Det Europæiske Økonomiske og Sociale Udvalgs udtalelse om sikkerhedsunionens industrielle dimension

(initiativudtalelse)

(2020/C 364/06)

Ordfører: **José CUSTÓDIO LEIRIÃO**

Medordfører: **Jan PIE**

Plenarforsamlingens beslutning	20.2.2020
Retsgrundlag	Forretningsordenens artikel 29, stk. 2
	Initiativudtalelse
Kompetence	Den Rådgivende Kommission for Industrielle Ændringer (CCMI)
Vedtaget i CCMI	26.6.2020
Vedtaget på plenarforsamlingen	16.7.2020
Plenarforsamling nr.	553
Resultat af afstemningen	
(for/imod/hverken for eller imod)	209/3/4

1. **Konklusioner og anbefalinger**

1.1. EØSU glæder sig over, at den nye Kommission er fast besluttet på at forbedre EU's teknologiske suverænitet, og fremhæver sikkerhedssektorens betydning på området. Uden teknologi er der ingen sikkerhed, og EU er nødt til at mestre de teknologier, som er afgørende for Unionens sikkerhed.

1.2. Til dette formål opfordrer udvalget Kommissionen til at lancere en strategi, der styrker Europas industrielle og teknologiske kapacitet på sikkerhedsområdet. Der er et stort behov for en sådan strategi, navnlig på følsomme områder, hvor afhængigheden af ikke-europæiske leverandører kan udgøre en sikkerhedsrisiko i sig selv. Strategien skal understøtte målene i den nye strategi for den indre sikkerhed og supplere den med en industriel dimension. Den bør bidrage til at imødekomme de europæiske slutbrugeres nuværende og fremtidige kapacitetsbehov og til at tage fat på de vigtige udfordringer, som sektoren står over for i Europa: markedsfragmentering, mangel på langsigtet kapacitets- og teknologiplanlægning og manglende sammenhæng mellem EU's politikker og finansieringsinstrumenter.

1.3. Strategien for sikkerhedsindustrien bør bygge på følgende principper:

a) en innovativ sikkerhedsindustri er afgørende for Europas teknologiske suverænitet og strategiske autonomi

b) sikkerhed er et suverænitetsspørgsmål, der ikke kan overlades til markedskræfterne alene. Det kræver politisk vilje og handling at opretholde kapaciteten til at udvikle komplekse højteknologiske sikkerhedsløsninger

c) i lyset af covid-19-pandemien skal modstandsdygtighed over for større naturkatastrofer og menneskeskabte katastrofer være en politisk topprioritet for EU og kan kun opnås med støtte fra den europæiske sikkerhedsindustri.

Strategien bør udvikles som led i sikkerhedsunionen og gøre EU's sikkerhedsrelaterede politikker mere effektive. Den bør have en helhedsorienteret tilgang og omfatte følgende mål:

— vurdering af Europas svagheder og kritiske afhængighed, når det gælder ikke-militær sikkerhed

— screening af nyudviklede teknologier for eventuelle sikkerhedsrisici

— definition af kritiske og uundværlige teknologier, som EU af sikkerhedsmæssige årsager ikke bør være afhængig af at få leveret fra tredjelandsleverandører

— identificering af strategiske værdikæder i sikkerhedssektoren

— brug af EU-agenturer som drivkræfter for kapacitetsplanlægning og harmonisering af nationale krav

— brug af sikkerhedsrelaterede EU-instrumenter (Fonden for intern sikkerhed, Fonden for Integreret Grænseforvaltning, programmet for et digitalt Europa, Horisont Europa og RescEU) til målrettede investeringer i kritiske sikkerhedsteknologier og -applikationer;

— brug af andre EU-instrumenter (strukturfonde, InvestEU osv.) til sikkerhedsrelevante investeringer (infrastruktur), fortrinsvis via oprettelsen af en facilitet for et sikkert Europa (i lighed med Connecting Europe-faciliteten)

— brug af europæiske indkøb og koordinering af nationale indkøb til støtte for det pågældende industrigrundlag

— brug af kapacitetsorienterede finansieringsinstrumenter (f.eks. Fonden for intern sikkerhed og Fonden for Integreret Grænseforvaltning) til udbredelse af EU's sikkerhedsforskning på markedet ud over Horisont Europa

— identificering af eventuelle nye lovgivningsinitiativer, herunder en revision af direktivet om beskyttelse af kritiske infrastrukturer eller et eventuelt instrument for sikkerhed i byerne

— koordinering af relevante EU-programmer (forsvar, sikkerhed, rummet og IT).

