COMMISSION
EUROPÉENNE

Strasbourg, le 15.2.2022
COM(2022) 60 final

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

Contribution de la Commission à la défense européenne

1. Introduction

Dans le monde d'aujourd'hui, l'Union européenne est confrontée à une instabilité mondiale et à des frictions géopolitiques croissantes, comme le souligne la toute première analyse globale des menaces à l'échelle de l'UE, réalisée en novembre 2020 dans le cadre de la préparation de la future boussole stratégique de l'UE. Les conflits et les crises dans notre voisinage et au-delà ont une incidence directe sur notre propre sécurité, tandis que nos sociétés et nos économies sont ciblées par des menaces hybrides sophistiquées, y compris des cyberattaques et des campagnes de désinformation qui trouvent leur origine à l'étranger. Dans le même temps, la crise climatique et la perte de biodiversité sont autant de défis qui se posent pour la sécurité mondiale en général et pour les opérations civilo-militaires en particulier.

Tous les événements qui ont eu lieu et continuent d'avoir lieu à nos frontières terrestres, aériennes et maritimes et autour de nos frontières, ainsi que dans le cyberespace, le long d'importantes routes maritimes et dans l'espace extra-atmosphérique, montrent que nous devons être mieux préparés, renforcer nos capacités et être plus résilients. Dans le contexte d'une course technologique accélérée entre les États-Unis et la Chine, l'Union européenne doit renforcer et garantir son avance technologique. L'Union doit évoluer au même rythme que l'évolution des relations géopolitiques et de notre environnement, et intensifier et accélérer ses capacités collectives à défendre ses citoyens et ses valeurs fondamentales ainsi qu'à garantir ces dernières. **Il est essentiel et indispensable de faire évoluer considérablement la défense européenne en vue de garantir la sécurité de l'Union et de ses citoyens dans les années et les décennies à venir.**

Les événements actuels et passés résonnent comme des avertissements quant à la nécessité pour les Européens de coopérer plus étroitement dans le domaine de la défense pour garantir leur propre sécurité et devenir un garant de la sécurité plus solide pour les autres, en recourant à la vaste panoplie d'outils de l'Union. L'UE est déjà engagée dans la résolution des multiples conflits ouverts et gelés dans notre voisinage oriental et méridional, ainsi que dans différentes régions d'Afrique, notre continent voisin. Le récent **déploiement militaire russe le long de la frontière orientale de l'Ukraine, en Biélorussie et dans la région de la mer Noire**, ainsi que les tentatives de Moscou visant à perturber, à diviser et à redéfinir l'architecture de sécurité en Europe remettent en cause l'ordre international fondé sur des règles. Ces événements nous rappellent également que nous devons mettre en œuvre une défense européenne plus forte, en partenariat étroit avec l'Organisation du traité de l'Atlantique Nord (OTAN). La fin brutale de la mission militaire internationale en **Afghanistan** en août 2021 nous a appris que l'Europe devait être mieux préparée à faire face seule à des tâches de stabilisation complexes et à des situations d'urgences soudaines. Nous avons vu comment l'instabilité peut devenir un terreau propice au terrorisme et déraciner des populations, et comment des puissances mondiales et régionales peuvent profiter de ces situations pour accroître leur influence et accéder aux ressources. L'effet multiplicateur du changement climatique sur les risques de conflits au sein des États et entre ceux-ci rend la situation plus complexe encore.

Dans le même temps, l'UE doit renforcer sa propre préparation, ses capacités et sa résilience afin de mieux protéger ses citoyens. **Les menaces qui pèsent sur la sécurité de l'UE ne sont pas**

seulement de nature militaire, et cette tendance s'accentue. Nous sommes confrontés à des cyberattaques plus préjudiciables ciblant nos entités critiques, qui paralysent des installations industrielles, des installations de production d'énergie, des services municipaux et des hôpitaux, tandis que la manipulation de l'information et l'ingérence étrangères touchent également à l'essence même de nos démocraties. L'attaque hybride commanditée par le régime de Loukachenko, qui instrumentalise les migrants à des fins politiques, illustre clairement le caractère évolutif des campagnes hybrides qui visent à nous nuire, à nous contraindre et à nous manipuler en dessous du seuil de l'agression armée. L'UE a réagi à cette situation en fournissant une aide humanitaire, en menant des actions diplomatiques auprès de pays tiers, en apportant un soutien à nos États membres et en adoptant des sanctions à l'encontre des responsables. Dans l'intervalle, la pandémie de COVID-19 a aussi mis en évidence la nécessité d'une résilience accrue, les forces armées fournissant une assistance logistique, sécuritaire et médicale aux autorités civiles au début de 2020. Dans cet environnement en mutation rapide, **l'Union européenne doit renforcer encore sa préparation, ses capacités et sa résilience, notamment en renforçant les mécanismes d'absorption des chocs et en mettant en place sa boîte à outils dans tous les secteurs concernés**.

Les États membres s'efforcent de s'attaquer plus vigoureusement à toutes les menaces et à tous les défis grâce à la nouvelle **boussole stratégique de l'UE en matière de sécurité et de défense** (ci-après la «boussole stratégique»), qui doit être adoptée par les États membres en mars 2022. Cette boussole stratégique 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 défendre 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. Par la présente communication, la Commission européenne contribue encore davantage à ces travaux.

L'Union européenne doit agir maintenant pour renforcer ses capacités de défense dans le contexte actuel et donner à l'UE les moyens de faire face aux futurs champs de bataille; cela englobe une nouvelle génération de technologies de pointe capables de lutter contre les menaces qui découlent de systèmes cybernétiques, hybrides et spatiaux collaboratifs et autonomes fondés sur la connectivité et l'intelligence artificielle (IA). Dans le même temps, l'écosystème industriel que forme la défense avec le secteur aérospatial et le secteur de la sécurité constitue un **écosystème industriel de haute technologie** qui représente non seulement un moteur essentiel de l'autonomie stratégique ouverte et de la souveraineté technologique de l'Europe, mais aussi une source majeure de croissance et d'innovation. En plus de contribuer à la sécurité des citoyens de l'Union européenne, le secteur européen de la défense peut contribuer à une **relance économique** durable après la pandémie et au caractère globalement innovant d'un écosystème qui peut contribuer grandement à la transition écologique et produire des retombées positives pour un usage civil.

La réalisation de nos objectifs n'est possible qu'**en développant, en achetant et en exploitant ensemble nos équipements militaires**. L'UE a mis en place de nouveaux outils et instruments[1] pour inverser les fragmentations de longue date qui entravent l'efficacité du secteur européen de la défense et réduisent la capacité de l'UE et de ses États membres à mettre sur pied la prochaine génération de capacités de défense qui seront essentielles à la sécurité future de l'Europe et à sa capacité à assurer la sécurité dans son voisinage et au-delà.

En particulier, le Fonds européen de la défense (FED)[2], doté d'un budget de près de 8 000 000 000 EUR pour la période 2021-2027, change déjà la donne pour ce qui est de mettre en place un écosystème européen de la défense capable de fournir des technologies et des équipements de défense interopérables et de pointe qui renforceront la liberté d'action de l'Union ainsi que sa souveraineté technologique et sa compétitivité.

Dans ce contexte difficile, la Commission européenne continuera de travailler en étroite collaboration avec le haut représentant et les États membres pour:

- garantir une **mise en œuvre efficace et ciblée** des instruments et initiatives innovants que nous avons mis en place, tels que le FED et le plan d'action sur la mobilité militaire, notamment au moyen d'un certain nombre de mesures supplémentaires exposées dans la présente communication;
- soutenir **une coopération plus étroite en matière de défense entre les États membres et entre les secteurs**, en s'appuyant sur les ressources financières nécessaires et sur le renforcement des dépenses collaboratives conformément aux engagements existants, afin d'améliorer le rapport coût-efficacité, de renforcer l'interopérabilité, de favoriser l'innovation et d'améliorer la compétitivité et la résilience du secteur industriel;
- renforcer notre capacité à **réagir face à des crises graves**, y compris à des cyberattaques et à des campagnes hybrides, **ainsi qu'à faire face à des défis à plus long terme et à des contestations géopolitiques dans des domaines stratégiques**, sur la base d'une approche pangouvernementale et en renforçant les synergies à double usage et les synergies entre le civil et le militaire dans un large éventail de politiques, d'outils et d'instruments de la Commission;
- maintenir et renforcer une **interaction étroite avec l'OTAN**, conformément aux engagements pris et aux principes convenus qui guident la coopération UE-OTAN dans le cadre des déclarations communes, ainsi qu'avec d'autres partenaires internationaux clés tels que les Nations unies et des partenaires bilatéraux partageant les mêmes valeurs, comme les États-Unis, la Norvège[3] et le Canada.

