



Raad van de
Europese Unie

Brussel, 17 februari 2022
(OR. en)

6316/22

LIMITE

COPS 68	PROCIV 16
POLMIL 33	ESPACE 11
EUMC 50	POLMAR 17
CIVCOM 21	MARE 17
CFSP/PESC 171	COMAR 15
CSDP/PSDC 70	COMPET 97
RELEX 196	IND 41
JAI 202	RECH 89
HYBRID 15	COTER 44
DISINFO 11	POLGEN 21
CYBER 53	

BEGELEIDENDE NOTA

van: de secretaris-generaal van de Europese Commissie, ondertekend door mevrouw Martine DEPREZ, directeur

aan: de heer Jeppe TRANHOLM-MIKKELSEN, secretaris-generaal van de Raad van de Europese Unie

nr. Comdoc.: COM(2022) 61 final

Betreft: MEDEDELING VAN DE COMMISSIE AAN HET EUROPEES PARLEMENT, DE RAAD, HET EUROPEES ECONOMISCH EN SOCIAAL COMITÉ EN HET COMITÉ VAN DE REGIO'S Routekaart voor kritieke technologieën voor veiligheid en defensie

Hierbij gaat voor de delegaties document COM(2022) 61 final.

Bijlage: COM(2022) 61 final



Straatsburg, 15.2.2022
COM(2022) 61 final

**MEDEDELING VAN DE COMMISSIE AAN HET EUROPEES PARLEMENT, DE
RAAD, HET EUROPEES ECONOMISCH EN SOCIAAL COMITÉ EN HET COMITÉ
VAN DE REGIO'S**

Routekaart voor kritieke technologieën voor veiligheid en defensie

1. Inleiding

Een voortrekkersrol blijven spelen op het gebied van technologische ontwikkeling is van cruciaal belang om de welvaart, veiligheid en levenswijze van Europa te waarborgen. Nieuwe technologieën veranderen de veiligheids- en defensiesector sneller dan ooit tevoren en vervagen de scheidslijn tussen het civiele en het militaire domein. Met name digitale technologieën zijn van invloed op gevestigde machtsverhoudingen binnen het mondiale veiligheidslandschap. Het is dan ook van essentieel belang ervoor te zorgen dat de Europese veiligheids- en defensiesectoren op technologisch gebied geschikt blijven voor het beoogde doel.

Veel kritieke technologieën voor veiligheid en defensie zijn in toenemende mate afkomstig uit het civiele domein en maken gebruik van kritieke componenten voor tweërlei gebruik. Om innovatie op verschillende gebieden te versnellen en de technologische soevereiniteit in de veiligheids- en defensiesectoren te bevorderen, is een betere uitwisseling tussen civiele en defensieonderzoeks- en innovatiegemeenschappen nodig. In het licht van haar jarenlange deskundigheid op het gebied van civiele technologische ontwikkeling en haar nieuwe instrumenten voor samenwerking op defensiegebied¹ bevindt de EU zich in een goede positie om het voortouw te nemen. Dit vereist echter een efficiënter gebruik van de middelen en de bereidheid om de mogelijkheden van duaal gebruik te onderzoeken, met inachtneming van de fundamentele waarden van de EU. Het betekent ook dat de strategische afhankelijkheden en kwetsbaarheden van de waarde- en toeleveringsketens in verband met deze technologieën moeten worden verminderd.

De versnippering van de veiligheids- en defensievermogens van Europa heeft geleid tot economische inefficiëntie, verminderde operationele capaciteit en grotere strategische afhankelijkheid. De huidige revolutie op het gebied van veiligheids- en defensietechnologieën en de nieuwe EU-instrumenten voor samenwerking op defensiegebied bieden de EU de kans om fouten uit het verleden te vermijden, voort te bouwen op haar bestaande capaciteiten en haar economische welvaart en veiligheid in stand te houden. **Het toekomstige Europese technologische en innovatielandschap op het gebied van veiligheid en defensie moet van meet af aan worden ontwikkeld in het kader van EU-samenwerkingskaders.**

In haar toespraak over de Staat van de Unie van 2021² erkende voorzitter Ursula von der Leyen dat er weliswaar een begin was gemaakt met de ontwikkeling van een Europees defensie-ecosysteem, maar dat er een Europese defensie-unie nodig was. Het strategisch kompas voor veiligheid en defensie van de EU (“strategisch kompas”), dat naar verwachting in maart 2022 door de lidstaten zal worden aangenomen, zal een gemeenschappelijke strategische visie voor het volgende decennium bevatten en aangeven hoe de EU haar capaciteit om op verschillende crises en uitdagingen te reageren, zal vergroten; haar belangen zal veiligstellen en haar burgers zal beschermen; zal investeren en innoveren om gezamenlijk de nodige vermogens en technologieën

¹ Het Europees Defensiefonds (EDF), de gecoördineerde jaarlijkse evaluatie inzake defensie (CARD) en de permanente gestructureerde samenwerking op defensiegebied (PESCO).

² [Toespraak van Commissievoorzitter Ursula von der Leyen over de Staat van de Unie van 2021.](#)

te ontwikkelen; en partnerschappen zal verdiepen op basis van de waarden en belangen van de EU.

Met deze routekaart voor kritieke technologieën voor veiligheid en defensie wordt tegemoetgekomen aan het verzoek van de Europese Raad van 25-26 februari 2021³ om een traject uit te stippelen om onderzoek, technologische ontwikkeling en innovatie (OTO&I) te stimuleren en de strategische afhankelijkheden van de EU op het gebied van kritieke technologieën en waardeketens voor veiligheid en defensie te verminderen. De routekaart zal worden gepresenteerd op de informele top in Parijs op 10 en 11 maart 2022 en zal worden meegenomen in het strategisch kompas. In de routekaart wordt voorgesteld hoe de EU en de lidstaten het bovengenoemde doel gezamenlijk kunnen bereiken, met name door:

- technologieën in kaart te brengen die van cruciaal belang zijn voor de veiligheid en defensie van de EU, en deze te stimuleren door middel van Europese OTO&I-programma's;
- ervoor te zorgen dat in civiele Europese OTO&I-programma's en in het industrie- en handelsbeleid, al naargelang het geval, meer rekening wordt gehouden met defensieoverwegingen, en dat in de OTO&I-programma's voor onderzoek en technologische ontwikkeling op defensiegebied ook meer aandacht wordt geschonken aan de mogelijke civiele toepassingen van de technologieën;
- van meet af aan een EU-brede strategische en gecoördineerde aanpak voor kritieke technologieën voor veiligheid en defensie te bevorderen om optimaal gebruik te maken van de OTO&I-programma's van de EU en de lidstaten, synergieën tot stand te brengen tussen civiele en defensiegerichte OTO&I-gemeenschappen en de strategische afhankelijkheid van externe bronnen te beperken, en
- zoveel mogelijk af te stemmen met andere gelijkgestemde partners, zoals de Verenigde Staten en de Noord-Atlantische Verdragsorganisatie (NAVO), onder wederzijds voordelige voorwaarden.

2. Kritieke technologieën en strategische afhankelijkheden voor veiligheid en defensie

De mededeling “Actualisering van de nieuwe industriestrategie van 2020: een sterkere eengemaakte markt tot stand brengen voor het herstel van Europa”⁴ (“geactualiseerde industriestrategie”) van mei 2021 bevestigt dat technologisch leiderschap een essentiële drijvende kracht blijft achter het concurrentie- en innovatievermogen van de EU, met name voor zogenaamde “kritieke technologieën”⁵. Ook wordt benadrukt hoe belangrijk het is strategische afhankelijkheden in “kwetsbare ecosystemen”, waaronder die van “nabijheid, sociale economie en civiele veiligheid” en “ruimtevaart en defensie”, in kaart te brengen en te beperken om de veerkracht van de EU te waarborgen.

