Det Europæiske Økonomiske og Sociale Udvalgs udtalelse om meddelelse fra Kommissionen til Europa-Parlamentet, Rådet, Det Europæiske Økonomiske og Sociale Udvalg og Regionsudvalget — En EU-værktøjskasse til udrulning af sikre 5G-net i EU

(COM(2020) 50 final)

(2020/C 429/37)

Ordfører: **Alberto MAZZOLA**

Medordfører: **Dumitru FORNEA**

Anmodning om udtalelse	Kommissionen, 9.3.2020
Retsgrundlag	Artikel 304 i traktaten om Den Europæiske Unions funktionsmåde
Kompetence	Sektionen for Transport, Energi, Infrastruktur og Informationssamfundet
Vedtaget i sektionen	3.9.2020
Vedtaget på plenarforsamlingen	16.9.2020
Plenarforsamling nr.	554
Resultat af afstemningen (for/imod/hverken for eller imod)	217/0/2

1. **Konklusioner og anbefalinger**

1.1. EØSU bifalder, at medlemsstaterne og Kommissionen har taget initiativ til at undersøge, hvor langt medlemsstaterne er nået med gennemførelsen af de nøgleforanstaltninger, der anbefales i konklusionerne om EU-værktøjskassen, der består af strategiske og tekniske foranstaltninger til en sikker udrulning af 5G-økosystemet.

1.2. EØSU mener — i betragtning af de stadig mere komplekse og de stadig flere anvendelsesmuligheder for 5G-nettene (Kommissionen har fastsat følgende konnektivitetsmål for 2025: skoler, universiteter, forskningscentre, hospitaler, hovedudbydere af offentlige tjenesteydelser og digitalt intensive virksomheder bør have mulighed for internetopkobling med en download-/uploadhastighed på 1 GB data pr. sekund. Husholdninger i byerne og i landdistrikterne bør have mulighed for internetopkobling med en downloadhastighed på mindst 100 megabit pr. sekund, og byområder samt større veje og jernbaner bør have uafbrudt 5G-dækning.) — at denne undersøgelse af 5G-økosystemet og af de foranstaltninger, som Kommissionen har truffet til sikring af cybersikkerhed i 5G-nettene, en diversificeret 5G-værdikæde, teknisk standardisering og certificering, udenlandske direkte investeringer, beskyttelse af handelen og konkurrencen, forpligtelser til offentlig tjeneste, offentlige indkøb og cyberdiplomati, bør omfatte geopolitisk sikkerhed, infrastruktur- og datasikkerhed samt sundhedsbeskyttelse, herunder som omhandlet i EUF-traktatens artikel 168, stk. 1.

1.3. EØSU finder det vigtigt, at det europæiske 5G-økosystem sikrer følgende: integritet, fortrolighed, forvaltnings- og driftsmæssig ansvarlighed, sikkerhed, leverandørernes substituerbarhed, hardware- og softwarekomponenternes interoperabilitet, fælles tekniske standarder, tjenestekontinuitet, pålidelige datastrømme og databeskyttelse, dækning i alle — også tyndtbefolkede — områder, klar kommunikation til brugerne som aktive deltagere på det digitale marked samt proaktiv tilslutning til ICNIRP-retningslinjerne for beskyttelse af folkesundheden, samtidig med at stråling reduceres mest muligt. ICNIRP har således ajourført den del af 1998-retningslinjerne, der vedrører elektromagnetiske felter i forbindelse med radiofrekvenser. I dette dokument opridses disse reviderede retningslinjer, som beskytter mennesker mod eksponering for elektromagnetiske felter mellem 100 kHz og 300 GHz (Health Physics, 118(5):483-524, maj 2020 — offentliggjort marts 2020). ICNIRP har foretaget en række ændringer for at sikre, at nye teknologier som 5G ikke kan volde skade, uanset vores nuværende forventninger.

1.4. EØSU anmoder Kommissionen om nøje at overvåge fremskridtene med hensyn til udbredelsen og den reelle anvendelse af 5G og opfordrer medlemsstaterne til yderligere at fremskynde processen og sørge for en ansvarlig gennemførelse, idet de tager hensyn til alle sikkerhedsaspekter, herunder de aspekter, der vedrører 5G-teknologiernes indvirkning på folkesundheden og de levende økosystemer, de sociale og økonomiske følger, indvirkningen på konkurrencen, den almene uddannelse og erhvervsuddannelse samt sikringen af, at de grundlæggende rettigheder overholdes.

1.5. EØSU ser gerne, at EU indtager en førerposition på verdensplan, når det gælder næste generation af 5G-mobilteknologi, med en sikker digital infrastruktur som et solidt fundament for en ny og moderne industristrategi for Europa ved hjælp af en radikal omstilling i den mobile konnektivitet og med et enormt dynamisk potentiale til at øge produktiviteten, sætte skub i økonomien og forbedre tjenesterne for borgerne.

1.6. EØSU finder det især afgørende at vurdere leverandørernes risikoprofil og anvende relevante restriktioner over for leverandører, der anses for at udgøre en høj risiko, — og om nødvendigt udelukke dem for på effektiv vis at begrænse risici og fastslå ansvar — for centrale aktiver, der er udpeget som kritiske og følsomme i EU's koordinerede risikovurdering.

