

**Avis du Comité économique et social européen sur la feuille de route sur les technologies de sécurité et de défense**

[COM(2022) 61 final]

(2022/C 443/16)

Rapporteur: **Maurizio MENSI**Corapporteur: **Jan PIE**

Consultation	Commission européenne, 2.5.2022
Base juridique	Article 304 du traité sur le fonctionnement de l'Union européenne
Compétence	Commission consultative des mutations industrielles
Adoption en section	24.6.2022
Adoption en session plénière	14.7.2022
Session plénière n°	571
Résultat du vote	
(pour/contre/abstentions)	165/1/3

**1. Conclusions et recommandations**

1.1. Le Comité économique et social européen (CESE) soutient pleinement les objectifs de la feuille de route sur les technologies critiques pour la sécurité et la défense, celle-ci arrivant à un moment particulièrement opportun compte tenu de l'agression russe contre l'Ukraine. Cette feuille de route prévoit notamment de stimuler la recherche, le développement technologique et l'innovation, et de réduire les dépendances stratégiques de l'Union européenne (UE) à l'égard des technologies et des chaînes de valeur critiques pour la sécurité et la défense.

1.2. Le CESE se félicite de l'ambition affichée dans l'objectif de développer une approche globale qui transcende la ligne de démarcation entre les domaines civil et militaire et combine les niveaux européen et national. Cette entreprise est aussi complexe que difficile et ne sera pas menée à bien du jour au lendemain mais elle devrait être mise en œuvre très rapidement. L'invasion de l'Ukraine est un signal d'alarme appelant à agir beaucoup plus vite que d'habitude.

1.3. Le CESE invite les États membres à faire en sorte que leurs réactions immédiates à l'agression russe contre l'Ukraine soient conformes au contenu et aux objectifs de la feuille de route, qui constitue une entreprise à long terme. Les investissements nationaux à court terme dans le domaine de la défense doivent être coordonnés au niveau européen afin d'éviter une extension de la fragmentation et des doubles emplois; les marchés publics «prêts à l'emploi» dans des pays tiers ne doivent pas étouffer les projets européens de développement en cours ou prévus.

1.4. Le CESE recommande que l'observatoire des technologies critiques soit doté d'une gouvernance claire, de ressources substantielles et d'un solide statut institutionnel. Le CESE se félicite de la coordination étroite proposée avec les États membres et plaide en faveur d'un forum supplémentaire pour les échanges avec l'industrie, qui possède les meilleures connaissances en matière de technologies, de chaînes d'approvisionnement et de dépendances critiques.

1.5. Le CESE estime qu'il convient d'assurer l'intégration des résultats de l'observatoire des technologies critiques dans des feuilles de route et de les traduire en initiatives phares. La transition entre les différentes phases du cycle technologique et industriel ne peut être gérée avec succès que s'il y a une réelle appropriation des initiatives et une répartition claire des responsabilités. La cohérence et les synergies sont nécessaires non seulement sur le plan horizontal, entre les programmes de recherche, de développement technologique et d'innovation (RDTI) en matière civile et de défense, mais aussi verticalement, entre ces programmes et les programmes de déploiement.

1.6. Le CESE estime que la simplification et la rationalisation des programmes et instruments de l'UE en faveur de la RDTI sont fondamentales, dans l'intérêt des bénéficiaires eux-mêmes.

1.7. Le CESE propose la création d'un guichet unique en ligne pour les PME et les jeunes pousses, un «coin des PME de l'UE» en ligne, offrant la possibilité d'introduire des données prédéfinies et de recevoir en retour des informations sur mesure sur les programmes de l'UE les plus adaptés susceptibles d'apporter un soutien.

## 2. Contexte

2.1. La 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, à savoir, tracer la voie à suivre pour améliorer la recherche, le développement technologique et l'innovation et réduire la dépendance stratégique de l'UE à l'égard des technologies et des chaînes de valeur critiques pour la sécurité et la défense.

2.2. Il ressort de la communication de mai 2021 intitulée «Mise à jour de la nouvelle stratégie industrielle de 2020: construire un marché unique plus solide pour soutenir la reprise en Europe» 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 critiques. Le plan d'action de la Commission de février 2021 sur les synergies entre les industries civile, spatiale et de la défense reconnaît l'importance croissante, pour la sécurité et la défense européennes, des technologies de rupture et des technologies génériques prenant leur source dans le domaine civil, et la nécessité de favoriser l'enrichissement mutuel entre le secteur civil et celui de la défense.