Baggrund

1.4. Europas sikkerhedssituation er uhyre kompleks. De aktuelle sikkerhedstrusler er ofte mangesidede, tværnationale, under hastig forandring og vanskelige at forudsige. De kan ramme en lang række mål i hele EU (f.eks. store arrangementer, transporten, kritisk infrastruktur og institutioner) og komme fra en lige så lang række trusselsaktører (f.eks. individuelle gerningsmænd, kriminelle organisationer, terrorgrupper og nationalstater), som kan have meget forskellige motiver (f.eks. geopolitik, religiøst og politisk motiveret ekstremisme, økonomiske og finansielle interesser og psykiske lidelser) og bruge alle former for midler til at udføre deres ondsindede hensigter (f.eks. skydevåben, improviserede sprængstoffer, nukleare, radiologiske, biologiske og kemiske materialer, cyberangreb og desinformation).

1.5. Ud over de menneskeskabte sikkerhedstrusler er der naturkatastrofer som f.eks. oversvømmelser, tørke, orkaner og pandemier, der udgør en stadig større risiko som følge af klimaforandringer, miljøforurening og overudnyttelse af naturressourcerne. Naturkatastrofer er som regel endnu mere ødelæggende end menneskeskabte katastrofer og truer sikkerheden både direkte og indirekte.

1.6. Sikkerhedstruslerne svinger, og det samme gør sikkerhedsstyrkerne og deres kapacitetsbehov. Samtidig samarbejder sikkerhedsstyrker ofte, f.eks. som beredskabsfolk i forbindelse med katastrofer, og har brug for interoperabelt udstyr, der gør det muligt at løfte de udfordringer, som de står over for.

1.7. Selv om de har forskellig karakter, har nutidens sikkerhedstrusler én ting til fælles: de kan ikke imødegås uden teknologisk bistand. Teknologi kan ikke i sig selv skabe sikkerhed, men er i vores komplekse og indbyrdes forbundne samfund en uundværlig katalysator på alle sikkerhedsområder og i alle faser af sikkerhedscyklussen (forebyggelse, forberedelse og genopretning). Den hurtige udvikling og udbredelse af nye digitale teknologier, såsom kunstig intelligens, kvantedatabehandling og blockchain, vil gøre teknologien endnu vigtigere for sikkerheden, da de ikke blot skaber nye muligheder, men også øger sårbarheden og mulighederne for at gøre skade.

1.8. Uden ekspertise fra en specialiseret sikkerhedsindustri er det umuligt at udvikle de avancerede teknologier, der er nødvendige for at håndtere aktuelle og fremtidige sikkerhedstrusler. Sikkerhedsindustrien er en vigtig partner, navnlig i forbindelse med komplekse sikkerhedssystemer og beskyttelse mod avancerede trusselsaktører.

1.9. Det sikkerhedsrelaterede industri- og teknologigrundlag i Europa er lige så forskelligartet som de moderne samfunds og økonomiers sikkerhedsbehov. Det omfatter virksomheder af alle størrelser fra hele EU med forskellige porteføljer og specialiseringer. Mange af dem udfører også forsvars-, luftfarts- eller kommercielle IT-aktiviteter eller er datterselskaber af større grupper fra disse sektorer. De udvikler og producerer højteknologiske systemer og leverer tjenester, der er nødvendige for at beskytte vores samfund, virksomheder, institutioner og borgere mod alle former for sikkerhedstrusler og katastrofer. Den seneste omfattende undersøgelse anslår, at sikkerhedsindustrien i EU har en omsætning på næsten 200 mia. EUR og beskæftiger 4,7 millioner mennesker ([1]).