1.7. Udvalget finder det altafgørende, at Europa på mellemlang sigt satser på uafhængighed og selvforsyning på dette område ved i stor stil at støtte forskning og tilstedeværelse af flere europæiske virksomheder. EØSU finder det vigtigt at øge EU's midler til digital F&I og støtte operatørernes og leverandørernes investeringer i nye tekniske sikkerhedsfunktioner. Disse investeringer bør gå hånd i hånd med markedets evne til at anerkende og belønne alle initiativer, som sigter mod at øge sikkerheden og modstandsdygtigheden i systemer.

1.8. Det er vigtigt at give alle medlemsstater en sikkerhedsgaranti, herunder ved at opretholde forskningscentre i flere af EU's regioner. EØSU holder desuden fast i sit forslag om, at der bør være mindst to leverandører for hvert land, herunder mindst én europæisk leverandør, der kan garantere for datas sikkerhed på politisk plan og overholdelsen af sundhedskravene.

1.9. EØSU finder det nødvendigt — ud over den vægt, der med rette lægges på at have passende foranstaltninger med hensyn til de nationale tilsynsmyndigheders beføjelser og telekommunikationsoperatørernes rolle — også at lægge større vægt på instrumenter til brugerne, borgerne og de relevante civilsamfundsorganisationer, da disse er begrænsede og ineffektive, med det formål at styrke forbrugernes indflydelse og forbedre deres muligheder for at blive proaktive markedsaktører.

1.10. Kommissionen, Europa-Parlamentet, Rådet og medlemsstaternes regeringer og parlamenter bør udstikke en demokratisk ramme for høringer, hvor offentligheden kan få redegjort for videnskabelige og teknologiske spørgsmål, retslige garantier og de pågældende institutioners svar på spørgsmål fra civilsamfundet.

1.11. Udvalget anbefaler at styrke Europas teknologiske diplomati, så EU kan sikre mere afbalancerede og gensidige handels- og investeringsbetingelser, navnlig når det gælder markedsadgang, tilskud, offentlige indkøb, teknologioverførsel, industriel ejendomsret samt sociale og miljømæssige standarder.

2. **Indledning**

2.1. 5G-nettenes sikkerhed er et spørgsmål af strategisk vigtighed for borgerne og virksomhederne samt hele det indre marked og EU's teknologiske suverænitet. Allerede i 2013 lancerede Kommissionen EU's flagskibsinitiativ gennem etableringen af et offentlig-privat 5G-partnerskab (5G PPP) med henblik på at fremme forskning og innovation inden for 5G-teknologi.

2.2. Med globale indtægter, der anslås til at overstige 100 mia. EUR i 2025, udgør 5G en central del af Europas konkurrenceevne på det globale marked, og cybersikkerhed i forbindelse med 5G er af vital betydning for at sikre Unionens strategiske autonomi.

2.3. 5G-nettene bygger på den nuværende fjerde generation (4G) af netteknologier og fiberoptisk infrastruktur. De giver en ny tjenestekapacitet og er ved at blive en central infrastruktur — og en væsentlig katalysator for en stor del af Unionens økonomi — da de danner grundlaget for en lang række vigtige tjenester af betydning for det indre markeds funktion og for opretholdelsen og forvaltningen af vigtige økonomiske og samfundsmæssige funktioner såsom energi, transport, banktjenester, sundhedstjenester samt landbrugets og industriens produktions-, distributions- og forbrugssystemer.

2.4. I betragtning af 5G-nettenes centrale rolle i gennemførelsen af den digitale omstilling i EU's økonomi og samfund og i betragtning af, at den infrastruktur, der ligger til grund for det digitale økosystem, er sammenkoblet og tværnational, og at de pågældende trusler har grænseoverskridende karakter, ville eventuelle sårbarheder og/eller væsentlige cybersikkerheds-hændelser i forbindelse med 5G-nettene i en medlemsstat påvirke Unionen som helhed. Der bør derfor træffes foranstaltninger, der understøtter et højt, fælles cybersikkerhedsniveau i 5G-nettene.

2.5. I 2016 vedtog Kommissionen — i forbindelse med lanceringen af en række initiativer begyndende med meddelelsen om »Konnektivitet med henblik på et konkurrencedygtigt digitalt indre marked — på vej mod et europæisk gigabitsamfund« ([1]) samt en revision ([2]) af regelsættet for elektronisk kommunikation ([3]), af de opgaver, som Sammenslutningen af Europæiske Tilsynsmyndigheder inden for Elektronisk Kommunikation (BEREC) ([4]) udfører, af IKT-standardiseringsprioriteterne for det digitale indre marked ([5]) og af foranstaltningerne til fremme af internetkonnektivitet i lokalsamfund ([6]) — en handlingsplan for 5G til Europa ([7]), som EØSU tidligere har udarbejdet en positiv udtalelse ([8]) om, med henblik på at styrke EU's indsats for udbredelsen af 5G-infrastruktur og -tjenester i det digitale indre marked med en køreplan for offentlige og private investeringer i 5G-infrastruktur i EU og en målsætning om at udrulle kommercielle 5G-net inden udgangen af 2020.