2.3. Il a donc été décidé d'élaborer cette feuille de route, un document stratégique qui vise à développer une approche globale des technologies de défense et de sécurité, transcendant la frontière entre le civil et le militaire, et combinant des programmes de l'UE et des programmes nationaux. L'objectif de la feuille de route est de consolider la souveraineté technologique de l'Europe dans des secteurs stratégiques clés en renforçant la cohérence de l'ensemble des instruments et politiques pertinents de l'UE, qu'il s'agisse du programme Horizon Europe et du Fonds européen de la défense, du règlement sur les semi-conducteurs <sup>(1)</sup> et de la loi sur les données <sup>(2)</sup>, des règlements relatifs au filtrage des investissements directs étrangers <sup>(3)</sup> et aux subventions étrangères <sup>(4)</sup>, ou encore de la proposition de directive sur la sécurité des réseaux et de l'information (SRI 2) <sup>(5)</sup> et de la directive sur la résilience des entités critiques (REC) <sup>(6)</sup>. Le document présente un vaste cadre politique conceptuel abordant plusieurs thèmes étroitement liés, dans le but de contribuer à la «boussole stratégique» de l'UE en matière de sécurité et de défense <sup>(7)</sup>. Il a été publié en même temps qu'une communication sur la contribution de la Commission à la défense européenne, qui appelle à mettre en place un marché européen de la défense plus intégré et plus compétitif dans un contexte géopolitique et technologique en constante évolution, notamment en renforçant la coopération au sein de l'UE, en réduisant les coûts et en améliorant l'efficacité opérationnelle.

2.4. La feuille de route sur les technologies critiques pour la sécurité et la défense trace la voie à suivre pour renforcer la compétitivité et la résilience des secteurs de la sécurité et de la défense de l'UE en s'appuyant sur les éléments suivants: cartographie des technologies critiques et des dépendances stratégiques, surveillance et évaluation des technologies et chaînes d'approvisionnement critiques ainsi que des lacunes et dépendances technologiques (par l'intermédiaire de l'observatoire des technologies critiques, actuellement mis en place); encouragement du double usage pour la recherche et l'innovation au niveau de l'UE; incitation des États membres à élaborer une approche stratégique coordonnée à l'échelle de l'UE pour les technologies critiques dans le contexte de la boussole stratégique; soutien à l'innovation et à l'esprit d'entreprise en matière de sécurité et de défense au moyen d'une série de nouveaux outils et création, avec l'Agence européenne de défense, d'un programme européen d'innovation dans le domaine de la défense afin de regrouper les efforts respectifs.

2.5. L'un des aspects importants de la feuille de route est l'objectif de réduction des dépendances recensées à l'égard des technologies et des chaînes de valeur critiques. Dans cette optique, la Commission propose d'intégrer, le cas échéant, les considérations liées à la défense dans les grandes initiatives industrielles et technologiques de l'UE (alliances et normes, par exemple), de faire rapport sur la nécessité de procéder à des évaluations des risques pesant sur les chaînes d'approvisionnement des infrastructures critiques (en particulier dans le domaine numérique) et de renforcer le filtrage des investissements directs étrangers en encourageant tous les États membres à mettre en place un mécanisme national de filtrage.

---

<sup>(1)</sup> Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions — Action européenne sur les semi-conducteurs, COM(2022) 45 final, 8 février 2022.

<sup>(2)</sup> Proposition de règlement du Parlement européen et du Conseil fixant des règles harmonisées pour l'équité de l'accès aux données et de l'utilisation des données (règlement sur les données), COM(2022) 68 final, 23 février 2022.

<sup>(3)</sup> Règlement (UE) 2019/452 du Parlement européen et du Conseil du 19 mars 2019 établissant un cadre pour le filtrage des investissements directs étrangers dans l'Union (JO L 79 I du 21.3.2019, p. 1).

<sup>(4)</sup> Proposition de règlement du Parlement européen et du Conseil relatif aux subventions étrangères faussant le marché intérieur, COM(2021) 223 final, 5 mai 2021.

<sup>(5)</sup> Proposition de directive du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, abrogeant la directive (UE) 2016/1148, COM(2020) 823 final, 16 décembre 2020.

<sup>(6)</sup> Proposition de directive du Parlement européen et du Conseil sur la résilience des entités critiques, COM(2020) 829 final, 16 décembre 2020.