Dans ce contexte géopolitique et technologique en constante évolution, et dans la perspective du prochain sommet informel qui se tiendra à Paris les 10 et 11 mars 2022, la présente

[1] Y compris le Fonds européen de la défense, la coopération structurée permanente (CSP) et l'examen annuel coordonné en matière de défense (EACD).
[2] PE/11/2021/INIT.
[3] En tant que membre de l'Espace économique européen.

communication expose de **nouvelles mesures et initiatives concrètes dans un certain nombre de domaines critiques** et recense les facteurs de réussite clés en vue d'un marché européen de la défense plus compétitif et harmonisé. Il s'agit notamment:

- **d'accroître les investissements en faveur de la recherche dans le domaine de la défense et du renforcement des capacités dans les cadres de coopération de l'UE;**
- **de faciliter les synergies entre la recherche et l'innovation dans les domaines civils et de la défense ainsi que de réduire les dépendances stratégiques;**
- **d'encourager l'acquisition conjointe de capacités de défense développées de manière collaborative au sein de l'UE;**
- **d'appeler les États membres à continuer de progresser vers des pratiques de contrôle des exportations rationalisées et plus convergentes, en particulier pour les capacités de défense développées dans un cadre de l'UE;**
- **de renforcer la dimension de sécurité et de défense des activités spatiales au niveau de l'UE;**
- **de renforcer la résilience européenne, notamment en intensifiant la cybersécurité et en luttant contre les cybermenaces et toute autre menace hybride, en renforçant la mobilité militaire et en relevant les défis liés au changement climatique pour la défense.**

Grâce à ces éléments constitutifs, et en s'appuyant sur les synergies entre les politiques intérieures et extérieures, y compris celles qui sont favorisées dans le cadre de la stratégie pour l'union de la sécurité de 2020, la Commission continuera, dans les années à venir, à contribuer activement au processus de mise en place d'une **Union européenne de la défense** au moyen d'initiatives et de projets ciblés, en utilisant l'ensemble des outils dont elle dispose pour être mieux à même de faire face aux menaces à plusieurs niveaux et en rapide évolution auxquelles nous sommes confrontés.

2. Accroître les investissements en faveur de la recherche en matière de défense et du renforcement des capacités dans les cadres de coopération de l'UE

Le FED est un **programme ambitieux, équilibré et inclusif** qui garantit une forte participation des États membres afin que les projets financés répondent aux besoins opérationnels des forces armées, ouvrant ainsi la voie à la production et à l'acquisition. Ses **critères d'éligibilité** maintiennent le marché ouvert tout en renforçant la compétitivité de l'industrie européenne de la défense et en protégeant la sécurité et les intérêts stratégiques de l'UE.

D'ici à la fin de 2022, la Commission européenne aura investi 1 900 000 000 EUR dans des projets de recherche et de renforcement des capacités dans le domaine de la défense répondant aux besoins des États membres en termes de capacités. Elle donnera ainsi le **coup d'envoi à des projets clés de collaboration en matière de renforcement des capacités à grande échelle** visant à combler des insuffisances critiques, tout en **stimulant l'innovation dans le domaine de la défense**, y compris dans des niches particulières. Ces investissements comprennent des projets de moindre envergure et des appels ouverts qui élargissent la participation transfrontière des jeunes pousses et des petites et moyennes entreprises (PME); jusqu'à 8 % de son budget 2021 sera consacré au financement de technologies de rupture en matière de défense et quelque 6 % à

des appels ouverts pour les PME. Cela représente 48 % des 1 100 entités qui ont présenté des propositions et 20 % de la demande de financement totale[4] pour les appels au titre du FED pour 2021[5]. La Commission continuera de promouvoir la participation des PME dans l'ensemble de l'UE, notamment en encourageant l'intégration des PME les plus innovantes et les plus compétitives dans les chaînes d'approvisionnement.

Les premiers appels à propositions publiés en **2021 prévoient déjà d'allouer environ 700 000 000 EUR à des projets portant sur des plateformes et des systèmes de défense complexes et à grande échelle**, tels que des systèmes de combat de nouvelle génération, des parcs de véhicules terrestres, des navires de patrouille de haute mer polyvalents et modulaires, ainsi que des systèmes de défense contre les missiles balistiques.

Par ailleurs, grâce à son précédent programme de développement[6], **deux projets majeurs de renforcement des capacités revêtant une importance stratégique ont bénéficié d'une subvention totale d'environ 140 000 000 EUR**. Le système MALE RPAS soutient le développement d'un drone de moyenne altitude et de longue endurance. Il contribue à renforcer la souveraineté technologique dans le domaine des drones, un atout essentiel pour les forces armées des États membres. La radio logicielle sécurisée européenne (ESSOR) stimulera l'interopérabilité en créant une normalisation européenne pour les technologies de communication sécurisées dans le domaine de la défense. D'autres projets significatifs financés sont axés, entre autres, sur le commandement et le contrôle, la prise de décision fondée sur l'IA, le combat collaboratif, la cyberdéfense ou l'observation spatiale.

Le renforcement des capacités de défense est un processus à long terme qui nécessite une planification coordonnée et préalable. **Une orientation stratégique du FED est prévue dans le cadre des priorités en matière de capacités de défense dont les États membres sont convenus d'un commun accord au titre de la politique de sécurité et de défense commune (PSDC),** et notamment dans le contexte du plan de développement des capacités, en veillant à la cohérence avec d'autres initiatives de l'UE liées à la défense comme l'examen annuel coordonné en matière de défense (EACD) et la coopération structurée permanente (CSP).

De surcroît, dans un souci de transparence et de prévisibilité, notamment en ce qui concerne la planification des budgets de défense nationaux, la Commission a élaboré une **perspective pluriannuelle indicative et flexible** pour les quatre années à venir, qui sera réexaminée chaque année en fonction de l'évolution de la situation. Elle garantit la cohérence des projets de collaboration dans le domaine des capacités de défense et la cohérence des programmes de travail tout au long de la durée du FED, tout en assurant à la fois la transparence et la prévisibilité. Dans ce contexte, la Commission et les États membres continueront de renforcer la perspective pluriannuelle **en tenant compte des capacités essentielles et des catalyseurs**

[4] Y compris les sous-traitants.

[5] Dans le cadre du programme qui l'a précédé, le programme européen de développement industriel dans le domaine de la défense (EDIDP), en 2020, année pour laquelle les résultats sont disponibles, les PME représentaient 35 % des entités et ont bénéficié de 30 % du financement total des 26 projets (avant prise en compte de la participation de sous-traitants, qui sont souvent des PME).

[6] Le programme européen de développement industriel dans le domaine de la défense (EDIDP).

stratégiques considérés comme prioritaires par les États membres à la suite de l'adoption de la boussole stratégique.

Grâce à son effet catalyseur, le FED continuera donc à ouvrir la voie à des investissements ciblés dans le domaine de la défense à l'appui de la base industrielle et technologique de défense européenne (BITDE) et à la mise en adéquation des priorités définies d'un commun accord par les États membres au sein de l'UE. Afin de mieux soutenir l'élaboration de projets de renforcement des capacités de défense à grande échelle, la possibilité de programmes de travail pluriannuels devrait être évaluée dans le cadre de l'examen à mi-parcours du FED. Il est tout aussi important de **veiller à ce que d'autres politiques horizontales**, telles que des initiatives en matière de finance durable, **restent compatibles avec les efforts de l'Union européenne visant à faciliter l'accès de l'industrie européenne de la défense à un financement et à des investissements suffisants**.

Afin de renforcer encore tant la coopération dans le cadre du FED que l'intégration du marché intérieur de la défense, la Commission continuera aussi à collaborer avec les États membres pour tirer parti des possibilités offertes par la directive 2009/43/CE[7] sur le transfert intra-UE de produits liés à la défense en vue de faciliter les transferts liés à des projets de collaboration financés par l'UE. En fournissant des conseils sur les règles et procédures prévues par la directive 2009/43/CE et en s'efforçant de dégager un consensus entre les États membres, la Commission aura pour objectif de simplifier le transfert de produits liés à la défense au sein du marché intérieur, notamment dans le cadre de projets de collaboration financés par l'UE, ainsi que de faciliter les échanges de bonnes pratiques.

Il est essentiel de renforcer la coordination, l'orientation et le niveau des investissements communs dans le domaine de la défense afin d'améliorer l'efficience globale des dépenses en matière de défense au sein de l'UE, tout en tenant compte des engagements existants, tels que ceux pris dans le cadre de la CSP en vue d'augmenter régulièrement les budgets de défense. La mise à disposition collective de capacités de défense stratégique ne peut être réalisée que par une planification coordonnée ainsi que par des investissements publics nationaux et de l'UE ciblant les priorités communes en matière de recherche et de développement dans le domaine de la défense.