2.6. I henhold til definitionen i Kommissionens henstilling ([9]) skal der ved »5G-net« forstås »et sæt af alle relevante netinfrastrukturelementer for mobil og trådløs kommunikationsteknologi, som anvendes til at skabe konnektivitet og værdiforøgende tjenester, med højydelsesegenskaber såsom meget høj datahastighed og -kapacitet, kommunikation med lav latenstid, ultrahøj pålidelighed og understøttelse af et stort antal forbundne enheder«.

2.7. Af henstillingen fremgår det, at Kommissionen vil støtte gennemførelsen af en EU-strategi for cybersikkerhed i forbindelse med 5G, og at den i tråd med medlemsstaternes ønsker vil bestræbe sig på at garantere sikkerheden i 5G-infrastrukturen og i forsyningskæden ved om nødvendigt at anvende alle tilgængelige instrumenter:

— regler for telekommunikation, multimedier og cybersikkerhed

— koordinering af standardisering og certificering på EU-plan

— udarbejdelse af et regelsæt for screening af udenlandske direkte investeringer med henblik på at beskytte den europæiske 5G-forsyningskæde

— handelspolitiske beskyttelsesinstrumenter

— konkurrenceregler

— sikring i forbindelse med offentlige indkøb, at der tages tilstrækkeligt hensyn til sikkerhedsaspekterne

— EU-finansieringsprogrammer, der skal sikre, at støttemodtagerne overholder de relevante sikkerhedskrav.

2.8. I juli 2019 fremlagde medlemsstaterne resultaterne af deres nationale risikovurderinger for den samarbejdsgruppe, der var blevet oprettet i henhold til NIS-direktivet ([10]) (og som består af repræsentanter for de enkelte medlemsstater), Kommissionen og ENISA, med oplysninger om de vigtigste aktiviteter, trusler og sårbarheder på 5G-området i henhold til standarden ISO/IEC 27005 og de vigtigste risikoscenarier med beskrivelse af de måder, trusselsaktørerne eventuelt vil kunne udnytte aktiviteters sårbarheder på. Disse nationale vurderinger dannede grundlaget for en efterfølgende koordineret vurdering og indførelsen af en fælles »værktøjskasse« med mulige risikobegrænsende foranstaltninger.

2.9. I oktober 2019 offentliggjorde NIS-samarbejdsgruppen, med støtte fra Kommissionen og ENISA, en rapport om EU's koordinerede risikovurdering for cybersikkerheden i 5G-net. I rapporten kortlægges forskellige vigtige sikkerhedsudfordringer i forbindelse med central teknologisk innovation inden for software, applikationer og tjenester samt leverandørernes rolle med hensyn til udbredelse og anvendelse af 5G-net og graden af de enkelte leverandørers afhængighed:

— øget eksponering for angreb og stigning i antallet af potentielle angrebsveje for gerningsmændene bag sådanne angreb

— øget følsomhed som følge af 5G-nettenes nye arkitektur og funktioner

— risici i forbindelse med mobilnetoperatørernes afhængighed af leverandører, hvilket øger antallet af de angrebsveje, som trusselsaktører kan udnytte

---

([1]) I EUF-traktatens artikel 168, stk. 1, hedder det: »Unionens indsats, der skal være et supplement til de nationale politikker, …«.
([2]) COM(2016) 587.
([3]) COM(2016) 590.
([4]) COM(2016) 591.
([5]) COM(2016) 176.
([6]) COM(2016) 589.
([7]) COM(2016) 588.
([8]) EUT C 125 af 21.4.2017, s. 74.
([9]) Kommissionens henstilling (EU) 2019/534 af 26.3.2019 om Cybersikkerheden i forbindelse med 5G-net, (EUT L 88 af 29.3.2019, s. 42).
([10]) Europa-Parlamentets og Rådets direktiv (EU) 2016/1148 af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen (EUT L 194 af 19.7.2016., s. 1).

— sammenhæng mellem de enkelte leverandørers risikoprofil og en eventuel indblanding fra tredjelande

— større risici som følge af en stor afhængighed af leverandører i tilfælde af en eventuel forsyningsafbrydelse forårsaget af handelsmæssige og andre former for spændinger

— trusler mod nettenes integritet og tilgængelighed, når det gælder sikkerhed, fortrolighed og privatlivets fred.

2.10. Disse udfordringer skaber et nyt sikkerhedsparadigme, som nødvendiggør en revurdering af den nuværende politiske og sikkerhedsmæssige ramme for sektoren og dens økosystem og tvinger medlemsstaterne til at træffe de nødvendige afhjælpende foranstaltninger.

2.11. Den 21. november 2019 offentliggjorde ENISA rapporten »Threat landscape for 5G networks«, hvori truslerne i forbindelse med den femte generation af mobile telekommunikationsnet vurderes, og som supplerer EU-medlemsstaternes rapport.

2.12. Den 29. januar 2020 offentliggjorde NIS-samarbejdsgruppen »Cybersecurity of 5G networks — EU toolbox of risk mitigating measures« ([11]), som indeholder en række mulige fælles foranstaltninger til afbødning af de største cybersikkerhedsrisici i 5G-nettene og til vejledning i forbindelse med udvælgelsen af de foranstaltninger, der bør have prioritet inden for rammerne af afbødningsplanerne på nationalt plan og EU-plan. Samme dag vedtog Kommissionen en meddelelse til støtte for den værktøjskasse ([12]), der behandles i nærværende udtalelse.

