui sera mis en place par l'AED.

Cette approche s'appuierait sur les rapports classifiés concernant les technologies critiques et sur les feuilles de route technologiques élaborées par la Commission, qui serviraient de point de départ pour les discussions entre les autorités des États membres et la Commission. L'objectif serait de recenser, sur la base des feuilles de route technologiques, les domaines dans lesquels il convient d'agir de toute urgence, ainsi que de mobiliser les programmes, instruments et stratégies de l'UE et des États membres en vue de garantir une approche coordonnée respectant les règles de l'UE en matière d'aides d'État. Cela permettrait de cibler les investissements au profit des domaines les plus importants pour la sécurité des citoyens de l'UE. Les priorités seraient revues à intervalles réguliers, de façon à garantir leur pertinence et des dépenses efficientes.

La Commission collaborera avec les États membres afin de déterminer le meilleur moyen de faciliter ce travail de coordination (par exemple, par l'intermédiaire du groupe d'experts de l'Observatoire).

3.3. Soutenir l'innovation et l'entrepreneuriat en matière de sécurité et de défense – Création d'un programme européen d'innovation dans le domaine de la défense

L'UE doit mieux utiliser tout le potentiel de sa communauté de l'innovation afin de soutenir la sécurité et la défense. À cet effet, il convient d'aider les acteurs non traditionnels ainsi que les jeunes pousses et les petites et moyennes entreprises (PME) innovantes existantes des deux secteurs à surmonter les importants obstacles technologiques, administratifs, réglementaires et à l'entrée sur le marché auxquels ils se trouvent confrontés, à se conformer aux normes de sécurité élevées et à avoir accès au financement. Le marché de la défense s'articule souvent autour de quelques grands acteurs, qui bénéficient du soutien d'une série de PME spécialisées ayant un accès direct limité à ce marché. L'accès au financement peut par conséquent s'avérer difficile pour les PME innovantes du secteur de la défense, qui peuvent de ce fait être plus enclines à se tourner vers des investisseurs étrangers ou être plus susceptibles d'être ciblées par ceux-ci. Les PME innovantes du secteur de la sécurité se trouvent dans une situation semblable et rencontrent des difficultés similaires lorsqu'elles doivent aborder des clients potentiels ou accéder à un financement adapté à leurs besoins[12].

Les jeunes pousses et les PME innovantes actives dans le domaine de la sécurité ont bénéficié du soutien de la Commission au titre d'Horizon 2020, dans le cadre duquel les petites entreprises innovantes ont reçu des fonds et obtenu des taux de réussite globaux supérieurs à la moyenne pour le défi sociétal 7 «Sécurité civile pour la société». Bien qu'elles continuent de bénéficier d'un tel soutien au titre d'Horizon Europe, les jeunes pousses et les PME du secteur de la sécurité auront encore besoin d'un soutien supplémentaire adapté pour pouvoir accélérer leur progression sur le marché. L'examen de nouveaux instruments en vue d'innovations à double usage pourrait stimuler leur capacité de production, leur compétitivité et leur durabilité.

La Commission a entamé le lancement d'activités similaires au titre du FED en vue de l'élaboration d'une boîte à outils en matière de défense et d'innovation à double usage couvrant les niveaux de maturité technologique (NMT)[13] 1 à 9. Des travaux sont actuellement menés en ce qui concerne les outils suivants, qui portent sur la défense, les nouvelles technologies et le double usage:

---

[12] Challenges and opportunities for SMEs and start-ups in EU security R&I (Défis et perspectives pour les PME et les jeunes pousses dans le domaine de la R&I en matière de sécurité dans l'UE), manifestation virtuelle du CERIS - Renforcement de la recherche et de l'innovation en matière de sécurité, 30 avril 2021

[13] Depuis 2014, l'UE a largement opté pour l'utilisation d'une échelle de niveau de maturité technologique (TRL) dans le cadre de ses programmes et instruments de RTDI. Cette échelle distingue neuf niveaux de maturité technologique, allant de la recherche fondamentale (TRL 1) à un produit final prêt à entrer sur le marché (TRL 9). Étant donné que l'application d'une technologie, et donc ses possibilités en termes de double usage, sont généralement révélés aux TRL 5 et 6, on peut considérer qu'une technologie est «neutre» aux niveaux TRL 1 à 4.