2. **Generelle bemærkninger**

2.1. Unionen har en økonomisk, men også en strategisk interesse i at skabe et dynamisk europæisk sikkerhedsrelateret industrigrundlag. Jo mere kritisk et sikkerhedsområde er, desto mere kan afhængighed af tredjelandsleverandører i sig selv udgøre en sikkerhedsrisiko. Det er altafgørende at anvende teknologier, tjenester og udstyr fra pålidelige kilder, navnlig når kritisk infrastruktur og statslige institutioner skal beskyttes mod trusler fra statslige eller statsstøttede aktører.

2.2. Covid-19-pandemien og dens direkte og indirekte konsekvenser har også vist, at der er behov for en stærk EU-baseret sikkerhedsindustri. F.eks. har den massive anvendelse af digitale værktøjer udløst en eksplosiv stigning i antallet af cyberangreb fra både ikkestatslige og statslige aktører over for virksomheder og operatører af væsentlige tjenester. En forbedring af cybermodstandsdygtigheden og cybersikkerheden inden for alle digitale processer i virksomheder og institutioner bør derfor være en vigtig lære af pandemien. Siden virussen brød ud, har vi igen været vidne til desinformationskampagner, der ofte finansieres af udenlandske regeringer, og som ikke kan bekæmpes effektivt uden brug af avancerede teknologiske værktøjer. Covid-19 har også afsløret enorme mangler i EU's krisestyringskapacitet. F.eks. mangler der en fælles pulje af nuklear, radiologisk, biologisk og kemisk materiel. Med andre ord er der behov for en lang række foranstaltninger for at gøre Europa mere modstandsdygtigt over for omfattende katastrofer. Da de fleste af disse foranstaltninger er meget følsomme, er det absolut nødvendigt at gennemføre dem med støtte fra leverandører, der er pålidelige og kan garantere forsyningssikkerheden i krisetider.

2.3. EU har derfor en strategisk interesse i at opretholde den industrielle kapacitet i Europa, der er nødvendig for at sikre en passende grad af uafhængighed og teknologisk suverænitet på kritiske sikkerhedsområder. De nuværende markedsforhold gør det desværre samtidig vanskeligt at tilgodese denne strategiske interesse. De særlige forhold på det europæiske sikkerhedsmarked gør det ofte svært for virksomhederne at opbygge et bæredygtigt forretningsgrundlag for de pågældende teknologier.

2.4. Kommercielt set er der kun begrænset efterspørgsel efter omkostningstunge, avancerede sikkerhedsprodukter. De private markedsoperatører forsøger konstant at nedbringe omkostningerne og begrænser derfor som regel deres investeringer i sikkerhed til det strengt nødvendige og foretrækker det billigste standardprodukt (ofte fra tredjelandsleverandører).

2.5. Hvad angår den offentlige efterspørgsel på sikkerhedsmarkedet, findes der en lang række forskellige købere og slutbrugere, hvoraf de fleste har begrænsede indkøbsbudgetter, lægger små ordrer og er juridisk forpligtet til at købe til den laveste pris. Hertil kommer, at langt størsteparten af de offentlige kunder på sikkerhedsmarkedet ikke har nogen plan for deres kapacitetsudvikling. De køber standardprodukter for at tilgodese deres umiddelbare behov uden at gøre sig nogen langsigtede overvejelser om, hvordan trusler og teknologier vil udvikle sig i fremtiden, og endnu mindre om, hvilke investeringer det vil kræve at forberede sig på dette.

2.6. I betragtning af de særlige forhold, der gør sig gældende på begge sider af sikkerhedsefterspørgslen, er der kun et lille marked for kritiske teknologier og applikationer. Komplekse sikkerhedsløsninger er ofte skræddersyede til én enkelt eller en håndfuld kunder, hvilket begrænser produktionsmængden og stordriftsfordelene til et minimum. I bedste fald kan de

([1]) På grund af sektorens mangfoldighed er der i øjeblikket ingen klar definition af sikkerhedsindustrien og derfor kun omtrentlige skøn over markedets størrelse. En række faktorer står i vejen for en metodisk klassificering af industrien: 1) sikkerhedsindustrien er ikke som sådan omfattet af de vigtigste statistiske nomenklaturer (NACE, Prodcom osv.), 2) produktion af sikkerhedsrelaterede produkter gemmer sig under en lang række forskellige udgiftsområder, og statistikker for disse udgiftsområder skelner ikke mellem sikkerhedsrelaterede og ikke-sikkerhedsrelaterede aktiviteter, 3) der findes ingen statistisk datakilde på europæisk plan fra denne branche. Se undersøgelsen af udviklingen af statistiske data om den europæiske sikkerheds- og industribase, Ecorys Final Report for the European Commission, DG Migration and Home Affairs, juni 2015.