2.13. De vigtigste aktører i 5G-nettenes infrastruktur er:

— borgerne, forbrugerne og slutbrugerne af 5G

— mobilnetoperatører: aktører, der leverer mobile netværkstjenester til brugerne og forvalter deres net med hjælp fra tredjeparter

— leverandører til mobilnetoperatører: aktører, der leverer tjenester eller infrastruktur til mobilnetoperatørerne med henblik på at opbygge og/eller forvalte deres net. Denne kategori omfatter producenter af telekommunikationsudstyr, andre tredjepartsleverandører såsom leverandører af cloudinfrastruktur, systemintegratorer, sikkerheds- og vedligeholdelseskontrahenter samt producenter af transmissionsudstyr

— producenter af netforbundne enheder og tilknyttede tjenesteudbydere: aktører, som leverer produkter og tjenester, som kan kobles til 5G-nettene (f.eks. smartphones, netforbundne køretøjer og elektronisk sundhedsudstyr), og dertil hørende tjenestekomponenter i 5G-kontrolplanen som defineret i den tjenestebaserede struktur eller »mobile edge computing«

— andre interessenter, herunder tjeneste- og indholdsudbydere.

Alle disse interessenter er vigtige for sikkerheden, både når det gælder om at bidrage til cybersikkerheden i 5G-nettene og som mulige angrebsveje og -vektorer. Det er således vigtigt at vurdere de risici, der er forbundet med deres plads i 5G-økosystemet.

2.14. De vigtigste traditionelle former for trusler vedrører tilsidesættelsen af fortrolighed, integritet og tilgængelighed. Der er helt konkret blevet kortlagt en række trusselsscenarier for 5G-nettene, som navnlig vedrører:

— afbrydelse af det lokale eller globale 5G-net (tilgængelighed)

— spionage af datatrafikken i 5G-netinfrastrukturen (fortrolighed)

— ændring eller omdirigering af datatrafikken i 5G-netinfrastrukturen (integritet og/eller fortrolighed)

— ødelæggelse eller ændring af andet infrastruktur eller digitale informationssystemer via 5G-nettene (integritet og/eller tilgængelighed).

2.15. Trusler fra stater og statsstøttede aktører betragtes med største alvor, eftersom disse er de farligste og mest sandsynlige trusselsaktører, da de kan have bevæggrunde, hensigter og ikke mindst kapacitet til at udføre vedvarende og sofistikerede angreb på 5G-nettenes sikkerhed.

([11]) https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5 g-networks-eu-toolbox-risk-mitigating-measures.
([12]) https://ec.europa.eu/digital-single-market/en/news/secure-5 g-deployment-eu-implementing-eu-toolbox-communication-commission.

Selv om mange af disse sårbarheder ikke er karakteristiske for 5G-nettene, vil deres antal og omfang sandsynligvis blive øget med 5G, eftersom teknologien er mere kompleks, og økonomierne og samfundet vil gøre mere brug af denne infrastruktur i fremtiden.

2.16. Eftersom 5G-nettene især vil være baseret på software, vil de største sikkerhedsmangler — som dem, der skyldes mangelfuld softwareudvikling hos leverandørerne af udstyr — kunne gøre det lettere for aktørerne bevidst at installere bagdøre i produkter og gøre dem sværere at opdage. Dette kan øge risikoen for, at udnyttelsen af dem får særdeles alvorlige og omfattende virkninger. Da problemerne med cybersikkerheden i forbindelse med 4G endnu ikke er blevet fuldt ud løst, risikerer problemerne at vokse eksponentielt med 5G.

2.17. Desuden bør der gøres overvejelser om følgende sårbarheder i processen og konfigurationen:

— manglen på specialiseret og uddannet personale til at beskytte, overvåge og vedligeholde 5G-nettene

— manglen på velegnede interne sikkerhedskontroller, overvågningsmetoder og sikkerhedskontrolsystemer samt utilstrækkelige risikostyringsmetoder

— mangelfulde procedurer for sikkerhed og driftsvedligeholdelse såsom opdatering af software og forvaltning af sikkerhedslapninger i 5G-nettene

— manglende overholdelse af 3GPP-standarderne eller forkert anvendelse af dem

— mangler i nettenes opbygning og struktur, herunder manglen på effektive nød- og kontinuitetsmekanismer samt utilstrækkelig konfiguration, f.eks. i forbindelse med virtualisering samt administrator- og adgangsrettigheder

— uhensigtsmæssige kriterier for lokal adgang og fjernadgang til netkomponenterne

— utilstrækkelige sikkerhedskrav i forsyningsprocessen, hvor denne sårbarhed kan tage form af uhensigtsmæssige tilgange til udvælgelsen af leverandører eller manglende prioritering af sikkerheden i forhold til andre aspekter.