Dans ce contexte, la Commission **développera également de nouvelles incitations pour favoriser les investissements communs des États membres dans les capacités stratégiques de défense, notamment lorsqu'elles sont développées et/ou acquises dans les cadres de coopération de l'Union européenne**. La Commission inclura un chapitre contenant des observations sur les évolutions, les obstacles et les possibilités concernant les **projets multinationaux de renforcement des capacités de défense dans le rapport annuel sur le marché unique**, qui est généralement publié conjointement avec le paquet d'automne du Semestre européen. Dans ce contexte, la Commission pourrait également réfléchir à la manière

[7] Directive 2009/43/CE du Parlement européen et du Conseil du 6 mai 2009 simplifiant les conditions des transferts de produits liés à la défense dans la Communauté.

d'intensifier les efforts collectifs visant à garantir et à coordonner le cofinancement des États membres acheminé par l'intermédiaire du FED, en vue d'optimiser l'utilisation des ressources.

Prochaines étapes

- Avec le FED, la Commission continuera d'encourager activement les États membres à définir plus précisément les priorités et les catalyseurs stratégiques en matière de capacités de défense à la suite de l'adoption de la boussole stratégique, dans le cadre du plan de développement des capacités révisé et des résultats de l'examen annuel coordonné en matière de défense. Elle contribuera à aligner la planification de la défense et les dépenses collectives afin de soutenir leur développement.
- La Commission développera des incitations supplémentaires pour favoriser les investissements communs des États membres dans les capacités stratégiques de défense, notamment celles qui doivent être développées et/ou acquises conjointement dans les cadres de coopération de l'Union européenne, et rendra compte de l'évolution des projets multinationaux de renforcement des capacités de défense, ainsi que des obstacles et des possibilités qui s'y rapportent, dans le rapport annuel sur le marché unique.
- En 2022, la Commission continuera de collaborer avec les États membres pour faciliter davantage le transfert de produits de défense financés par l'UE au sein du marché intérieur, tout particulièrement en soutenant la pleine exploitation des possibilités offertes par la directive 2009/43/CE.

3. Faciliter les synergies entre la recherche et l'innovation dans les domaines civils et de la défense et réduire les dépendances stratégiques

Dans sa feuille de route sur les technologies critiques pour la sécurité et la défense, adoptée parallèlement à la présente communication[8], la Commission définit la voie à suivre pour stimuler la recherche, le développement technologique et l'innovation ainsi que pour réduire les dépendances stratégiques de l'UE en matière de technologies critiques et de chaînes de valeur dans les secteurs de la sécurité et de la défense.

Sur la base de la «Mise à jour de la nouvelle stratégie industrielle de 2020: construire un marché unique plus solide pour soutenir la reprise en Europe»[9] et du plan d'action sur les synergies entre les industries civile, spatiale et de la défense[10], elle propose une voie à suivre pour l'UE et les États membres afin:

- de recenser les technologies critiques pour la sécurité et la défense de l'UE;
- de promouvoir dès le départ une approche stratégique et coordonnée à l'échelle de l'UE pour ces technologies critiques en tirant parti des programmes de recherche, de développement technologique et d'innovation;

[8] Espace réservé pour une référence.
[9] COM(2021) 350 final.
[10] COM(2021) 70 final.

– de réduire les dépendances stratégiques.

Cela nécessite une meilleure prise de conscience du caractère critique de certaines technologies, telles que les semi-conducteurs, pour les secteurs de la sécurité et de la défense, un meilleur recensement des dépendances stratégiques connexes et des éventuelles mesures d'atténuation, en tenant compte de la diversité des sources et de l'éventualité que l'utilisation opérationnelle de la technologie puisse être compromise ou refusée[11]. L'observatoire des technologies critiques[12] (ci-après l'«observatoire») mettra en place un mécanisme spécifique pour recenser ces évaluations, sur la base des contributions des États membres et de l'industrie. Les conclusions de l'observatoire seront essentielles pour stimuler la recherche, le développement technologique et l'innovation au sein de l'UE en ce qui concerne ces technologies, dans le cadre d'une approche coordonnée à l'échelle de l'UE. Ces travaux viennent compléter les efforts plus vastes déployés pour garantir la sécurité de l'approvisionnement de biens civils critiques, dans des secteurs tels que la santé et l'énergie[13].

La Commission élaborera également une **approche visant à encourager le double usage pour la recherche et l'innovation au niveau de l'UE** et déploiera un programme d'innovation dans le domaine de la défense afin de soutenir l'innovation et l'entrepreneuriat dans le domaine des technologies critiques, en étroite coordination avec le pôle d'innovation dans le domaine de la défense, qui sera mis en place par l'Agence européenne de défense (AED).

Enfin, afin de réduire les dépendances stratégiques, la Commission continuera d'évaluer systématiquement les considérations liées à la sécurité et à la défense lorsqu'elle mettra en œuvre et réexaminera les instruments existants de l'UE ou en concevra de nouveaux.

4. Encourager l'acquisition conjointe de capacités développées de manière collaborative au sein de l'UE

L'**acquisition conjointe de capacités de défense européennes** par les États membres **renforce sensiblement l'interopérabilité** des forces armées nationales européennes et **soutient la compétitivité de la BITDE**, notamment grâce à de plus grandes économies d'échelle.

Toutefois, les États membres ne respectent pas encore le critère collectif de longue date concernant l'acquisition collaborative européenne d'équipements[14] (35 % des dépenses d'équipement de défense), qu'ils ont confirmé dans le cadre de la CSP[15]. Selon l'AED, en 2020,

[11] En ce qui concerne les semi-conducteurs, voir la feuille de route sur les technologies critiques pour la sécurité et la défense, section 2.2 (adoptée parallèlement), et la communication de la Commission intitulée «Action européenne sur les semi-conducteurs», COM(2022) 45 final.

[12] En association avec les services compétents de la Commission et l'Agence européenne de défense.

[13] Conformément à la proposition COM(2021) 577 de la Commission du 16.9.2021 établissant un cadre de mesures visant à garantir la fourniture des contre-mesures médicales nécessaires en cas d'urgence de santé publique au niveau de l'Union, à la proposition COM(2021) 660 de la Commission du 13.10.2021 sur la lutte contre la hausse des prix de l'énergie et à la proposition COM(2021) 350 de la Commission sur la mise à jour de la nouvelle stratégie industrielle.

[14] En novembre 2007, le comité directeur de l'AED réuni au niveau ministériel a approuvé quatre critères d'investissement collectifs, y compris le critère de 35 % du total des dépenses d'équipement pour l'acquisition collaborative européenne d'équipements.

[15] EUR-Lex - 32021H1117(01) - FR - EUR-Lex (europa.eu)

les États membres[16] ont dépensé environ 37 000 000 000 EUR pour l'acquisition d'équipements de défense (c'est-à-dire l'acquisition de nouveaux équipements de défense). Sur ce montant, environ 11 % seulement (approximativement 4 100 000 000 EUR)[17] ont été consacrés aux dépenses portant sur l'acquisition collaborative d'équipements de défense (à savoir l'acquisition de nouveaux équipements de défense en collaboration avec d'autres États membres). Cela signifie que l'essentiel des dépenses des États membres portant sur l'acquisition d'équipements de défense (environ 89 %) ont été effectuées sur une base nationale et/ou en coopération avec des pays tiers.

L'année 2020 ne fait pas exception et peut même être considérée comme s'inscrivant dans une tendance qui s'est aggravée ces dernières années. En effet, le pourcentage d'acquisitions collaboratives européennes d'équipements de défense diminue constamment depuis 2016 et ce chiffre est le plus bas depuis que ces données sont collectées (2005).

Deux instruments de l'UE ouvrent déjà la voie à l'acquisition conjointe. Le règlement sur le **FED** subordonne le soutien financier aux actions de développement au fait que les États membres aient l'intention d'acquérir le produit final ou d'utiliser la technologie de manière coordonnée. **La directive 2009/81/CE sur la passation de marchés publics dans le domaine de la défense** prévoit une exclusion spécifique des règles de passation des marchés publics pour les projets de coopération fondés sur des activités de recherche et développement (R&D)[18]. Cette exclusion s'applique également aux phases du cycle de vie qui suivent la R&D si les marchés sont attribués dans le cadre du même projet coopératif. En 2019, la Commission a publié une communication[19] fournissant des orientations sur diverses possibilités de passation de marchés basée sur la coopération prévues par la directive. Un soutien supplémentaire sera disponible pour les États membres, notamment dans le cadre du groupe d'experts pour les marchés publics dans les domaines de la défense et de la sécurité.