³ [Verklaring van de leden van de Europese Raad van 26 februari 2021.](#)

⁴ [COM\(2021\) 350 final.](#)

⁵ In het kader van haar werkzaamheden met betrekking tot het waarnemingscentrum voor kritieke technologieën is de Commissie bezig met het definiëren van “kriticiteit” ten behoeve van de ruimtevaart, defensie en aanverwante civiele sectoren (met inbegrip van veiligheid).

In het Actieplan voor synergieën tussen de civiele, de defensie- en de ruimtevaartindustrie van de Commissie⁶ (“actieplan voor synergieën”) van februari 2021 wordt het toenemende belang erkend van disruptieve en ontsluitende technologieën die afkomstig zijn uit het civiele domein voor de toekomstige veiligheid en defensie van Europa en de noodzaak om kruisbestuiving en synergieën tussen civiele en defensietechnologieën te bevorderen. Het bevat een aantal kernactiviteiten om de uitwisseling van informatie en de samenwerking tussen civiele en defensiegemeenschappen aan te moedigen door gebruik te maken van de OTO&I-programma’s en -instrumenten van de EU als uitgangspunt.

2.1. De specifieke kenmerken van de veiligheids- en defensiesectoren

De defensie-industrie van de EU heeft een diverse structuur, met grote multinationals en kleine tot middelgrote spelers. De vraag is bijna uitsluitend afkomstig van nationale overheden, die ook alle aankopen van defensiegerelateerde producten en technologieën en de uitvoer ervan controleren. De uiteenlopende nationale vereisten en nationale overheidsuitgaven en -investeringen blijven de EU-markt voor defensie fragmenteren, waarbij soms de interoperabiliteit tussen de nationale strijdkrachten van de lidstaten dreigt te worden belemmerd. De defensiesector volgt daarom niet de conventionele regels en bedrijfsmodellen die op meer traditionele markten van toepassing zijn, en heeft dus weinig ruimte om de daarmee verband houdende investeringen en marktkeuzes te beïnvloeden. Dit maakt het voor de industrie moeilijk om aanzienlijke zelfgefinancierde OTO&I-projecten op defensiegebied uit te voeren.

De veiligheidsindustrie in de EU staat voor soortgelijke uitdagingen, aangezien de markten ook overwegend nationaal zijn, maar nog meer gefragmenteerd. De klanten zijn divers (bv. politiediensten, binnenlandse veiligheidsdiensten, douanediensden, grensautoriteiten, particuliere beveiligingsdiensten), de activiteiten vinden plaats op verschillende niveaus (lokaal, regionaal, nationaal) en de organisatie verschilt van lidstaat tot lidstaat. **De Commissie zal in 2022 een studie over de veiligheidsmarkt van de EU presenteren om meer inzicht te krijgen in deze complexe sector.** Daarnaast zullen de diensten van de Commissie in de eerste helft van 2022 een samenvatting maken van de voorstellen ter bevordering van de vaststelling van vermogensgerichte benaderingen die in alle veiligheidssectoren moeten worden toegepast. Deze voorstellen zullen de vroegtijdige en toekomstgerichte vaststelling van behoeften en oplossingen op het gebied van veiligheid en rechtshandhaving versterken.

De ruimtevaart- en cybersectoren zijn strategische “katalysatoren” voor de veiligheids- en defensiesectoren. De ruimtevaartsector heeft met de veiligheids- en defensiesectoren veel van zijn specifieke kenmerken gemeen, met zijn kleine marktvolumes en beperkte hefboomwerking op de particuliere markt voor componenten. De veerkracht van de ruimtevaartprogramma’s en -waardeketens is van cruciaal belang voor de veiligheids- en defensiedoelstellingen van de EU. Cyberspace speelt ook een steeds belangrijker rol in alle defensievermogens en vereist aandacht en investeringen. Gezien de snel toenemende cyberaanvallen op zowel civiele als defensie-activa en -netwerken, en de toenemende rol van de civiele sector bij cyberinnovatie en -normalisatie, zijn nauwere banden tussen cyberbeveiliging en cyberdefensie nodig. In de bijdrage van de

⁶ [COM\(2021\) 70 final](#).

Commissie aan de Europese defensie in het kader van het strategisch kompas (“defensiedelivering”), dat deel uitmaakt van dit defensiepakket, zijn verdere maatregelen voor deze twee sectoren voorzien.

2.2. Kritieke technologieën en strategische afhankelijkheden voor veiligheid en defensie in kaart brengen

De geactualiseerde industriestrategie voorziet in een brede inventarisatie en analyse van de strategische afhankelijkheden en capaciteiten van de EU, op basis van een eerste ronde van diepgaande evaluaties van kwetsbare ecosystemen⁷. Deze werkzaamheden hebben weliswaar de basis gelegd voor beleidsmaatregelen ter ondersteuning van een grotere weerbaarheid van de EU, maar in de strategie wordt ook erkend dat er meer moet worden gedaan om ons inzicht in de strategische afhankelijkheden van de EU en de wijze waarop zij zich kunnen ontwikkelen en tot verdere kwetsbaarheden kunnen leiden, te vergroten. Deze werkzaamheden omvatten een tweede ronde van diepgaande evaluaties van kwetsbare ecosystemen en een monitoringsysteem via het waarnemingscentrum voor kritieke technologieën (“waarnemingscentrum”), zie punt 2.3.

De diensten van de Commissie zijn begonnen met diepgaande evaluaties van defensie- en veiligheidstechnologieën, onder meer op het gebied van cyberbeveiliging, ter ondersteuning van de geactualiseerde industriële strategie en de ontwikkeling van het waarnemingscentrum. Tot dusver zijn twee voorlopige casestudy's uitgevoerd met betrekking tot de defensietechnologiegebieden van autonome systemen en halfgeleiders, die als representatief werden beschouwd vanwege hun transversale relevantie voor militaire vermogens op verschillende gebieden, zie kader 1. Het doel was gemeenschappelijke patronen tussen deze defensietechnologiegebieden in kaart te brengen, met name wat betreft de oorzaken van afhankelijkheden en de daaraan verbonden risico's, alsook de eerste mogelijkheden om deze te beperken.

De casestudy's bevestigen dat de defensiesector in grote lijnen dezelfde strategische afhankelijkheden en kwetsbaarheden kent als andere kwetsbare ecosystemen, met name wat betreft technologische lacunes, (kritieke) grondstoffen, vaardigheden, lage OTO&I-investeringen en extraterritoriale regelgeving door niet-EU-landen. Zij wijzen er ook op dat de kwetsbaarheden van de sector over het algemeen worden verergerd door de strategische en gevoelige aard van zijn activiteiten (bv. strengere normen voor de beveiliging van informatie en de voorzieningszekerheid) en de relatief marginale omvang van de markt.

Uit de casestudy's blijkt verder dat sommige concurrenten van de EU wereldwijd meer offensieve en defensieve acties ondernemen om kritieke technologieën te bevorderen en strategische afhankelijkheden aan te pakken dan de EU tot nu toe heeft gedaan. Zo koppelen zij nationale defensieoverwegingen systematischer aan civiele technologische ontwikkeling, investeren zij zwaar in hun eigen OTO&I en industriële capaciteit, trekken zij externe investeerders aan en zetten zij soms agressieve overnamestrategieën in derde landen in. Zij beschermen ook hun eigen industriële expertise en invloed door gebruik te maken van onderlinge

⁷ [SWD\(2021\) 352 final](#).

afhankelijkheden of strikte extraterritoriale regelgeving om de toegang van derde landen tot technologieën te beperken.

