EUROPA-
KOMMISSIONEN

Bruxelles, den 29.1.2020
COM(2020) 50 final

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

1. ***Indledning***

Den femte generation (5G) af telekommunikationsnet forventes at spille en væsentlig rolle i udviklingen af Europas samfund og økonomi. Den forventes at medføre enorme økonomiske muligheder og danne grundlag for både den digitale og den grønne omstilling på områder som transport, energi, fremstillingsvirksomhed, sundhed, landbrug og medier.

5G vil derfor potentielt påvirke alle aspekter af EU-borgernes liv. Cybersikkerhed i 5G-net er derfor en forudsætning, ikke blot for at beskytte vores økonomier, samfund og demokratiske processer, men også for at sikre en tillidsfuld digital omstilling til gavn for alle EU's borgere.

Det forhold, at mange kritiske tjenester bliver afhængige af 5G-net, vil gøre følgerne af systemiske og omfattende forstyrrelser særligt alvorlige og vil kunne få betydelige konsekvenser ud over de nationale grænser, eftersom de digitale økosystemer er så tæt forbundet med hinanden. Det er følgelig af strategisk vigtighed for Unionen at sørge for cybersikkerheden i 5G-net i en tid, hvor der kommer stadig flere og mere avancerede cyberangreb end nogensinde før, og de kommer fra en bred vifte af trusselsaktører, navnlig statslige eller statsstøttede aktører fra tredjelande. Man har for at garantere kritisk 5G-infrastrukturs sikkerhed for første gang valgt at indføre en fælles europæisk tilgang. Tilgangen respekterer fuldt ud den åbenhed, der karakteriserer det indre marked, for så vidt som EU's risikobaserede sikkerhedskrav overholdes.

Det Europæiske Råd opfordrede den 22. marts 2019 til en fælles tilgang til sikkerheden i 5G-net. Kommissionen vedtog den 26. marts 2019 henstilling (EU) 2019/534 om cybersikkerheden i forbindelse med 5G-net[1]. I henstillingen opfordredes medlemsstaterne til at foretage nationale risikovurderinger og evaluere de nationale foranstaltninger, at samarbejde på EU-plan om en koordineret risikovurdering og at forberede en værktøjskasse med mulige risikobegrænsende foranstaltninger. Denne meddelelse udgør en integreret del af Kommissionens overordnede europæiske digitale dagsorden, som Det Europæiske Råd har opfordret den til at udarbejde.

2. ***5G-udrulning i EU***

Indførelsen af 5G-netinfrastruktur i Europa er af central betydning for den europæiske industripolitiske strategi og konkurrenceevnen. Kommissionen ser udrulningen af 5G-netteknologi som en væsentlig katalysator for fremtidige digitale tjenester. I 2016 vedtog Kommissionen en 5G-handlingsplan for at sikre, at Unionen har den netinfrastruktur, der er en nødvendig forudsætning for den digitale omstilling fra og med 2020 og for en omfattende udrulning i byområder og langs vigtige transportveje inden 2025[2]. I meddelelsen om overgangen til et gigabitsamfund skitseres målsætningen om, at der skal være adgang til mobile dataforbindelser overalt[3], herunder i landdistrikter og fjerntliggende områder.

[1] Henstilling (EU) 2019/534 om cybersikkerheden i forbindelse med 5G-net (EUT L 88 af 29.3.2019, s. 42).

[2] COM(2016) 588 af 14. juni 2016 om 5G til Europa: En handlingsplan.

[3] COM(2016) 587 "Konnektivitet med henblik på et konkurrencedygtigt digitalt indre marked – På vej mod et europæisk gigabitsamfund".

Medlemsstaterne har tildelt 16 % af frekvenserne i 5G-pionerbåndene[4]. I betragtning af den retlige forpligtelse til at tillade brugen af alle 5G-pionerbåndene inden årets udgang forventes det, at der de kommende måneder gennemføres høringer i forbindelse med en række frekvenstildelingsprocedurer.

Europa er en af de mest avancerede regioner i verden inden for kommerciel lancering af 5G-tjenester[5]. På nuværende tidspunkt forventes de første 5G-tjenester at være tilgængelige i 138 europæiske byer ved udgangen af 2020. Tidlige 5G-net bygger på den nuværende fjerde generation (4G) af netteknologier, og 5G-tjenester tilbydes primært til den brede offentlighed i form af enten en forbedring af 4G-nettets kapacitet og hastighed eller som omkostningseffektive trådløse alternativer til faste net[6].

For så vidt angår mulighederne for at udbyde nye tjenester mellem virksomheder som f.eks. inden for sektorerne for energi, fødevarer og landbrug, sundhed, fremstillingsvirksomhed og transport er Europa langt fremme med en investering i størrelsesordenen 1 mia. EUR, herunder bl.a. 300 mio. EUR i EU-finansiering i forbindelse med det offentligt-private 5G-partnerskab under Horisont 2020. Investeringen omfatter flere end 160 store forsøg med 5G i Europa, herunder 10 grænseoverskridende motorvejskorridorer til afprøvning i stor skala af 5G-baserede netforbundne og automatiserede mobilitetstjenester. Forsøgene omfatter anvendelse af 5G-net inden for områder så forskellige som bæredygtige sundhedsydelser og automatiseret mobilitet over ressourceeffektivt landbrug til smarte elnet og Industri 4.0. Derudover har EIB med støtte fra Den Europæiske Fond for Strategiske Investeringer ydet lån med henblik på at fremskynde forskning i og udvikling af 5G-teknologi.