a) *Innovation en matière de défense au titre du FED* – Des actions spécifiques sont actuellement étudiées en vue de soutenir plus efficacement les projets relatifs aux technologies de rupture et aux solutions de défense innovantes et tournées vers l'avenir, ainsi que d'encourager en particulier la participation de PME innovantes, de laboratoires innovants et d'organismes de recherche et de technologie (ORT). Ces actions peuvent prendre différentes formes, telles que, par exemple, le coaching d'entreprise (programme de travail 2021), l'organisation de défis technologiques (programme de travail 2022), l'organisation de marathons de programmation (hackathons) ou la remise de prix (programme de travail 2023 ou suivants). Elles s'appuieront également sur l'expérience pertinente du CEI et pourraient être liées à la nouvelle initiative CASSINI en matière de défense.

b) *Mécanisme de mixage en faveur des investissements dans le domaine de la défense au titre d'InvestEU* – La création d'un tel mécanisme permettrait à la Commission de garantir des investissements réalisés par des intermédiaires financiers dans l'ensemble de l'UE en faveur de PME innovantes ou de PME du secteur de la défense stratégique. Cela permettrait d'atténuer les problèmes liés à l'accès limité au financement pour les PME mettant au point des technologies prometteuses pour la défense européenne, tout en fournissant des capitaux sûrs et en évitant des rachats hostiles de la part d'entités établies dans des pays tiers. Le fait de permettre aux PME et aux entreprises à moyenne capitalisation innovantes du secteur de la défense de bénéficier d'un meilleur accès au financement en fonds propres contribuerait à leur croissance et serait, en fin de compte, bénéfique pour la capacité d'innovation de la BITDE. La Commission examinera également s'il est nécessaire de mettre en place d'autres instruments afin de soutenir les principaux acteurs du marché au sein de la chaîne de valeur.

c) *Initiative CASSINI en faveur de la défense* – Cette initiative s'inspirerait de l'actuelle initiative CASSINI en faveur des PME et des jeunes pousses de l'industrie spatiale. Elle prévoirait des services tels que le développement d'entreprises et de réseaux d'entreprises (par exemple, l'appariement d'entreprises et l'accélération d'entreprises), la remise de prix et l'organisation de concours [parmi lesquelles des marathons de programmation (hackathons), des tutorats, etc.], qui complèteraient le mécanisme de mixage des investissements en faveur du secteur de la défense décrit plus haut.

d) *Incubateur d'innovation* – En 2022, la Commission mettra en place un incubateur d'innovation afin de soutenir le développement de nouvelles technologies et de façonner l'innovation à double usage, conformément au plan d'action sur les synergies (action 6), qui pourrait jouer un rôle important en comblant le fossé entre les programmes de RTDI du secteur civil et du secteur de la défense. Après une analyse systématique des résultats du développement technologique à un stade précoce, l'incubateur signalerait aux services compétents de la Commission et aux États membres les projets et/ou technologies susceptibles de conduire à des applications potentielles en matière de sécurité, d'espace ou de défense en vue de leur adoption éventuelle. La Commission se pencherait sur l'orientation pouvant être donnée aux projets ainsi signalés au profit, le cas échéant, d'autres mécanismes de financement, tels que le mécanisme de financement de la transition du CEI ou le FED.

e) *Soutien aux réseaux d'innovation* – Les réseaux transfrontières d'innovation en matière de défense pourraient jouer le rôle de courtiers en innovation et encourager l'intégration de solutions innovantes dans des projets collaboratifs. La veille technologique permettrait de déceler et de déterminer de nouvelles solutions et technologies innovantes susceptibles de présenter un intérêt pour les applications en matière de défense. Les centres de recherche et les installations d'essais techniques examineraient ensuite la pertinence de ces technologies dans le domaine civil et procéderaient à des échanges de bonnes pratiques. L'AED serait un partenaire essentiel de la Commission en vue de la mise en œuvre d'une autre partie de l'action 6 dans le cadre du plan d'action sur les synergies.