teknologier, der anvendes i sådanne systemer, anvendes til andre mindre følsomme applikationer til et større kommercielt marked. De nuværende markedsforhold gør det således umuligt at opretholde et teknologi- og industrigrundlag i EU, der kan udvikle den sikkerhedskapacitet, som Europa har brug for med henblik på at beskytte sine ydre grænser, sit territorium og sine borgere. Dette underminerer sikkerhedsunionens troværdighed og stiller krav om en forbedret indsats fra EU's side.

EU's sikkerhedspolitiske situation

2.7. Lige siden lanceringen af den europæiske dagsorden om sikkerhed i april 2015 har EU arbejdet for en ægte sikkerhedsunion, der gør det muligt for de nationale myndigheder og EU's myndigheder at samarbejde effektivt om håndteringen af fælles udfordringer og samtidig beskytte borgernes rettigheder og friheder ([2]). Alene det store antal initiativer på dette område viser, at sikkerhed så afgjort er blevet en af EU's centrale politiske prioriteter:

— direktiv om bekæmpelse af terrorisme ([3])

— reviderede regler om bekæmpelse af hvidvask af penge ([4])

— oprettelse af Schengeninformationssystemet (SIS) ([5])

— interoperabilitet mellem EU's informationssystemer for sikkerhed og grænse- og migrationsforvaltning ([6])

— oprettelse af Den Europæiske Unions Agentur for den Operationelle Forvaltning af Store IT-Systemer inden for Området med Frihed, Sikkerhed og Retfærdighed (eu-LISA) ([7])

— forordning om cybersikkerhed ([8])

— forstærket europæisk grænse- og kystvagt (»Frontex«) ([9])

— EU-system vedrørende rejseinformation og rejsetilladelse (ETIAS) ([10]).

Disse initiativer supplerer allerede oprettede programmer og finansieringsinstrumenter såsom Fonden for Intern Sikkerhed.

2.8. Kommissionens forslag til den næste flerårige finansielle ramme omfatter en betydelig forøgelse af de vigtigste relevante budgetposter (f.eks. 35,3 mia. EUR til grænseforvaltning og migrationsstyring, 4 mia. EUR til intern sikkerhed og 15,6 mia. EUR til modstandsdygtighed og kriserespons) i forhold til den forrige FFR ([11]). EU vil desuden finansiere endnu et sikkerhedsforskningsprogram under Horisont Europa, som allerede har ydet et vigtigt bidrag til udformningen og udviklingen af den fremtidige sikkerhedskapacitet under Horisont 2020.

([2]) Meddelelse fra Kommissionen til Europa-Parlamentet, Det Europæiske Råd og Rådet om gennemførelse af den europæiske dagsorden om sikkerhed for at bekæmpe terrorisme og bane vejen for en effektiv og ægte sikkerhedsunion, 20.4.2016, COM(2016) 230 final https://eur-lex.europa.eu/legal-content/DA/TXT/?qid=1591816169567&uri=CELEX:52016DC0230.

([3]) Direktiv om bekæmpelse af terrorisme (EUT L 88 af 31.3.2017, s. 6).

([4]) Direktiv om forebyggende foranstaltninger mod anvendelse af det finansielle system til hvidvask af penge eller finansiering af terrorisme (EUT L 141 af 5.6.2015, s. 73).

([5]) Forordning om oprettelse, drift og brug af Schengeninformationssystemet (SIS) på området ind- og udrejsekontrol (EUT L 312 af 7.12.2018, s 14) og forordning om oprettelse, drift og brug af Schengeninformationssystemet (SIS) på området politisamarbejde og strafferetligt samarbejde (EUT L 312 af 7.12.2018, s. 56).

([6]) Forordning om interoperabilitet (grænser og visa) (EUT L 135 af 22.5.2019, s. 27) og forordning om interoperabilitet (politisamarbejde og retligt samarbejde, asyl og migration) (EUT L 135 af 22.5.2019, s. 85).