Den europæiske kodeks for elektronisk kommunikation ("kodeksen")[7], som vil finde anvendelse fra den 21. december 2020, danner et vigtigt grundlag for at skabe et investeringsvenligt miljø for 5G-nettet og dettes efterfølger. Ydermere vil offentlige finansieringsprogrammer, f.eks. Connecting Europe-facilitetens digitale område[8] og de europæiske struktur- og investeringsfonde, yde en væsentlig støtte til den fremtidige udrulning af 5G-net, navnlig ved at give f.eks. skoler, hospitaler, byer og lokale forvaltninger adgang til 5G-tjenester.

I betragtning af Europas strategiske muligheder inden for 5G-tjenester til adskillige brancher er det af afgørende betydning, at operatører og tjenesteudbydere investerer i avancerede 5G-net og -tjenesteløsninger. De vil ikke alene kræve nye 5G-radionet, men også såkaldte "selvstændige" 5G-kernenet med henblik på at muliggøre avancerede 5G-funktioner som "network slicing"[9] og "edge computing"[10].

---

[4] http://www.5GObservatory.eu

[5] http://www.5GObservatory.eu

[6] Nogle af de nye 5G-funktionaliteter vil blive indført i forskellige faser. I en første fase (meget kort og kort sigt) vil 5G-udrulningen primært bestå af "ikkeselvstændige" net, hvor kun radioadgangsnettet (RAN) opgraderes til 5G-teknologi, men ellers stadig afhænger af det eksisterende 4G-kernenet, hvilket vil give slutbrugerne bedre mobilt bredbånd. I de efterfølgende faser (kort/mellemlang til lang sigt) vil udrulningen af "selvstændige" 5G-net, herunder 5G-kernenetfunktioner, kræve og med tiden medføre en meget omfattende ændring af netarkitekturen.

[7] Europa-Parlamentets og Rådets direktiv (EU) 2018/1972 om oprettelse af en europæisk kodeks for elektronisk kommunikation (omarbejdning).

[8] Forslag til en forordning COM(2018) 438 af 6. juni 2018 om oprettelse af Connecting Europe-faciliteten og om ophævelse af forordning (EU) nr. 1316/2013 og forordning (EU) nr. 283/2014.

[9] "Network slicing" af 5G-nettet giver mulighed for en høj grad af adskillelse mellem forskellige servicelag på det samme fysiske net, og det øger muligheden for at tilbyde forskellige tjenester i hele nettet.

Kommissionen støtter fortsat en succesrig udrulning af 5G i EU, bl.a. ved at samarbejde med medlemsstaterne og interessenter om at gribe de muligheder, 5G-teknologien giver. Der vil blive taget behørigt hensyn til relevante sundhedsaspekter med udgangspunkt i forsigtighedsprincippet[11] og i samarbejde med relevante internationale organisationer og det videnskabelige samfund.

3. EU's koordinerede risikovurdering om cybersikkerhed i 5G-net

I forbindelse med arbejdet i NIS[12]-samarbejdsgruppen afsluttede hver medlemsstat sin nationale risikovurdering af sin egen 5G-netinfrastuktur og videresendte resultaterne til Kommissionen og ENISA, Den Europæiske Unions Agentur for Cybersikkerhed, i starten af juli 2019.

Den 9. oktober 2019 offentliggjorde NIS-samarbejdsgruppen, som består af repræsentanter fra medlemsstaterne, Kommissionen og ENISA, på grundlag af de nationale risikovurderinger en rapport om EU's koordinerede risikovurdering om cybersikkerhed i 5G-net[13]. I rapporten kortlægges de vigtigste trusler og trusselsaktører, de mest følsomme aktiver, de primære sårbarheder (herunder tekniske og andre typer sårbarheder), der berører 5G-net. På baggrund heraf opstilles i rapporten også en række risikokategorier, som er af strategisk vigtighed set fra et EU-perspektiv, og de illustreres med konkrete risikoscenarier, der afspejler relevante kombinationer af forskellige parametre (sårbarheder, trusler og trusselsaktører) set i forhold til forskellige aktiver (se tillæg).

For at komplementere rapporten og som yderligere input til værktøjskassen gennemførte ENISA en målrettet kortlægning af truslerne[14], som består af en detaljeret analyse af visse tekniske aspekter, herunder især udpegning af netaktiver og trusler, der kan påvirke dem.