La Commission examinera comment lier la boîte à outils aux instruments de soutien de l'innovation dans les domaines de la sécurité (par exemple, Horizon Europe) ou de la cybersécurité (par exemple, le réseau de centres nationaux de coordination en matière de cybersécurité, en collaboration avec les pôles européens d'innovation numérique).

Les points forts complémentaires de la Commission et de l'AED devraient être regroupés dans un «**programme européen d'innovation en matière de défense**». Dans le cadre de ce programme, la Commission, forte de son expérience concernant l'exécution du budget de l'UE en faveur de la RTDI dans les secteurs civil et de la défense et de RTDI à double usage, jouera un rôle central dans la promotion de l'innovation pour la BITDE. Se fondant sur son savoir-faire en matière de défense, y compris en ce qui concerne le rapprochement des technologies émergentes et de rupture et des besoins en capacités militaires, l'AED continuera de créer des liens entre les États membres et de soutenir les efforts déployés par ceux-ci au moyen de son pôle d'innovation dans le domaine de la défense. La Commission et l'AED, grâce à une étroite collaboration, accéléreront en synergie l'innovation en matière de sécurité et de défense pour l'UE et ses États membres.

3.4. Compétences

Le manque de compétences et la pénurie de main-d'œuvre, et notamment de travailleurs qualifiés ayant une formation en sciences, en technologie, en ingénierie et en mathématiques, constituent des défis majeurs pour les secteurs de la défense et de la sécurité, qui en sont fortement tributaires, à l'instar de nombreuses autres industries de haute technologie. Vu l'évolution rapide des technologies et du panorama des menaces, il importe que l'industrie se tourne davantage vers de nouveaux et jeunes chercheurs et entrepreneurs, y compris des femmes, en adoptant une approche inclusive et accessible à l'égard de l'ensemble des talents, compétences et main-d'œuvre disponibles.

En novembre 2020, la Commission a lancé le pacte sur les compétences avec une première vague de partenariats en matière de compétences dans les trois principaux écosystèmes industriels que sont la microélectronique, le secteur automobile et les industries aérospatiale et de la défense. Les membres du pacte (industrie, universités et organismes de formation, partenaires sociaux) se sont engagés à garantir une offre de compétences continue et durable dans les domaines où cela est le plus nécessaire, en renforçant les compétences de 200 000 salariés et en permettant à 300 000 personnes de se reconvertir, grâce à des investissements publics et privés de l'ordre de 1 milliard d'euros d'ici à 2030.

Prochaines étapes:

- La Commission invite les États membres à s'engager, dans le cadre de la boussole stratégique, à élaborer d'emblée une approche stratégique coordonnée à l'échelle de l'UE en ce qui concerne les technologies critiques pertinentes pour la sécurité et la défense.
- En 2023, la Commission procédera à l'examen des instruments existants de l'UE et proposera d'autres moyens d'encourager la RTDI à double usage au niveau de l'UE.
- La Commission soutiendra l'innovation et l'entrepreneuriat dans le domaine des technologies critiques pour la sécurité et la défense, en s'appuyant sur: a) des actions spécifiques du FED; b) un nouveau mécanisme de mixage des investissements en faveur de la défense au titre d'InvestEU; c) une nouvelle initiative CASSINI en faveur de la défense; d) un nouvel incubateur d'innovation pour les nouvelles technologies et l'innovation à double usage en 2022; et e) un soutien accru aux réseaux d'innovation.
- La Commission, conjointement avec l'AED et son pôle d'innovation dans le domaine de la défense, mettra en place un programme européen d'innovation en matière de défense afin d'accélérer l'innovation dans le domaine de la sécurité et de la défense pour l'UE et ses États membres.