Hoewel de EU over eigen instrumenten beschikt om haar industriële capaciteit in overeenstemming met de EU-regels te versterken, wordt zij gehinderd door de nog steeds grotendeels gefragmenteerde vraag op de defensiemarkt in de EU, haar historisch strikte scheiding van civiele en defensiegerelateerde OTO&I op EU-niveau en relatieve onderinvesteringen door de lidstaten in de Europese technologische en industriële defensiebasis (EDTIB). De collectieve uitgaven van de lidstaten voor defensie-innovatie (2,5 miljard EUR of 1,2 % van de defensie-uitgaven) blijven immers achterop ten aanzien van het EDA-streefcijfer van 2 % dat 15 jaar geleden werd vastgelegd.

Hoewel de marktkrachten hebben geleid tot een situatie waarin geen enkel land volledige technologische soevereiniteit op technologisch gebied kan verwerven, is er een wereldwijde wedloop om technologisch leiderschap en de daaraan verbonden economische en militaire voordelen. Dit zou de bestaande strategische afhankelijkheden van de EU kunnen verergeren en nieuwe afhankelijkheden kunnen genereren als zij geen actie onderneemt. Een gestructureerde aanpak is nodig om de EU in staat te stellen een voortrekkersrol te blijven spelen op het gebied van kritieke technologieën en strategische afhankelijkheden op het gebied van veiligheid en defensie in kaart te brengen en te beperken. Met deze routekaart wordt beoogd een dergelijke aanpak te bieden, die moet worden geïntegreerd in het strategisch kompas van de EU.

Kader 1: Casestudy's – Autonome systemen en halfgeleiders voor defensie

In de analytische werkzaamheden van de Commissie op het gebied van autonome defensiesystemen, met bijzondere aandacht voor kunstmatige intelligentie (AI) en machinaal leren, zijn relevante kritieke technologieën en vier essentiële gebieden vastgesteld waarop de EU achterloopt, namelijk: vaardigheden, gegevens, hardware en tests. Mogelijke maatregelen om deze aan te pakken, zouden voortbouwen op de bestaande AI-strategie van de EU⁸ en de bijbehorende beleidsinitiatieven, alsook op de nationale AI-strategieën van de lidstaten. Het gaat onder meer om OTO&I-activiteiten (bv. grotere beschikbaarheid van gegevens en opleiding op het gebied van AI, koppeling met het European Processor Initiative), infrastructuur (bv. cloudcomputingcapaciteit voor defensiedoeleinden, binnenlandse testfaciliteiten) en de bescherming van bestaande kritieke activa (bv. screening van buitenlandse directe investeringen).

Uit de analytische werkzaamheden met betrekking tot halfgeleiders voor defensie bleken duidelijk de alomtegenwoordige aanwezigheid van halfgeleiders in defensiematerieel en de bestaande en toekomstige afhankelijkheden, met name als gevolg van het gebrek aan eigen EU-capaciteiten (foundries) voor de meest geavanceerde procesknooppunten. De Commissie heeft risicobeperkende maatregelen opgenomen in het voorstel voor een Europese chipverordening van 8 februari 2022⁹, dat tot doel heeft een geavanceerd Europees chipecosysteem tot stand te brengen om de vermogens van de EU op dit gebied te verbeteren en zo ook in de defensiebehoeften te voorzien.

⁸ [COM\(2018\) 237 final.](#)

⁹ [COM\(2022\) 45 final.](#)

2.3. *Het waarnemingscentrum voor kritieke technologieën*

Een gebrek aan vooruitziendheid over het toekomstige belang van technologieën ligt deels ten grondslag aan een aantal van de bestaande strategische afhankelijkheden van de EU ten opzichte van derde landen (bv. op afstand bestuurd systemen, halfgeleiders). De EU heeft behoefte aan meer gestructureerde vooruitziendheid en strategische reflectie over kritieke technologieën voor veiligheid en defensie om prioritaire gebieden vast te stellen om onderzoek en innovatie te stimuleren, bestaande strategische afhankelijkheden te verminderen en het ontstaan van nieuwe afhankelijkheden te voorkomen.

Het waarnemingscentrum voor kritieke technologieën, dat momenteel door de Commissie wordt opgericht in overeenstemming met het actieplan voor synergieën (actie 4), zal bijdragen aan deze reflectie. In de werkmethode van het waarnemingscentrum zal rekening worden gehouden met andere soortgelijke initiatieven¹⁰ om dubbel werk te voorkomen. Dit zal het mogelijk maken de lijst van kritieke technologieën uit het actieplan voor synergieën aan te passen aan het evoluerende technologielandschap en de vermogensbehoeften.

Het waarnemingscentrum zal kritieke technologieën voor de ruimtevaart-, defensie- en aanverwante civiele sectoren, de potentiële toepassing ervan en de bijbehorende waarde- en toeleveringsketens identificeren, monitoren en beoordelen. Het zal ook bestaande en voorspelbare technologische lacunes, onderliggende oorzaken van strategische afhankelijkheden en kwetsbaarheden in kaart brengen, monitoren en analyseren.

Het is van essentieel belang dat met de lidstaten overeenstemming wordt bereikt over een zinvolle mate van gedetailleerdheid om deze kwesties op EU-niveau te bespreken en over de noodzaak om relevante gegevens tussen de lidstaten en met de Commissie te delen. Binnen het waarnemingscentrum zal een mechanisme in de vorm van een speciale deskundigengroep worden ingesteld voor uitwisselingen en besprekingen met de lidstaten in een gerubriceerde omgeving. Dit omvat besprekingen over de opkomst van nieuwe en disruptieve technologieën om nieuwe afhankelijkheden voor de veiligheids-, defensie- en ruimtevaartindustrieën te voorkomen. De hoge vertegenwoordiger en zijn diensten zullen bij dit proces worden betrokken.

Op basis van de gegevens van het waarnemingscentrum zal de Commissie de lidstaten uiterlijk eind 2022 en vervolgens om de twee jaar een gerubriceerd verslag voorleggen over kritieke technologieën en risico's in verband met strategische afhankelijkheden die van invloed zijn op veiligheid, ruimtevaart en defensie. De Commissie zal op basis van deze verslagen technologie-routekaarten opstellen, die mitigerende maatregelen zullen omvatten om OTO&I te stimuleren en strategische afhankelijkheden die van invloed zijn op veiligheid en defensie te verminderen.

¹⁰ Bijvoorbeeld de ondersteuning en instrumenten van het project inzake geavanceerde technologieën voor de industrie (ATI), de monitoring van kritieke technologieën voor de ruimtevaart, de overkoepelende strategische onderzoeksagenda (OSRA), de technologie-bouwstenen (TBB) en de belangrijke strategische activiteiten (KSA) van het Europees Defensieagentschap (EDA).

Zodra de werkzaamheden van het waarnemingscentrum goed operationeel zijn, zou de reikwijdte van de werkzaamheden ervan kunnen worden uitgebreid tot andere bedrijfstakken, zoals aangegeven in de geactualiseerde industriestrategie.