I rapporten om EU's koordinerede risikovurdering understreges en række aspekter af betydning for 5G-net. Der er tale om følgende:

a) De teknologiske ændringer, som 5G medfører, vil øge den overordnede eksponering for angreb og antallet af mulige indgange for angribere:

- Forbedret funktionalitet i udkanten af nettet og en mindre centraliseret arkitektur end i tidligere generationer af mobilnet medfører, at visse funktioner i kernenettene kan integreres i andre dele af nettene, hvilket gør det tilsvarende udstyr mere følsomt (f. eks. basisstationer eller netforvaltnings- og netstyringsfunktioner (MANO-funktioner))

- Da software spiller en større rolle i 5G-udstyr, er der en større risiko forbundet med softwareudviklings- og -opdateringsprocesserne, og det skaber nye risici for

[10] "Edge computing" er en form for distribueret databehandling, der bringer databehandling og dataopbevaring tættere på det sted, hvor der er behov for dem, hvilket forbedrer svartiderne og sparer båndbredde.
[11] Rådets henstilling af 12. juli 1999 om begrænsning af befolkningens eksponering for elektromagnetiske felter (0 Hz-300 GHz)(1999/519/EF).
[12] 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 (NIS-direktivet). NIS-samarbejdsgruppen blev oprettet ved NIS-direktivet for at sikre strategisk samarbejde og udveksling af oplysninger om cybersikkerhed mellem medlemsstaterne.
[13] https://ec.europa.eu/digital-single-market/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security
[14] ENISA Threat landscape for 5G networks: https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks.

konfigurationsfejl og betyder, at de valg, der træffes af den enkelte mobilnetoperatør i nettets udrulningsfase, bliver et vigtigere element i sikkerhedsanalysen.

b) De nye teknologiske egenskaber gør mobilnetoperatører mere afhængige af tredjepartsleverandører, som kommer til at spille en vigtigere rolle i 5G-forsyningskæden.

Dette vil så øge antallet af angrebsveje, som trusselsaktører kan udnytte, herunder især statslige eller statsstøttede aktører fra tredjelande, på grund af deres kapacitet (hensigt og ressourcer) til at gennemføre angreb på EU-medlemsstaters telekommunikationsnet samt de eventuelle alvorlige konsekvenser af sådanne angreb.

Som følge af den øgede eksponering for angreb på grund af samarbejdet med tredjepartsleverandører vil leverandørernes individuelle risikoprofil blive af allerstørste vigtighed, især hvis en leverandør er meget brugt i visse net eller områder.

c) Stor afhængighed af en enkelt leverandør øger eksponeringen for og følgerne af et eventuelt svigt hos denne leverandør. Den forværrer også de potentielle følger af svagheder eller sårbarheder og af, at disse kan udnyttes af trusselsaktører, navnlig når afhængigheden vedrører en leverandør, der udgør en høj risiko.

d) Hvis nogle af de nye anvendelsesmuligheder, der er påtænkt for 5G-net, bliver ført ud i livet, vil 5G-net blive en væsentlig del af forsyningskæden for mange kritiske IT-applikationer, og derfor er det ikke kun kravene om fortrolighed og beskyttelse af privatlivets fred, der påvirkes, men også nettenes integritet og tilgængelighed, der bliver et særlig vigtigt nationalt sikkerhedsanliggende og en stor sikkerhedsmæssig udfordring set ud fra et EU-perspektiv.

Kilde: EU's koordinerede risikovurdering

I rapporten om EU's koordinerede risikovurdering konkluderes det endvidere, at disse udfordringer danner grundlag for et nyt sikkerhedsparadigme, at de gør det nødvendigt at revurdere den nuværende politiske og sikkerhedsmæssige ramme for 5G-sektoren og dens økosystem, og at det bliver af allerstørste vigtighed, at medlemsstaterne træffer de nødvendige risikobegrænsende foranstaltninger.

Vi har brug for en samlet tilgang for at kunne håndtere de konstaterede risici på en effektiv måde og styrke 5G-nettenes sikkerhed og modstandsdygtighed, og det kræver, at der indføres en række nøgleforanstaltninger samt tilknyttede støttetiltag, som samtidig kan nedbringe risiciene. På grundlag af EU's koordinerede risikovurdering blev der udvalgt en række risikobegrænsende foranstaltninger, som kan anvendes på nationalt og europæisk plan.

Rådets konklusioner af 3. december 2019 støttede resultaterne af den koordinerede risikovurdering og understregede "betydningen af en koordineret tilgang og effektiv gennemførelse af henstillingen for at undgå opsplitning af det indre marked"[15]. Med henblik herpå opfordrede Rådet medlemsstaterne, Kommissionen og ENISA til "at træffe alle nødvendige foranstaltninger inden for deres beføjelser til at garantere sikkerheden og sikre integriteten af elektroniske kommunikationsnet, navnlig 5G-net, og fortsætte konsolideringen

[15] Rådets konklusioner om betydningen af 5G for den europæiske økonomi og behovet for at afbøde de sikkerhedsrisici, der er forbundet med 5G. 3. december 2019, 14517/19 https://data.consilium.europa.eu/doc/document/ST-14517-2019-INIT/da/pdf.

af en koordineret tilgang til tackling af de sikkerhedsudfordringer, der er forbundet med 5G-teknologier".

4. EU-værktøjskassen til cybersikkerhed i 5G-net

Den 29. januar 2020 offentliggjorde NIS-samarbejdsgruppen en EU-værktøjskasse med risikobegrænsende foranstaltninger[16]. Den omhandler alle de risici, der er blevet identificeret i den koordinerede risikovurderingsrapport.