La Commission vise à **encourager davantage l'acquisition conjointe de capacités de défense européennes par les États membres**, y compris en ce qui concerne les opérations et l'entretien. Toutefois, pour ce faire, il convient de lever plusieurs obstacles financiers et fiscaux pratiques.

La Commission examinera la possibilité de permettre une **exonération de la taxe sur la valeur ajoutée (TVA) afin de soutenir l'acquisition conjointe et la propriété commune de capacités de défense développées de manière collaborative au sein de l'UE**. Ces capacités seront mises à la disposition des États membres pour des missions et opérations menées dans le cadre de la PSDC[20] ou dans le cadre des activités menées au niveau national, de l'ONU ou de l'OTAN. Une telle mesure pourrait en particulier bénéficier aux capacités développées dans les cadres coopératifs de l'UE (FED et/ou CSP et/ou au sein de l'AED). L'établissement d'un cadre

[16] À l'exception du Danemark.
[17] Sur la base des données fournies par onze États membres.
[18] Article 13 de la directive 2009/81/CE.
[19] 2019/C 157/01
[20] Dans le respect des forces multinationales prévues à l'article 42, paragraphe 3, du traité sur l'Union européenne.

juridique inspiré par le Consortium pour une infrastructure européenne de recherche[21] qui bénéficierait d'une exonération de la TVA sur les équipements que les consortiums d'États membres achèteraient et posséderaient pourrait être envisagé dans ce contexte.

De même, sur la base des enseignements tirés de l'évaluation intermédiaire du FED, la Commission envisagera de renforcer le **système actuel de primes FED, afin de fournir une incitation financière** à condition que **les États membres s'engagent à acquérir et/ou à détenir conjointement les capacités de défense en cours de développement[22]**. Cela inciterait davantage à faire en sorte que la collaboration se poursuive au-delà des phases de R&D, à savoir les phases d'acquisitions, d'opérations et d'entretien.

En outre, sur la base des travaux du groupe d'experts sur la boîte à outils financiers, de **nouvelles solutions de financement** pourraient mener à une utilisation accrue, par les États membres, d'entités déjà existantes d'acquisition conjointe comme l'AED ou l'Organisation conjointe de coopération en matière d'armement (OCCAR). En particulier, la Commission examinera si les dispositions du règlement sur le FED, comme celles liées aux achats publics avant commercialisation[23], peuvent prévoir un soutien financier aux pouvoirs adjudicateurs et aux entités d'acquisition conjointe, afin de coordonner davantage leurs procédures d'acquisition, y compris en couvrant les coûts administratifs/de transaction liés à l'acquisition conjointe de services de recherche et de développement dans le domaine de la défense.

Prochaines étapes

- D'ici au début de 2023, la Commission fera une proposition qui permettra une **exonération de la TVA** pour soutenir l'acquisition et la propriété conjointes de capacités de défense développées de manière collaborative au sein de l'UE, tout en veillant à respecter les règles de l'Organisation mondiale du commerce.
- D'ici à la mi-2023, la Commission s'appuiera sur les travaux du groupe d'experts sur la boîte à outils financiers afin de proposer de **nouvelles solutions de financement** pour faciliter l'acquisition conjointe, par les États membres, de capacités stratégiques de défense de l'UE s'appuyant sur une expertise déjà disponible.
- À la suite de l'évaluation intermédiaire du FED[24], la Commission envisagera une modification éventuelle de l'article 13 du règlement (UE) 2021/697 établissant le Fonds européen de la défense, afin de renforcer **le système de primes FED lorsque les États membres s'engagent à acquérir et/ou à posséder conjointement les capacités de défense en cours de développement**.

[21] Le Consortium pour une infrastructure européenne de recherche (ERIC) est une forme juridique spécifique qui facilite l'établissement et le fonctionnement des infrastructures de recherche d'intérêt européen.

[22] Au-delà du critère d'éligibilité visé à l'article 21, paragraphe 3, point a), du règlement sur le FED, qui exige une intention d'acquérir le produit final ou d'utiliser la technologie de manière coordonnée.

[23] Article 17 du règlement sur le FED.

[24] L'évaluation intermédiaire doit être effectuée au plus tard quatre ans après le début de la période de mise en œuvre du Fonds (en 2025) conformément à l'article 29 du règlement établissant le FED.

5. Appeler les États membres à continuer de progresser vers des pratiques de contrôle des exportations rationalisées et plus convergentes

Bien que les États membres soient chargés de délivrer les licences d'exportation pour les équipements militaires, ils prennent leurs décisions sur la base de la position commune du Conseil[25], qui définit des critères communs pour le contrôle des exportations de technologies et d'équipements militaires. Cette position commune établit également des mécanismes de notification des refus et de consultation afin d'accroître la convergence dans l'application de leurs politiques d'exportation de produits liés à la défense.

Toutefois, étant donné que le développement conjoint des capacités de défense deviendra progressivement la norme dans l'UE plutôt que l'exception, **les États membres bénéficieront d'un échange accru de bonnes pratiques, ce qui conduira progressivement à une approche plus convergente en matière de contrôle des exportations d'armes**. S'appuyant sur les travaux déjà réalisés et reconnaissant que les exportations constituent un facteur de réussite clé pour le modèle économique de l'industrie européenne de la défense, la Commission encourage les États membres à se diriger progressivement vers une rationalisation et une convergence accrues des pratiques en matière de contrôle des exportations d'armes, en particulier en ce qui concerne les capacités de défense qu'ils développent ensemble, notamment dans le cadre du FED.

Dans ce contexte, **la Commission salue la réflexion engagée au sein du Conseil[26]** sur l'exportation de capacités qui ont été développées dans un cadre de l'UE et encourage les États membres à poursuivre ces discussions afin de faciliter les procédures de contrôle des exportations pour ces produits. Ce processus pourrait également s'appuyer sur l'expérience des accords bilatéraux et multilatéraux entre les États membres portant sur des capacités développées conjointement.

Afin de ne pas entraver la coopération, ces travaux devraient faciliter la définition de règles et procédures claires et faciles à mettre en œuvre. Des mesures efficaces de contrôle des exportations devraient être définies pour fournir aux produits financés par le FED un accès adéquat et concurrentiel aux marchés internationaux tout en préservant les décisions souveraines des États membres, dans le respect total de leurs obligations légales applicables et en tenant compte de leurs intérêts en matière de sécurité nationale. Afin de préserver l'attractivité des projets communs en matière de capacités de défense, **la Commission invite les États membres à adopter une approche prévoyant qu'en principe, ils ne s'empêcheraient pas mutuellement d'exporter vers les pays tiers des équipements et technologies militaires développés en coopération**. Cela pourrait s'appliquer aux exportations prévues d'équipements ou de technologies comportant des composants en provenance d'un autre État membre dépassant un certain seuil de minimis.

[25] Position commune 2008/944/PESC.

[26] Au sein du sous-groupe «Exportations d'armes conventionnelles» (COARM) du groupe «Non-prolifération et exportations d'armes».

Prochaines étapes

- La Commission invite les États membres à examiner des moyens de rationaliser et de faire converger progressivement leurs pratiques de contrôle des exportations d'armes, en particulier en ce qui concerne les capacités de défense développées conjointement, notamment dans un cadre de l'UE, garantissant ainsi que les produits financés par le FED bénéficieront d'un accès adéquat et concurrentiel aux marchés internationaux sans préjudice des décisions souveraines des États membres.

6. Renforcer la dimension «défense» de l'espace au niveau de l'UE

L'espace est un domaine stratégique pour la **liberté d'action et la sécurité de l'UE**. Dans le même temps, il est de plus en plus congestionné et contesté, et la concurrence entre puissances y est de plus en plus marquée.

Il est urgent de faire face à ces enjeux. Une nouvelle stratégie spatiale de l'UE pour la sécurité et la défense, qui est actuellement examinée par les États membres dans le cadre de la boussole stratégique, devrait aider à établir une compréhension commune des risques et des menaces liés à l'espace, à élaborer des réponses appropriées pour réagir mieux et plus rapidement aux crises, à renforcer notre résilience et à tirer pleinement parti des bénéfices et des possibilités liés au domaine spatial. Sans préjudice du contenu de la future stratégie conjointe, les actions suivantes seront envisagées.

Premièrement, les moyens spatiaux de l'UE[27] devraient être davantage protégés afin de renforcer la résilience de l'UE dans l'espace et depuis l'espace.