2.18. De enkelte leverandørers risikoprofil bør vurderes på grundlag af forskellige faktorer, navnlig: risikoen for, at en leverandør er under indflydelse fra et tredjeland, særligt når der er tætte bånd mellem leverandøren og et bestemt tredjelands regering; tredjelandets lovgivning, navnlig i de tilfælde, hvor der savnes retslig eller demokratisk kontrol og modvægt, og hvor en virksomheds datterselskab, der har sæde i EU, følgelig kan blive afskrækket fra at følge EU-lovgivningen, eller når der ikke findes aftaler mellem EU og det pågældende tredjeland om sikkerhed og databeskyttelse; ejerforholdene i leverandørens virksomhed; tredjelandets kapacitet til at udøve en hvilken som helst form for pres, herunder med hensyn til udstyrs produktionssted; den generelle kvalitet af leverandørens cybersikkerhedspraksis og produkter, herunder graden af leverandørens kontrol med sin egen forsyningskæde, og hvordan sikkerhedsprocedurerne prioriteres.

2.19. Medlemsstaterne er blevet enige om at træffe foranstaltninger, der gør det muligt at reagere hensigtsmæssigt og forholdsmæssigt på kendte og potentielle fremtidige risici. De er navnlig blevet enige om at sikre, at de inden for rammerne af en risikobaseret tilgang vil være i stand til at begrænse, forbyde og/eller fastsætte specifikke krav og betingelser for levering, udrulning og drift af 5G-netudstyr.

2.20. Med henblik herpå bør medlemsstaterne:

— stramme sikkerhedskravene til mobilnetoperatører, f.eks. i form af en streng adgangskontrol, regler om sikker drift, overvågning og begrænsning af outsourcing af specifikke funktioner

— vurdere leverandørernes risikoprofil på grundlag af objektive og klare kriterier; følgelig anvende relevante restriktioner, der er i tråd med proportionalitets- og retssikkerhedsprincippet, over for leverandører, der anses for at udgøre en høj risiko, — og om nødvendigt udelukke dem for på effektiv vis at begrænse risici — for centrale aktiver, der er udpeget som kritiske og følsomme i EU's koordinerede risikovurdering

— vedtage globalt anerkendte, implementerede og konsensusbaserede sikkerhedsstandarder og bedste praksis

— sikre, at de enkelte operatører har en passende flersælgerstrategi (»multi-vendor strategy«) for at undgå og begrænse en stor afhængighed af én enkelt leverandør eller af leverandører med en tilsvarende risikoprofil

— sikre en streng adgangskontrol og en sikker forvaltning, drift og overvågning af nettene samt anvende certificering for komponenter og/eller processer i 5G-nettene. Denne strategi skal baseres på en risikoanalyse foretaget af medlemsstaterne og operatørerne, således at valget af en flersælgerstrategi ikke øger risikoniveauet for operatørens net

— sikre en passende balance mellem leverandører på nationalt plan og undgå afhængighed af leverandører, der anses for at udgøre en høj risiko, bl.a. ved at fremme større interoperabilitet mellem udstyr

— bevare en diversificeret og bæredygtig 5G-forsyningskæde for at undgå en langvarig afhængighed ved fuldt ud at benytte EU's værktøjer til kontrol af udenlandske direkte investeringer, de handelspolitiske beskyttelsesinstrumenter, konkurrencelovgivningen og EU's udbudslovgivning

— styrke EU's interne kapacitet inden for 5G- og post-5G-teknologier ved hjælp af relevante EU-programmer og -midler samt sikre koordinering mellem medlemsstaterne på standardiseringsområdet ved at øge ressourcerne til testning og revision med henblik på at nå specifikke sikkerhedsmål, udvikle relevante ordninger for EU-certificering i overensstemmelse med lovgivningen om cybersikkerhed og fremme interoperabiliteten.

2.21. Som allerede påpeget af Kommissionen ved flere lejligheder er og bliver EU's indre marked åbent for dem, der gerne vil ind i Europa, forudsat at de respekterer klare og strenge regler, som bygger på objektive kriterier.

2.22. Den 6. juni 2020 fremhævede Rådet vigtigheden af at styrke den digitale suverænitet og det digitale samarbejde i EU og skabe synergier ved hjælp af EU-programmer som f.eks. Connecting Europe-faciliteten og programmet for et digitalt Europa med udvikling af digitale kompetencer og dataøkonomi samt vigtigheden af kunstig intelligens og cybersikkerhed, hvor det digitale område spiller en aktiv rolle, når det gælder om at nå målene i den grønne pagt.

3. **Kommissionens meddelelse**

3.1. Som svar på NIS-samarbejdsgruppens værktøjskasse for sikkerhed i 5G-net vil Kommissionen:

— som anmodet af medlemsstaterne bestræbe sig på at garantere sikkerheden i 5G-infrastrukturen og forsyningskæden ved om nødvendigt at anvende alle tilgængelige instrumenter

— opfordre medlemsstaterne til at gennemføre effektive strategier for risikobegrænsning og til at træffe yderligere koordineringstiltag på EU-plan med henblik på en fælles strategi for sikkerhed i 5G-nettene

— opfordre medlemsstaterne til at gennemføre alle de foranstaltninger, der anbefales i konklusionerne om EU-værktøjskassen, og til at udarbejde en fælles rapport om deres gennemførelse, samtidig med at NIS-samarbejdsgruppen fortsætter sit arbejde med at understøtte værktøjskassens indførelse

— på de områder, hvor den har beføjelser, træffe foranstaltninger til sikring af cybersikkerhed i 5G-nettene, en diversificeret 5G-værdikæde, teknisk standardisering og certificering, udenlandske direkte investeringer, beskyttelse af handelen og konkurrencen, offentlige indkøb og cyberdiplomati samt sine programmer og fonde vedrørende F&I, samhørighed og udvikling.