EU-værktøjskassen indeholder og beskriver en række strategiske og tekniske foranstaltninger samt tilknyttede støttetiltag til understøttelse af deres effektivitet, som kan indføres for at afbøde de konstaterede risici. **Strategiske foranstaltninger** omfatter foranstaltninger som øgede reguleringsbeføjelser til myndighederne, således at de kan føre nøje kontrol med netudbud og -udrulning, specifikke foranstaltninger til at imødegå risici ved ikketekniske sårbarheder samt mulige initiativer til at fremme en bæredygtig og diversificeret 5G-forsynings- og -værdikæde med henblik på at undgå langsigtede systemiske afhængighedsrisici. **Tekniske foranstaltninger** omfatter foranstaltninger til at styrke sikkerheden i 5G-net og -udstyr ved at afbøde de risici, der hidrører fra teknologier, processer, menneskelige og fysiske faktorer. Endvidere indeholder værktøjskassen for hvert af risikoområderne i EU's koordinerede risikovurdering **risikobegrænsningsplaner**, der er baseret på de mest effektive foranstaltninger.

Ifølge de konklusioner om EU-værktøjskassen, der er vedtaget af NIS-samarbejdsgruppen, anbefales det, at medlemsstaterne og Kommissionen indfører en række **nøgleforanstaltninger**:

Konklusioner om EU-værktøjskassen

I EU-værktøjskassen fastsættes en række foranstaltninger og tiltag, som – hvis de gennemføres effektivt og kombineres på passende vis – danner grundlag for en samordnet tilgang på området. Eftersom der er identificeret en bred vifte af risikoområder i EU's koordinerede risikovurdering, og de er så forskellige af natur, er der ikke nogen enkeltstående foranstaltning, der vil være tilstrækkelig. I stedet vil der være behov for, at der anvendes en række foranstaltninger i en hensigtsmæssig kombination for at dække alle centrale risikoområder.

På grundlag af vurderingen af mulige risikobegrænsningsplaner og identificeringen af de mest effektive foranstaltninger anbefales det, at:

1. Alle medlemsstater bør sikre, at de har indført foranstaltninger (herunder beføjelser til nationale myndigheder) til at reagere hensigtsmæssigt og forholdsmæssigt på kendte og fremtidige risici, og de bør navnlig sikre, at de ud fra en risikobaseret tilgang er i stand til at indføre forbud mod og/eller fastsætte begrænsninger, specifikke krav eller betingelser for levering, udrulning og drift af 5G-netudstyr på grundlag af en række sikkerhedsovervejelser.

De bør især:

- *Styrke sikkerhedskravene til mobilnetoperatører (f.eks. i form af streng adgangskontrol, indførelse af regler om sikker drift og overvågning, begrænsninger på outsourcing af specifikke funktioner osv.)*

[16] Cybersikkerhed i 5G-net - En EU-værktøjskasse med risikobegrænsende foranstaltninger af 29. januar 2020. https://ec.europa.eu/digital-single-market/en/nis-cooperation-group.

- *Vurdere leverandørernes risikoprofil, og som følge heraf **anvende relevante restriktioner over for leverandører, der anses for at udgøre en høj risiko, og f.eks. — for på effektiv vis at begrænse risici — udelukke dem fra at levere centrale aktiver**, der er udpeget som kritiske og følsomme i EU's koordinerede risikovurdering (f.eks. kernenetfunktioner, netforvaltnings- og netstyringsfunktioner (MANO-funktioner) og adgangsnetfunktioner)*

- *Sikre, at hver operatør har en passende strategi med flere leverandører for at **undgå eller begrænse enhver væsentlig afhængighed** af en enkelt leverandør (eller leverandører med en tilsvarende risikoprofil), sikre en passende balance mellem leverandører på nationalt plan og **undgå at blive afhængig af leverandører, der vurderes at udgøre en høj risiko**. Dette kræver også, at man undgår at låse sig fast til en enkelt leverandør, bl.a. ved at fremme større interoperabilitet af udstyr.*

2. Europa-Kommissionen bør sammen med medlemsstaterne bidrage til at:

- *Bevare en **diversificeret og bæredygtig 5G-forsyningskæde** for at undgå afhængighed på lang sigt, bl.a. ved at:*

  - *udnytte de eksisterende EU-værktøjer og -instrumenter fuldt ud, navnlig ved screening af potentielle **direkte udenlandske investeringer**, der påvirker centrale 5G-aktiver, og ved at undgå **forvridning** på 5G-forsyningsmarkedet som følge af eventuel prisdumping eller subsidiering samt*

  - *styrke **EU's kapacitet inden for 5G- og post-5G-teknologier** yderligere ved hjælp af relevante EU-programmer og -finansiering.*

- *Fremme koordineringen mellem medlemsstaterne inden for **standardisering** for at nå specifikke sikkerhedsmål og udvikle **relevante certificeringsordninger i hele EU** med henblik på at fremme produkter og processer, der er mere sikre.*

3. For at sikre at den koordinerede tilgang forbliver relevant, bør NIS-samarbejdsgruppens mandat forlænges og udvides til også at omfatte samarbejde med andre relevante organer og enheder med henblik på:

