



Strasbourg, den 15.2.2022
COM(2022) 61 final

**MEDDELELSE FRA KOMMISSIONEN TIL EUROPA-PARLAMENTET, RÅDET,
DET EUROPÆISKE ØKONOMISKE OG SOCIALE UDVALG OG
REGIONSUDVALGET**

Køreplan for kritiske teknologier inden for sikkerhed og forsvar

1. Indledning

Europas velstand, sikkerhed og levevis kan kun sikres ved, at vi forbliver på forkant med den teknologiske udvikling. Nye teknologier skaber forandring i sikkerheds- og forsvarssektorerne hurtigere end nogensinde før og udviser skillelinjen mellem det civile og det militære område. Digitale teknologier påvirker i særlig grad den etablerede magtbalance i det globale sikkerhedslandskab. Det er derfor afgørende at sikre, at Unionens sikkerheds- og forsvarssektorer forbliver teknologisk egnede til formålet.

Mange kritiske teknologier inden for sikkerhed og forsvar stammer stadig oftere fra det civile område og anvender kritiske komponenter med dobbelt anvendelse. For at øge tempoet i innovationen på tværs af områder og fremme teknologisk suverænitet inden for sikkerheds- og forsvarssektorerne er der behov for en bedre udveksling mellem civile og forsvarsrelaterede forsknings- og innovationskredse. Unionen har i lyset af sin mangeårige ekspertise inden for den civile sektors teknologiske udvikling og sine nye forsvarssamarbejdsinstrumenter¹ gode forudsætninger for at påtage sig en ledende rolle. Dette forudsætter dog, at ressourcerne udnyttes mere effektivt, og at der er vilje til at udforske mulighederne for dobbelt anvendelse, samtidig med at Unionens grundlæggende værdier opretholdes. Det indebærer også, at strategiske afhængighedsforhold og sårbarheder i værdi- og forsyningskæderne for disse teknologier skal mindskes.

Opsplitningen af Europas sikkerheds- og forsvarskapacitet har ført til økonomisk ineffektivitet, mindsket den operationelle kapacitet og øget den strategiske afhængighed. Den igangværende revolution inden for sikkerheds- og forsvarsteknologier og Unionens nye forsvarssamarbejdsinstrumenter giver Unionen mulighed for at undgå at gentage fortidens fejltagelser, udbygge sin eksisterende kapacitet og opretholde sin økonomiske velstand og sikkerhed. **Det fremtidige europæiske teknologi- og innovationslandskab inden for sikkerheds- og forsvarssektoren bør fra første færd udvikles inden for rammerne af EU-samarbejdet.**

Kommissionsformand Ursula von der Leyen anerkendte i sin tale om Unionens tilstand i 2021², at arbejdet med at udvikle et europæisk forsvarøkosystem er påbegyndt, men at der er behov for en europæisk forsvarsunion. Inden for rammerne af EU's strategiske kompas ("det strategiske kompas"), der skal vedtages af medlemsstaterne i marts 2022, vil der blive fastlagt en fælles strategisk vision for det kommende årti, og det vil blive skitseret, hvordan Unionen vil styrke sin handlekraft og evne til at reagere på forskellige kriser og udfordringer, sikre sine interesser og beskytte sine borgere samt investere og innovere med henblik på i fællesskab at udvikle den nødvendige kapacitet og teknologi og udbygge partnerskaber baseret på Unionens værdier og interesser.

¹ Den Europæiske Forsvarsfond, den samordnede årlige gennemgang vedrørende forsvar (CARD) og det permanente strukturerede samarbejde vedrørende forsvar (PESCO).

² [Kommissionsformand Ursula von der Leyens tale om Unionens tilstand 2021.](#)

Med denne køreplan for kritiske teknologier inden for sikkerhed og forsvar følges der op på en anmodning fra Det Europæiske Råd af 25.-26. februar 2021³ om at forelægge en køreplan for at fremme forskning, teknologisk udvikling og innovation (FTU&I) og mindske Unionens strategiske afhængighed, når det gælder kritiske teknologier og værdikæder inden for sikkerhed og forsvar. Køreplanen vil blive forelagt på det uformelle topmøde i Paris den 10.-11. marts 2022, og den vil indgå i det strategiske kompas. I køreplanen beskrives Unionens og medlemsstaternes kommende tiltag med henblik på i fællesskab at nå ovennævnte mål, navnlig ved at:

- udpege teknologier af kritisk betydning for Unionens sikkerhed og forsvar og fremme disse gennem Unionens FTU&I-programmer
- sikre, at forsvarshensyn tages mere i betragtning dels i Unionens civile FTU&I-programmer og dels i industri- og handelspolitikker, alt efter hvad der er relevant, samtidig med at der i FTU&I-programmerne på forsvarsområdet også tages bedre højde for teknologiers civile anvendelsesmuligheder
- fra første færd fremme en EU-dækkende strategisk og koordineret tilgang til kritiske teknologier inden for sikkerhed og forsvar for at gøre bedst mulig brug af Unionens og medlemsstaternes FTU&I-programmer, opnå synergier mellem civile og forsvarsrelaterede kredse inden for forskning, teknologisk udvikling og innovation og afbøde den strategiske afhængighed af eksterne kilder og
- så vidt muligt koordinere med andre ligesindede partnere såsom USA og Den Nordatlantiske Traktats Organisation (NATO) på gensidigt fordelagtige vilkår.

2. Kritiske teknologier og strategisk afhængighed på sikkerheds- og forsvarsområdet

I ajourføringen af "Den nye industristrategi fra 2020: Opbygning af et stærkere indre marked til fremme af Europas genopretning" ("den ajourførte industristrategi")⁴ af maj 2021 bekræftes det, at teknologisk lederskab fortsat er en væsentlig drivkraft for Unionens konkurrenceevne og innovation — navnlig inden for såkaldt "kritiske teknologier"⁵. Endvidere understreges betydningen af at afdække og afbøde strategisk afhængighed inden for "følsomme økosystemer", bl.a. "nær- og social økonomi og civilsikkerhed" og "luft- og rumfart og forsvar", for at sikre Unionens modstandsdygtighed.

I Kommissionens handlingsplan om synergier mellem den civile industri og forsvars- og rumindustrien ("handlingsplanen for synergier")⁶ af februar 2021 anerkendes den voksende betydning, som disruptive teknologier og støtteteknologier fra det civile område har for Europas fremtidige sikkerhed og forsvar, og behovet for at fremme gensidig inspiration og synergier mellem civile og forsvarsrelaterede teknologier. Den indeholder en række nøgleaktioner med det

³ [Erklæring fra medlemmerne af Det Europæiske Råd af 26. februar 2021.](#)

⁴ [COM\(2021\) 350 final.](#)

⁵ Kommissionen er som led i sit arbejde med Observatoriet for Kritiske Teknologier i færd med at definere, hvad der forstås ved "kritisk" i rumfartssektoren, forsvarssektoren og tilknyttede civile sektorer (herunder sikkerhed).