4. Réduire les dépendances stratégiques en matière de technologies critiques et de chaînes de valeur dans les secteurs de la sécurité et de la défense

Outre ses programmes et instruments de RTDI, l'UE dispose de plusieurs outils d'intervention qui peuvent contribuer à réduire ses dépendances stratégiques en matière de technologies critiques et de chaînes de valeur dans les secteurs de la sécurité et de la défense. Ces outils aident à renforcer la capacité industrielle, la compétitivité, la souveraineté technologique et la résilience de l'UE, mais aussi à protéger les innovations et capacités technologiques actuelles et futures.

Si cela se justifie, la Commission, sur la base des travaux de l'observatoire des technologies critiques et dans le cadre de la stratégie industrielle actualisée, tiendra compte systématiquement des considérations liées à la sécurité et à la défense lorsqu'elle mettra en œuvre et réexaminera les instruments industriels et commerciaux existants de l'UE ou en concevra de nouveaux, pour faire en sorte qu'ils soient adaptés à leur finalité.

– *Alliances industrielles* – Dans le cadre des alliances industrielles, un large éventail de partenaires (des acteurs publics et privés et la société civile, par exemple) s'associent pour agir ensemble concernant des objectifs stratégiques clés de l'UE dans des industries ou des chaînes de valeur spécifiques. Les alliances industrielles sont fondées sur les principes d'ouverture, de transparence, de diversité et d'inclusivité et opèrent dans le plein respect des règles de concurrence. Elles peuvent comprendre, lorsque cela se justifie, des axes de travail spécifiques visant à réduire les dépendances stratégiques dans les secteurs de la sécurité et de la défense. Cette question est à l'étude dans le cadre de l'alliance européenne pour les données industrielles, la périphérie et le nuage et de l'alliance industrielle pour les processeurs et les technologies des semi-conducteurs.

– *Projets importants d'intérêt européen commun (PIIEC)* – Les PIIEC sont lancés par les États membres et soumis aux règles de l'UE en matière d'aides d'État. Ils visent à regrouper des connaissances, du savoir-faire, des ressources financières et des acteurs économiques de toute l'UE afin de pallier des défaillances du marché ou des défaillances systémiques et de relever des défis sociétaux que des acteurs privés ne pourraient pas surmonter seuls, en particulier dans les domaines de l'innovation radicale et des infrastructures essentielles. Les PIIEC peuvent tenir compte d'aspects liés à la sécurité et à la défense. Tel pourrait être le cas du deuxième PIIEC sur la microélectronique annoncé dans la législation sur les semi-conducteurs.

– *Programmes de financement de l'UE* – L'UE a toujours eu une politique ouverte en matière de recherche et d'innovation. Cette politique est guidée par le principe de l'autonomie stratégique ouverte et vise à garantir des conditions de concurrence équitables et la réciprocité. L'approche mondiale de l'UE en matière de recherche et d'innovation encourage les partenariats stratégiques avec des partenaires partageant les mêmes valeurs, dans le respect des obligations internationales de l'UE (par exemple, l'OTAN, les États-Unis, le Canada, le Japon, la Corée du Sud, etc.)[14].

  Dans le même temps, il est nécessaire que l'Europe veille à ce que ses intérêts stratégiques soient préservés. Pour la période 2021-2027, la Commission a clarifié et harmonisé les règles de participation des pays tiers et d'éligibilité des entités pour les différents programmes et instruments de l'UE. Des conditions d'éligibilité spécifiques applicables aux activités sensibles sur le plan de la sécurité ont été établies pour certains programmes (Horizon Europe, le programme pour une Europe numérique, le FED, le programme spatial, le MIE) et précisées dans les programmes de travail correspondants afin de protéger les intérêts essentiels de l'UE en matière de sécurité. Le réexamen en cours du règlement financier de la Commission apportera également plus de clarté sur la manière de maintenir l'approche d'autonomie stratégique ouverte de l'UE, c'est-à-dire de préserver pleinement les intérêts essentiels de l'UE en matière de sécurité tout en respectant ses obligations internationales.

