

**KOMMISSIONENS SVAR PÅ DEN EUROPÆISKE REVISIONSRETS  
SÆRBERETNING:  
"5G-UDRULNINGEN I EU: Udrulningen af net er forsinket, og der er stadig  
uafklarede sikkerhedsspørgsmål"**

RESUMÉ

**Kommissionens indledende bemærkninger**

I. Udrulningen af 5G-net på en hurtig og sikker måde er en vigtig prioritet for Europa-Kommissionen. Beskyttelse af 5G-net mod cybertrusler handler om at vurdere og mindske trusler og risici. Disse trusler og risici er blevet udpeget og vurderet af medlemsstaterne i fællesskab med støtte fra Kommissionen og ENISA, og på grundlag heraf er der blevet fastlagt en række omfattende foranstaltninger med henblik på at mindske disse risici. Der arbejdes stadig herpå i nogle medlemsstater, men langt de fleste medlemsstater har allerede skærpet eller er i færd med at skærpe sikkerhedskravene til 5G-net baseret på EU-værktøjskassen.

EU-værktøjskassen er blevet anerkendt som en omfattende ramme for håndtering af 5G-sikkerhedsrisici.

Den koordinerede indsats vedrørende 5G-cybersikkerhed på EU-plan og EU-værktøjskassen indgår i en bredere europæisk ramme for beskyttelse af elektroniske kommunikationsnet og andre kritiske infrastrukturer og supplerer eksisterende foranstaltninger såsom den europæiske kodeks for elektronisk kommunikation, telekommunikationsrammen, forordningen om cybersikkerhed og direktivet om sikkerhed i net- og informationssystemer (NIS-direktivet) og, alt efter tilfældet, traktatens bestemmelser om fri bevægelighed og EU's charter om grundlæggende rettigheder.

III. 5G vil spille en central rolle i vores digitale økonomi og samfund i de kommende år. Vi er nødt til at sikre, at 5G-net er modstandsdygtige over for cyberangreb og voksende cybertrusler og -hændelser. Derfor har Kommissionen og medlemsstaterne indført en koordineringsproces med henblik på at fastlægge og gennemføre en omfattende 5G-sikkerhedsramme i form af en værktøjskasse med risikobegrænsende foranstaltninger, der blev vedtaget i januar 2020, med henblik på effektivt at imødegå store risici for 5G-net, som f.eks. kriminel hacking, spionage og sabotage, på en koordineret måde. Der arbejdes stadig herpå i nogle medlemsstater, men langt de fleste medlemsstater har allerede skærpet eller er i færd med at skærpe sikkerhedskravene til 5G-net baseret på EU-værktøjskassen.

VII. EU-værktøjskassen udgør en ramme for fremme af sammenhæng i det indre marked, samtidig med at de nationale sikkerhedskompetencer på dette område respekteres.

Med hensyn til medlemsstaternes tilgang til højrisikoleverandører mener Kommissionen, at det først vil være muligt at foretage en endelig vurdering, når der foreligger flere oplysninger.

Selv om gennemførelsen er i gang, samarbejder Kommissionen med medlemsstaterne i NIS-samarbejdsgruppen om at fremme tilpasning og konvergens mellem de nationale tilgange.

IX. Første led — Kommissionen accepterer anbefalingen.

Andet led — Kommissionen accepterer anbefalingen.

Tredje led — Kommissionen accepterer anbefalingen.

Kommissionen vil foretage vurderingen under hensyntagen til de nationale kompetencer.

INDLEDNING

04. Kommissionen erkender, at der er nogle sikkerhedsrisici i forbindelse med 5G, men påpeger, at 5G-netteknologi og -standarder også kan medføre sikkerhedsmæssige forbedringer i forhold til tidligere generationer af net.

#### BEMÆRKNINGER

30. Selv om 4G allerede kan håndtere en bred vifte af tjenester, bør 5G udgøre et "spring fremad", altså en væsentlig ændring i forhold til 4G, så den største udfordring er overgangen fra 4G til 5G og udrulning af 5G i hele EU. Risikoen for en digital kløft eksisterer altid, men det er planen at gribe denne risiko an som en politisk prioritet i politikprogrammet "Vejen mod det digitale årti" i forbindelse med forløbet hen imod 5G-målet om en dækning på 100 % af alle befolkede områder inden 2030 og dermed støtte medlemsstaterne i deres bestræbelser for at træffe foranstaltninger på dette område, navnlig med hensyn til adgang i landdistrikter.

32. 5G-observatoriet har været en pålidelig kilde til overvågning af 5G-udrulningen i og uden for EU, selv om der opstod visse mangler. Kommissionens tjenestegrene forventer at have mere ajourførte oplysninger til rådighed med den nye leverandør.