⁶ [COM\(2021\) 70 final.](#)

formål at tilskynde til at udveksle oplysninger og samarbejde mellem civile og forsvarsrelaterede kredse med udgangspunkt i Unionens FTU&I-programmer og -instrumenter.

2.1. De særlige træk ved sikkerheds- og forsvarssektorerne

Strukturen af Unionens forsvarsindustri spænder bredt, idet den består af store multinationale selskaber og små og mellemstore aktører. Efterspørgslen kommer næsten udelukkende fra de nationale regeringer, som også holder kontrol med alle indkøb af forsvarsrelaterede produkter og teknologier samt eksporten heraf. Uensartetheden, hvad angår nationale krav og nationale offentlige udgifter og investeringer, fragmenterer fortsat Unionens forsvarsmarked og risikerer i visse tilfælde at hæmme interoperabiliteten mellem medlemsstaternes nationale væbnede styrker. Forsvarssektoren følger derfor ikke de konventionelle regler og forretningsmodeller, der gælder for mere traditionelle markeder, og den har derfor begrænset råderum til at påvirke tilknyttede investeringer og markedsvalg. Dette gør det vanskeligt for industrien at gennemføre betydelige selvfinansierede FTU&I-projekter på forsvarsområdet.

Unionens sikkerhedsindustri står over for de samme udfordringer, da markederne ligeledes overvejende er nationale, men endnu mere fragmenterede. Dens kundegruppe spænder bredt (f.eks. politistyrker, interne sikkerhedsagenturer, toldkontorer, grænsemyndigheder og private sikkerhedstjenester), aktiviteterne finder sted på forskellige niveauer (lokalt, regionalt og nationalt), og organisationen varierer fra medlemsstat til medlemsstat. **Kommissionen vil forelægge en undersøgelse af Unionens sikkerhedsmarked i 2022 for at opnå yderligere indsigt i denne komplekse sektor.** Desuden vil Kommissionen i første halvår af 2022 sammenfatte forslag med henblik på at fremme vedtagelsen af de kapacitetsdrevne tilgange, der skal anvendes på tværs af sikkerhedssektorer. Disse forslag vil styrke den tidlige og fremadskuende udpegning af behov og løsninger inden for sikkerhed og retshåndhævelse.

Rummet og cyberspace er strategiske "katalysatorer" for sikkerheds- og forsvarssektorerne. Rumsektoren deler mange af disse sektors særlige træk, bl.a. lav markedsvolumen og begrænset indflydelse på det private marked for komponenter. Modstandsdygtigheden i rumsektorens programmer og værdikæder har kritisk betydning for Unionens sikkerheds- og forsvarsmål. Cyberspace spiller også en stadig vigtigere rolle på tværs af forsvarskapaciteter, og dette område kræver opmærksomhed og investeringer. Med den hastige stigning i antallet af cyberangreb, der er rettet mod både civile og forsvarsrelaterede aktiver og net, og den civile sektors styrkede rolle med hensyn til innovation og standardisering på cyberområdet er der behov for at knytte cybersikkerhed og cyberforsvar tættere sammen. I Kommissionens bidrag til det europæiske forsvar i forbindelse med det strategiske kompas ("meddelelsen om forsvar"), der indgår i denne forsvarspakke, skitseres yderligere foranstaltninger for disse to sektorer.

2.2. Kortlægning af kritiske teknologier og strategisk afhængighed på sikkerheds- og forsvarsområdet

Den ajourførte industristrategi rummer en bredt funderet kortlægning og analyse af Unionens strategiske afhængighed og kapacitet baseret på en første runde af dybdegående undersøgelser af

følsomme økosystemer⁷. Dette arbejde har dannet grundlag for politiske tiltag til støtte for øget modstandsdygtighed i Unionen, men det anerkendes også, at der er behov for en større indsats for yderligere at øge vores forståelse af Unionens strategiske afhængighed, og hvordan den kan udvikle sig og risikere at føre til yderligere sårbarheder. Dette arbejde omfatter en anden runde af dybdegående undersøgelser af følsomme økosystemer og et overvågningssystem inden for rammerne af Observatoriet for Kritiske Teknologier ("observationscentret"), se afsnit 2.3.

Kommissionen har påbegyndt arbejdet på dybdegående undersøgelser af forsvars- og sikkerhedsteknologiske områder, herunder cybersikkerhedsområdet, for at støtte den ajourførte industristrategi og udviklingen af observationscentret. Der er indtil videre gennemført to indledende casestudier inden for de forsvarsteknologiske områder autonome systemer og halvledere, der betragtes som repræsentative stikprøver i kraft af deres tværgående relevans for militære kapaciteter på forskellige områder, jf. tekstboks 1. Formålet var at udpege fælles mønstre på tværs af disse forsvarsteknologiske områder, navnlig hvad angår årsagerne til afhængighed og de dermed forbundne risici samt de indledende muligheder for at afbøde dem.

Ifølge casestudierne præges forsvarssektoren af stort set de samme strategiske afhængighedsforhold og sårbarheder som andre følsomme økosystemer, navnlig hvad angår teknologikløfter, (kritiske) råstoffer, færdigheder og lave FTU&I-investeringer samt eksterritoriale bestemmelser i lande uden for Unionen. Der peges også på, at den strategiske og følsomme karakter (f.eks. højere standarder for informationssikkerhed og forsyningssikkerhed) af sektorens aktiviteter og dens forholdsvis marginale markedsstørrelse generelt gør sårbarheden mere udtalt.

Det fremgår endvidere af casestudierne, at nogle af Unionens globale konkurrenter iværksætter mere offensive og defensive foranstaltninger for at fremme kritiske teknologier og håndtere strategisk afhængighed, end det hidtil har været tilfældet i Unionen. De knytter f.eks. på en mere systematisk måde nationale forsvarshensyn til den civile sektors teknologiske udvikling, de investerer kraftigt i deres indenlandske forskning, teknologiske udvikling, innovation og industrielle kapacitet, de tiltrækker eksterne investorer og anvender til tider aggressive overtagelsesstrategier i tredjelande. De beskytter desuden deres egen industrielle ekspertise og indflydelse ved at udnytte den indbyrdes afhængigheds afsmittende virkninger eller ved at anvende strenge eksterritoriale bestemmelser for at begrænse tredjelandes adgang til teknologier.

Unionen råder selv over værktøjer til at styrke sin industrielle kapacitet i overensstemmelse med EU-reglerne, men en hæmsko består i den stadig relativt fragmenterede efterspørgsel på Unionens forsvarsmarked, det historisk betingede strenge skel mellem civil henholdsvis forsvarsrelateret FTU&I på EU-niveau og medlemsstaternes komparative underinvestering i den europæiske forsvarsteknologiske og -industrielle base (EDTIB). Medlemsstaternes kollektive udgifter til forsvarsinnovation (2,5 mia. EUR eller 1,2 % af forsvarsudgifterne) halter fortsat bagefter det mål på 2 %, som Det Europæiske Forsvarsagentur fastsatte for 15 år siden.

⁷ [SWD\(2021\) 352 final](#).