4. **Generelle bemærkninger**

4.1. EØSU er overbevist om, at de nye 5G-teknologier vil kunne ændre den måde, vi interagerer med verden på, idet de giver mulighed for nye anvendelser og forretningsmodeller, en ny livsstil, intelligente fabrikker, større produktivitet og nye tjenester af høj kvalitet til borgerne, og de kan bane vejen for revolutionerende teknologier såsom automatiserede biler og avancerede produktions- og distributionssystemer foruden at muliggøre flere tusinde indbyrdes forbundne enheder, der kunne blive en del af vores hverdag inden for rammerne af tingenes internet. EØSU ser dog gerne, at Kommissionen i højere grad foretager konsekvens- og gennemførlighedsundersøgelser samt cost-benefit-analyser af 5G med en sammenligning med anvendelsen af 4G-teknologi og fiberoptisk telekommunikation. EØSU finder det altafgørende at rette 5G mod en mere cirkulær ressourceanvendelse og en reduktion af det store energirelaterede CO_2-fodaftryk. Udvalget fremhæver betydningen af at tage fat på de sociale strukturændringer ved at fremme en retfærdig og smidig omstilling og tage hånd om manglen på kvalificeret arbejdskraft for at bane vejen for bedre betalte, fleksible og højt kvalificerede job.

4.2. Denne tredobbelte risiko — dvs. ukontrollerede pandemier, utilstrækkelige økonomipolitiske værktøjskasser og geopolitiske »sorte svaner« — kan skubbe verdensøkonomien ud i en varig depression og føre til et sammenbrud af finansmarkederne og kapitalflugt. Og det netop som alle segmenter i det europæiske samfund bliver stadig mere bevidste om, at en bæredygtig økonomisk vækst og **den igangværende digitale revolution — hvor 5G er en hjørnesten** — kræver, at man på én og samme tid kombinerer teknologisk suverænitet, produktivitetsforøgelse og en mere effektiv anvendelse af ressourcerne understøttet af passende lovgivnings-, reguleringsmæssige, økonomiske og finansielle rammer.

4.3. EØSU opfordrer EU-institutionerne og medlemsstaterne til at fuldføre det digitale indre marked og i den forbindelse udvikle kapacitet til at integrere 5G-tjenester og anvende dem med henblik på at forsvare og forbedre de europæiske industriers konkurrenceevne. Udvalget anmoder Kommissionen om nøje at overvåge fremskridtene med hensyn til udbredelsen og den reelle anvendelse af 5G og opfordrer medlemsstaterne til at fremskynde processen yderligere, idet de tager højde for alle sikkerhedsaspekter, herunder de aspekter, der vedrører 5G-teknologiernes indvirkning på folkesundheden og de levende økosystemer, de socioøkonomiske og konkurrencemæssige virkninger, den uddannelsesmæssige indvirkning og sikringen af, at de grundlæggende rettigheder overholdes, såsom ejendomsretten og retten til beskyttelse af personoplysninger.

4.4. EØSU ser gerne, at EU indtager en førerposition på verdensplan, når det gælder den næste generation af 5G-mobilteknologi, med en sikker digital infrastruktur som et solidt fundament for en ny og moderne industristrategi for Europa ved hjælp af en radikal omstilling i den mobile konnektivitet og med et enormt dynamisk potentiale til at øge produktiviteten, sætte skub i økonomien og forbedre tjenesterne for borgerne, deres velfærd og beskyttelsen af klimaet og miljøet ved at lade EU stå i spidsen for 5G-revolutionen.

4.5. Eftersom cybersikkerhed og national sikkerhed er to uløseligt forbundne aspekter, mener EØSU, at alle beslutninger om en EU-medlemsstats nationale sikkerhed bør træffes i EU-regi, og at ikke-tekniske vurderinger bør udarbejdes på en objektiv måde ud fra risikovurderingskriterier, der er fastlagt på europæisk plan, og som er nødvendige for at sikre harmoniserede og forudsigelige lovgivningsrammer i hele Europa, der sikrer fuld interoperabilitet.

4.6. EØSU mener, at kvaliteten af oplysninger og den måde, de formidles på — dvs. den såkaldte rammeeffekt, der skabes ved at sætte noget i en sammenhæng eller fremhæve noget — har en væsentlig indflydelse på modtagerens adfærd. Målsætningen om at styrke forbrugernes indflydelse kommer således til udtryk i, at man identificerer de instrumenter, der sigter mod at uddanne forbrugerne, øge deres kapacitet og gøre dem til aktive deltagere på det digitale marked. EØSU bemærker, at det er nødvendigt at give borgerne ajourførte og nøjagtige oplysninger om de risici og fordele ved 5G, som der er bred enighed om i det videnskabelige miljø, og gøre opmærksom på de aspekter, hvor der ikke hersker fuld enighed.

4.7. Udvalget mener, at der fortsat bør være fri adgang til EU's digitale marked for alle virksomheder uden forskelsbehandling, men at dette forudsætter overholdelse af EU's regler, standarder samt faste og klare vurderings- og sikkerhedskriterier, hvor genopretning og genoplivning af Europas teknologiske suverænitet på ny sættes i centrum for den europæiske strategi.

