Cybersikkerhed i 5G-net EU-værktøjskasse med risikobegrænsende

CG-publikation

01/2020

NIS COOPERATION GROUP

Indholdsfortegnelse

1. Indledning

5G-net kommer til at spille en central rolle i forbindelse med den digitale omstilling af EU's økonomi og samfund. 5G-net kan potentielt muliggøre og støtte en bred vifte af applikationer og funktioner, der går langt videre end levering af mobile kommunikationstjenester mellem slutbrugere. I en situation, hvor indtægterne fra 5G på globalt plan anslås at nå op på 225 mia. EUR i 2025[1], vil 5G-teknologier og -tjenester være et vigtigt aktiv for Europa for at kunne konkurrere på det globale marked.

Cybersikkerheden i forbindelse med 5G-net er derfor afgørende for at beskytte vores økonomier og samfund og for at udnytte det fulde potentiale af de vigtige muligheder, de tilbyder. Den er også afgørende for at sikre EU's teknologiske suverænitet.

Som svar på Det Europæiske Råds opfordring til en fælles tilgang til sikkerheden i 5G-net den 22. marts 2019 vedtog Europa-Kommissionen sin henstilling om cybersikkerhed i forbindelse med 5G-net (herefter "henstillingen") den 26. marts 2019. 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.

Hver medlemsstat afsluttede sin nationale risikovurdering af sin egen 5G-netinfrastruktur og fremsendte resultaterne til Kommissionen og ENISA, Den Europæiske Unions Agentur for Cybersikkerhed.

På grundlag af disse nationale risikovurderinger offentliggjorde medlemsstaterne med støtte fra ENISA og Kommissionen den 9. oktober 2019 en rapport om EU's koordinerede risikovurdering om cybersikkerhed i 5G-net[2]. I denne rapport kortlægges de vigtigste trusler og trusselsaktører, de mest følsomme aktiver, de primære sårbarheder (herunder tekniske og andre typer sårbarheder som f.eks. de retlige og politiske rammer, som udbydere af informations- og kommunikationsteknologi og udstyr kan være omfattet af i tredjelande) og de primære risici, der er forbundet hermed. For at komplementere rapporten og som yderligere input til værktøjskassen gennemførte ENISA en målrettet kortlægning af truslerne[3], som består af en detaljeret analyse af visse tekniske aspekter, herunder især udpegning af netaktiver og trusler, der kan påvirke dem.

Rådet godkendte i sine konklusioner af 3. december 2019 arbejdet i medlemsstaternes samarbejdsgruppe for net- og informationssystemer (NIS-samarbejdsgruppen) og støttede resultaterne af den koordinerede risikovurdering. Rådet så navnlig med tilfredshed på "de igangværende fælles europæiske bestræbelser på at beskytte sikkerheden i forbindelse med 5G-nettene, der navnlig er baseret på Kommissionens henstilling om cybersikkerhed i forbindelse med 5G-net", og understregede "betydningen af en koordineret tilgang og effektiv gennemførelse af henstillingen for at undgå opsplitning af det indre marked". 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,

[1] Prognose fra ABI Research: https://www.abiresearch.com/press/abi-research-projects-5g-worldwide-service-revenue.

[2] https://ec.europa.eu/digital-single-market/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security.

[3] ENISA Threat landscape for 5G networks: https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks.

navnlig 5G-net, og fortsætte konsolideringen af en koordineret tilgang til tackling af de sikkerhedsudfordringer, der er forbundet med 5G-teknologier". [4]

I rapporten om EU's koordinerede risikovurdering understreges en række vigtige sikkerhedsudfordringer, som sandsynligvis vil opstå eller blive mere fremtrædende i 5G-net. Disse sikkerhedsmæssige udfordringer er hovedsagelig knyttet til:

- de voksende sikkerhedsproblemer i forbindelse med 5G-nettenes integritet og tilgængelighed, foruden fortrolighed og privatlivets fred

- centrale nyskabelser inden for 5G-teknologien (som også vil medføre en række specifikke sikkerhedsforbedringer), navnlig den stadig større betydning af software og den brede vifte af tjenester og applikationer, der muliggøres af 5G-net, og

- leverandørernes rolle i forbindelse med opbygning og drift af 5G-net, kompleksiteten af interaktionen mellem leverandører og operatører og graden af afhængighed af de enkelte leverandører.

I rapporten 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 sektoren og dens økosystem, og at det bliver af allerstørste vigtighed, at medlemsstaterne træffer de nødvendige risikobegrænsende foranstaltninger.