Markedskræfterne har ført til en situation, hvor intet land i sig selv kan opnå fuld teknologisk suverænitet inden for et givet teknologiområde, men hvor der foregår et globalt kapløb om teknologisk lederskab og de dermed forbundne økonomiske og militære fordele. Dette kan forværre Unionens eksisterende strategiske afhængighed og skabe afhængighedsforhold på nye områder, medmindre den griber ind. En struktureret tilgang er nødvendig, for at Unionen kan holde sig på forkant med kritiske teknologier og tillige afdække og afbøde strategisk afhængighed på sikkerheds- og forsvarsområdet. Denne køreplan har til formål at tilvejebringe en sådan tilgang, der vil skulle integreres i EU's strategiske kompas.

Tekstboks 1: Casestudier — autonome systemer og halvledere til forsvarsområdet

I Kommissionens analysearbejde angående autonome forsvarssystemer med særlig vægt på kunstig intelligens (AI) og maskinlæring blev der udpeget relevante kritiske teknologier og fire hovedområder, hvor Unionen har et efterslæb: færdigheder, data, hardware og test. De mulige foranstaltninger, hvormed disse områder kan styrkes, vil bygge på Unionens eksisterende strategi for kunstig intelligens⁸ og dertil knyttede politiske initiativer samt medlemsstaternes nationale strategier for kunstig intelligens. De omfatter FTU&I-aktiviteter (f.eks. øget tilgængelighed af data og AI-træning samt link til det europæiske processorinitiativ), infrastruktur (f.eks. cloud computing-kapacitet til forsvarsformål og indenlandske testfaciliteter) og beskyttelse af eksisterende kritiske aktiver (f.eks. screening af udenlandske direkte investeringer).

Det fremgik af analysearbejdet vedrørende halvledere til forsvarsområdet, at halvledere benyttes overalt i forsvarsmateriel, og at det eksisterende og fremtidige afhængighedsforhold for de mest avancerede halvlederes vedkommende navnlig skyldes manglen på EU-intern kapacitet (produktionsanlæg). Kommissionen har indføjjet afbødende foranstaltninger i forslaget til en lovpakke om europæiske mikrochips, som blev vedtaget den 8. februar 2022⁹, og som har til formål at skabe et avanceret europæisk økosystem for mikrochips for at forbedre Unionens kapacitet på dette område og dermed også imødekomme forsvarssektorens behov.

2.3. Observatoriet for Kritiske Teknologier

Manglende fremsyn med hensyn til teknologiernes fremtidige betydning ligger til grund for en del af Unionens eksisterende strategiske afhængighed af tredjelande (f.eks. fjernstyrede systemer og halvledere). Unionen har behov for et mere struktureret fremsyn og strategiske overvejelser angående kritiske teknologier inden for sikkerhed og forsvar med henblik på at udpege prioriterede områder for derigennem at fremme forskning og innovation, nedbringe den eksisterende strategiske afhængighed og undgå, at afhængighedsforhold opstår på andre områder.

Observatoriet for Kritiske Teknologier, som Kommissionen for indeværende er ved at oprette i overensstemmelse med handlingsplanen for synergier (foranstaltning nr. 4), vil bidrage til disse

⁸ [COM\(2018\) 237 final.](#)

⁹ [COM\(2022\) 45 final.](#)

overvejelser. Der vil i arbejdsmetoderne blive taget hensyn til andre lignende initiativer¹⁰ for at undgå dobbeltarbejde. Dette vil gøre det muligt at finjustere listen over kritiske teknologier i handlingsplanen for synergier for at afspejle udviklingen i teknologilandskabet og kapacitetsbehovene.

Observationscentret vil udpege, overvåge og vurdere kritiske teknologier for rumsektoren, forsvarssektoren og relaterede civile sektorer samt deres potentielle anvendelse og relaterede værdi- og forsyningskæder. Det vil også udpege, overvåge og analysere eksisterende og forventelige teknologikløfter samt grundlæggende årsager til strategiske afhængighedsforhold og sårbarheder.

Det vil være afgørende at nå til enighed med medlemsstaterne om en meningsfuld detaljeringsgrad for at drøfte disse spørgsmål på EU-niveau og om behovet for at dele relevante data mellem medlemsstaterne og med Kommissionen. En mekanisme i form af en særlig ekspertgruppe til udveksling og drøftelse i et fortroligt miljø med medlemsstaterne vil blive oprettet i observationscentret. Her drøftes bl.a. fremkomsten af nye og disruptive teknologier for at undgå nye afhængighedsforhold for sikkerheds-, forsvars- og rumindustrien. Den højtstående repræsentant og de tilknyttede tjenestegrene vil blive inddraget i denne proces.

Kommissionen vil inden udgangen af 2022 og derefter hvert andet år på grundlag af data fra observationscentret forelægge medlemsstaterne en klassificeret rapport om kritiske teknologier og risici i forbindelse med strategiske afhængighedsforhold, der påvirker sikkerheden, rummet og forsvaret. Kommissionen vil på grundlag af disse rapporter udarbejde teknologikøreplaner, som vil omfatte afbødende foranstaltninger med henblik på dels at fremme FTU&I og dels mindske den strategiske afhængighed, der påvirker sikkerheden og forsvaret.

Når observationscentrets aktiviteter er veletablerede, kan dets opgaver udvides til at omfatte andre sektorer som anført i den ajourførte industristrategi.

Kommende tiltag:

- I 2022 vil Kommissionen nedsætte en ekspertgruppe for at lette udvekslingen med medlemsstaterne angående kritiske teknologier og kritiske værdi- og forsyningskæder. Den vil indgå i Observatoriet for Kritiske Teknologier på områderne forsvar, rumfart og tilknyttede civile sektorer. Formålet vil være at:
 - gennemføre regelmæssige samråd med medlemsstaternes myndigheder med henblik på at udarbejde den klassificerede rapport
 - sikre en hensigtsmæssig håndtering af følsomme og klassificerede oplysninger, der kan udveksles inden for rammerne af Observatoriet for Kritiske Teknologier, og af tilhørende rapporter og køreplaner.
- Medio 2022 vil Kommissionen forelægge en undersøgelse af Unionens sikkerhedsmarked; undersøgelsen vil bidrage til at lette forståelsen af de særlige vilkår på markedet for civil sikkerhed, støtte udpegningen af kritiske teknologier og strategisk afhængighed og

¹⁰ Det kan dreje sig om støtte og værktøjer inden for avancerede teknologier til industrien (ATI), overvågning af kritiske teknologier for rumsektoren, den overordnede strategiske forskningsdagsorden (OSRA), teknologibygeblokke (TBB) og Det Europæiske Forsvarsagenturs vigtige strategiske aktiviteter.

underbygge den nye kapacitetsdrevne tilgang til sikkerhedsaktiviteter og andre FTU&I-aktiviteter.

- Desuden vil Kommissionen senest medio 2022 udarbejde en sammenfatning af forslag med henblik på at fremme vedtagelsen af de kapacitetsdrevne tilgange, der skal anvendes på tværs af sikkerhedssektorer.