– *Normes* – Dans le cadre du plan d'action sur les synergies, la Commission encourage l'utilisation des normes hybrides existantes dans les secteurs civil et de la défense et l'élaboration de nouvelles normes de ce type d'ici la fin de 2022 (action nº 5) ainsi que la prise en considération de la défense dans sa politique et ses actions de normalisation. Si la stratégie de l'UE en matière de normalisation[15] vise à faire en sorte que l'UE joue un rôle de premier plan dans la définition des normes civiles, elle sera très pertinente pour le secteur de la défense également, étant donné que près de 80 % des normes utilisées dans ce dernier proviennent de secteurs civils. La Commission, en collaboration avec les parties prenantes (par exemple l'AED), étudiera la possibilité d'inclure des exigences liées à la défense dans les actions de normalisation qu'elle soutiendra dans le futur afin d'améliorer leur compatibilité avec les besoins en matière de défense.

---

[14] Il convient toutefois de noter que les programmes de recherche et de développement liés à la défense de la plupart de nos partenaires ne sont pas ouverts aux entreprises de l'UE.

[15] COM(2022) 31 final.

– *Filtrage des investissements directs étrangers* – L'UE est l'un des environnements les plus ouverts aux investissements étrangers et l'une des principales destinations des investissements directs étrangers (IDE) dans le monde. Cependant, certains investissements peuvent aussi porter atteinte aux intérêts essentiels de l'UE en matière de sécurité. Pour prévenir de tels risques, l'UE a mis en place un cadre de filtrage des IDE, qui est opérationnel depuis octobre 2020. Le premier rapport annuel sur le filtrage des IDE confirme l'importance d'un filtrage efficace des IDE au niveau des États membres et d'une coopération étroite au niveau de l'UE, mettant l'accent sur les risques potentiels pour la sécurité ou l'ordre public. Les États membres sont encouragés à mettre en place des mécanismes nationaux de filtrage des IDE; c'est chose faite dans 18 d'entre eux et en cours dans six autres. La Commission évaluera le règlement et présentera un rapport au Parlement européen et au Conseil d'ici octobre 2023.

– *Infrastructures critiques* – L'émergence de plus en plus rapide de technologies nouvelles et de technologies de rupture a une incidence significative sur la sécurité des équipements, des infrastructures, des services et des chaînes de valeur et d'approvisionnement des secteurs stratégiques, y compris ceux de la sécurité et de la défense. L'UE et les États membres doivent tenir compte de manière plus globale de ces vulnérabilités lorsqu'ils évaluent les risques et procèdent au suivi de ces derniers et lorsqu'ils mettent en œuvre des mesures visant à renforcer la résilience face aux menaces pour la sécurité, par exemple les menaces hybrides ou les cybermenaces. Une coordination au niveau de l'UE sera nécessaire pour faire en sorte que les États membres maintiennent un niveau de résilience à l'épreuve du temps et des normes de sécurité cohérentes à l'échelle de l'UE afin d'éviter les vulnérabilités.

– *Utilisation intelligente et circulaire des matériaux* – Le nouveau plan d'action pour une économie circulaire de mars 2020 est l'un des principaux éléments constitutifs du pacte vert pour l'Europe, le nouveau programme européen en faveur d'une croissance durable. L'innovation et de nouveaux modèles d'entreprise fondés sur une utilisation plus efficace des ressources, la création de nouveaux matériaux, la promotion des matières premières secondaires et des marchés publics plus durables permettront non seulement de préserver l'environnement, mais aussi de garantir l'accès de l'industrie aux matériaux. Les techniques de fabrication additive, les marchés publics écologiques et le recyclage des matériaux, s'ils sont correctement mis en œuvre, pourraient également contribuer à renforcer la compétitivité des industries de la sécurité et de la défense de l'UE, ainsi que la résilience de cette dernière.

– *Sécurité des données* – La stratégie européenne pour les données définit des mesures visant à faire en sorte que les particuliers et les entreprises puissent garder le contrôle de leurs données. Cette question sera abordée dans la loi sur les données que la Commission adoptera au début de l'année 2022.