Verdere maatregelen:

- In 2022 zal de Commissie een deskundigengroep oprichten om uitwisselingen met de lidstaten over kritieke technologieën en waarde- en toeleveringsketens te vergemakkelijken. Het zal deel uitmaken van het waarnemingscentrum voor kritieke technologieën voor defensie, ruimtevaart en aanverwante civiele industrieën. De bedoeling daarvan moet zijn:
 - regelmatig overleg te plegen met de autoriteiten van de lidstaten om het gerubriceerde verslag op te stellen;
 - te zorgen voor de passende behandeling van gevoelige en gerubriceerde informatie die kan worden uitgewisseld in het kader van het waarnemingscentrum voor kritieke technologieën, gerelateerde verslagen en routekaarten.
- Tegen medio 2022 zal de Commissie een studie over de veiligheidsmarkt van de EU presenteren die zal dienen om een beter inzicht te krijgen in de specifieke kenmerken van de markt voor civiele veiligheid, om de identificatie van kritieke technologieën en strategische afhankelijkheden te ondersteunen en om de nieuwe vermogensgestuurde aanpak voor veiligheid en andere OTO&I-activiteiten te onderbouwen.
- Tegen medio 2022 zullen de diensten van de Commissie een document opstellen met een samenvatting van de voorstellen ter bevordering van de vaststelling van vermogensgerichte benaderingen die in alle veiligheidssectoren moeten worden toegepast.

3. OTO&I inzake kritieke technologieën voor veiligheid en defensie stimuleren

De technologische routekaarten die de Commissie op basis van de beoordelingen van het waarnemingscentrum zal opstellen, zullen de basis vormen voor activiteiten variërend van het programmeren van OTO&I inzake kritieke technologieën tot de ontwikkeling van grotere vlaggenschipinitiatieven die zullen bijdragen tot de versterking van het concurrentievermogen en de veerkracht van de EU in de veiligheids- en defensiesectoren. Om deze doelstellingen te verwezenlijken, moet efficiënter gebruik worden gemaakt van de beschikbare financiële middelen door betere coördinatie van de bestaande EU- en nationale OTO&I-programma's en -instrumenten.

3.1. Een einde maken aan de scheiding tussen EU-OTO&I op civiel en defensiegebied

De Commissie heeft zich er in het kader van haar actieplan voor synergieën (actie 2) toe verbonden de interne coördinatie tussen EU-programma's en -instrumenten tegen 2022 te verbeteren (zie kader 2) om de enorme voordelen te ontsluiten die voortvloeien uit synergieën tussen OTO&I op civiel en defensiegebied voor economische groei, de eengemaakte markt en de veiligheid van de Europese burgers.

Hoewel de verwezenlijking van deze doelstelling ook in 2023 kan worden voortgezet (bv. door betere planning en synchronisatie, richtsnoeren voor beheersautoriteiten in de lidstaten enz.), zullen sommige belemmeringen op korte en middellange termijn moeilijker aan te pakken zijn en

kan het nodig zijn andere belanghebbenden hierbij te betrekken. Dit is met name het geval wanneer wettelijke bepalingen in de basishandelingen van EU-programma's en -instrumenten praktische beperkingen opleggen. Terwijl activiteiten voor tweërlei gebruik bijvoorbeeld kunnen worden gefinancierd in het kader van de Connecting Europe Facility (CEF) en de Europese structuur- en investeringsfondsen (ESIF), zijn de activiteiten in het kader van Horizon Europa¹¹ gericht op civiele toepassingen; er is geen kader voor rechtstreekse steun voor dergelijke activiteiten in het kader van OTO&I-programma's en -instrumenten. Ook het kredietverleningsbeleid van de Europese Investeringsbank kent nog steeds beperkingen voor de defensiesector.

Om de uitwisseling tussen civiele en defensiegemeenschappen, met name op het gebied van kritieke technologieën, te vergemakkelijken, zal de Commissie in 2023 een aanpak uitwerken om de volledige implementatie op EU-niveau van OTO&I voor tweërlei gebruik op de middellange tot lange termijn in alle EU-programma's en -instrumenten aan te moedigen. Deze werkzaamheden zullen ook worden meegenomen in de tussentijdse evaluatie van relevante sectorale programma's, zoals de fondsen in het kader van de verordening gemeenschappelijke bepalingen, met inbegrip van fondsen voor paraatheid bij noodsituaties op gezondheidsgebied.

Kader 2: EU-programma's en -instrumenten ter ondersteuning van OTO&I inzake kritieke technologieën die van belang zijn voor veiligheid en defensie en de uitrol van de infrastructuur daarvoor in het kader van het meerjarig financieel programma (2021-2027)

- Het EDF besteedt 8 miljard euro aan onderzoek en ontwikkeling op defensiegebied. 4-8 % van de EDF-begroting voor onderzoek en ontwikkeling zal worden toegewezen aan disruptieve technologieën, d.w.z. maximaal 100 miljoen EUR per jaar.
- In het kader van pijler II ("Wereldwijde uitdagingen en Europees industrieel concurrentievermogen") van Horizon Europa wordt 1,6 miljard EUR toegewezen aan onderzoek en innovatie op het gebied van civiele veiligheid in het kader van de cluster "Civiele veiligheid voor de samenleving", terwijl kritieke technologieën worden ondersteund in het kader van de clusters "Digitale wereld, industrie en ruimte", "Klimaat, energie en mobiliteit" en "Levensmiddelen, bio-economie, natuurlijke hulpbronnen, landbouw en milieu". Aanvullende activiteiten worden gefinancierd in het kader van pijler I ("Wetenschappelijke excellentie"), de Europese Innovatieraad (EIC) en het Europees Instituut voor innovatie en technologie (EIT) in pijler III ("Innovatief Europa"), alsook Europese partnerschappen die middelen bundelen en mobiliseren om het technologisch leiderschap van de EU en de open strategische autonomie op kritieke gebieden te waarborgen;
- het programma Digitaal Europa (DEP) zal uitrolactiviteiten bevorderen die relevant zijn voor kritieke technologieën op de prioritaire gebieden cyberbeveiliging, AI en supercomputing;
- het kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging en het netwerk van nationale coördinatiecentra zullen naar verwachting in 2022 een strategische agenda vaststellen voor cyberinvesteringen die bijdragen aan Horizon

¹¹ De term "Horizon Europa" verwijst in dit document naar het specifieke programma tot uitvoering van Horizon Europa en het Europees Instituut voor innovatie en technologie. De activiteiten in het kader van deze programma's zijn uitsluitend gericht op civiele toepassingen.

Europa en het DEP. Synergieën tussen civiele en defensietechnologieën en toepassingen voor tweërlei gebruik kunnen worden onderzocht door middel van koppelingen met het EDF in overeenstemming met de toepasselijke regels.

- De ESIF (met name het Europees Fonds voor regionale ontwikkeling en het Europees Sociaal Fonds Plus) kunnen worden gebruikt ter ondersteuning van de EDTIB;
- andere relevante EU-programma's, -fondsen en -instrumenten zijn onder meer het ruimtevaartprogramma, de CEF, het InvestEU-programma, de herstel- en veerkrachtfaciliteit (RRF), het LIFE-programma, publiek-private partnerschappen en blendingfaciliteiten.

3.2. Koppeling van EU- en nationale programma's en instrumenten ter ondersteuning van OTO&I inzake kritieke technologieën voor veiligheid en defensie

Hoewel EU-programma's en -instrumenten voorzien in aanzienlijke financiering voor OTO&I-activiteiten op het gebied van veiligheid en defensie in de EU, komt het grootste deel van de financiering voor dergelijke activiteiten nog steeds van de lidstaten, en blijft de versnippering van de veiligheids- en defensiemarkten een ernstig probleem. Het bereiken van technologische soevereiniteit op sommige kritieke technologiegebieden en het beperken van strategische afhankelijkheden op andere gebieden vereist derhalve EU-brede coördinatie.