3. Fremme af forskning, teknologisk udvikling og innovation for kritiske teknologier inden for sikkerhed og forsvar

De teknologikøreplaner, som Kommissionen vil udarbejde på grundlag af observationscentrets vurderinger, vil underbygge en vifte af aktiviteter fra FTU&I-programmering inden for kritiske teknologier til udvikling af større flagskibsinitiativer, der vil bidrage til at styrke Unionens konkurrenceevne og modstandsdygtighed i sikkerheds- og forsvarssektorerne. For at opfylde disse mål må anvendelsen af de disponible finansielle ressourcer effektiviseres gennem en bedre koordinering af Unionens og de nationale eksisterende FTU&I-programmer og -instrumenter.

3.1. Overvindelse af skellet mellem Unionens civile og forsvarsrelaterede FTU&I

Kommissionen forpligtede sig i henhold til sin handlingsplan for synergier (foranstaltning nr. 2) til senest i 2022 at styrke den interne koordinering mellem EU-programmer og -instrumenter, jf. tekstboks 2, for at frigøre de enorme fordele for økonomisk vækst, det indre marked og de europæiske borgeres sikkerhed, der opstår i kraft af synergier mellem civil og forsvarsrelateret FTU&I.

Gennemførelsen af dette mål kan videreføres i 2023 (f.eks. gennem bedre planlægning og synkronisering samt vejledning af medlemsstaternes forvaltningsmyndigheder), men visse hindringer vil være vanskeligere at imødegå på kort og mellemlang sigt og kan forudsætte andre berørte parters medvirken. Dette er navnlig tilfældet, hvis der i de retlige bestemmelser i EU-programmers og -instrumenters basisretsakter fastsættes praktiske begrænsninger. Aktiviteter med dobbelt anvendelse kan eksempelvis finansieres inden for rammerne af Connecting Europe-faciliteten (CEF) og de europæiske struktur- og investeringsfonde (ESI-fondene), hvorimod der i aktiviteter, som gennemføres inden for rammerne af Horisont Europa¹¹, fokuseres på civile anvendelsesformål; der findes ingen ramme for direkte støtte til sådanne aktiviteter i FTU&I-programmer og -instrumenter. Tilsvarende rummer Den Europæiske Investeringsbanks udlånspolitik stadig restriktioner for forsvarssektoren.

For at lette udvekslingen mellem den civile sektor og forsvarssektoren, navnlig hvad angår kritiske teknologier, vil Kommissionen i 2023 forberede en tilgang på EU-plan, som skal gennemføres fuldt ud på mellemlang til lang sigt på tværs af EU-programmer og -instrumenter, med henblik på at fremme FTU&I med dobbelt anvendelse. Denne indsats vil også indgå i

¹¹ Ved udtrykket "Horisont Europa" forstås i dette dokument særprogrammet til gennemførelse af Horisont Europa og Det Europæiske Institut for Innovation og Teknologi, og aktiviteterne herunder fokuserer udelukkende på civile anvendelsesformål.

midtvejsevalueringen af relevante sektorprogrammer, f.eks. fondene, som er omfattet af forordningen om fælles bestemmelser, herunder midler til beredskab på sundhedsområdet.

Tekstboks 2: EU-programmer og -instrumenter til støtte for FTU&I for kritiske teknologier af relevans for sikkerhed og forsvar og etableringen af deres infrastruktur inden for rammerne af det flerårige finansielle program (2021-2027)

- I Den Europæiske Forsvarsfond afsættes 8 mia. EUR til forsvarsrelateret forskning og udvikling. 4-8 % af Den Europæiske Forsvarsfonds forsknings- og udviklingsbudget vil blive øremærket til disruptive teknologier, dvs. op til 100 mio. EUR om året.
- I Horisont Europa, under søjle II "Globale udfordringer og europæisk industriel konkurrenceevne", afsættes 1,6 mia. EUR til forskning og innovation på området civilsikkerhed under klyngen "Civilsikkerhed for samfundet", samtidig med at kritiske teknologier støttes under klyngerne "Det digitale område, industri og rummet", "Klima, energi og mobilitet" og "Fødevarer, bioøkonomi, naturressourcer, landbrug og miljø". Supplerende aktiviteter finansieres under søjle I "Videnskabelig topkvalitet" af Det Europæiske Innovationsråd (EIC) og Det Europæiske Institut for Innovation og Teknologi (EIT) under søjle III "Et innovativt Europa" samt europæiske partnerskaber, der samler og mobiliserer ressourcer for at sikre Unionens teknologiske lederskab og åbne strategiske autonomi på kritiske områder.
- Programmet for et digitalt Europa vil fremme udbredelsesaktiviteter, der er relevante for kritiske teknologier inden for de prioriterede områder cybersikkerhed, kunstig intelligens og supercomputere.
- Industri-, Teknologi- og Forskningskompetencecentret for Cybersikkerhed og Netværket af Koordinationscentre vedtager i 2022 en strategisk dagsorden for investeringer på cyberområdet, der bidrager til Horisont Europa og Programmet for et digitalt Europa. Synergier mellem civile og forsvarsrelaterede teknologier og teknologier med dobbelt anvendelse kan udforskes via forbindelser til Den Europæiske Forsvarsfond i overensstemmelse med de gældende regler.
- ESI-fondene (navnlig hvad angår Den Europæiske Fond for Regionaludvikling og Den Europæiske Socialfond Plus) kan anvendes til støtte for EDTIB.
- Blandt andre relevante EU-programmer, -fonde og -instrumenter tælles rumprogrammet, Connecting Europe-faciliteten, InvestEU-programmet, genopretnings- og resiliensfaciliteten, Life-programmet, offentlig-private partnerskaber og blandingsfaciliteter.

3.2. *Sammenkædning af EU-programmer og -instrumenter med nationale programmer og instrumenter til støtte for FTU&I målrettet kritiske teknologier inden for sikkerhed og forsvar*

EU-programmer og -instrumenter yder en betydelig finansiering til FTU&I-aktiviteter inden for sikkerhed og forsvar i Unionen, men medlemsstaterne finansierer fortsat størstedelen af sådanne aktiviteter, og opsplitningen af sikkerheds- og forsvarsmarkedene udgør fortsat et alvorligt problem. Derfor er en EU-dækkende koordinering påkrævet for at opnå teknologisk suverænitet på visse kritiske teknologiområder og mindske den strategiske afhængighed inden for andre.

Medlemsstaterne opfordres til i det strategiske kompas at påtage sig fra første færd sammen med Kommissionen at udvikle en EU-dækkende strategisk koordineret tilgang til

kritiske teknologier, der er relevante for sikkerhed og forsvar, under fuld hensyntagen til den alsidighed og kompleksitet, der er forbundet med at forvalte Unionens og de nationale programmer og instrumenter. I denne tilgang vil der også blive taget hensyn til andre koordineringsstrukturer såsom det nye EU-Innovationscenter for Indre Sikkerhed, der ledes af Den Stående Komité for det Operationelle Samarbejde om den Indre Sikkerhed (COSI), og det nye EU-Innovationscenter for Forsvar, som Det Europæiske Forsvarsagentur skal oprette.