Dans la communication conjointe sur la **gestion du trafic spatial (GTS)**[28], la Commission et le haut représentant fournissent des orientations concrètes sur la manière sur la manière d'accroître la protection des moyens spatiaux de l'UE et de promouvoir une utilisation plus durable de l'espace. En particulier, la Commission renforcera ses **moyens de surveillance de l'espace** grâce à une amélioration des services de **surveillance de l'espace et de suivi des objets en orbite (SST)** et au développement de technologies connexes, comme les dispositifs automatiques de prévention des collisions ou l'intelligence artificielle.

La Commission soutiendra également davantage le développement de projets liés à **la surveillance de l'espace (SSA) et aux capacités d'alerte précoce en matière de défense**. Ces projets contribueront à la mise en place de capacités avancées de commandement et de contrôle spatiaux (SC2), de capteurs SSA avancés et d'un système d'alerte précoce contre les menaces de missiles balistiques et les nouvelles menaces hypersoniques[29].

---

[27] Le programme spatial de l'UE comporte quatre volets: Galileo/EGNOS pour le positionnement, la navigation et la datation, Copernicus pour l'observation terrestre, Govsatcom pour les communications gouvernementales par satellite et SSA pour la surveillance de l'espace.

[28] [place holder for reference]

[29] Ces projets sont soutenus par le FED et les programmes qui l'ont précédé.

Deuxièmement, la Commission renforcera la dimension «sécurité et défense» dans les infrastructures spatiales de l'UE existantes et futures, en coopération avec le haut représentant.

Le **service public réglementé (PRS) Galileo**[30] offre un service de navigation réservé aux utilisateurs autorisés par les gouvernements pour les applications sensibles. Celles-ci exigent un niveau élevé de continuité du service, utilisant des signaux robustes et cryptés, notamment en matière de sécurité et de défense. Le PRS est conçu pour offrir un service illimité et ininterrompu dans le monde entier. Il démontre clairement qu'une infrastructure commune sous contrôle civil peut répondre aux besoins en matière de défense et de sécurité.

La proposition de règlement établissant le **programme de l'Union pour une connectivité sécurisée** pour la période 2022-2027[31], adoptée parallèlement à la présente communication dans le cadre du paquet «Espace», renforcera la résilience de l'UE en matière de connectivité grâce à des communications gouvernementales sécurisées. Elle inclura dès le départ des exigences en termes de résilience dans le domaine de la défense, et la constellation de satellites en orbite terrestre basse (LEO) offrira une possibilité d'embarquer des charges utiles contribuant à d'autres composantes du programme spatial de l'UE. Le système s'appuiera sur Govsatcom et sur les synergies avec le Fonds européen de la défense.

L'évolution de Copernicus devrait également tenir compte des exigences en matière de défense, dans la mesure du possible, en accordant une attention particulière aux niveaux requis de sécurité et de performance et en s'appuyant sur une bonne gouvernance fondée sur la confiance.

Pour soutenir le développement de la dimension «défense» des infrastructures spatiales de l'UE existantes et futures, la Commission soutiendra le développement des **capacités de défense dans le domaine spatial au moyen du FED**. À ce jour, quelque 130 000 000 EUR ont été alloués au financement d'actions liées à l'espace au titre du FED et des programmes qui l'ont précédé.

Alors que la Commission soutient le développement de plateformes collaboratives pour relever les défis futurs en matière de défense, elle cherche également à améliorer leurs performances en faisant le meilleur usage des moyens spatiaux européens existants et futurs. Par exemple, le projet **Galileo pour la défense de l'UE** (GEODE) est cofinancé à hauteur de 44 000 000 EUR[32] et vise à développer des récepteurs de navigation militaire normalisés européens compatibles avec le PRS Galileo. Plus de 22 000 000 EUR seront également investis pour renforcer les capteurs ainsi que le commandement et le contrôle (C2) pour une surveillance spatiale militaire de l'UE et pour développer une capacité d'alerte précoce fondée sur l'espace.

[30] Décision nº 1104/2011/UE du Parlement européen et du Conseil du 25 octobre 2011 relative aux modalités d'accès au service public réglementé offert par le système mondial de radionavigation par satellite issu du programme Galileo (JO L 287 du 4.11.2011, p. 1).

[31] [place holder for reference]

[32] Au titre du programme européen de développement industriel dans le domaine de la défense (EDIDP).

Dans le cadre du programme de travail 2021 du FED, ce dernier affectera 50 000 000 EUR tant à la surveillance **de la guerre de la navigation dans l'espace et au sol (NAVWAR)** qu'aux **technologies européennes de communications par satellite résilientes contre le brouillage**.

Troisièmement, la Commission œuvrera à la réduction des dépendances stratégiques connexes de l'UE en matière de technologies critiques, par exemple dans le domaine des puces électroniques, de l'informatique quantique et de l'IA. À cette fin, la Commission optimisera les synergies avec les initiatives liées à l'espace mises en œuvre dans le cadre des instruments existants pilotés par la Commission (dont le FED, Horizon Europe[33], le programme spatial, le Conseil européen de l'innovation et InvestEU) et tirera profit de l'observatoire des technologies critiques. La Commission renforcera également la **résilience des chaînes d'approvisionnement européennes connexes** afin de garantir l'intégrité, la sécurité et le fonctionnement des infrastructures spatiales.

Quatrièmement, la Commission, en coopération avec le haut représentant et dans le cadre de leurs mandats respectifs, mettra en œuvre l'élargissement de l'actuel mécanisme de réaction aux menaces Galileo[34] aux systèmes et services relevant des autres composantes du programme spatial de l'UE. Cela renforcera encore la gouvernance en matière de sécurité des infrastructures spatiales de l'UE afin de mieux répondre aux menaces et promouvra la mise en place d'une gouvernance adéquate par les acteurs concernés. La Commission et le haut représentant amélioreront la surveillance de l'espace au niveau de l'UE grâce à une meilleure utilisation des données spatiales, en étroite coopération avec les États membres, ainsi que dans le cadre d'une coopération systématique entre les agences/organes concernés qui exploitent les infrastructures de l'UE.

La Commission et le haut représentant contribueront également aux efforts déployés par les États membres pour renforcer encore les mécanismes d'assistance mutuelle et de réaction aux crises, notamment au moyen d'exercices et en stimulant la capacité de réaction face aux menaces, en favorisant l'interopérabilité et en soutenant une culture stratégique commune.

Prochaines étapes

- À la suite de l'adoption de la boussole stratégique, la Commission et le haut représentant proposeront une stratégie spatiale conjointe de l'UE pour la sécurité et la défense.
- D'ici à la fin de 2022, la Commission examinera comment renforcer encore la **protection des moyens spatiaux de l'UE**, notamment grâce à des services SST supplémentaires, à une amélioration des performances de la SST de l'UE et à une utilisation optimale du potentiel de l'industrie de l'UE.
- À partir de 2022, la Commission promouvra une approche du «**double usage dès la**

[33] Dans le présent document, le terme «Horizon Europe» désigne le programme spécifique d'exécution d'Horizon Europe et l'Institut européen d'innovation et de technologie; les activités menées dans leur cadre se concentrent exclusivement sur les applications civiles.

[34] Comme le prévoient le règlement (UE) 2021/696 sur le programme spatial de l'Union et la décision (PESC) 2021/698 du Conseil du 30 avril 2021 sur la sécurité des systèmes et services déployés, exploités et utilisés dans le cadre du programme spatial de l'Union qui pourraient porter atteinte à la sécurité de l'Union.

conception» pour les infrastructures spatiales de l'UE, afin de proposer de nouveaux services résilients qui répondent aux besoins des gouvernements. Dans ce contexte, la Commission encourage les colégislateurs à adopter rapidement la proposition de règlement établissant le programme de l'Union pour une connectivité sécurisée pour la période 2022-2027.

- La Commission intensifiera ses travaux en vue de réduire les dépendances technologiques stratégiques et d'améliorer la résilience des chaînes d'approvisionnement liées aux infrastructures spatiales, notamment au moyen d'instruments de financement de l'UE, ainsi que de l'observatoire des technologies critiques.
- La Commission établira une gouvernance adéquate pour les infrastructures spatiales de l'UE, en étroite coopération avec les États membres, sur la base du modèle du PRS Galileo. Elle évaluera la faisabilité du développement et du déploiement d'un service Copernicus plus résilient et plus sécurisé à des fins gouvernementales[35], en tenant compte, dans la mesure du possible, des exigences en matière de défense.
- D'ici à la fin de 2022, la Commission et le haut représentant examineront la possibilité d'activer des mécanismes de solidarité, d'assistance mutuelle et de réaction aux crises en cas d'attaques provenant de l'espace ou de menaces contre les moyens spatiaux.