([7]) Forordning om oprettelse af Den Europæiske Unions Agentur for den Operationelle Forvaltning af Store IT-Systemer inden for Området med Frihed, Sikkerhed og Retfærdighed (eu-LISA) (EUT L 295 af 21.11.2018, s. 99).

([8]) Forordning om ENISA (Den Europæiske Unions Agentur for Cybersikkerhed) og om cybersikkerhedscertificering af informations- og kommunikationsteknologi (EUT L 151 af 7.6.2019. s. 15).

([9]) Forordning om den europæiske grænse- og kystvagt (EUT L 295 af 14.11.2019, s. 1).

([10]) Forordning om oprettelse af et europæisk system vedrørende rejseinformation og rejsetilladelse (ETIAS) (EUT L 236 af 19.9.2018, s. 1).

([11]) I løbende priser. Se Kommissionens meddelelse om EU-budgettet som drivkraft bag genopretningsplanen for Europa, 27.5.2020, COM(2020) 442 final: https://eur-lex.europa.eu/legal-content/DA/TXT/?qid=1601471256722&uri=CELEX:52020DC0442R(01) .

2.9. Med hensyn til digitale teknologier foreslår Kommissionen også en betydelig forøgelse af udgifterne (f.eks. Horisont Europa og programmet for et digitalt Europa) for at styrke Europas teknologiske suverænitet på områder af strategisk betydning. I den forbindelse lægger Kommissionen også op til at fremme synergierne mellem rumfarts-, forsvars- og sikkerhedssektorerne.

2.10. Teknologisk suverænitet er også et vigtigt aspekt i den nye industristrategi for Europa. Kommissionen understreger således, at Europas »digitale omstilling, sikkerhed og fremtidige teknologiske suverænitet afhænger af vores strategiske digitale infrastrukturer«, og bebuder, at den vil »støtte udviklingen af centrale støtteteknologier, der er strategisk vigtige for Europas industrielle fremtid« ([12]).

Særlige bemærkninger

2.11. EU's kompetence på sikkerhedsområdet er stadig beskeden og begrænser sig som oftest til en koordinerende rolle mellem de nationale myndigheder. Derfor er sikkerhedspolitikkerne fortsat fragmenterede og ofte ineffektive. Det samme gør sig gældende i andre sikkerhedsrelevante sektorer som den offentlige sundhedssektor.

2.12. Sikkerheden i EU er en politisk prioritet uden en industriel dimension. Der findes et imponerende antal sikkerhedsrelaterede politikker og finansieringsinstrumenter med betydelige budgetter. Derimod findes der hverken en koordinering af kapacitetsbehovene eller en sammenhængende politik til støtte af det relevante industrielle og teknologiske fundament. Begreber som industriel konkurrenceevne, strategisk uafhængighed, kapacitetsplanlægning og kritiske teknologier har ikke været en del af debatten om sikkerhedsunionen og er aldrig blevet betragtet som mål for sikkerhedsrelaterede finansieringsprogrammer.

2.13. Kommissionens *handlingsplan for en innovativ og konkurrencedygtig sikkerhedsindustri* fra 2012 er ikke ambitiøs nok, dens rækkevidde er begrænset, og den har derfor ikke fået nogen nævneværdig gennemslagskraft.

2.14. EU's program for sikkerhedsforskning mobiliserer betydelige ressourcer, men har en række alvorlige svagheder. At få markedet til at anvende forskningsresultater er fortsat en stor udfordring, fordi der hverken findes en fælles kapacitetsplanlægningsproces for sikkerhed, der kan bidrage til at konsolidere efterspørgslen fra de offentlige slutbrugere, eller nogen systematisk anvendelse af andre kapacitetsorienterede EU-finansieringsinstrumenter til støtte for udbredelsen af sikkerhedsløsninger.

2.15. Den nye strategi for den indre sikkerhed er retningsgivende for EU's sikkerhedspolitik og bør derfor søge at løse disse problemer. Den bør tage højde for teknologiens hurtige udvikling og konsekvenserne heraf på sikkerheden, presse på for en fælles definition af sikkerhedskapacitetsbehov og fremme europæisk samarbejde med henblik på at opfylde disse behov. Dette vil styrke sikkerhedsunionen samt bidrage betydeligt til at skabe et ægte indre marked for sikkerhed og til at fastholde sikkerhedsindustriens konkurrenceevne i Europa.