4.8. Selv om der blandt de fem største udbydere af infrastruktur er to europæiske, to kinesiske og en koreansk ([13]), er der ingen større europæiske virksomheder blandt de førende producenter af udstyr og chipsæt til 5G. EØSU er af den klare opfattelse, at man bør sikre, at der er flere leverandører, herunder mindst én med et europæisk moderselskab, og at der bør udstikkes en ramme for interoperabilitet og fuld substituerbarhed mellem hardware- og softwarekomponenterne, ikke mindst for at sikre Europas fulde teknologiske suverænitet inden for rammerne af et stærkt internationalt samarbejde og fuld gensidighed med hensyn til markedernes åbenhed, tilgængelighed og drift. En sådan diversificering er mulig, så længe der er interoperabilitet mellem tjenesterne, og cybersikkerhedsrisiciene ikke øges som følge af diversiteten.

4.9. Udvalget finder det altafgørende, at Europa på mellemlang sigt satser på uafhængighed og selvforsyning på dette område ved i stor stil at støtte forskning og tilstedeværelse af flere europæiske virksomheder. EØSU bifalder den værktøjskasse, som medlemsstaterne har vedtaget for at håndtere de sikkerhedsrisici i forbindelse med 5G-teknologiens indførelse, som allerede er blevet kortlagt i EU's vurdering. Udvalget mener dog, at de strenge og sikre grænseværdier for eksponering for elektromagnetiske felter, der anbefales på EU-plan og bygger på de ajourførte retningslinjer fra Den Internationale Kommission for Beskyttelse mod Ikkeioniserende Stråling (ICNIRP), som Verdenssundhedsorganisationen (WHO) har anerkendt, bør gælde for alle 5G-frekvensbånd ([14]). ICNIRP-grænseværdierne bygger nemlig på forsigtighedsprincippet, idet de er 50 gange lavere end de niveauer, der kan have indvirkning på folkesundheden, og som er fastsat på grundlag af den tilgængelige videnskabelige viden.

([13]) De fem globale leverandører er p.t. Ericsson, Nokia, Huawei, ZTE og Samsung.
([14]) Europa-Parlamentet — E-003040/2019. Svar fra Stella Kyriakides på Kommissionens vegne (17.1.2020).

4.10. EØSU bemærker dog, at ICNIRP-grænseværdierne ikke anerkendes af alle, og at nogle forskere går ind for meget strengere grænseværdier for befolkningens eksponering i overensstemmelse med »ALARA«-princippet (As Low As Reasonably Achievable — »så lavt, som det med rimelighed er opnåeligt«). De løsninger, der kan tænkes at blive foreslået som et supplement til 5G-kommunikationsinfrastrukturen, omfatter anvendelse af faste dataforbindelser gennem tilgængelige ikke-radiobaserede teknologier (ethernetkabler, fiberoptik osv.) i de tilfælde, hvor anvendelsen ikke er mobil (f.eks. pengeautomater, bankterminaler, industrirobotter, fjernstyrede medicinske robotter osv.), og i sektorer med store dataoverførsler (leverandører af digitale tjenester, virksomheder osv.) samt tingenes internet i faste ikke-mobile anordninger (Smart Home, Smart City, sensorer på udstyr til offentlige forsyningstjenester osv.).

4.11. Kommissionen, Europa-Parlamentet, Rådet og medlemsstaternes regeringer og parlamenter bør udstikke en demokratisk ramme for høringer, hvor offentligheden kan få redegjort for videnskabelige og teknologiske spørgsmål, retslige garantier og de pågældende institutioners svar på spørgsmål fra civilsamfundet.

4.12. EØSU finder det nødvendigt — ud over den vægt, der med rette lægges på at have passende foranstaltninger med hensyn til de nationale tilsynsmyndigheders beføjelser og telekommunikationsoperatørernes rolle — også at lægge større vægt på instrumenter til brugerne, borgerne og de relevante civilsamfundsorganisationer, da disse er begrænsede og ineffektive.

4.13. Udvalget har anerkendt ([15]), at problemet med elektromagnetisk overfølsomhed eksisterer og givet udtryk for sin bekymring i den henseende, men bemærker med tilfredshed, at der forskes grundigt i dette problem og dets årsager, og udvalget har opfordret Kommissionen til at fortsætte og ajourføre sit arbejde på dette område.

4.14. Troværdigheden hos leverandørerne af 5G-kommunikations- og applikationstjenester er efter EØSU's opfattelse af afgørende betydning, da forvaltningen af onlineinformation danner grundlaget for tjenester med aggregerede data, der indsamles og behandles af brugerne ved hjælp af teknologiske, juridiske og skattemæssige mekanismer, og skaber en direkte forbindelse mellem ting, maskiner og algoritmer.

4.15. EØSU har foreslået ([16]), at man går fra begrebet dataejerskab over til en definition af datarettigheder for fysiske og juridiske personer. Forbrugerne bør have kontrol over de data, der produceres af forbundne enheder, således at privatlivets fred sikres i forbindelse med adgang, tilgængelighed og overførslen af data, samtidig med at der sikres tilstrækkelig databeskyttelse og fortrolighed, fair konkurrence og flere valgmuligheder for forbrugerne.