De klassificerede rapporter om kritiske teknologier og de teknologikøreplaner, som Kommissionen har forberedt, danner et udgangspunkt for drøftelser mellem medlemsstaternes myndigheder og Kommissionen. Målet vil være ud fra teknologikøreplanerne at udpege de områder, hvor indsatsen haster mest, og mobilisere Unionens og medlemsstaternes programmer, instrumenter og politikker for at håndtere dem på en koordineret måde i overensstemmelse med EU-statsstøttereglerne. Derved sikres det, at investeringerne målrettes de områder, der har størst betydning for EU-borgernes sikkerhed. Prioriteterne ajourføres regelmæssigt for at sikre, at de fortsat er relevante, og at der skabes værdi for pengene.

Kommissionen vil samarbejde med medlemsstaterne om at finde frem til den bedste mekanisme til at lette dette koordineringsarbejde (f.eks. observationscentrets ekspertgruppe).

3.3. Støtte til innovation og iværksætteri på sikkerheds- og forsvarsområdet — oprettelse af en EU-ordning for forsvarsinnovation

Unionen må udnytte sit innovationssamfunds fulde potentiale bedre til støtte for sikkerhed og forsvar. Dette kræver, at ikke-traditionelle aktører og eksisterende innovative nystartede virksomheder og små og mellemstore virksomheder (SMV'er) inden for de to sektorer bistås med at overvinde deres betydelige teknologiske, administrative og reguleringsmæssige hindringer og hindringer for markedsadgang samt med at overholde de høje sikkerhedsstandarder og opnå adgang til finansiering. Forsvarsmarkedet er ofte bygget op omkring enkelte store aktører, der støttes af en række specialiserede SMV'er, som har begrænset direkte adgang til dette marked. Som følge heraf kan det være vanskeligt for innovative SMV'er på forsvarsområdet at opnå adgang til finansiering, hvilket kan gøre dem mere tilbøjelige til at henvende sig til eller blive opsøgt af udenlandske investorer. Der er tale om en lignende situation for innovative SMV'er på sikkerhedsområdet, som står over for tilsvarende udfordringer med hensyn til at opsøge potentielle kunder eller opnå adgang til målrettet finansiering¹².

Kommissionen støtter innovative nystartede virksomheder og SMV'er, som beskæftiger sig med sikkerhed, inden for rammerne af Horisont 2020, hvor den tildelte finansiering og de samlede succesrater inden for rammerne af den samfundsmæssige udfordring 7 "Civilsikkerhed for samfundet" har ligget over gennemsnittet for små innovatorer. Horisont Europa vil fortsat yde denne støtte, men nystartede virksomheder og SMV'er på sikkerhedsområdet vil stadig have behov for yderligere målrettet støtte for at lette deres adgang til markedet. Ved at udforske nye instrumenter med henblik på at støtte innovation med dobbelt anvendelse kan deres produktionskapacitet, konkurrenceevne og bæredygtighed styrkes.

¹² [Trusler og muligheder for SMV'er og nystartede virksomheder inden for EU's forskning og innovation på sikkerhedsområdet](#), CERIS SSRI virtuelt arrangement, 30. april 2021.

Kommissionen har iværksat lignende aktiviteter inden for rammerne af Den Europæiske Forsvarsfond for at udvikle en værktøjskasse for forsvarssektoren og innovation med dobbelt anvendelse, der dækker de teknologiske modenhedsniveauer (TRL)¹³ 1-9. Der arbejdes i øjeblikket på følgende værktøjer, der dækker forsvarssektoren, nye teknologier og dobbelt anvendelse:

- a) *Forsvarsinnovation gennem Den Europæiske Forsvarsfond* — nærmere bestemte aktioner undersøges i øjeblikket for bedre at støtte projekter, som er målrettet disruptive teknologier og innovative og fremtidsorienterede forsvarsløsninger, der navnlig tilskynder innovative SMV'er, innovative laboratorier og forsknings- og teknologioorganisationer til at deltage. Disse aktioner kan antage forskellige former, f.eks. virksomhedscoaching (arbejdsprogrammet for 2021), teknologiske udfordringer (arbejdsprogrammet for 2022) og hackathons eller præmier (arbejdsprogrammet for 2023 eller derefter). De vil også trække på relevante erfaringer fra EIC og kan knyttes til det nye CASSINI-initiativ målrettet forsvarsområdet.
- b) *En blandingsfacilitet for forsvarsinvesteringer under InvestEU* — oprettelsen af en sådan facilitet vil gøre det muligt for Kommissionen at garantere investeringer, som foretages af finansielle formidlere i hele Unionen, i SMV'er, der beskæftiger sig med innovation eller strategisk forsvar. Dette vil lette problemerne i forbindelse med den begrænsede adgang til finansiering for SMV'er, der udvikler lovende teknologier til det europæiske forsvar, samtidig med at der stilles pålidelig kapital til rådighed, og fjendtlige overtagelser fra tredjelands enheder undgås. Hvis innovative SMV'er på forsvarsområdet og midcapselskaber får bedre adgang til egenkapitalfinansiering, vil det støtte deres vækst og i sidste instans gavne EDTIB's innovationsevne. Kommissionen vil også undersøge, om der er behov for yderligere instrumenter til støtte for centrale markedsaktører i værdikæden.
- c) *CASSINI-initiativ målrettet forsvarsområdet* — dette initiativ søger inspiration fra det eksisterende CASSINI-initiativ til støtte for SMV'er og nystartede virksomheder i rumindustrien. De vil blive tilbudt tjenester såsom virksomhedsudvikling og -netværk (f.eks. matchmaking og business accelerator) samt præmier og konkurrencer (herunder hackathons og mentorordninger mv.), der supplerer ovennævnte blandingsfacilitet for forsvarsinvesteringer.
- d) *Innovationsvæksthus* — Kommissionen vil i 2022 oprette et innovationsvæksthus, der skal støtte udviklingen af nye teknologier og forme innovation med dobbelt anvendelse i tråd med handlingsplanen for synergier (foranstaltning nr. 6), som kan spille en vigtig rolle med hensyn til at bygge bro over kløften mellem civile og forsvarsrelaterede FTU&I-programmer. Efter en systematisk analyse af resultaterne af den teknologiske udviklings tidlige fase vil væksthuset fremhæve projekter og/eller teknologier, der potentielt kan anvendes i

¹³ Siden 2014 har Unionen i vid udstrækning anvendt en TRL-skala (Technology Readiness Level) i forbindelse med sine FTU&I-programmer og -instrumenter. På skalaen skelnes der mellem ni niveauer af teknologisk modenhed, der spænder fra grundforskning på TRL 1 til et slutprodukt, der er klar til at komme ind på markedet på TRL 9. Da en teknologisk anvendelsespotentiale og dermed potentiale for dobbelt anvendelse typisk afdækkes ved TRL 5-6, kan det antages, at en teknologi er "neutral" ved TRL 1-4.

sikkerheds-, rum- eller forsvarssektoren, over for relevante tjenester i Kommissionen og medlemsstaterne med henblik på potentiel udbredelse. Kommissionen vil vurdere, hvordan adgangen til yderligere finansieringsmuligheder, f.eks. EIC's overgangsfinansieringsordning eller Den Europæiske Forsvarsfond, kan lettes for disse fremhævede projekter, hvis det er relevant.