De lidstaten wordt verzocht zich er in het strategisch kompas toe te verbinden om samen met de Commissie van meet af aan een EU-brede strategische gecoördineerde aanpak te ontwikkelen voor kritieke technologieën die relevant zijn voor veiligheid en defensie, met volledige inachtneming van de verscheidenheid en complexiteit van het beheer van EU- en nationale programma's en instrumenten. Bij deze aanpak zou ook rekening worden gehouden met andere coördinatiestructuren, zoals de nieuwe EU-innovatiehub voor interne veiligheid, die wordt voorgezeten door het Permanent Comité operationele samenwerking op het gebied van de binnenlandse veiligheid (COSI), en de nieuwe door het EDA op te richten EU-innovatiehub voor defensie.

De aanpak zou gebruikmaken van de gerubriceerde verslagen over kritieke technologieën en de technologische routekaarten die door de Commissie zijn opgesteld als uitgangspunt voor besprekingen tussen de autoriteiten van de lidstaten en de Commissie. Het doel zou zijn om op basis van de technologische routekaarten vast te stellen op welke gebieden het meest dringend moet worden opgetreden en om de programma's, instrumenten en beleidsmaatregelen van de EU en de lidstaten te mobiliseren om deze op gecoördineerde wijze in te zetten, in overeenstemming met de staatssteunregels van de EU. Dit zou ervoor zorgen dat investeringen gericht zijn op de gebieden die het meest van belang zijn voor de veiligheid van de EU-burgers. De prioriteiten zouden regelmatig worden geactualiseerd om ervoor te zorgen dat zij relevant blijven en dat de uitgaven efficiënt zijn.

De Commissie zal met de lidstaten samenwerken om het beste mechanisme vast te stellen om deze coördinatiewerkzaamheden te vergemakkelijken (bv. de deskundigengroep van het waarnemingscentrum).

3.3. Ondersteuning van innovatie en ondernemerschap op het gebied van veiligheid en defensie – Invoering van een EU-innovatieregeling voor defensie

De EU moet het volledige potentieel van haar innovatiegemeenschap ter ondersteuning van veiligheid en defensie beter benutten. Daartoe moeten niet-traditionele spelers en bestaande innovatieve start-ups en kleine en middelgrote ondernemingen (kmo's) in beide sectoren worden geholpen om hun hoge technologische, administratieve, regelgevende en markttoegangsbelemmeringen te overwinnen, om aan de hoge beveiligingsnormen te voldoen en om toegang te verkrijgen tot financiering. De defensiemarkt is vaak opgebouwd rond enkele grote spelers die worden ondersteund door een reeks gespecialiseerde kmo's die beperkte rechtstreekse toegang tot deze markt hebben. Daardoor kan het voor innovatieve kmo's op defensiegebied moeilijk zijn om toegang te krijgen tot financiering, waardoor zij zich mogelijk eerder tot buitenlandse investeerders wenden of daar het doelwit van zijn. De situatie is vergelijkbaar voor innovatieve kmo's die actief zijn op het gebied van veiligheid. Zij worden met vergelijkbare uitdagingen geconfronteerd bij het benaderen van potentiële klanten of het verkrijgen van toegang tot financiering op maat¹².

De Commissie ondersteunt innovatieve start-ups en -kmo's die actief zijn op het gebied van veiligheid in het kader van Horizon 2020. De toegewezen financiering en de algemene succespercentages in het kader van maatschappelijke uitdaging 7 ("Civiele veiligheid voor de samenleving") liggen boven het gemiddelde voor kleine innovatoren. Hoewel deze steun in het kader van Horizon Europa zal worden voortgezet, zullen start-ups en kmo's die actief zijn op het gebied van veiligheid nog steeds aanvullende, op maat gesneden steun nodig hebben om hun weg naar de markt te versnellen. Het verkennen van nieuwe instrumenten voor innovatie voor tweërlei gebruik zou hun productiecapaciteit, concurrentievermogen en duurzaamheid kunnen vergroten.

De Commissie is in het kader van het EDF begonnen met het opzetten van soortgelijke activiteiten voor de ontwikkeling van een instrumentarium voor innovatie op het gebied van defensie en tweërlei gebruik met betrekking tot niveaus van technologische paraatheid¹³ (TRL's) 1-9. Er wordt gewerkt aan de volgende instrumenten op het gebied van defensie, nieuwe technologieën en tweërlei gebruik:

- a) *Defensie-innovatie via het EDF* — Specifieke acties worden onderzocht om projecten op het gebied van disruptieve technologieën en innovatieve en toekomstgerichte defensieoplossingen beter te ondersteunen, waarbij met name de deelname van innovatieve kmo's, innovatieve laboratoria en onderzoeks- en technologieorganisaties (RTO's) wordt aangemoedigd. Deze acties kunnen verschillende vormen aannemen, bijvoorbeeld bedrijfscoaching (werkprogramma 2021); technologische uitdagingen (werkprogramma 2022),

¹² Virtueel evenement van CERIS over [uitdagingen en kansen voor kmo's en start-ups inzake onderzoek en innovatie op het gebied van veiligheid in de EU](#), 30 april 2021.

¹³ De EU heeft in het kader van haar OTO&I-programma's en -instrumenten sinds 2014 in brede zin gebruikgemaakt van een schaalstelsel op basis van niveaus van technologische paraatheid (TRL's). De schaal onderscheidt negen niveaus van technologische rijpheid, variërend van fundamenteel onderzoek op TRL 1 tot een eindproduct dat klaar is om op TRL 9 op de markt te worden gebracht. Aangezien de toepassing en dus het potentieel voor tweërlei gebruik van een technologie doorgaans duidelijk wordt op TRL's 5-6, kan worden aangenomen dat een technologie "neutraal" is op TRL's 1-4.

hackathons of prijzen (werkprogramma 2023 of later). Zij zullen ook voortbouwen op relevante ervaringen van de EIC en kunnen verband houden met het nieuwe Cassini voor defensie.