  Dans le cadre du projet plurinational sur les infrastructures et services de données communs (réunissant la fédération européenne de l'informatique en nuage et les espaces européens communs des données), la Commission facilite des investissements (au moyen du programme pour une Europe numérique, du MIE et du fonds Next Generation EU, par exemple) dans des capacités «cloud-to-edge» (nuage-périphérie) sécurisées, résilientes, économes en énergie, accessibles en temps réel et fournissant un service de qualité dans toute

l'Europe. Garantir le transfert de technologies en nuage et de périphérie entre l'industrie civile (notamment l'industrie de la sécurité), l'industrie de la défense et l'industrie de l'espace renforcerait la souveraineté technologique. L'alliance européenne pour les données industrielles, la périphérie et le nuage pourrait servir à promouvoir de telles synergies.

– *Politique commerciale* – Il n'y a pas que pour l'UE que la complexité et la vulnérabilité des chaînes d'approvisionnement mondiales sont problématiques. D'autres pays dépendent de l'UE («dépendances inversées») et le commerce (ou l'«interdépendance») peut contribuer à la stabilité des chaînes de valeur mondiales. L'UE est également prête à agir avec fermeté et à se défendre contre les pratiques commerciales déloyales, telles que le recours à des subventions étrangères générant des distorsions, tout en respectant ses engagements internationaux. Elle continuera à utiliser au mieux sa panoplie d'instruments en matière de commerce et de concurrence, en veillant à ce qu'ils soient efficients et à jour. La Commission a donc proposé de nouveaux instruments, tels que le règlement relatif aux subventions étrangères[16], qui vise à remédier aux distorsions dans le marché intérieur causées par des subventions étrangères.

D'autres mesures pertinentes [l'introduction d'une éventuelle exonération de la taxe sur la valeur ajoutée (TVA) et la facilitation du transfert de produits de défense financés par l'UE, par exemple] sont énumérées dans la communication sur la défense.

Prochaines étapes:

- La Commission étudie la possibilité d'ajouter des axes de travail liés à la défense dans des initiatives telles que l'alliance européenne pour les données industrielles, la périphérie et le nuage et de l'alliance industrielle pour les processeurs et les technologies des semi-conducteurs.
- La Commission, en collaboration avec les États membres, déterminera la nécessité d'évaluer les risques des chaînes d'approvisionnement des infrastructures critiques, en particulier dans le domaine numérique, afin de mieux protéger les intérêts de l'UE en matière de sécurité et de défense, et fera rapport à ce sujet en 2023.
- La Commission encourage tous les États membres qui ne l'ont pas encore fait à mettre en place un mécanisme national de filtrage des IDE.

5. Dimension extérieure

Il est essentiel de coopérer avec des partenaires du monde entier partageant les mêmes valeurs pour renforcer la résilience et la sécurité de l'approvisionnement de l'UE tout en réduisant les dépendances stratégiques et en maximisant les avantages mutuels. Le principe de réciprocité joue un rôle important dans ce contexte. Traditionnellement, les partenaires de l'UE dans les domaines de la technologie, de la sécurité et de la défense sont les membres de l'Espace économique européen (en particulier la Norvège), les pays candidats, les pays du voisinage et d'autres pays tiers (comme les États-Unis, le Canada, le Japon et la Corée du Sud), ainsi que des

[16] COM(2021) 223 final.

organisations internationales (l'OTAN, par exemple). Parmi les échanges récents figurent notamment ceux qui sont mentionnés ci-dessous.