- e) *Støtte til innovationsnetværk* — tværnationale forsvarsinnovationsnetværk kan spille rollen som innovationsformidlere og tilskynde til, at der indarbejdes innovative løsninger i samarbejdsprojekter. Med teknologiscouting afdækkes og udpeges nye innovative løsninger og teknologier med potentielt fordelagtige anvendelsesmuligheder i forsvarssektoren. Forskningscentre og tekniske testfaciliteter vil derefter teste relevansen af sådanne teknologier fra det civile område og udveksle bedste praksis. Det Europæiske Forsvarsagentur bliver en central partner for Kommissionen i forbindelse med gennemførelsen af en anden del af foranstaltning nr. 6 inden for rammerne af handlingsplanen for synergier.

Kommissionen vil påpege, hvordan værktøjskassen kan knyttes til instrumenter til støtte for innovation inden for sikkerhed (f.eks. Horisont Europa) eller cybersikkerhed (f.eks. netværket af nationale koordinationscentre for cybersikkerhed i samarbejde med de europæiske digitale innovationsknudepunkter).

Kommissionens og Den Europæiske Forsvarsfonds komplementære stærke sider bør samles under en "**EU-ordning for forsvarsinnovation**". I denne ordning vil Kommissionen på grundlag af sine erfaringer med gennemførelsen af EU-budgettet med henblik på at støtte FTU&I til forsvarsformål, civile formål og dobbelte anvendelsesformål spille en central rolle med hensyn til at stimulere innovation inden for rammerne af EDTIB. Den Europæiske Forsvarsfond vil yderligere sammenknytte og understøtte medlemsstaternes indsats via sit forsvarsinnovationscenter i kraft af sin forsvarsekspertise, herunder med hensyn til at sammenføre nye og disruptive teknologier og militære kapacitetsbehov. Kommissionen og Den Europæiske Forsvarsfond vil i et tæt og synergipræget samarbejde fremskynde sikkerheds- og forsvarsinnovation for Unionen og dens medlemsstater.

3.4. Færdigheder

Mangel på færdigheder og mangel på arbejdskraft, navnlig højt kvalificerede medarbejdere med baggrund i naturvidenskab, teknologi, ingeniørvirksomhed og matematik, udgør store udfordringer for forsvars- og sikkerhedsindustrien, der i lighed med mange andre højteknologiske industrier er yderst afhængige af disse ressourcer. Da teknologierne og trusselsbilledet er i hastig forandring, er det vigtigt for industrien i højere grad at nå ud til nye og unge forskere og iværksættere, bl.a. kvinder, ved at anlægge en inklusiv og imødekommende tilgang, der omfatter alle talenter og færdigheder og hele den disponible arbejdsstyrke.

I november 2020 lancerede Kommissionen pagten for færdigheder med en første bølge af færdighedspartnerskaber i de tre vigtigste industrielle økosystemer, dvs. industrien for mikroelektronik, bilindustrien samt luft- og rumfartsindustrien og forsvarsindustrien under ét. Medlemmerne af pagten (industrien, universiteter og uddannelsesorganisationer samt arbejdsmarkedets parter) har forpligtet sig til at sikre et kontinuerligt og bæredygtigt udbud af

færdigheder på de områder, hvor behovet er størst, ved at opkvalificere 200 000 arbejdstagere og omskole 300 000 personer med en offentlig og privat investering på 1 mia. EUR senest i 2030.

Kommende tiltag:

- Kommissionen opfordrer medlemsstaterne til i det strategiske kompas at påtage sig fra første færd at udvikle en EU-dækkende strategisk koordineret tilgang til kritiske teknologier, der er relevante for sikkerhed og forsvar.
- I 2023 vil Kommissionen gennemgå eksisterende EU-instrumenter og foreslå yderligere måder, hvorpå der på EU-niveau kan bakkes op om FTU&I med dobbelt anvendelse.
- Kommissionen vil støtte innovation og iværksætterier for kritiske teknologier inden for sikkerhed og forsvar baseret på følgende værktøjer: a) Den Europæiske Forsvarsfonds særlige aktioner, b) en ny blandingsfacilitet for forsvarsinvesteringer inden for rammerne af InvestEU, c) et nyt CASSINI-initiativ målrettet forsvarsområdet, d) et nyt innovationsvæksthus for nye teknologier og innovation med dobbelt anvendelse i 2022 og e) øget støtte til innovationsnetværk.
- Kommissionen vil sammen med Den Europæiske Forsvarsfond og dens forsvarsinnovationscenter oprette en EU-ordning for forsvarsinnovation for at øge tempoet i sikkerheds- og forsvarsinnovation inden for Unionen og dens medlemsstater.

4. Mindsket strategisk afhængighed, hvad angår kritiske teknologier og værdikæder inden for sikkerhed og forsvar

Unionen har foruden sine FTU&I-programmer og -instrumenter flere politiske værktøjer, der kan bidrage til at mindske dens strategiske afhængighed, hvad angår kritiske teknologier og værdikæder inden for sikkerheds- og forsvarssektorerne. De bidrager til at styrke Unionens industrielle kapacitet, konkurrenceevne, teknologiske suverænitæt og modstandsdygtighed, men også til at beskytte den igangværende og fremtidige teknologiske udvikling og kapacitet.

Kommissionen vil på grundlag af arbejdet i Observatoriet for Kritiske Teknologier og den ajourførte industristrategi systematisk vurdere hensynet til sikkerheden og forsvaret, hvis det er relevant, når den gennemfører og gennemgår eksisterende eller udformer nye industrielle og handelsmæssige EU-instrumenter for at sikre, at de egner sig til formålet.

- *Industrialliancer* — industrialliancer samler en bred vifte af partnere (f.eks. offentlige og private aktører samt civilsamfundet) i fælles tiltag vedrørende centrale EU-politiske mål i specifikke industrisektorer eller værdikæder. De bygger på principperne om åbenhed, gennemsigtighed, mangfoldighed og inklusion og fungerer i fuld overensstemmelse med konkurrencereglerne. Industrialliancer kan, hvis det er relevant, omfatte specifikke arbejdsområder med henblik på at mindske den strategiske afhængighed inden for sikkerheds- og forsvarssektorerne. Dette overvejes i den europæiske alliance for industrielle data og edge- og cloudteknologier og i industrialliancen om processorer og halvlederteknologier.
- *Vigtige projekter af fælleseuropæisk interesse* — vigtige projekter af fælleseuropæisk interesse iværksættes af medlemsstaterne og er underlagt Unionens statsstøtteregele. De er

udformet til at samle viden, ekspertise, finansielle ressourcer og økonomiske aktører i hele Unionen med henblik på at overvinde markedssvigt eller systemiske svigt og samfundsmæssige udfordringer, som ikke har kunnet imødegås af private aktører alene. Dette gælder navnlig banebrydende innovation og central infrastruktur. Der kan tages hensyn til sikkerheds- og forsvarsaspekter i vigtige projekter af fælleseuropæisk interesse. Dette kan være tilfældet i det kommende andet vigtige projekt af fælleseuropæisk interesse om mikroelektronik, der blev bebudet i lovpakken om mikrochips.