- b) *Een blindingfaciliteit voor defensie-investeringen in het kader van InvestEU* — De oprichting van een dergelijke faciliteit zou de Commissie in staat stellen te garanderen dat financiële intermediairs in de hele EU investeren in innovatieve of strategische kmo's op defensiegebied. Dit zou de problemen in verband met de beperkte toegang tot financiering voor kmo's die veelbelovende technologieën voor de Europese defensie ontwikkelen, verlichten en tegelijkertijd betrouwbaar kapitaal verschaffen en vijandige overnames door entiteiten uit derde landen voorkomen. Een betere toegang tot aandelenfinanciering voor innovatieve kmo's en midcaps op defensiegebied zou hun groei ondersteunen en uiteindelijk het innovatievermogen van de EDTIB ten goede komen. De Commissie zal ook onderzoeken of er behoefte is aan verdere instrumenten ter ondersteuning van belangrijke marktdeelnemers in de waardeketen.
- c) *Cassini voor defensie* — Dit initiatief zou geïnspireerd zijn op het bestaande Cassini-initiatief ter ondersteuning van kmo's en start-ups in de ruimtevaartindustrie. Het zou hun diensten verlenen zoals: bedrijfsontwikkeling en -netwerken (bv. matchmaking, bedrijfsaccelerator) en prijzen en wedstrijden (met inbegrip van hackathons, mentorschap enz.), ter aanvulling van de bovenvermelde blindingfaciliteit voor defensie-investeringen.
- d) *Innovatie-incubator* — De Commissie zal in 2022 een innovatie-incubator opzetten om de ontwikkeling van nieuwe technologieën te ondersteunen en innovatie voor tweërlei gebruik vorm te geven in overeenstemming met het actieplan voor synergieën (actie 6). Dit zou een belangrijke rol kunnen spelen bij het overbruggen van de kloof tussen OTO&I-programma's op civiel en defensiegebied. Na een systematische analyse van de resultaten van de technologische ontwikkeling in een vroeg stadium, zou de incubator projecten en/of technologieën die potentiële veiligheids-, ruimtevaart- of defensietoepassingen zouden kunnen bieden, signaleren aan relevante diensten van de Commissie en de lidstaten met het oog op de mogelijke invoering ervan. De Commissie zou nagaan hoe deze gemarkeerde projecten in voorkomend geval kunnen worden doorverwezen naar verdere financieringsmogelijkheden, zoals de financieringsregeling voor transitie van de EIC of het EDF.
- e) *Ondersteuning van innovatienetwerken* — Grensoverschrijdende innovatienetwerken op defensiegebied kunnen de rol van innovatiemakelaars spelen en samenwerkingsprojecten aanmoedigen om innovatieve oplossingen te integreren. Door middel van technologische scouting zouden nieuwe innovatieve oplossingen en technologieën met potentiële voordelen voor defensietoepassingen kunnen worden geïdentificeerd. Onderzoekscentra en technische testfaciliteiten zouden vervolgens de relevantie van dergelijke technologieën uit het civiele domein testen en beste praktijken uitwisselen. Het EDA zou een kernpartner van de Commissie zijn voor de uitvoering van een ander deel van actie 6 van het actieplan voor synergieën.

De Commissie zal nagaan hoe het instrumentarium kan worden gekoppeld aan instrumenten ter ondersteuning van innovatie op het gebied van veiligheid (bv. Horizon Europa) of cyberbeveiliging (bv. het netwerk van nationale coördinatiecentra voor cyberbeveiliging in samenwerking met de Europese digitale-innovatiehubs).

De complementaire sterke punten van de Commissie en het EDA moeten worden samengebracht in een “**EU-innovatieregeling voor defensie**”. Op basis van haar ervaring met de uitvoering van de EU-begroting ter ondersteuning van OTO&I voor defensie alsmede voor civiel en tweërlei gebruik, zal de Commissie in het kader van de regeling een centrale rol spelen in het stimuleren van innovatie voor de EDTIB. Gezien zijn deskundigheid op defensiegebied, onder meer bij het samenbrengen van opkomende en disruptieve technologieën en militaire vermogensbehoeften, zal het EDA de inspanningen van de lidstaten verder verbinden en ondersteunen via zijn defensie-innovatiehub. Door nauw samen te werken zullen de Commissie en het EDA in synergie de innovatie op het gebied van veiligheid en defensie voor de EU en haar lidstaten versnellen.

3.4. Vaardigheden

Het gebrek aan vaardigheden en het tekort aan arbeidskrachten, met name aan geschoolde werknemers met een achtergrond op het gebied van wetenschap, technologie, engineering en wiskunde, zijn grote uitdagingen voor de defensie- en veiligheidsindustrie, die net als vele andere hightechindustrieën er sterk van afhankelijk zijn. Aangezien de technologieën en het dreigingslandschap zich snel ontwikkelen, is het belangrijk dat de industrie meer de hand reikt aan nieuwe en jonge onderzoekers en ondernemers, met inbegrip van vrouwen, op basis van een inclusieve en toegankelijke benadering van alle talenten, vaardigheden en beschikbare arbeidskrachten.

In november 2020 lanceerde de Commissie het pact voor vaardigheden met een eerste golf van vaardighedenpartnerschappen in drie belangrijke industriële ecosystemen, namelijk de micro-elektronica, de automobielenindustrie en de lucht- en ruimtevaartindustrieën. De leden van het pact (industrie, universiteiten en opleidingsorganisaties, sociale partners) hebben zich ertoe verbonden te zorgen voor een continu en duurzaam aanbod van vaardigheden op de meest noodzakelijke gebieden door 200 000 werknemers bij te scholen en 300 000 mensen om te scholen, met een gecombineerde publieke en particuliere investering van 1 miljard EUR tegen 2030.

Verdere maatregelen:

- De Commissie verzoekt de lidstaten zich er in het strategisch kompas toe te verbinden van meet af aan een EU-brede strategische gecoördineerde aanpak te ontwikkelen voor kritieke technologieën die van belang zijn voor veiligheid en defensie.
- In 2023 zal de Commissie de bestaande EU-instrumenten evalueren en verdere manieren voorstellen om OTO&I voor tweërlei gebruik op EU-niveau aan te moedigen.
- De Commissie zal innovatie en ondernemerschap op het gebied van kritieke technologieën voor veiligheid en defensie ondersteunen op basis van de volgende instrumenten: a) specifieke EDF-acties; b) een nieuwe blendingfaciliteit voor defensie-investeringen in het

kader van InvestEU; c) een nieuw Cassini voor defensie; d) een nieuwe incubator voor innovatie op het gebied van nieuwe technologieën en innovatie voor tweërlei gebruik in 2022, en e) meer steun voor innovatienetwerken.

- De Commissie zal samen met het EDA en zijn defensie-innovatiehub een EU-innovatieregeling voor defensie opzetten om de innovatie op het gebied van veiligheid en defensie voor de EU en haar lidstaten te versnellen.

4. Vermindering van strategische afhankelijkheden in kritieke technologieën en waardeketens voor veiligheid en defensie

Naast haar OTO&I-programma's en -instrumenten beschikt de EU over verschillende beleidsinstrumenten die kunnen bijdragen tot het verminderen van haar strategische afhankelijkheid in kritieke technologieën en waardeketens in de veiligheids- en defensiesectoren. Deze dragen bij tot de versterking van de industriële capaciteit, het concurrentievermogen, de technologische soevereiniteit en de veerkracht van de EU, maar ook tot de bescherming van de huidige en toekomstige technologische ontwikkelingen en vermogens.

De Commissie zal, op basis van de werkzaamheden van het waarnemingscentrum voor kritieke technologieën en in het kader van de geactualiseerde industriestrategie, in voorkomend geval systematisch veiligheids- en defensieoverwegingen beoordelen bij de uitvoering en herziening van bestaande industriële en handelsinstrumenten van de EU of bij het ontwerpen van nieuwe industriële en handelsinstrumenten van de EU om ervoor te zorgen dat deze geschikt zijn voor het beoogde doel.