7. Renforcer la résilience européenne

L'Europe doit renforcer sa résilience pour prévenir les chocs futurs, s'en protéger et y résister. Compte tenu des liens intrinsèques avec les politiques nationales de sécurité et de défense, il incombe d'abord aux États membres de faire face à ces menaces. Dans l'intervalle, certaines vulnérabilités sont communes à tous les États membres et certaines menaces s'étendent au-delà des frontières, telles que le ciblage des réseaux ou des infrastructures transfrontières et le changement climatique.

L'approche de l'Union européenne vise à intégrer la dimension externe et interne dans un flux continu. Cette approche fait la synthèse des considérations civiles et militaires tant au niveau national qu'au niveau de l'UE afin de promouvoir des solutions concrètes, tout en facilitant une résilience accrue et une efficacité opérationnelle permanente.

7.1. Lutte contre les menaces hybrides

En 2020, la **stratégie de l'UE pour l'union de la sécurité**[36] a défini les menaces hybrides comme l'une des priorités à traiter afin de renforcer la sécurité de l'UE. La stratégie jette les bases d'une approche renouvelée face à ces menaces en constante évolution, qui couvre tout l'éventail des actions, depuis la détection précoce, l'analyse, la sensibilisation, le renforcement de la résilience et la prévention jusqu'à la réaction aux crises et la gestion des conséquences.

[35] Services de type PRS Copernicus.
[36] COM(2020) 605

La **cartographie des mesures**[37] **liées au renforcement de la résilience et à la lutte contre les menaces hybrides comprend plus de deux cents outils et mesures au niveau de l'UE**, dont la grande majorité sont pilotés ou soutenus par la Commission. Les propositions de la Commission dans différents domaines, y compris la législation sur les services numériques[38], la proposition de directive sur la résilience des entités critiques[39] et la révision du mécanisme de protection civile de l'Union[40], s'ajouteront aussi à ce nombre croissant d'outils de l'UE disponibles pour lutter contre les menaces hybrides.

La résilience est l'un des principaux piliers de la lutte contre les menaces hybrides. Un document de travail conjoint des services de la Commission de janvier 2022[41] a recensé 53 **exigences de base** en matière de résilience[42] au niveau de l'UE. Cette identification, annoncée dans la stratégie pour l'union de la sécurité, a constitué une première étape cruciale pour suivre et mesurer objectivement les progrès accomplis dans ce domaine.

Dans ce contexte, les services de la Commission, en coopération avec le Service européen pour l'action extérieure (SEAE) et le secrétariat général du Conseil, mèneront en novembre 2022 l'exercice EU Integrated Resolve PACE pour lutter notamment contre les menaces hybrides, y compris dans leur cyberdimension. Cet exercice sera mené sous la responsabilité générale du haut représentant, avec la participation des États membres et des agences de l'UE, et dans un format parallèle et coordonné (PACE) avec l'OTAN.

La Commission s'est également **adaptée à l'évolution rapide de la nature des menaces**. À la suite de la crise survenue à la frontière de l'UE avec la Biélorussie, la Commission a proposé des mesures visant à lutter contre l'**instrumentalisation de la migration**, y compris la mise sur liste noire des opérateurs de transport mêlés au trafic de migrants ou la traite des êtres humains vers l'UE[43].

La pandémie de COVID-19 a mis en lumière la nécessité de renforcer l'action coordonnée à l'échelle de l'Union pour faire face aux urgences sanitaires. À l'heure où les menaces chimiques, biologiques, radiologiques et nucléaires pourraient mettre en danger la santé publique, l'Autorité européenne de préparation et de réaction en cas d'urgence sanitaire (HERA) est un élément central du renforcement de la préparation et de la réaction de l'UE face aux menaces transfrontières graves pour la santé, car elle fait en sorte que les contre-mesures nécessaires soient rapidement disponibles, accessibles et diffusées. S'inspirant des enseignements tirés des phases préliminaires de la pandémie, les travaux se poursuivront pour renforcer l'assistance militaire apportée aux autorités civiles à cet égard.

[37] SWD(2020) 152 final
[38] COM(2020) 825 final
[39] COM(2020) 829 final
[40] Règlement (UE) 2021/836 du Parlement européen et du Conseil du 20 mai 2021
[41] SWD(2022) 21 final
[42] Critères de référence, couvrant les situations dans lesquelles il s'agit d'un point de départ, ainsi que d'un objectif ou d'un conseil envisagés concernant des exigences en matière de niveau minimal.
[43] COM(2021) 753 final

Prochaines étapes

- D'ici à 2023, la Commission, en coopération avec le haut représentant et les États membres, évaluera les exigences de base sectorielles en matière de résilience afin de recenser **les lacunes et les besoins** ainsi que les mesures à prendre pour y remédier.
- À la suite de l'adoption de la boussole stratégique, la Commission contribuera à la future boîte à outils hybride de l'UE en veillant à ce que les États membres disposent d'une vue d'ensemble complète des instruments et mesures internes existants pour lutter contre les menaces hybrides qui touchent l'UE et ses États membres. Les mesures figurant dans la cartographie de 2020 sur la lutte contre les menaces hybrides et les propositions récentes de la Commission et du haut représentant dans des domaines tels que les infrastructures critiques et la désinformation seront prises en compte.
- À la suite de l'adoption de la boussole stratégique, la Commission envisagera de trouver des experts dans les domaines d'action pertinents, qui pourraient être déployés sur demande dans le cadre de l'équipe d'intervention rapide en cas de menaces hybrides, en synergie avec les équipes proposées d'intervention rapide de l'UCC.
- Parallèlement, les services de la Commission et le SEAE réexamineront conjointement le protocole opérationnel de l'UE pour la lutte contre les menaces hybrides («EU Playbook»).
- D'ici à la fin de 2022, la Commission, en coopération avec le haut représentant, définira une vision globale de ses mécanismes d'alerte rapide et, en particulier, de la possibilité de dresser un meilleur tableau de la situation, en coordination et en complémentarité avec d'autres mécanismes existants de l'UE. Cela renforcera la capacité de l'Union en matière de suivi et de détection précoce, de prévention et de préparation, y compris la résilience, et de réaction aux menaces hybrides.
- En s'appuyant sur son expertise et ses instruments, la Commission contribuera à l'effort de l'UE visant à renforcer la résilience dans les pays partenaires.

7.2. Renforcer la cybersécurité et la cyberdéfense

La lutte contre les menaces qui pèsent sur la cybersécurité constitue aujourd'hui l'un des défis les plus complexes en matière de sécurité et de défense, compte tenu notamment de leur nombre et de leur impact croissants, et bien que les acteurs étatiques aient développé des capacités sophistiquées spécifiques.

L'UE doit protéger les réseaux et systèmes d'information clés et jouer un rôle de premier plan pour garantir la sécurité, la stabilité et la résilience ainsi que la liberté de l'internet mondial. Nous devons renforcer la cybersécurité et la cyberdéfense en Europe en renforçant notre coopération, en investissant plus efficacement dans des capacités avancées et en définissant des règles appropriées qui permettront de mieux relier toutes les dimensions du cyberespace. Ces efforts devront se concentrer sur la **protection** des citoyens, des entreprises et des intérêts de

l'UE, sur la **détection** et la **dissuasion** des actes de cybermalveillance et sur notre **défense** contre les cyberattaques, ce qui contribuera à la sécurité et à la stabilité internationales et consolidera le potentiel de l'UE en matière de cyberdissuasion.

La Commission et le haut représentant ont déjà défini des actions ambitieuses contribuant à la réalisation de ces objectifs dans la stratégie de cybersécurité de l'UE de décembre 2020[44]. Divers instruments importants existent pour améliorer la résilience de l'UE, notamment la **directive sur les mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union** (SRI)[45], le **règlement sur la cybersécurité**[46], la **directive sur les attaques contre les systèmes d'information**[47], la mise en œuvre de la **boîte à outils de l'UE sur la cybersécurité des réseaux 5G**[48], la **recommandation sur un plan d'action pour une réaction coordonnée aux incidents et crises transfrontières de cybersécurité majeurs** [49]et le **cadre stratégique de cyberdéfense de l'UE [mises à jour de 2018]**[50]. La Commission a également adopté un acte délégué[51] au titre de la directive sur les équipements radioélectriques[52] énonçant des exigences juridiques en matière de garanties relatives à la cybersécurité, et dont les fabricants devront tenir compte lors de la conception et de la production des équipements radioélectriques. Enfin, elle a publié une recommandation en vue de la création d'une **unité conjointe de cybersécurité (UCC)**[53] et a présenté, en décembre 2020, une proposition de **révision de la directive SRI**[54], qui est actuellement examinée par les colégislateurs. Conformément à ce niveau d'ambition, la Commission présentera prochainement des propositions visant à renforcer la cybersécurité et la sécurité de l'information des institutions, organes et agences de l'UE.