#### Kommissionens fælles svar på punkt 48 og 49:

Kommissionen mener, at valget af instrument (henstilling) og samarbejdet med medlemsstaterne om at fastlægge risici og afbødende foranstaltninger er den mest hensigtsmæssige fremgangsmåde til at imødegå 5G-sikkerhedsrisici på en hurtig, effektiv og samordnet måde.

Kommissionen valgte en henstilling og samarbejde med medlemsstaterne med henblik på at fastlægge risici og afbødende foranstaltninger i lyset af emnets kompleksitet og tværgående karakter på tværs af nationale kompetencer og EU-kompetencer og den betydelige nationale sikkerhedsdimension. Derudover tog Kommissionen også hensyn til, at der hersker meget forskellige nationale forhold i medlemsstaterne (markedsstruktur, cybersikkerhedskapaciteter, trusselsefterretninger osv.).

EU-værktøjskassen er et smidigt risikobaseret instrument til håndtering af sikkerhedsudfordringer, som gjorde det muligt at håndtere 5G-cybersikkerhedsaspekter på en rettidig og effektiv måde.

I sin meddelelse "En EU-værktøjskasse til udrulning af sikre 5G-net i EU" fra januar 2020 meddelte Kommissionen, at den ville yde støtte til gennemførelsen af værktøjskassens foranstaltninger, der vedrører sikkerhedskrav, herunder især for så vidt angår relevante bestemmelser i det europæiske regelsæt om elektronisk kommunikation, og undersøge, hvilken merværdi der kan opnås ved eventuelle gennemførelsesretsakter med tekniske og organisatoriske sikkerhedsforanstaltninger, med henblik på at komplementere nationale regler og øge effektiviteten og sammenhængen i de sikkerhedsforanstaltninger, der pålægges operatørerne.

#### Kommissionens fælles svar på punkt 51 og 52:

I forbindelse med gennemgangen af Kommissionens henstilling, der fandt sted i december 2020, interviewede Kommissionen alle medlemsstaternes kompetente myndigheder. De beskrev Europas koordinerede indsats inden for 5G-cybersikkerhed som rettidig, effektiv og forholdsmæssig. Den samarbejdsbaserede tilgang mellem de nationale myndigheder, Kommissionen, ENISA og andre relevante interessenter blev anset for velegnet til at løse dette komplekse spørgsmål. Den muliggjorde en rettidig fastlæggelse af fælles mål og metoder, samtidig med at medlemsstaterne fik mulighed for at tilpasse foranstaltningerne til deres nationale forhold.

I EU-værktøjskassen og den statusrapport, der blev offentliggjort af NIS-samarbejdsgruppen i juli 2020, anbefales det at fastlægge gennemførelsesplaner og/eller overgangsperioder for de operatører, der for øjeblikket anvender udstyr fra højrisikoleverandører, eller som allerede har indgået kontrakter med højrisikoleverandører inden vedtagelsen af EU-værktøjskassen (f.eks. ved at tage hensyn til opgraderingscyklusser for udstyr, navnlig migrationen fra "non-stand-alone"- til "stand-alone"-5G-net).

55. Kommissionen noterer sig Revisionsrettens bemærkninger.

For yderligere at støtte gennemførelsen af værktøjskassens kriterier for vurdering af højrisikoleverandører har de været genstand for talrige drøftelser mellem de kompetente nationale myndigheder i NIS-samarbejdsgruppen, siden der blev opnået enighed om EU-værktøjskassen.

56. I EU-værktøjskassen anbefales det, at der tages hensyn til de risikofaktorer, som fremlægges i forbindelse med EU's koordinerede risikovurdering, og at der anvendes landespecifikke oplysninger (f.eks. trusselsvurdering fra nationale sikkerhedstjenester osv.) ved vurderingen af leverandørernes risikoprofil.

61. Leverandørens evne til at sikre levering er et af de kriterier, der anbefales i EU-værktøjskassen for at vurdere leverandørernes risikoprofil. Evnen til at sikre levering kan også blive påvirket af eventuelle handelssanktioner, som en bestemt sælger står over for, sådan som det er nævnt i risikoscenariet for "afhængighed" i EU's koordinerede risikovurdering.

#### Kommissionens fælles svar på punkt 70 og 73:

Kommissionen og medlemsstaterne udveksler detaljerede oplysninger om gennemførelsen af værktøjskassen på nationalt plan i NIS-samarbejdsgruppen. Det er medlemsstaternes ansvar at offentliggøre ikkeoffentliggjort information.

#### Kommissionens fælles svar på punkt 74-76 og tekstboks 5:

EU-værktøjskassen udgør en ramme for fremme af sammenhæng i det indre marked, samtidig med at de nationale sikkerhedskompetencer på dette område respekteres.