- *Industriële allianties* — Industriële allianties betrekken een breed scala van partners (bv. publieke en private spelers, het maatschappelijk middenveld) bij gezamenlijke actie met betrekking tot belangrijke beleidsdoelstellingen van de EU in specifieke bedrijfstakken of waardeketens. Zij zijn gebaseerd op de beginselen van openheid, transparantie, diversiteit en inclusiviteit en werken met volledige inachtneming van de mededingingsregels. Industriële allianties kunnen in voorkomend geval specifieke werkterreinen omvatten om de strategische afhankelijkheid van de veiligheids- en defensiesector te verminderen. Dit wordt overwogen in de Europese alliantie voor industriële gegevens, edge en cloud en in de industriële alliantie op het gebied van processors en halfgeleider technologieën.
- *Belangrijke projecten van gemeenschappelijk Europees belang (IPCEI)* — IPCEI's worden geïnitieerd door de lidstaten en zijn onderworpen aan de EU-staatssteunregels. Zij zijn bedoeld om kennis, deskundigheid, financiële middelen en economische actoren in de hele EU samen te brengen met als doel markt- of systeemtekortkomingen en maatschappelijke uitdagingen aan te pakken die niet door particuliere actoren alleen kunnen worden aangepakt, met name op het gebied van baanbrekende innovatie en belangrijke infrastructuur. Bij IPCEI's kan rekening worden gehouden met veiligheids- en defensieaspecten. Dit zou het geval kunnen zijn bij het komende tweede IPCEI inzake micro-elektronica dat in de chipverordening is aangekondigd.
- *EU-financieringsprogramma's* — De EU heeft altijd een open onderzoeks- en innovatiebeleid gevoerd. Het is gebaseerd op het beginsel van open strategische autonomie

en is gericht op het waarborgen van een gelijk speelveld en wederkerigheid. De mondiale aanpak van de EU op het gebied van onderzoek en innovatie moedigt strategische partnerschappen met gelijkgestemde partners aan, in overeenstemming met de internationale verplichtingen van de EU (bv. NAVO, Verenigde Staten, Canada, Japan, Zuid-Korea enz.)¹⁴.

Tegelijkertijd moet Europa ervoor zorgen dat zijn strategische belang wordt gevrijwaard. Voor de periode 2021-2027 heeft de Commissie de regels voor deelname voor niet-EU-landen en de subsidiabiliteit van entiteiten voor alle EU-programma's en -instrumenten verduidelijkt en geharmoniseerd. Er zijn specifieke subsidiabiliteitsvoorwaarden voor veiligheidsgevoelige activiteiten vastgesteld voor bepaalde programma's (Horizon Europa, Digitaal Europa, EDF, ruimtevaartprogramma, CEF) en verder verfijnd in de desbetreffende werkprogramma's om de essentiële veiligheidsbelangen van de EU te beschermen. De lopende herziening van het Financieel Reglement van de Commissie zal ook meer duidelijkheid verschaffen over de wijze waarop de open strategische autonomie van de EU kan worden gehandhaafd, waarbij de essentiële veiligheidsbelangen van de EU volledig kunnen worden beschermd met inachtneming van haar internationale verplichtingen.

- *Normen* — In het kader van het actieplan voor synergieën bevordert de Commissie het gebruik van bestaande hybride civiele/defensienormen en de ontwikkeling van nieuwe normen tegen eind 2022 (actie 5) en de inachtneming van defensie in het normalisatiebeleid en de normalisatieacties van de Commissie. Hoewel de EU-strategie voor normalisatie¹⁵ tot doel heeft het leiderschap van de EU bij het vaststellen van civiele normen te waarborgen, zal zij zeer relevant zijn voor de defensiesector, aangezien bijna 80 % van de normen die in defensie worden gebruikt, afkomstig is uit civiele sectoren. De Commissie zal samen met de belanghebbenden (bv. het EDA) onderzoeken of het mogelijk is defensievereisten op te nemen in de toekomstige normalisatie-inspanningen die zij ondersteunt om de verenigbaarheid ervan met de defensiebehoeften te verbeteren.
- *Screening van buitenlandse directe investeringen* — De EU is een van 's werelds meest open omgevingen voor buitenlandse investeringen en een van de belangrijkste bestemmingen voor buitenlandse directe investeringen (BDI) ter wereld. Specifieke investeringen kunnen echter ook de wezenlijke veiligheidsbelangen van de EU ondermijnen. Om dergelijke risico's te voorkomen, heeft de EU een kader voor de screening van BDI opgezet dat sinds oktober 2020 operationeel is. Het eerste jaarverslag over de screening van BDI bevestigt het belang van een doeltreffende screening van BDI op het niveau van de lidstaten en van nauwe samenwerking op EU-niveau, waarbij de nadruk ligt op potentiële risico's voor de veiligheid of de openbare orde. De lidstaten worden aangemoedigd om nationale screeningmechanismen voor BDI op te zetten; 18 lidstaten hebben er al één, terwijl er nog zes in de pijplijn zitten. De Commissie zal de verordening evalueren en uiterlijk in oktober 2023 een verslag indienen bij het Europees Parlement en de Raad.

¹⁴ Er zij echter op gewezen dat de onderzoeks- en ontwikkelingsprogramma's op het gebied van defensie van de meeste van onze partners niet openstaan voor EU-bedrijven.

¹⁵ [COM\(2022\) 31 final](#).

- *Kritieke infrastructuur* — De steeds snellere opkomst van nieuwe en disruptieve technologieën heeft aanzienlijke gevolgen gehad voor de beveiliging van uitrusting, infrastructuur, diensten, waarde- en toeleveringsketens van strategische sectoren, waaronder die van veiligheid en defensie. De EU en de lidstaten moeten dergelijke kwetsbaarheden uitgebreider in aanmerking nemen in relevante risicobeoordelingen en -monitoring en in de uitvoering van veerkrachtbevorderende maatregelen tegen veiligheidsdreigingen (bv. hybride of cyberdreigingen). Coördinatie op EU-niveau is nodig om ervoor te zorgen dat de lidstaten een toekomstbestendig niveau van veerkracht en consistente beveiligingsnormen op EU-niveau handhaven om kwetsbaarheden te voorkomen.
- *Slim en circulair gebruik van materialen* — Het nieuwe actieplan voor de circulaire economie van maart 2020 is een van de belangrijkste bouwstenen van de Europese Green Deal, Europa's nieuwe agenda voor duurzame groei. Innovatie en nieuwe bedrijfsmodellen op basis van een efficiënter gebruik van hulpbronnen, de ontwikkeling van nieuwe materialen, de bevordering van secundaire grondstoffen en duurzamere overheidsopdrachten zullen niet alleen het milieu beschermen, maar ook de toegang tot materialen voor de industrie veiligstellen. Technieken voor additieve productie, groene overheidsopdrachten en recycling van materialen kunnen, mits goed toegepast, ook bijdragen tot de versterking van het concurrentievermogen van de veiligheids- en defensie-industrie van de EU en de veerkracht van de EU.
- *Gegevensbeveiliging* — De Europese datastrategie bevat maatregelen om ervoor te zorgen dat personen en bedrijven de controle over hun gegevens kunnen behouden. Dit zal aan de orde komen in de dataverordening die de Commissie naar verwachting begin 2022 zal goedkeuren.

In het kader van het meerlandenproject inzake gemeenschappelijke data-infrastructuur en -diensten (waarbij de Europese cloudfederatie en gemeenschappelijke Europese dataruimten worden samengebracht) faciliteert de Commissie investeringen (bv. DEP, CEF, NextGenerationEU) in cloud-to-edge-capaciteiten die veilig, veerkrachtig, energie-efficiënt en in real time toegankelijk zijn en die in heel Europa een goede dienstverlening bieden. Het waarborgen van technologieoverdracht op het gebied van cloud- en edge-technologieën tussen de civiele (met name veiligheids-), defensie- en ruimtevaartindustrieën zou de technologische soevereiniteit vergroten. De Europese alliantie voor industriële gegevens, edge en cloud biedt een mogelijk platform om dergelijke synergieën te bevorderen.