- *regelmæssigt at tage **de nationale risikovurderinger og EU's risikovurdering** af sikkerheden i 5G-net og post-5G-net op til revurdering med støtte fra Kommissionen og ENISA, og yderligere udvikle og harmonisere den vurderingsmetode, der følges, samt tilpasse den til udviklingen i 5G-teknologien*

- *at gennemføre en detaljeret og regelmæssig **opfølgning på og evaluering af indførelsen** af værktøjskassen på grundlag af en struktureret rapportering fra medlemsstaterne*

- *at samordne og understøtte gennemførelsen af **støttetiltag**, som kræver samarbejde på EU-plan, navnlig i form af udarbejdelse af retningslinjer og udveksling af bedste praksis inden for de forskellige foranstaltninger*

- *at understøtte eventuel yderligere samordning på EU-niveau, hvor det er hensigtsmæssigt, navnlig med henblik på at fremme yderligere konvergens **inden for tekniske og organisatoriske sikkerhedskrav til netoperatører.***

Kilde: EU-værktøjskassen.

Konklusionerne om værkstøjskassen viser medlemsstaternes stærke vilje til i fællesskab at reagere på de sikkerhedsmæssige udfordringer ved 5G-net. Dette er af afgørende betydning for sikkerheden i medlemsstaterne, i hele EU, for de nationale økonomier samt for EU's indre marked og Europas teknologiske suverænitet. Både EU's koordinerede risikovurdering og EU-værktøjskassen afspejler, hvor høj værdi det kollektive arbejde i NIS-samarbejdsgruppen

har, og hvor intensivt samarbejdet mellem alle repræsentanter fra medlemsstaterne, Kommissionen og ENISA er.

Værktøjskassen giver mulighed for en fælles EU-tilgang til 5G-cybersikkerhed, der sikrer sammenhæng på tværs af det indre marked ved hjælp af EU-politikker og samordning samt medlemsstaternes udøvelse af nationale sikkerhedskompetencer. Værktøjskassens risikobegrænsende foranstaltninger og risikobegrænsningsplaner muliggør en passende, effektiv og forholdsmæssig reaktion fra EU på fælles udfordringer i forbindelse med cybersikkerhed i 5G-net.

Kommissionen glæder sig over offentliggørelsen af EU-værktøjskassen til cybersikkerhed i 5G-net og støtter fuldt ud alle dens ovennævnte konklusioner.

Kommissionen opfordrer medlemsstaterne og relevante EU-institutioner, agenturer og andre organer til at:

i) sikre en hurtig gennemførelse af effektive og passende risikobegrænsningsstrategier i hele EU i tråd med EU-værktøjskassen

ii) tage alle nødvendige skridt til at sikre koordinering på EU-plan, bl.a. gennem fortsat arbejde i NIS-samarbejdsgruppen og ved at indføre en robust mekanisme til at kontrollere anvendelsen af EU-værktøjskassen, så der kan sikres effektive foranstaltninger og et velfungerende indre marked.

5. Anvendelse af værktøjskassen

Medlemsstaternes vilje til at gøre fuld brug af værktøjskassen er en væsentlig forudsætning for en troværdig og vellykket europæisk tilgang til 5G-sikkerhed. Det er medlemsstaterne, der afgør, om en bestemt foranstaltning passer til de nationale omstændigheder, men det er absolut nødvendigt, at **der indføres en række nøgleforanstaltninger, som anbefalet af NIS-samarbejdsgruppen (se konklusionerne om værktøjskassen ovenfor), i hver medlemsstat, og at nogle indføres på EU-plan**, således at vi kan afbøde de risici, der er konstateret.

Kommissionen er rede til fortsat at yde sin fulde støtte i de næste faser, og den opfordrer medlemsstaterne til:

- **inden 30. april 2020** at tage konkrete og målbare skridt til at gennemføre en række nøgleforanstaltninger som anbefalet i konklusionerne om EU-værktøjskassen

- **inden 30. juni 2020** at forberede en rapport fra NIS-samarbejdsgruppen, der gør status over gennemførelsen i hver medlemsstat af nøgleforanstaltningerne på grundlag af den regelmæssige overvågning og rapportering, der allerede gennemføres via NIS-samarbejdsgruppen, med støtte fra Kommissionen og ENISA.

5.1. En risikobaseret fælles tilgang til 5G-leverandører

På baggrund af det endelig mål om at sikre 5G-nettenes sikkerhed, modstandsdygtighed og bæredygtighed er medlemsstaterne nået til enighed om, at det er nødvendigt at vurdere de enkelte leverandørers risikoprofil og på grundlag heraf pålægge leverandører, der anses for at udgøre en høj risiko, relevante restriktioner, bl.a. ved om nødvendigt at udelukke dem for

effektivt at afbøde risici for centrale aktiver som angivet i værktøjskassen. Kommissionen er rede til at støtte medlemsstaterne i gennemførelsen af disse foranstaltninger.

For at støtte gennemførelsen af foranstaltningerne i hele EU er der i EU's koordinerede risikovurdering og i EU-værktøjskassen vejledning at hente til 1) vurdering af leverandørernes risikoprofil[17] og 2) netelementer og -funktioners[18] samt andre aktivers følsomhed. Både foranstaltningerne i EU's koordinerede risikovurdering og i værkstøjskassen omfatter risici forbundet med leverandører af 5G-netværksudstyr og -nettjenester. De omfatter ikke andre varer eller tjenester, som disse eller andre leverandører måtte levere.