- *EU's finansieringsprogrammer* — Unionen har altid haft en åben forsknings- og innovationspolitik. Den er styret af princippet om åben strategisk autonomi og har til formål at sikre lige vilkår og gensidighed. I Unionens globale tilgang til forskning og innovation tilskyndes der til strategiske partnerskaber med ligesindede partnere i overensstemmelse med Unionens internationale forpligtelser (f.eks. NATO, USA, Canada, Japan og Sydkorea)¹⁴.

Samtidig er det nødvendigt for Unionen at sikre, at dens strategiske interesser bevares. For 2021-2027 har Kommissionen præciseret og harmoniseret reglerne for tredjelandes deltagelse — og hvorvidt enheder kan komme i betragtning til at deltage — på tværs af EU-programmer og -instrumenter. Der er fastsat særlige betingelser for deltagelse i sikkerhedsfølsomme aktiviteter for visse programmer (Horisont Europa, Programmet for et digitalt Europa, Den Europæiske Forsvarsfond, rumprogrammet og Connecting Europe-faciliteten), og de er yderligere præciseret i de relevante arbejdsprogrammer for at beskytte Unionens væsentlige sikkerhedsinteresser. Den igangværende gennemgang af Kommissionens finansforordning vil også skabe større klarhed om, hvordan Unionens åbne strategiske autonomi kan opretholdes, dvs. fuldt ud beskytte Unionens væsentlige sikkerhedsinteresser under overholdelse af dennes internationale forpligtelser.

- *Standarder* — ifølge handlingsplanen for synergier fremmer Kommissionen anvendelsen af eksisterende hybride standarder for det civile område og forsvarsområdet og udviklingen af nye standarder senest ved udgangen af 2022 (foranstaltning nr. 5) og hensynet til forsvaret i Kommissionens standardiseringspolitik og -tiltag. EU-strategien for standardisering¹⁵ har til formål at sikre Unionens lederskab med hensyn til at fastsætte civile standarder, men den vil også være yderst relevant for forsvarssektoren, eftersom næsten 80 % af de standarder, der anvendes i forsvarssektoren, stammer fra civile sektorer. Kommissionen vil sammen med interesserede parter (f.eks. Det Europæiske Forsvarsagentur) undersøge muligheden for at medtage forsvarets behov i den fremtidige standardiseringsindsats, som den støtter for at gøre standarderne mere forenelige med forsvarets behov.
- *Screening af udenlandske direkte investeringer* — Unionen er et af verdens mest åbne miljøer for udenlandske investeringer og et af de vigtigste mål for udenlandske direkte investeringer i verden. Nærmere bestemte investeringer kan dog også undergrave Unionens væsentlige sikkerhedsinteresser. For at forebygge sådanne risici har Unionen indført en ramme, der har været operationel siden oktober 2020, for screening af udenlandske direkte

¹⁴ Det må dog bemærkes, at EU-virksomheder ikke har adgang til hovedparten af vores partnerses forsvarsrelaterede forsknings- og udviklingsprogrammer.

¹⁵ [COM\(2022\) 31 final](#)

investeringer. I den første årsrapport om screening af udenlandske direkte investeringer bekræftes betydningen af en effektiv screening af udenlandske direkte investeringer på medlemsstatsniveau og et tæt samarbejde på EU-niveau med fokus på potentielle risici for sikkerheden eller den offentlige orden. Medlemsstaterne opfordres til at oprette nationale mekanismer til screening af udenlandske direkte investeringer; 18 medlemsstater har allerede indført en sådan mekanisme, og yderligere seks medlemsstater arbejder på at indføre en. Kommissionen vil evaluere forordningen og forelægge Europa-Parlamentet og Rådet en rapport senest i oktober 2023.

- *Kritisk infrastruktur* — nye og disruptive teknologier opstår i et stadig hurtigere tempo, hvilket har haft en betydelig indvirkning på sikkerheden af udstyr, infrastruktur og tjenester samt værdi- og forsyningskæder inden for strategiske sektorer, herunder inden for sikkerheds- og forsvarssektorerne. Unionen og medlemsstaterne må i højere grad tage højde for sårbarheder af den art i forbindelse med relevante risikovurderinger og overvågning og i forbindelse med gennemførelsen af forholdsregler, som opbygger modstandsdygtighed over for sikkerhedstrusler, f.eks. hybride trusler eller cybertrusler. Der vil være behov for EU-koordinering for at sikre, at medlemsstaterne opretholder et fremtidssikret niveau af modstandsdygtighed og konsekvente sikkerhedsstandarder på EU-plan for derved at undgå sårbarheder.
- *Intelligent og cirkulær materialeanvendelse* — den nye handlingsplan for den cirkulære økonomi af marts 2020 er en hjørnesten i den europæiske grønne pagt, Unionens nye dagsorden for bæredygtig vækst. Innovation og nye forretningsmodeller, der er baseret på øget ressourceeffektivitet, udvikling af nye materialer, fremme af sekundære råmaterialer og mere bæredygtige offentlige indkøb, vil ikke blot bevare miljøet, men også sikre industrien adgang til materialer. Additive fremstillingsteknikker, grønne indkøb og materialeanvendelse kan, hvis de gennemføres korrekt, også bidrage til at styrke konkurrenceevnen i Unionens sikkerheds- og forsvarsindustri og til Unionens modstandsdygtighed.
- *Datasikkerhed* — den europæiske strategi for data indeholder foranstaltninger, hvormed det sikres, at enkeltpersoner og virksomheder kan bevare kontrollen over deres data. Dette vil blive taget op i den datalov, som Kommissionen vil vedtage i begyndelsen af 2022.

Som led i det multilaterale projekt om fælles datainfrastrukturer og -tjenester (der samler den europæiske cloudsammenslutning og det fælles europæiske dataområde) fremmer Kommissionen investeringer (f.eks. via programmet for et digitalt Europa, Connecting Europe-faciliteten og Next Generation EU-fonden) i cloud-to-edge kapacitet, som er sikker, modstandsdygtig, energieffektiv og tilgængelig i realtid, og som sikrer tjenestekvaliteten i hele Europa. Sikring af teknologioverførsel inden for cloud- og edgeteknologi mellem den civile industri (navnlig sikkerhedsindustrien) og forsvars- og rumindustrien vil øge den teknologiske suverænitet. Den europæiske alliance for industrielle data og edge- og cloudteknologier danner en platform, hvor det vil være muligt at fremme sådanne synergier.