Le programme de travail pluriannuel 2021-25 du volet numérique du mécanisme pour l'interconnexion en Europe (MIE - volet numérique) soutiendra le déploiement d'une infrastructure de communication quantique sécurisée (Euro ICQ). Le MIE soutiendra également d'autres infrastructures de communication critiques, y compris certaines infrastructures dorsales entre États membres et avec des pays tiers, présentant les normes de sécurité les plus élevées.

Afin de compléter ces instruments et de réduire davantage la surface d'attaque et l'exposition aux risques, il convient de renforcer la sécurité et la normalisation des produits et services liés

[44] JOIN(2020) 18 final
[45] Directive (UE) 2016/1148 sur la sécurité des réseaux et des systèmes d'information (SRI)
[46] Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) nº 526/2013
[47] Directive 2013/40/UE (12/8/2013)
[48] COM(2020) 50 final
[49] Recommandation (UE) 2017/1584 de la Commission du 13 septembre 2017 sur la réaction coordonnée aux incidents et crises de cybersécurité majeurs (C/2017/6100)
[50] 14413/18 (19/11/2018)
[51] C(2021) 7672
[52] Directive 2014/53/UE du Parlement européen et du Conseil du 16 avril 2014 relative à l'harmonisation des législations des États membres concernant la mise à disposition sur le marché d'équipements radioélectriques
[53] C(2021) 4520 final
[54] COM(2020) 823 final

aux technologies de l'information et de la communication (TIC). Cela vaut en particulier pour la sécurité des composants matériels et logiciels critiques. La Commission prépare donc de nouvelles propositions établissant des exigences horizontales en matière de sécurité, qui constitueront la pièce maîtresse de la **loi sur la cyber-résilience** annoncée dans le discours sur l'état de l'Union[55]. Une dimension «défense» pourrait être envisagée dans ce contexte, en particulier en ce qui concerne l'élaboration éventuelle de normes de cybersécurité communes ou hybrides.

Afin de renforcer encore les capacités technologiques de l'UE et de ses acteurs de la cyberdéfense (principalement les forces de défense des États membres), les acteurs concernés chercheront à collaborer davantage en vue de planifier des investissements dans le domaine civil et de la défense afin de développer les technologies pertinentes et de les utiliser. Le **Centre européen de compétences industrielles, technologiques et de recherche en matière de cybersécurité et le Réseau de centres nationaux de coordination** (CCCN)[56] adopteront en 2022 leur programme stratégique sur les cyberinvestissements. Le programme pourrait couvrir les synergies possibles entre les technologies civiles et de défense et les applications potentielles à double usage, cherchant ainsi à établir des synergies avec d'autres programmes de l'UE, notamment Horizon Europe, le programme pour une Europe numérique et le FED, de manière coordonnée et dans le respect des règles de gouvernance applicables.

La Commission a déjà consacré 38 600 000 EUR[57] à six projets de cyberdéfense. Ce budget soutient, entre autres, le développement d'une plateforme européenne de l'appréciation de la situation en matière de cybersécurité et de cyberdéfense et un projet sur les technologies pour une communication sûre et résiliente. Le FED continuera de soutenir le développement des cybercapacités de défense. En 2021, deux appels spécifiques ont été lancés dans le cadre du FED pour une enveloppe financière de 33 500 000 EUR. Si tous les projets de capacités de défense revêtent une cyberdimension, la cyberdéfense restera une priorité pour le FED dans les années à venir.

Afin de mieux se préparer aux éventuels incidents et crises de grande ampleur dans l'Union, il est essentiel de renforcer la coordination pour garantir une appréciation de la situation, recenser rapidement les besoins et les ressources potentiels en matière de réaction et harmoniser une communication efficace entre les acteurs concernés au niveau des États membres et de l'UE, afin d'atténuer les incidences potentielles dans l'Union.

Afin d'intensifier la **détection des actes de cybermalveillance et d'améliorer l'appréciation de la situation**, la Commission collabore avec les États membres à la mise en place de **plateformes transfrontières de partage des renseignements sur les menaces en matière de cybersécurité (EU SOC),** tout en renforçant les capacités des centres d'opération de sécurité (SOC) au niveau national dans l'ensemble de l'UE. L'objectif de ces plateformes transfrontières (EU SOC) est de permettre l'échange à grande échelle de données sur les menaces liées à la

[55] Discours sur l'état de l'Union 2021 — Renforcer l'âme de l'Union — 15 septembre 2021
[56] PE/28/2021/INIT
[57] Au titre du PEDID

cybersécurité provenant de diverses sources, ainsi que d'outils et de capacités, dans un environnement de confiance. Elles seront équipées d'outils et d'infrastructures de nouvelle génération très sécurisés. Cela devrait permettre d'améliorer les capacités de détection collective et d'alerter en temps utile les autorités et les entités concernées. Ces actions bénéficieront du soutien financier au titre du programme pour une Europe numérique, notamment au travers d'une procédure conjointe de passation de marché pour le développement et l'exploitation des EU SOC, dont des outils et des infrastructures avancés, ainsi que d'un appel à subventions visant à soutenir les capacités des SOC dans les États membres. Dans un second temps, il pourrait également être envisagé de promouvoir la coopération civile et militaire au niveau national dans ce domaine, en collaboration avec les États membres.

Le degré de coopération en matière de cybersécurité entre les États membres en cas de réaction à des incidents devrait être renforcé, y compris par une éventuelle coopération entre les **équipes d'intervention des secteurs civil et de la défense**. L'unité conjointe de cybersécurité vise à réunir toutes les communautés de cybersécurité concernées (à savoir diplomatique, civile, répressive et de la défense) afin d'assurer une réaction coordonnée de l'UE aux incidents et crises de cybersécurité majeurs, ainsi que de prêter assistance aux pays touchés par ces attaques pour qu'ils puissent se rétablir. L'armée pourrait donc assurer une coopération et une coordination structurelles avec d'autres communautés de cybersécurité par l'intermédiaire de l'UCC.

Le **développement de cybercompétences** au moyen de formations et d'exercices conjoints est également essentiel pour une résilience efficace aux cyberattaques, cela permettrait d'améliorer les cybercapacités, de développer une compréhension partagée et de mettre en place une capacité de réaction commune. Si les États membres le décident, ils pourraient envisager de renforcer la coopération civilo-militaire en matière de cyberformation et d'exercices conjoints, en s'appuyant sur les programmes d'éducation, de formation et d'exercices en cybersécurité du Collège européen de sécurité et de défense et de l'AED.

Prochaines étapes

- D'ici au troisième trimestre de 2022, la Commission proposera la **loi sur la cyber-résilience**, qui visera à renforcer la cybersécurité des produits et des services connexes dans le marché intérieur.
- Afin de mettre en place les nouvelles plateformes «EU SOC» de partage de renseignements et d'outils sur les cybermenaces, la Commission publiera, d'ici au deuxième trimestre de 2022, un appel à manifestation d'intérêt visant à sélectionner des entités d'hébergement pour les EU SOC, accompagné d'une feuille de route spécifique. Cela devrait ouvrir la voie à la mise en place d'une capacité stratégique de l'UE en matière de détection et de partage d'informations sur les cybermenaces.
- La Commission collaborera avec les États membres pour renforcer la préparation aux cyberincidents majeurs grâce à une meilleure coordination, notamment en recensant les besoins et les ressources potentiels pour gérer la réaction.
- En 2022, un programme stratégique pour le Centre de compétences en matière de

cybersécurité sera proposé, notamment sur les technologies à double usage et les synergies civilo-militaires qu'il conviendra de mettre en œuvre de manière coordonnée avec les acteurs concernés.

- La Commission, en collaboration avec le haut représentant, continuera d'aider les États membres à mettre en place l'UCC, en particulier son mécanisme d'assistance mutuelle, et encouragera la coopération civilo-militaire afin de faciliter les échanges d'informations et la coordination entre les experts de la défense et d'autres communautés (civile, répressive et diplomatique).
- La Commission demandera aux organisations européennes de normalisation d'élaborer des normes harmonisées pour soutenir l'acte délégué récemment adopté au titre de la directive sur les équipements radioélectriques en ce qui concerne la cybersécurité et la vie privée.
- La Commission collaborera avec le haut représentant pour développer plus en avant la politique de cyberdéfense de l'UE, qui sera présentée aux États membres d'ici à la fin de 2022.
- La Commission invite les États membres à envisager des formations et des exercices conjoints en matière de cyberdéfense, en coopération avec les cadres civils et de défense existants en matière de formation et d'exercices.