Som det fremgår af i afsnit 2.37 i EU's koordinerede risikovurdering, kan individuelle leverandørers risikoprofiler vurderes på grundlag af flere forskellige faktorer.

Vurderingen af leverandørernes risikoprofiler bør udelukkende foretages af sikkerhedsmæssige årsager og på grundlag af objektive kriterier. For at lette en samordnet tilgang til gennemførelsen af disse foranstaltninger anbefales det i værktøjskassen, at medlemsstaterne udveksler oplysninger om nationale tilgange og bedste praksis. Det er endvidere Kommissionens opfattelse, at dette bør være en af de første prioriteter i næste fase af arbejdet i NIS-samarbejdsgruppen i samarbejde med Kommissionen og ENISA.

Det er vigtigt, at alle restriktioner over for leverandør, der anses for at udgøre en høj risiko, herunder nødvendige udelukkelser for effektivt at afbøde risici samt foranstaltninger til at undgå afhængighed af sådanne leverandører, træffes rettidigt. Det vil øge forudsigeligheden for markedsoperatørerne, hvis dette gøres tidligst muligt, herunder så vidt muligt i forbindelse med procedurerne for tildeling af 5G-tilladelser, og dermed bidrage til en hurtig udrulning af 5G-net og garantere 5G-nettenes sikkerhed på lang sigt og 5G-forsyningskædens modstandsdygtighed.

Imidlertid kan den nationale gennemførelse af disse foranstaltninger, hvor det er nødvendigt og berettiget, give anledning til forskellige frister, navnlig i situationer, hvor man i høj grad er afhængig af udstyr og tjenester fra en leverandør, der anses for at udgøre en høj risiko (f.eks. fordi der skal tages hensyn til cyklussen for opgradering af udstyr og migrationen fra "ikkeselvstændige" til "selvstændige" 5G-net). Medlemsstaterne kan overveje at fastlægge gennemførelsesplaner, der omfatter passende overgangsperioder for de berørte netoperatører. I den forbindelse bør overgangsperioder fastlægges på en sådan måde, at incitamenterne til at investere i moderne netudstyr bevares eller sågar styrkes, f.eks. ved at man fremskynder udrulningen af fuldt udviklede ("selvstændige") 5G-kernenet eller erstatter eksisterende 4G-udstyr i andre dele af nettet (f.eks. i radioadgangsnettet), jf. målene i 5G-handlingsplanen[19].

Ydermere kan teleoperatører på grund af kompleksiteten i 5G-softwarebaserede net i stigende grad overlade til tredjeparter at udføre visse opgaver, som f.eks. vedligeholdelse og opgradering af 5G-net og -software såvel som andre outsourcede tjenester, ud over levering af netudstyr. Som beskrevet i EU's koordinerede risikovurdering er dette en kilde til en alvorlig sikkerhedsrisiko. Der bør derfor lægges særlig vægt på dette aspekt. Det er afgørende, at der

[17] Afsnit 2.37 i EU's koordinerede risikovurdering.

[18] Af afsnit 2.21 i EU's koordinerede risikovurdering fremgår hovedkategorierne af elementer og funktioner og deres overordnede følsomhedsniveau sammen med en liste over centrale elementer, der er udpeget af medlemsstaterne for hver kategori, og i afsnit 2.28 og 2.29 anføres en række andre typer følsomme aktiver og områder (f.eks. specifikke enheder og geografiske områder).

[19] COM(2016) 588 af 14. juni 2016 om 5G til Europa: En handlingsplan.

også gennemføres en grundig sikkerhedsvurdering af risikoprofilen for de leverandører, der har til opgave at levere bemeldte tjenester, især når opgaverne ikke udføres i EU. Der bør træffes passende foranstaltninger for at bevare 5G-infrastrukturens langsigtede integritet, bl.a. ved at indføre begrænsninger for særligt følsomme dele af 5G-nettet eller om nødvendigt udelukke højrisikoenheder herfra i overensstemmelse med de risikobegrænsende foranstaltninger i værktøjskassen.

5.2. Kommissionens bidrag til anvendelsen af værktøjskassen

Kommissionen vil fortsat støtte gennemførelsen af EU's tilgang til cybersikkerhed i 5G-net generelt samt igangsætte specifikke initiativer i forbindelse med værktøjskassens foranstaltninger og målsætninger, hvor det kan tilføre værdi. Kommissionen vil udnytte alle sine beføjelser og relevante instrumenter fuldt ud, hvor det er nødvendigt for at afbøde risikoen ved de identificerede sikkerhedsproblemer. Derved og ved at handle sammen med medlemsstaterne og den private sektor søger Kommissionen at understøtte strategiske tiltag, der skal bidrage til at sikre EU teknologisk uafhængighed og lederskab inden for den fremtidige udvikling af netteknologier, cybersikkerhedsteknologier og alle de relevante byggesten, som hele vores økonomi og sikkerhed er baseret på.