- *Handelsbeleid* — De complexiteit en kwetsbaarheid van mondiale toeleveringsketens is niet alleen voor de EU een probleem. Andere landen zijn afhankelijk van de EU (“omgekeerde afhankelijkheden”) en handel (“onderlinge afhankelijkheid”) kan bijdragen tot de stabiliteit van mondiale waardeketens. De EU is ook bereid assertief op te treden en zich te verdedigen tegen oneerlijke handelspraktijken, zoals het gebruik van versturende buitenlandse subsidies, en tegelijkertijd te handelen in overeenstemming met haar internationale verplichtingen. De EU zal haar instrumentarium van handels- en mededingingsinstrumenten optimaal blijven benutten en er tegelijkertijd voor zorgen dat de EU-instrumenten efficiënt en actueel zijn. De Commissie heeft daarom nieuwe instrumenten voorgesteld, zoals de verordening betreffende

buitenlandse subsidies¹⁶, die verstoringen van de interne markt als gevolg van buitenlandse subsidies aanpakt.

Andere relevante beleidsmaatregelen (zoals de invoering van een mogelijke vrijstelling van belasting over de toegevoegde waarde (btw), waardoor de overdracht van door de EU gefinancierde defensieproducten vergemakkelijkt wordt) zijn opgenomen in de mededeling over defensie.

Verdere maatregelen:

- De Commissie onderzoekt de mogelijkheid om defensiegerelateerde werkerreinen toe te voegen aan initiatieven als de Europese alliantie voor industriële gegevens, edge en cloud en de industriële alliantie op het gebied van processors en halfgeleidertechnologieën.
- Samen met de lidstaten zal de Commissie in 2023 vaststellingen doen en verslag uitbrengen over de noodzaak van een risicobeoordeling van toeleveringsketens van kritieke infrastructuur, met name op digitaal gebied, om de veiligheids- en defensiebelangen van de EU beter te beschermen.
- De Commissie moedigt alle resterende lidstaten aan een nationaal BDI-screeningmechanisme op te zetten.

5. Externe dimensie

Samenwerking met gelijkgestemde partners overal ter wereld is essentieel om de veerkracht en voorzieningszekerheid van de EU te vergroten en tegelijkertijd de strategische afhankelijkheid te verminderen en de wederzijdse voordelen te vergroten. Het wederkerigheidsbeginsel speelt in dit verband een belangrijke rol. Tot de traditionele partners van de EU op het gebied van technologie, veiligheid en defensie behoren de leden van de Europese Economische Ruimte (met name Noorwegen), kandidaat-lidstaten, nabuurschapslanden en andere derde landen (bv. de Verenigde Staten, Canada, Japan, Zuid-Korea), alsook internationale organisaties (bv. de NAVO). Recente uitwisselingen vonden met name plaats binnen onder meer:

5.1. De Handels- en Technologieraad EU-VS

De Handels- en Technologieraad EU-VS heeft op 29 september 2021 voor het eerst vergaderd. In de gezamenlijke verklaring herbevestigden de EU en de VS dat zij zich ertoe verbinden “de aandacht toe te spitsen op het bevorderen van de veerkracht van de respectieve toeleveringsketens en de voorzieningszekerheid in belangrijke sectoren voor de groene en digitale transitie en op het waarborgen van de bescherming van onze burgers” en dat het doel erin bestaat om “de transparantie van vraag en aanbod te vergroten; de respectieve bestaande sectorale vermogens in kaart te brengen; informatie uit te wisselen over beleidsmaatregelen en prioriteiten op het gebied van onderzoek en ontwikkeling; en samen te werken aan strategieën om de veerkracht en diversificatie van de toeleveringsketen te bevorderen”. De lopende werkzaamheden in werkgroepen op het gebied van veilige toeleveringsketens (met inbegrip van halfgeleiders in een gespecialiseerde werkgroep), beveiliging van informatie- en

¹⁶ [COM\(2021\) 223 final](#).

communicatietechnologie, uitvoercontroles en screening van investeringen zijn uiterst relevant voor deze routekaart. De onlangs gestarte dialoog tussen de EU en de VS over veiligheid en defensie zou ook kunnen dienen als forum voor besprekingen over deze kwesties.

5.2. *Het partnerschap met de NAVO*

Tijdens hun topontmoeting in Brussel in 2021 hebben de NAVO-leiders een ambitieuze agenda voor technologieën, met name opkomende en disruptieve technologieën (EDT's), vastgesteld¹⁷. Deze bood verdere sturing aan de werkzaamheden die worden verricht in overeenstemming met de uitvoeringsstrategie van de NAVO inzake EDT's, die in februari 2021 door de ministers van Defensie van de NAVO is goedgekeurd.

De Commissie en de hoge vertegenwoordiger zullen toezicht houden op de voortgang van de desbetreffende NAVO-initiatieven op dit gebied door middel van regelmatige contacten met de NAVO op werkniveau met het oog op een mogelijke wederzijds aanvaardbare en voordelige interactie met relevante EU-initiatieven in volledige transparantie ten aanzien van de lidstaten, waarbij wordt vermeden dat er nieuwe technologische of vermogensafhankelijkheden ontstaan of bestaande afhankelijkheden verder toenemen.

Verdere maatregelen:

- De Commissie en de hoge vertegenwoordiger zullen in het kader van de Handels- en Technologieraad EU-VS en de onlangs gestarte dialoog tussen de EU en de VS over veiligheid en defensie onderzoeken hoe de veerkracht van de toeleveringsketen kan worden vergroot en de bescherming van onze burgers kan worden gewaarborgd.
- De Commissie en de hoge vertegenwoordiger zullen samen met de NAVO, in het kader van de gezamenlijke verklaringen over de samenwerking tussen de EU en de NAVO en in volledige transparantie met de lidstaten, onderzoeken hoe een wederzijds aanvaardbare en voordelige interactie tussen hun respectieve relevante initiatieven kan worden bevorderd.

6. Conclusies

Aangezien de mondiale geopolitieke situatie complex blijft en de wedloop naar nieuwe technologieën die relevant zijn voor veiligheid en defensie voortduurt, moeten de EU en haar lidstaten de samenwerking versterken op het gebied van technologieën die van cruciaal belang zijn voor de veiligheid en defensie van Europa op de lange termijn en de inspanningen om de daarmee verband houdende strategische afhankelijkheden te verminderen.

In deze routekaart wordt voorgesteld nauw samen te werken met de lidstaten bij het identificeren van kritieke technologieën en waardeketens voor veiligheid en defensie – alsook van de onderliggende oorzaken van de bijbehorende strategische afhankelijkheden in het kader van het waarnemingscentrum voor kritieke technologieën – ter ondersteuning van een EU-brede strategische gecoördineerde aanpak van kritieke technologieën die relevant zijn voor veiligheid

¹⁷ Het ging onder meer om het besluit om de Defence Innovation Accelerator for the North Atlantic (DIANA) en een innovatiefonds van de NAVO te lanceren.

en defensie, waarbij optimaal gebruik wordt gemaakt van EU- en nationale OTO&I-programma's en -instrumenten.

Om het concurrentievermogen en de veerkracht van de veiligheids- en defensiesectoren te vergroten, zullen de bevindingen van het waarnemingscentrum en de daarmee verband houdende werkzaamheden in het kader van de geactualiseerde industriestrategie er, waar passend en in overeenstemming met de mededingingsregels van de EU en de internationale verplichtingen van de EU, ook toe bijdragen dat veiligheids- en defensieoverwegingen beter in aanmerking worden genomen in het industrie- en handelsbeleid van de EU.

Met de voorstellen van deze routekaart wordt beoogd bij te dragen aan de OTO&I-dimensie van het komende strategisch kompas van de EU, waarmee de lidstaten ambitieuze langetermijndoelstellingen zullen vaststellen om de veiligheid en defensie van Europa aanzienlijk te versterken.