<sup>(7)</sup> Conseil de l'Union européenne, Bruxelles, 21 mars 2022.

### 3. Observations générales

3.1. La feuille de route reflète précisément l'évolution du paysage technologique, où les technologies critiques pour la sécurité et la défense sont de plus en plus guidées par l'innovation des secteurs commerciaux. Le CESE se félicite de l'intention de la Commission d'élaborer une approche globale qui transcende la fracture entre les secteurs civil et militaire et combine les niveaux européen et national. Il s'agira toutefois d'une tâche difficile et complexe, car elle implique une reconfiguration générale de l'approche actuelle. Cela ne se produira pas du jour au lendemain, mais devrait se faire très rapidement. Le CESE est fermement convaincu que l'invasion de l'Ukraine par la Russie doit être considérée comme un signal d'alarme appelant à agir beaucoup plus vite que d'habitude.

3.2. Dans le même temps, il souligne que la feuille de route est un plan à long terme et qu'il convient de veiller à éviter tout décalage avec les décisions actuelles des États membres en matière de marchés publics afin de combler le plus rapidement possible les lacunes les plus urgentes en matière de capacités. Le CESE a la ferme conviction que les investissements nationaux à court terme doivent être coordonnés au niveau européen afin d'éviter une extension de la fragmentation et des doubles emplois et de veiller à ce que les marchés publics «prêts à l'emploi» de pays tiers ne nuisent pas à la base industrielle et technologique de défense européenne en étouffant les projets européens de développement en cours ou prévus.

3.3. Le CESE est également d'avis que, pour favoriser les synergies, il est important de se pencher non seulement sur les technologies et les chaînes de valeur individuelles, mais aussi sur l'écosystème dans lequel ces chaînes de valeur sont intégrées. En effet, les transferts de technologie sont les plus susceptibles de se produire (ou de voir le jour) entre entreprises faisant partie d'un tel écosystème.

3.4. L'attention accordée dans la feuille de route aux technologies à double usage et aux synergies entre la sécurité, la défense et l'espace est importante pour atteindre les objectifs de l'UE dans ces domaines. Dans le même temps, le double usage et les synergies ne sont ni une fin en soi ni suffisants. L'objectif général de la feuille de route est que l'UE devienne résiliente et capable de se défendre elle-même, également contre les attaques à grande échelle (hybrides et militaires). Cela signifie qu'il est nécessaire d'accroître en outre les investissements dans la défense et la sécurité et d'inclure dans la feuille de route les technologies de défense «pures».

3.5. Le CESE invite la Commission européenne à évaluer le coût économique et social des dépendances critiques et de l'absence de souveraineté technologique dans le domaine de la défense.

### 4. Observations particulières

4.1. L'observatoire des technologies critiques sera la pièce maîtresse de l'approche proposée. Il recensera, surveillera et évaluera les technologies critiques, leurs applications potentielles et les chaînes de valeur et d'approvisionnement qui y sont liées, et surveillera les lacunes technologiques et les causes profondes des dépendances et des vulnérabilités stratégiques. Pour que l'observatoire puisse s'acquitter de ces tâches, le CESE souligne la nécessité de le doter de ressources substantielles, d'un statut institutionnel solide et d'une gouvernance claire.

4.2. Le CESE estime qu'il est important de comprendre comment l'observatoire sera mis en place et comment il fonctionnera dans la pratique. Pour remplir sa mission, l'observatoire doit définir des objectifs, des règles et des critères d'évaluation des technologies. Afin de recenser les technologies critiques, il devra établir des liens étroits avec les processus de recensement et de planification des capacités et des besoins, et en vue de mettre les capacités en adéquation avec les technologies, il devra élaborer une taxinomie appropriée qui sera idéalement applicable à la fois à la défense, à la sécurité et à l'espace. À cet égard, il est essentiel que l'observatoire travaille en étroite collaboration avec l'Agence européenne de défense et d'autres acteurs. Enfin, pour pouvoir dresser un état des lieux des dépendances critiques, il devra acquérir une connaissance et une compréhension très solides des chaînes de valeur et d'approvisionnement sous-jacentes.