Kommissionen vil mere specifikt foretage sig følgende for at sikre indførelsen af de tilsvarende risikobegrænsende foranstaltninger i værktøjskassen på de områder, hvor den har beføjelser:

Sikring af cybersikkerheden i 5G-net og en diversificeret 5G-forsyningskæde:

-**Cybersikkerhedssamarbejde**: Fortsat yde støtte til medlemsstaterne med henblik på effektiv, samordnet og rettidig gennemførelse af nationale foranstaltninger via NIS-samarbejdsgruppen.

- **Telekommunikations- og cybersikkerhedsregler**: Yde støtte til gennemførelse af de 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 af 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.

- **Standardisering**: Træffe foranstaltninger for at bidrage til at bevare og - hvor nødvendigt - øge europæisk deltagelse i de respektive standardiseringsorganer med henblik på at nå Europas sikkerheds- og interoperabilitetsmål. Kommissionen vil sammen med medlemsstaterne især vurdere og fremme de tekniske specifikationer og standarder, der giver mulighed for interoperabilitet mellem leverandører af 5G-udstyr i forskellige dele af nettet, herunder også i gamle net, så der de facto kan opnås et miljø med flere leverandører, eksempelvis gennem åbne og interoperable grænseflader.

- **Certificering**: Støtte udviklingen af 5G-certificeringsordninger, der tager højde for behovene i 5G-net, under den europæiske ramme for cybersikkerhedscertificering.

- **Screening af direkte udenlandske investeringer (FDI)**: Støtte gennemførelsen af den europæiske screeningsramme ved at kortlægge 5G-værdikæden, bl.a. følsomme netaktiver, og regelmæssig overvågning af FDI'er i hele værdikæden. I overensstemmelse med tidsplanen

for screening af FDI'er (fra oktober 2020) vil Kommissionen undersøge udenlandske investeringer i 5G-området ud fra de retningslinjer, der fremgår af forordning (EU) 2019/452, og under hensyntagen til EU's koordinerede risikovurdering og EU-værktøjskassen.

- Handelspolitiske beskyttelsesinstrumenter: Overvåge alle relevante markedstendenser i EU og i tredjelande og beskytte EU-aktører på det europæiske 5G-marked med handelspolitiske beskyttelsesforanstaltninger for at imødegå potentiel handelsforvridende praksis (prisdumping eller subsidiering), bl.a. ved at igangsætte foreløbige undersøgelser, hvor det er relevant.

- Konkurrenceregler: Overvåge at markederne for levering af 5G-hardware og -software fungerer ordentligt, så det kan sikres, at markederne er konkurrenceprægede, og at der ikke opstår kontraktmæssige eller tekniske situationer, hvor man er "fastlåst".

- **EU-finansieringsprogrammer**: Sikre at deltagelse i EU's finansieringsprogrammer på relevante teknologiområder er betinget af overholdelse af sikkerhedskravene derved, at der gøres fuld brug af og yderligere indarbejdes sikkerhedsbetingelser i FoI-programmer, herunder navnlig Horisont Europa, programmet for et digitalt Europa og Connecting Europe-faciliteten 2, i de europæiske struktur- og investeringsfonde og i andre relevante programmer. Der bør også anlægges en lignende tilgang i EU's eksterne finansieringsprogrammer og finansielle instrumenter, herunder for så vidt angår finansiering via internationale finansielle institutioner.

- Offentlige udbud: Udnytte offentlige udbud af 5G-net til at støtte de udpegede mål for 5G-nets sikkerhed, leverandørdiversificering og langsigtede bæredygtighed, herunder især søge at sikre tilstrækkelig hensyntagen til sikkerhedsaspekter i forbindelse med tildeling af offentlige udbudsaftaler på 5G-området, i overensstemmelse med EU's regler om offentlige udbud.

- Beredskabs- og krisestyring og cybersikkerhedsøvelser: Gøre fuld brug af EU's plan[20] for en koordineret reaktion på væsentlige cybersikkerhedshændelser. Sammen med ENISA overveje muligheden for at gennemføre en 5G-cybersikkerhedsøvelse så snart markedet er modent nok til det.

Og under det ansvarsområde, der hører under Unionens højtstående repræsentant for udenrigsanliggender og sikkerhedspolitik og Rådet:

- **Ramme for EU's fælles diplomatiske reaktion på ondsindede cyberaktiviteter ("cyberdiplomatisk værktøjskasse")[21]**: I tilfælde af ondsindede cyberaktiviteter, der truer EU's integritet og sikkerhed, opfordres medlemsstaterne til at anvende relevante fælles udenrigs- og sikkerhedspolitiske foranstaltninger, der udgør en del af EU's cyberdiplomatiske værktøjskasse (herunder om nødvendigt restriktive foranstaltninger), til at fremme samarbejde, lette afværgelse af trusler og påvirke eventuelle aggressorers adfærd.

Endvidere vil en række programmer bidrage til målet om at undgå eller begrænse risikoen for afhængighed på lang sigt ved at fremme et diversificeret og bæredygtigt marked for 5G, bl.a. ved at bevare EU's kapaciteter inden for 5G-værdikæden og ved at investere i innovation, i overensstemmelse med EU's internationale forpligtelser.

[20] Kommissionens henstilling om en koordineret reaktion på væsentlige cybersikkerhedshændelser og -kriser (EU 2017/1584).