4.16. Den generelle forordning om databeskyttelse (GDPR) bør suppleres med klare gennemførelsesretningslinjer for at sikre en ensartet anvendelse og et højt data- og forbrugerbeskyttelsesniveau i lyset af sammenkoblingen af maskiner og ting, og reglerne for produktansvar og -forsikring bør revideres for at tilpasse dem til en situation, hvor beslutninger i stadig større grad træffes af software inden for fuldstændigt sikre rammer.

4.17. Udvalget finder det vigtigt, at medlemsstaterne følger de strategiske og tekniske anbefalinger i EU-værktøjskassen, og at de undgår at udvikle specifikke nationale tilgange, f.eks. yderligere tests og certificeringer, der ville resultere i en opsplitning af markedet, forsinkelser i teknologiernes gennemførelse og uoverensstemmelser mellem markederne, hvilket risikerer at underminere tilliden til test- og certificeringssystemerne.

4.18. EØSU anser det for vigtigt, at der anvendes globale standarder med øget europæisk støtte samt fælles og anerkendt bedste praksis for at muliggøre en effektiv håndtering af trusler, skabe stordriftsfordele, undgå opsplitning og sikre interoperabilitet i de europæiske systemer. Drøftelser om de tekniske standarder kan give den afklaring, der er nødvendig for på ny at gøre virksomhederne konkurrencedygtige og sætte dem i stand til at udføre disse vigtige aktiviteter, der gør det muligt at indføre avanceret teknologi som 5G og kunstig intelligens på alle markeder.

4.19. EØSU finder det især nødvendigt at vurdere leverandørernes risikoprofil og anvende relevante restriktioner over for leverandører, der anses for at udgøre en høj risiko, — og om nødvendigt udelukke dem for på effektiv vis at begrænse risici — for centrale aktiver, der er udpeget som kritiske og følsomme i EU's koordinerede risikovurdering.

4.20. Udvalget finder det vigtigt at øge de erhvervsdrivendes og leverandørernes investeringer i nye tekniske sikkerhedsfunktioner — investeringer, der bør gå hånd i hånd med markedets evne til at anerkende og belønne alle de initiativer, som sigter mod at forbedre systemernes sikkerhed og modstandsdygtighed. Større fokus på sikkerhedsrelaterede investeringer kunne resultere i belønninger fra markederne.

([15]) EUT C 242 af 2.7.2015, s. 31.
([16]) EUT C 353 af 18.10.2019, s. 79.

4.21. EØSU går stærkt ind for en fælles indsats til støtte for industriel udvikling og udrulning af 5G, hvor man kortlægger eventuelle huller eller svigt i markedet langs 5G-værdikæden, som kan berettige målrettede tiltage i forbindelse med det næste langsigtede budget eller et eventuelt vigtigt projekt af fælleseuropæisk interesse vedrørende 5G-cybersikkerhed (»security and safety«).

4.22. Udvalget understreger, at selv om den digitale infrastruktur har vist sig at være modstandsdygtig og robust under covid-19-krisen, er det nødvendigt med yderligere investeringer i 5G-infrastrukturen for at overvinde den digitale kløft, der stadig eksisterer, og som kan begrænse borgernes adgang til e-sundhed, e-læring og hjemmearbejde.

4.23. Hvad angår teknologisk diplomati, finder EØSU det vigtigt, at EU sikrer mere afbalancerede og gensidige handels- og investeringsbetingelser, navnlig når det gælder markedsadgang, tilskud, offentlige udbud, teknologioverførsel, industriel ejendomsret samt sociale og miljømæssige standarder, især hvis der findes systemrivaler, som fremmer alternative forvaltningsmodeller, samtidig med at der tilskyndes til fuld konkurrence og teknisk innovation på markedet.

4.24. Ifølge udvalget er det absolut nødvendigt at bevare en diversificeret og bæredygtig 5G-forsyningskæde for at undgå langvarig afhængighed ved at sikre, at der findes flere substituerbare og interoperable leverandører og yderligere styrke programmer og initiativer, der øger EU's kapacitet og teknologiske suverænitet inden for 5G- og post-5G-teknologier, i den finansielle ramme for 2021-2027.

4.25. I forbindelse med den genopretningsplan for Europa, der blev vedtaget den 27. maj 2020, vil 2020-indekset for den digitale økonomi og det digitale samfund (DESI-indekset) tjene som input i den landespecifikke analyse til støtte for de digitale anbefalinger i det europæiske semester. Dette vil hjælpe medlemsstaterne med at målrette og prioritere deres reform- og investeringsbehov og således lette adgangen til instrumentet for genopretning og resiliens, som har en værdi af 560 mia. EUR. Instrumentet vil give medlemsstaterne de midler, der skal til for at gøre deres økonomier mere modstandsdygtige og sikre, at investeringerne og reformerne fremmer den grønne og digitale omstilling. Eftersom pandemien har haft stor indflydelse på de fem DESI-dimensioner, bør 2020-konklusionerne om 5G ses i sammenhæng med de mange foranstaltninger, som Kommissionen og medlemsstaterne har vedtaget med henblik på at håndtere krisen og støtte genopretningen.

Bruxelles, den 16. september 2020.

Luca JAHIER
Formand
for Det Europæiske Økonomiske og Sociale Udvalg