2.16. Industrien er uundværlig for omsættelsen af teknologier til løsninger. En ambitiøs industripolitik for centrale suverænitetsområder bør derfor være en politisk prioritet for EU. Udviklingen af en sådan politik haster især inden for sikkerhedssektoren, der på nuværende tidspunkt lider under alvorlige markedssvigt, som gør det meget vanskeligt at opretholde en kritisk industriel og teknologisk kapacitet.

2.17. Udvalget opfordrer derfor Kommissionen til at udvikle en særlig sikkerhedsrelateret industristrategi med henblik på at støtte den nye strategi for den indre sikkerhed og gøre sikkerhedsunionen mere effektiv. Industristrategien bør være ambitiøs og vidtspændende og sikre, at alle relevante politikområder og instrumenter bidrager til EU's teknologiske suverænitet inden for kritiske sikkerhedsområder. Den bør også sikre, at alle sikkerhedsrelaterede EU-instrumenter (Fonden for intern sikkerhed og Fonden for Integreret Grænseforvaltning, RescEU) omfatter en industriel dimension, og at alle teknologirelaterede programmer (Digitalt Europa, Horisont Europa) omfatter en sikkerhedsdimension. Dette vil bidrage til at dække de offentlige kunders sikkerhedsbehov, give den europæiske industri nye muligheder og gøre det lettere at håndtere de sikkerhedsmæssige følger af de nye teknologier i god tid.

([12]) Meddelelse fra Kommissionen om en ny industristrategi for Europa, Bruxelles, 10.3.2020, COM(2020) 102 final https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:52020DC0102&qid=1591816769288&from=DA.

2.18. Med henblik herpå skal begrebet teknologisk suverænitet defineres yderligere og omsættes i praksis. Kommissionens aktuelle fokus på digitale teknologier hilses velkommen, men bør ikke begrænses til disse. Alle kritiske teknologier inden for de vigtigste områder vedrørende suverænitet, nemlig sikkerhed, forsvar og rummet, bør have prioritet. Konceptet bør ligeledes ses efter i sømmene i lyset af covid-19-pandemien og omfatte modstandsdygtighed som et strategisk mål.

2.19. Kommissionens nye industristrategi for Europa indeholder elementer, der er vigtige for at fremme den teknologiske suverænitet på kritiske sikkerhedsområder. Navnlig begrebet strategiske værdikæder bør anvendes som ramme for en overordnet strategi, der omfatter hele den industrielle cyklus fra levering af kritiske materialer til industrialisering og vedligeholdelse, og som koordinerer anvendelsen af alle relevante politikinstrumenter, herunder kontrollen med udenlandske direkte investeringer.

2.20. Den næste flerårige finansielle ramme skal tilpasses behovene både under og efter covid-19-æraen ligesom de politikker, som FFR støtter, og de programmer, den finansierer. Tidligere definerede prioriteter og instrumenter skal revideres og tage hensyn til de erfaringer, der er gjort med Europas vanskeligheder med at håndtere pandemien. Dette gælder også for sikkerhedsunionen og den nye strategi for den indre sikkerhed, der bør afspejle behovet for større teknologisk suverænitet og modstandsdygtighed.

2.21. For at overvinde den recession, som pandemien har affødt, bør EU i næste budgetperiode koncentrere sine investeringer om højteknologiske sektorer, da de har den største merværdi og multiplikatoreffekt for økonomien som helhed ([13]). En EU-strategi for sikkerhedsindustrien, der bidrager til at gøre Europa mere uafhængigt og modstandsdygtigt, ville passe perfekt ind i denne strategi og bør derfor snarest muligt søsættes inden for rammerne af EU's covid-19-genopretningsplan.

Bruxelles, den 16. juli 2020.

Luca JAHIER
Formand
for Det Europæiske Økonomiske og Sociale Udvalg

([13]) Se f.eks. »Il ruolo dell'innovazione et dell'alta technologia in Italia nel confronto con il contesta internazionale« (innovationens og højteknologiens rolle i Italien i forhold til resten af verden), Centro economia digitale, Rom, oktober 2019.