7.3. Renforcer la mobilité militaire

Grâce à la mise en œuvre du plan d'action sur la mobilité militaire, l'UE prend déjà des mesures importantes pour renforcer la mobilité du personnel, du matériel et des équipements militaires à l'intérieur et à l'extérieur de l'UE, améliorant ainsi notre capacité à réagir rapidement en cas de crise ou dans la perspective d'activités de routine telles que des exercices. La mobilité militaire est également un projet phare dans le cadre de la coopération UE-OTAN.

Avec un **budget de l'UE de 1 690 000 000 EUR pour la période 2021-2027**, destiné à soutenir les infrastructures de transport à double usage, la mobilité militaire est un élément clé du nouveau mécanisme pour l'interconnexion en Europe (MIE)[58]. Le programme de travail 2021-2023 prévoit un budget annuel spécifique de 330 000 000 EUR et les premiers appels à propositions ont été lancés en septembre 2021.

La mobilité militaire est également un thème du programme de travail 2021 du FED. Le développement d'un système numérique pour un échange sécurisé et rapide d'informations relatives à la mobilité militaire est l'un des deux thèmes de l'appel à propositions relatif aux systèmes fantassin et logistique, doté d'un budget indicatif de 50 000 000 EUR pour l'ensemble de l'appel.

[58] Règlement (UE) 2021/1153 du Parlement européen et du Conseil du 7 juillet 2021 établissant le mécanisme pour l'interconnexion en Europe et abrogeant les règlements (UE) nº 1316/2013 et (UE) nº 283/2014.

Le 14 décembre 2021, la Commission a proposé de revoir le règlement relatif au réseau transeuropéen de transport (RTE-T). Entre autres mesures, la proposition vise à renforcer les normes en matière de mobilité civile et militaire et à élargir les cartes RTE-T afin d'y inclure de nouvelles routes importantes pour la mobilité militaire.

La Commission poursuivra ses efforts pour contribuer à la mobilité militaire à l'intérieur et à l'extérieur de l'UE; cette mobilité sera notamment prise en compte dans les propositions et initiatives législatives pertinentes, en particulier dans le domaine des transports et des procédures transfrontières.

Prochaines étapes

- D'ici à la fin de 2022, la Commission, conjointement avec le haut représentant, proposera une mise à jour du plan d'action conjoint sur la mobilité militaire, qui pourrait couvrir des besoins identifiables liés à la numérisation dans les transports, à la cyber-résilience des infrastructures de transport et à l'intelligence artificielle.

7.4. Relever les défis liés au changement climatique pour la défense

Le changement climatique et la perte de biodiversité font peser de nouvelles menaces sur la sécurité. Bien que le maintien de l'efficacité opérationnelle reste une priorité, le secteur de la défense doit relever le défi que constitue l'adaptation aux effets du changement climatique sur la sécurité, dont les opérations menées dans des conditions climatiques plus extrêmes, et contribuer à l'atténuation de ces effets dans le cadre de son action pour le climat, et notamment du pacte vert pour l'Europe. L'amélioration de l'efficacité énergétique, par une utilisation accrue des énergies renouvelables dans la mesure du possible, et la réduction des émissions dans ce secteur, devraient devenir une partie intégrante de nos efforts collectifs en faveur de la neutralité climatique à l'horizon 2050, de même que la protection de la biodiversité et le renforcement de l'économie circulaire.

Les systèmes circulaires peuvent présenter des avantages majeurs pour les industries de la défense et les acquisitions dans ce domaine, en augmentant l'efficacité des ressources et l'autonomie stratégique ouverte pour certains matériaux critiques et en prolongeant et optimisant l'utilité des équipements de défense[59]. Les possibilités d'améliorer la conception du démontage, de la collecte des composants, de la réparation, de la remise à neuf et du remanufacturage des équipements de défense seront recensées et soutenues. Cela vaut également pour les possibilités de mise à niveau des équipements de défense afin que ceux-ci restent opérationnels dans des environnements de plus en plus hostiles sur les théâtres d'opérations.

Dans ce contexte, la Commission s'est engagée à mettre en œuvre la feuille de route conjointe de l'UE sur le changement climatique et la défense à l'horizon 2020[60], sur laquelle ses services présenteront un premier rapport annuel d'avancement avec le SEAE et l'AED au cours du

[59] IF CEED (europa.eu)Circular defence - News & insight - Cambridge Judge Business School
[60] 12741/20

premier semestre de 2022. Le programme de travail 2021 du FED[61] recense déjà des thèmes liés à la gestion de l'énergie et à l'efficacité énergétique. Un montant de 133 000 000 EUR a été consacré à un appel spécifique visant à soutenir la recherche et le développement de technologies et de produits liés à la défense traitant de ces thèmes. Étant donné que des projets similaires sont développés au sein de l'OTAN, des Nations unies et par les États-Unis et d'autres partenaires, l'UE intensifiera ses dialogues interservices sur le lien entre le climat, la sécurité et la défense.

Prochaines étapes

- Au cours du premier semestre de 2022, les services de la Commission, le SEAE et l'AED présenteront le premier rapport sur l'état d'avancement de la mise en œuvre de la feuille de route sur le changement climatique et la défense.
- Au cours de l'année 2022, la Commission évaluera les initiatives liées au climat et à la défense mises en œuvre dans le cadre des instruments existants pilotés par la Commission (dont le FED, Horizon Europe, Horizon 2020, le MIE et LIFE) afin de renforcer les synergies potentielles.
- D'ici la fin de 2022, la Commission établira un cadre d'action, s'appuyant sur les aspects climatiques et de défense des instruments pilotés par la Commission pour contribuer à réduire la demande énergétique et à accroître la résilience énergétique des technologies critiques utilisées par les acteurs de la sécurité civile et les forces armées, et elle développera des solutions concrètes résilientes au changement climatique dans ce contexte.
- En 2022, la Commission étudiera les possibilités de renforcement de l'impact des directives relatives à l'énergie sur les infrastructures militaires (telles que les bureaux, les quartiers généraux, les casernes, les hôpitaux, les académies), y compris les options en matière de marchés publics écologiques, dans le cadre du pacte vert pour l'Europe (à savoir la nouvelle action en faveur de l'efficacité énergétique intitulée «vague de rénovations», la révision de la directive relative à l'efficacité énergétique et la directive sur la performance énergétique des bâtiments).
- En 2022, la Commission et le haut représentant augmenteront et intensifieront les travaux interservices sur le lien entre le climat, la sécurité et la défense, avec l'OTAN, les Nations unies et les partenaires bilatéraux concernés, tels que les États-Unis et le Canada.

8. Conclusions

Dans un monde plus complexe, plus contesté, plus compétitif et plus connecté que jamais, l'UE doit redoubler d'efforts pour défendre ses intérêts stratégiques et ses valeurs. La future boussole stratégique de l'UE pour la sécurité et la défense définira des objectifs ambitieux pour la sécurité

[61] Le règlement FED dispose que «le Fonds contribue à intégrer les actions en faveur du climat dans les politiques de l'Union et à réaliser l'objectif global consistant à consacrer 30 % des dépenses du budget de l'Union au soutien des objectifs en matière de climat».

et la défense à long terme de l'Europe, objectifs auxquels la présente communication contribue activement.

À cette fin, la Commission a recensé les principaux nouveaux domaines suivants en vue de renforcer encore la compétitivité du marché européen de la défense:

- **étudier comment stimuler davantage les investissements des États membres dans les capacités stratégiques clés et les catalyseurs critiques** qui sont développés et/ou acquis dans les cadres de coopération de l'Union européenne;
- **encourager davantage l'acquisition conjointe de capacités de défense développées de manière collaborative au sein de l'Union**, notamment au moyen d'une exonération de TVA et d'un éventuel renforcement des primes du FED;
- **appeler les États membres à continuer de progresser vers des pratiques de contrôle des exportations d'armes rationalisées et plus convergentes**, en particulier pour les capacités de défense développées dans un cadre coopératif de l'UE.

La Commission mettra également en œuvre les initiatives déjà lancées qui sont des catalyseurs essentiels pour la défense européenne, tels que le **FED et la mobilité militaire**, ainsi que celles qui sont essentielles pour renforcer la résilience européenne, en particulier dans le domaine spatial, pour lutter contre les menaces hybrides, renforcer la cybersécurité et relever les défis en matière de changement climatique liés à la défense.

La Commission reste disposée à envisager de nouvelles mesures à la lumière des progrès accomplis et de l'évolution des menaces et des défis auxquels l'Union sera confrontée à l'avenir.