- *Handelspolitik* — de globale forsyningskæders kompleksitet og sårbarhed er ikke kun et problem for Unionen. Andre lande er afhængige af Unionen ("omvendt afhængighed"), og handel (eller "indbyrdes afhængighed") kan bidrage til at stabilisere de globale værdikæder.

Unionen står også rede til at handle beslutsomt og forsvare sig mod illoyal handelspraksis, f.eks. brug af konkurrenceforvridende udenlandske subsidier, samtidig med at den agerer i overensstemmelse med sine internationale forpligtelser. Unionen vil fortsat udnytte sine handels- og konkurrenceredskaber bedst muligt, samtidig med at det sikres, at EU-værktøjerne er effektive og ajourførte. Kommissionen har derfor foreslået nye instrumenter, f.eks. forordningen om udenlandske subsidier¹⁶, der tager fat på konkurrenceforvridning på det indre marked som følge af udenlandske subsidier.

Andre relevante politiske foranstaltninger (f.eks. indførelse af en potentiel fritagelse for merværdiafgift (moms) og lettelse af overførslen af EU-finansierede forsvarsprodukter) er nævnt i meddelelsen om forsvar.

Kommende tiltag:

- Kommissionen undersøger muligheden for at indføje forsvarsrelaterede aspekter i arbejdsområderne inden for initiativer såsom den europæiske alliance for industrielle data og edge- og cloudteknologier samt industrialliancen om processorer og halvlederteknologier.
- I 2023 vil Kommissionen sammen med medlemsstaterne kortlægge og aflægge rapport om behovet for en risikovurdering af forsyningskæder for kritisk infrastruktur, navnlig på det digitale område, for bedre at beskytte Unionens sikkerheds- og forsvarsinteresser.
- Kommissionen opfordrer alle de resterende medlemsstater til at oprette en national mekanisme til screening af udenlandske direkte investeringer.

5. Den eksterne dimension

Samarbejde med ligesindede partnere i hele verden er afgørende for at øge Unionens modstandsdygtighed og forsyningsikkerhed og samtidig mindske den strategiske afhængighed og øge de gensidige fordele. Princippet om gensidighed spiller en vigtig rolle i denne forbindelse. Unionens traditionelle partnere inden for teknologi, sikkerhed og forsvar omfatter medlemmerne af Det Europæiske Økonomiske Samarbejdsområde (navnlig Norge), kandidatlandene, nabolandslandene og andre tredjelande (f.eks. USA, Canada, Japan og Sydkorea) samt internationale organisationer (f.eks. NATO). De seneste udvekslinger foregik navnlig i følgende fora:

5.1. Handels- og teknologirådet mellem EU og USA

Handels- og teknologirådet mellem EU og USA holdt sit første møde den 29. september 2021. I den fælles erklæring bekræftede Unionen og USA deres tilsagn om at "fokusere på at fremme modstandsdygtighed i forsyningskæden og forsyningsikkerhed i nøglesektorer med henblik på den grønne og digitale omstilling og beskyttelsen af vores borgere" og dens mål om at "øge gennemsigtigheden af udbud og efterspørgsel, kortlægge de respektive eksisterende sektorkapaciteter, udveksle oplysninger om politiske foranstaltninger og forsknings- og udviklingsprioriteter og samarbejde om strategier til fremme af modstandsdygtighed i

¹⁶ [COM\(2021\) 223 final](#).

forsyningskæden samt diversificering". Det igangværende arbejde i arbejdsgrupperne om sikre forsyningskæder (herunder behandles halvledere for sig), IKT-sikkerhed, eksportkontrol og screening af investeringer er yderst relevant for denne køreplan. Den nyligt indledte dialog mellem Unionen og USA om sikkerhed og forsvar kan også danne et forum for at drøfte disse spørgsmål.

5.2. Partnerskab med NATO

På topmødet i Bruxelles i 2021 fastlagde NATO's ledere en ambitiøs dagsorden for teknologier, navnlig ny og disruptiv teknologi¹⁷. Dette affødte yderligere retningslinjer for det arbejde, der udføres i overensstemmelse med NATO's gennemførelsesstrategi for ny og disruptiv teknologi, som blev godkendt af NATO's forsvarsministre i februar 2021.

Kommissionen og den højtstående repræsentant vil overvåge fremskridtene med hensyn til relevante NATO-initiativer på området gennem regelmæssig kontakt med NATO på arbejdsgruppeniveau med henblik på en eventuel gensidigt acceptabel og gavnlig interaktion med relevante EU-initiativer i fuld åbenhed over for medlemsstaterne, samtidig med det undgås at skabe nye eller øge eksisterende teknologi- eller kapacitetsrelaterede afhængighedsforhold.

Kommende tiltag:

- Kommissionen og den højtstående repræsentant vil i forbindelse med handels- og teknologirådet mellem EU og USA og den nyligt indledte dialog mellem Unionen og USA om sikkerhed og forsvar undersøge, hvordan modstandsdygtigheden i forsyningskæden kan fremmes, og beskyttelsen af vores borgere sikres.
- Kommissionen og den højtstående repræsentant vil sammen med NATO inden for rammerne af de fælles erklæringer om samarbejdet mellem EU og NATO og i fuld åbenhed over for medlemsstaterne undersøge, hvordan gensidigt acceptabel og gavnlig interaktion kan fremmes mellem deres respektive relevante initiativer.

6. Konklusion

Den globale geopolitiske situation er fortsat kompleks, og kapløbet om nye teknologier af relevans for sikkerhed og forsvar fortsætter. Derfor må Unionen og dens medlemsstater styrke samarbejdet om teknologier, der er afgørende for Europas sikkerhed og forsvar på lang sigt, og bestræbelserne på at mindske den dermed forbundne strategiske afhængighed.

I denne køreplan foreslås et tæt samarbejde med medlemsstaterne om at udpege teknologier og værdikæder af kritisk betydning for sikkerhed og forsvar — og de grundlæggende årsager til den dermed forbundne strategiske afhængighed inden for rammerne af Observatoriet for Kritiske Teknologier — for at understøtte en EU-dækkende strategisk koordineret tilgang til kritiske teknologier, der er relevante for sikkerhed og forsvar, hvorved Unionens og de nationale FTU&I-programmer og -instrumenter udnyttes optimalt.

¹⁷ Dette omfattede beslutningen om at lancere DIANA (Defence Innovation Accelerator for the North Atlantic) og en NATO-innovationsfond.

For at forbedre sikkerheds- og forsvarssektorenes konkurrenceevne og modstandsdygtighed vil observationscentrets arbejde og det relaterede arbejde inden for rammerne af den ajourførte industristrategi også bidrage til at sikre, at sikkerheds- og forsvarshensyn tages mere i betragtning i Unionens industri- og handelspolitikker, hvis det er relevant og i overensstemmelse med Unionens konkurrenceregler og internationale forpligtelser.

Forslagene i denne køreplan har til formål at bidrage til FTU&I-dimensionen i EU's strategiske kompas, hvorigennem medlemsstaterne vil fastsætte ambitiøse, langsigtede mål for en væsentlig forbedring af Europas sikkerhed og forsvar.