[21] Rådets konklusioner 9916/17 af 20. november 2017

Fremme innovation og investering i cybersikkerhed og netværksinfrastrukturteknologier:

- EU-finansierings**programmer**: Øge investeringerne i forskning, udvikling og udrulning af netteknologier og relevante underliggende byggesten. Kommissionen har fremsat forslag om at investere nær ved 3 mia. EUR i cybersikkerhedsteknologier under det næste EU-budget 2021-27. Det omfatter forskning og innovation under Horisont Europa og støtte til cybersikkerhedskapaciteter i forbindelse med programmet for et digitalt Europa. InvestEU kan også yde finansiel støtte til forskning og udvikling på 5G-området samt til udrulning af 5G-net.

Endvidere har Kommissionen i forbindelse med det næste Horisont Europa-program[22] foreslået at oprette et institutionaliseret EU-partnerskab om næstegenerationsinternet/6G ("intelligente netværk og tjenester") i partnerskab med branchen og koordineret med medlemsstaterne med henblik på at udrulle 5G og hovedsagelig **forberede 6G**, næste generation af mobilteknologi. Der er fremsat forslag om at afsætte mere end 2,5 mia. EUR i EU-investeringer i EU's budget (2021-2027), som skal følges op af mindst 7,5 mia. EUR i private investeringer under dette initiativ.

- Industriel udvikling og udrulning: Identificere eventuelle huller eller svigt i markedet langs 5G-værdikæden, som kan berettige målrettede indgreb i forbindelse med det næste langsigtede budget eller et muligt vigtigt projekt af fælleseuropæisk interesse inden for cybersikkerhed, i tråd med forummet på højt plan om vigtige projekter af fælleseuropæisk interesse. Beslutningen om at udforme og oprette vigtige projekter af fælleseuropæisk interesse ligger hos medlemsstaterne og virksomhederne. EU-reglerne stiller en ramme til rådighed, og Kommissionen er klar til at formidle de nødvendige kontakter og yde vejledning.

[22] Der kan også ydes finansiering gennem Connection Europa-faciliteten 2.0 og programmet for et digitalt Europa.

6. Konklusion

5G-net forventes at ville give Europas borgere, samfund og økonomi en bred vifte af muligheder. Det er derfor vigtigt at sikre, at 5G-nettet er sikkert og robust. Samtidig udgør cybersikkerhedstrusler (herunder risikoen for indblanding fra statslige eller statsstøttede aktører fra tredjelande) en udfordring, der vokser i takt med vores stigende afhængighed af teknologi og data. Hvis vi forsømmer cybersikkerheden, vil det underminere tilliden til udviklingen af den digitale økonomi og det digitale samfund og forhindre EU i at høste det fulde udbytte af denne udvikling. Derfor må vi reagere med en styrket indsats, der justeres i takt med udviklingen.

Det er væsentligt at EU har en samordnet og sammenhængende tilgang til cybersikkerhed for kritiske teknologier og net, så vi kan sikre vores teknologiske suverænitet og bevare og udvikle vores kapacitet på området. Kommissionen vil støtte gennemførelsen af EU's tilgang til cybersikkerhed i 5G-net fuldt ud og sikre, at EU's markeder fortsat er åbne for produkter og tjenester, der lever op til de seneste krav til cybersikkerhed og tillid.

Det er i den forbindelse vigtigt, at alle interessenters engagement i 5G-sikkerhed forbliver højt, og det vil kræve et fortsat samarbejde mellem medlemsstaterne, Kommissionen og ENISA.

Som det umiddelbart næste skridt opfordrer Kommissionen som angivet ovenfor medlemsstaterne til at handle hurtigt for på en effektiv og objektiv måde at gennemføre de foranstaltninger, der er aftalt som en del af værktøjskassen, og til at fortsætte samarbejdet med støtte fra Kommissionen og ENISA, så der sikres samordning på EU-plan. Kommissionen vil sideløbende hermed igangsætte alle relevante foranstaltninger inden for sine beføjelser for at bistå medlemsstaterne i anvendelsen af værktøjskassen og forstærke dens virkning.

Tillæg: Risikokategorier (kilde: EU's koordinerede risikovurdering).

	Risikokategori
Risikoscenarier ved utilstrækkelige sikkerhedsforanstaltninger	*R1: Fejlkonfigurering af net*
	R2: Manglende adgangskontrol
Risikoscenarier i forbindelse med 5G-forsyningskæden	*R3: Dårlig kvalitet af produkterne*
	R4: Afhængighed af en enkelt leverandør inden for de enkelte net eller mangel på diversitet på landsplan
Risikoscenarier i forbindelse med de primære trusselsaktørers modus operandi	*R5: Statslig indblanding via 5G-forsyningskæden*
	R6: Organiserede kriminelle gruppers udnyttelse af 5G-net eller angreb på slutbrugere
Risikoscenarier i forbindelse med de indbyrdes afhængigheder mellem 5G-net og andre kritiske systemer	*R7: Væsentlige forstyrrelser af kritiske infrastrukturer eller tjenester*
	R8: Massive netnedbrud som følge af afbrydelse af elforsyningen eller andre støttesystemer
Risikoscenarier vedrørende slutbrugerudstyr	*R9: Udnyttelse af tingenes internet (IoT)*