4.3. Il est prévu de présenter un rapport classifié aux États membres tous les deux ans. Le CESE s'interroge sur ce long intervalle entre les rapports, compte tenu de l'évolution rapide de l'environnement technologique et industriel. Les informations recueillies par l'observatoire seront très sensibles, étant donné que cartographier les dépendances critiques équivaut à signaler les vulnérabilités; il convient dès lors de classer et de gérer correctement les informations et de veiller à ce que les positions adoptées puissent être rapidement adaptées à l'évolution de l'environnement stratégique.

4.4. La feuille de route prévoit également la création, dans le cadre de l'observatoire et avec les États membres, d'un groupe d'experts afin d'échanger des informations dans un environnement sécurisé. Le CESE plaide résolument en faveur de l'établissement d'un lien fort et permanent avec les industries européennes de la défense, de la sécurité et de l'aérospatiale, qui ont la meilleure connaissance des chaînes d'approvisionnement et des dépendances critiques. Des mécanismes appropriés doivent être trouvés pour permettre un échange fiable d'informations confidentielles avec l'industrie.

4.5. Le CESE estime qu'il est également essentiel d'intégrer les résultats de l'observatoire dans les feuilles de route et de les traduire en initiatives phares. Les transitions entre les différentes phases du cycle technologique et industriel ne peuvent être gérées avec succès que s'il y a une réelle appropriation des initiatives et une répartition claire des responsabilités à chaque étape. La cohérence et les synergies sont donc nécessaires non seulement sur le plan horizontal, entre la RDTI civile et celle de la défense, mais aussi verticalement, entre les programmes de RDTI et les programmes de déploiement.

4.6. Afin de renforcer la cybersécurité et la cyberdéfense, la Commission proposera des mesures réglementaires en matière de cyberrésilience et demandera aux organismes européens de normalisation d'élaborer des normes harmonisées en matière de cybersécurité et de respect de la vie privée. En collaboration avec les États membres, elle renforcera également la préparation aux cyberincidents majeurs. Le CESE est fermement convaincu que les cybercapacités devraient être développées à des fins non seulement défensives, mais aussi offensives.

4.7. Le CESE estime que les programmes et instruments européens de soutien à la RDTI décrits dans l'encadré n° 2 (page 8) ainsi qu'à la page 11 de la feuille de route, sont complexes et mal coordonnés; par conséquent, une simplification et une rationalisation sont nécessaires dans l'intérêt des bénéficiaires eux-mêmes. Il est proposé de créer un guichet unique en ligne pour les PME et les jeunes pousses. En commençant par une phase pilote avec les PME actives dans les domaines de la défense et de la sécurité, ce «coin PME de l'UE» en ligne permettrait de saisir des données prédéfinies et d'obtenir une première évaluation du ou des programme(s) le(s) plus adapté(s) susceptible(s) de fournir un soutien public au niveau de l'UE.

4.8. Il est souligné à juste titre dans la feuille de route que l'UE dispose, outre ses programmes et instruments de RDTI, d'outils politiques qui peuvent contribuer à réduire ses dépendances stratégiques dans les secteurs de la sécurité et de la défense. Le CESE est d'avis que ces outils sont importants pour combler le fossé entre le développement et l'industrialisation, c'est-à-dire pour favoriser la commercialisation des résultats de la RDTI.

4.9. Un problème majeur est également de veiller à ce que les États membres de l'UE achètent auprès de fournisseurs européens une fois que la technologie critique aura été développée et partiellement financée au moyen du soutien public de l'UE. Le CESE craint qu'en l'absence d'une politique d'achat cohérente au niveau de l'UE comme à celui des États membres, les marchés européens, en raison de leur fragmentation et de leur petite taille à l'échelle mondiale, ne soient en mesure ni de réaliser les économies d'échelle nécessaires pour réduire les coûts ni de générer une activité suffisante pour garantir l'existence de jeunes pousses naissantes. Dans l'ensemble, le marché européen total est potentiellement très vaste, mais les dépenses ne sont pas coordonnées<sup>(8)</sup>.

Bruxelles, le 14 juillet 2022.

*La présidente*  
*du Comité économique et social européen*  
Christa SCHWENG

---

<sup>(8)</sup> Les États-Unis consacrent 750 milliards de dollars par an à la défense; la Chine dépense à cette fin entre 200 et 300 milliards de dollars (ce chiffre variant fortement selon les sources), tandis que les dépenses de l'OTAN (si l'on ne considère que les pays européens, sans le Royaume-Uni et la Turquie, mais avec la Norvège) s'élèvent à 250,7 milliards de dollars.