Med hensyn til medlemsstaternes tilgang til højrisikoleverandører mener Kommissionen, at det først vil være muligt at foretage en endelig vurdering, når der foreligger flere oplysninger.

Selv om gennemførelsen er i gang, samarbejder Kommissionen med medlemsstaterne i NIS-samarbejdsgruppen om at fremme tilpasning og konvergens mellem de nationale tilgange.

#### KONKLUSIONER OG ANBEFALINGER

81. Hurtig og sikker udrulning af 5G-net har højeste prioritet for Kommissionen. Beskyttelse af 5G-net mod cybertrusler handler om at vurdere og mindske trusler og risici. Disse trusler og risici er blevet udpeget og vurderet af medlemsstaterne i fællesskab med støtte fra Kommissionen og ENISA, og på grundlag heraf er der blevet fastlagt en række omfattende foranstaltninger med henblik på at mindske disse risici. Der arbejdes stadig herpå i nogle medlemsstater, men langt de fleste medlemsstater har allerede skærpet eller er i færd med at skærpe sikkerhedskravene til 5G-net baseret på EU-værktøjskassen.

EU-værktøjskassen udgør en omfattende ramme for håndtering af 5G-sikkerhedsrisici.

83. 5G udgør et "spring fremad", altså en væsentlig ændring i forhold til 4G, så den største udfordring med at undgå en digital kløft er overgangen fra 4G til 5G i hele EU.

5G-specifikationer dækker en lang række resultatindikatorer, navnlig i forbindelse med vertikale anvendelser. Dette kan bl.a. omfatte pålidelighedskrav, hastighed i instantieringen af tjenester, fleksibilitet i gennemførelsen og sikkerhedsniveauer.

#### **Anbefaling 1 — Fremme en jævn og rettidig udrulning af 5G-net i EU**

a) Kommissionen accepterer anbefalingen.

Kommissionen samarbejder med medlemsstaterne om at udvikle en fælles definition af den forventede servicekvalitet i 5G-net. Inden for rammerne af det digitale årti og den foreslåede afgørelse om for det digitale politikprogram 2030 har Kommissionen til hensigt at samarbejde med medlemsstaterne om en fælles tilgang til 5G-tjenestekvalitet i EU, herunder med henblik på sammenlignelige målinger og overvågningsdata.

Servicekvaliteten omfatter ikke kun hastighed og latenstid, men en lang række resultatindikatorer, navnlig i forbindelse med vertikale anvendelser.

Kommissionen har til hensigt at samarbejde med medlemsstaterne om at fastlægge sådanne målinger og gennemføre årlige kontroller og anbefale politikker, foranstaltninger og tiltag for at opnå fuld 5G-dækning senest i 2030.

Inden for rammerne af det digitale politikprogram vil der blive etableret en solid forvaltning gennem en overvågnings- og samarbejdsmechanisme for at sikre fremskridt hen imod opfyldelsen af målene i politikprogrammet, herunder udrulning af 5G, og det vil blive anbefalet medlemsstaterne at træffe afhjælpende foranstaltninger i denne henseende.

b) Kommissionen accepterer anbefalingen.

c) Kommissionen accepterer anbefalingen.

### **Anbefaling 2 — Fremme en samordnet tilgang til 5G-sikkerhed blandt medlemsstaterne**

a) Kommissionen accepterer anbefalingen.

Kommissionen vil sammen med medlemsstaterne vurdere behovet for yderligere tiltag eller støtte, f.eks. i form af vejledning om visse aspekter af EU-værktøjskassen.

b) Kommissionen accepterer anbefalingen.

Overvågningen og rapporteringen vil blive udført af Kommissionen i fuldt samarbejde med medlemsstaterne og ENISA.

c) Kommissionen accepterer anbefalingen.

### **Anbefaling 3 — Adressere konsekvenserne for det indre markeds effektive funktion af medlemsstaternes forskellige tilgange til 5G-sikkerhed**

a) Kommissionen accepterer anbefalingen.

b) Kommissionen accepterer anbefalingen.

Kommissionen vil foretage vurderingen under hensyntagen til de nationale kompetencer.

Inden for rammerne af EU-værktøjskassen er det op til medlemsstaterne at træffe afgørelse om det nøjagtige omfang af passende begrænsninger og/eller nødvendige udelukkelse for centrale aktiver, der er beskrevet som kritiske og følsomme i forbindelse med EU's koordinerede risikovurdering (f.eks. centrale netfunktioner, netforvaltning- og netstyringsfunktioner og adgangsnetfunktioner), for effektivt at afbøde udpegede risici, også under hensyntagen til de nationale efterretningstjenesters trusselvurdering. Medlemsstaterne har ret til at træffe foranstaltninger vedrørende den nationale sikkerhed, herunder eventuelle begrænsninger for eller udelukkelse af højrisikoleverandører.