5.1. Conseil du commerce et des technologies UE - États-Unis

Le Conseil du commerce et des technologies UE - États-Unis (CCT) s'est réuni pour la première fois le 29 septembre 2021. Dans leur déclaration commune, l'UE et les États-Unis ont réaffirmé leur détermination à «se concentrer sur le renforcement de la résilience de leurs chaînes d'approvisionnement respectives et de la sécurité de l'approvisionnement dans des secteurs clés pour la transition écologique et numérique et pour assurer la protection des citoyens», ainsi que leur objectif consistant à «accroître la transparence de l'offre et de la demande, recenser leurs capacités sectorielles existantes respectives, échanger des informations sur les mesures stratégiques et sur les priorités en matière de recherche et de développement et coopérer concernant des stratégies visant à promouvoir la résilience et la diversification des chaînes d'approvisionnement». Les travaux les plus pertinents pour la présente feuille de route sont ceux qui sont en cours au sein des groupes de travail sur la sécurité des chaînes d'approvisionnement (y compris sur les semi-conducteurs dans le cadre d'un volet spécialisé), sur la sécurité des technologies de l'information et de la communication, sur les contrôles des exportations et sur le filtrage des investissements. Ces questions pourraient également être examinées dans le cadre du dialogue UE - États-Unis sur la sécurité et la défense lancé récemment.

5.2. Partenariat avec l'OTAN

Lors du sommet de Bruxelles de 2021, les dirigeants de l'OTAN ont défini un programme ambitieux en matière de technologies, en particulier concernant les technologies émergentes et les technologies de rupture (TE/TR)[17]. Ce programme a permis d'orienter encore davantage les travaux menés conformément à la stratégie de mise en œuvre de l'OTAN concernant les TE/TR, approuvée par les ministres de la défense de l'OTAN en février 2021.

La Commission et le haut représentant suivront l'état d'avancement des initiatives de l'OTAN dans ce domaine en entretenant des contacts réguliers avec l'OTAN au niveau opérationnel en vue d'éventuelles interactions mutuellement acceptables et bénéfiques avec les initiatives pertinentes de l'UE dans la plus grande transparence vis-à-vis des États membres, tout en évitant de créer de nouvelles dépendances technologiques ou capacitaires ou d'accroître les dépendances existantes.

Prochaines étapes:

- La Commission et le haut représentant examineront, dans le cadre du CCT UE - États-Unis et du dialogue UE - États-Unis sur la sécurité et la défense lancé récemment, les moyens de renforcer la résilience des chaînes d'approvisionnement et de garantir la protection des citoyens.
- La Commission et le haut représentant examineront avec l'OTAN, dans le cadre des déclarations communes sur la coopération UE-OTAN et dans la plus grande transparence

[17] Il a notamment été décidé de lancer l'accélérateur d'innovation de défense pour l'Atlantique Nord (DIANA) et un fonds OTAN pour l'innovation.

vis-à-vis des États membres, les moyens de promouvoir des interactions mutuellement acceptables et bénéfiques entre leurs initiatives pertinentes respectives.

6. Conclusions

Alors que la situation géopolitique mondiale reste complexe et que la course aux nouvelles technologies présentant un intérêt pour la sécurité et la défense se poursuit, l'UE et ses États membres doivent renforcer leur coopération en ce qui concerne les technologies qui sont essentielles pour la sécurité et la défense à long terme de l'Europe, ainsi que leurs efforts visant à réduire les dépendances stratégiques connexes.

Dans la présente feuille de route, la Commission propose de travailler en étroite collaboration avec les États membres pour recenser les technologies et les chaînes de valeur critiques pour la sécurité et la défense – ainsi que les causes profondes des dépendances stratégiques connexes dans le cadre de l'observatoire des technologies critiques – afin de soutenir une approche stratégique coordonnée à l'échelle de l'UE concernant les technologies critiques pertinentes pour la sécurité et la défense, qui permettra de tirer le meilleur parti des programmes et des instruments de l'UE et des États membres en matière de RTDI.

Afin de renforcer la compétitivité et la résilience des secteurs de la sécurité et de la défense, les conclusions de l'observatoire et les travaux connexes menés dans le cadre de la stratégie industrielle actualisée contribueront également à faire en sorte que les considérations liées à la sécurité et à la défense soient mieux prises en compte dans les politiques industrielle et commerciale de l'UE, dans les cas où cela se justifie et dans le respect des règles de concurrence et des obligations internationales de l'UE.

Les propositions contenues dans la présente feuille de route visent à contribuer à la dimension «RTDI» de la future boussole stratégique de l'UE, au moyen de laquelle les États membres fixeront des objectifs ambitieux à long terme pour renforcer sensiblement la sécurité et la défense de l'Europe.