På grundlag af rapporten om EU's koordinerede risikovurdering er der udvalgt en række risikobegrænsende foranstaltninger, som kan anvendes på nationalt og europæisk plan.

2. Formålet med værktøjskassen

Formålet med denne værktøjskasse er at identificere et muligt fælles sæt foranstaltninger, som kan afbøde de største cybersikkerhedsrisici ved 5G-net, som de er blevet identificeret i rapporten om EU's koordinerede risikovurdering, og at give vejledning i, hvordan de foranstaltninger, der bør prioriteres i afbødningsplaner på nationalt plan og EU-plan, udvælges. Dette gøres for at skabe en robust ramme af foranstaltninger, som kan sikre et tilstrækkeligt niveau af cybersikkerhed i 5G-net på tværs af EU og sikre koordinerede tilgange blandt medlemsstaterne.

I EU's koordinerede risikovurdering identificeres en række kategorier af risici, som har strategisk betydning set fra et EU-perspektiv, og de illustreres af konkrete risikoscenarier. Disse afspejler relevante kombinationer af sårbarheder, trusler og trusselsaktører og de identificerede aktiver.

[4] Rådets konklusioner om betydningen af 5G for den europæiske økonomi og behovet for at afbøde de sikkerhedsrisici, der er forbundet med 5G, 3.12.2019 (14517/19 https://www.consilium.europa.eu/media/41595/st14517-en19.pdf).

Tabel 1 – Risikokategorier og -scenarier

(kilde: rapporten om EU's koordinerede risikovurdering)

I – Risikoscenarier ved utilstrækkelige sikkerhedsforanstaltninger	**R1 –** Fejlkonfigurering af net **R2 –** Manglende adgangskontrol
II – Risikoscenarier i forbindelse med 5G-forsyningskæden	**R3 –** Dårlig kvalitet af produkterne **R4 –** Afhængighed af en enkelt leverandør inden for de enkelte net eller manglende diversificering på landsplan
III – 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
IV – 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
V – Risikoscenarier vedrørende slutbrugerudstyr	**R9 –** Udnyttelse af tingenes internet (IoT), håndsæt eller intelligente enheder

For at kunne håndtere de konstaterede risici på en effektiv måde og styrke 5G-nettenes sikkerhed og modstandsdygtighed er der brug for en samlet tilgang. Dette kræver, at der indføres en række nøgleforanstaltninger samt tilknyttede støttetiltag, som samtidig kan nedbringe risiciene. Nøglen til at sikre koordinerede tilgange blandt medlemsstaterne vil være den effektive gennemførelse af risikoafbødningsforanstaltninger og -tiltag i alle medlemsstater, som er tilpasset situationen i hver medlemsstat.

Denne værktøjskasse indeholder også en vejledende vurdering af foranstaltninger, som kræver eller bliver bedre af en fælles tilgang og/eller en form for koordinering på EU-plan, eller som bedst gennemføres i samarbejde med andre medlemsstater eller af individuelle medlemsstater, afhængigt af den specifikke nationale kontekst.

De foranstaltninger, der præsenteres i denne værktøjskasse, bidrager samlet set til at nå en række vigtige og gensidigt forstærkende sikkerhedsmål, som er relevante for at håndtere de risici, der er identificeret i risikovurderingsrapporten, og som beskytter 5G-nettenes fortrolighed, integritet og tilgængelighed:

- styrke sikkerheden i forbindelse med design, udrulning og drift af net
- hæve de grundlæggende sikkerhedsstandarder for produkt- og tjenesteydelsessikkerhed
- minimere eksponeringen for risici, der udspringer af individuelle leverandørers risikoprofil

- undgå eller begrænse stor afhængighed af en enkelt leverandør af 5G-net og
- fremme et diversificeret, konkurrencedygtigt og bæredygtigt marked for 5G-udstyr, herunder ved at opretholde EU's kapacitet inden for 5G-værdikæden.

De identificerede foranstaltninger præsenteres i *afsnit 4* i denne rapport og i yderligere detaljer i de vedlagte tabeller.

3. Eksisterende rammer og foranstaltninger

Dette afsnit har til formål at kortlægge og beskrive de relevante eksisterende lovgivningsmæssige rammer og instrumenter og de foranstaltninger og begrænsninger, der allerede findes, således at de kan tages i betragtning i forbindelse med opstillingen af planer for risikobegrænsning og eventuelt også ved indførelsen af nye foranstaltninger.

3.1. Instrumenter på EU-plan

3.1.1 EU's vigtigste lovgivningsmæssige rammer

EU anvender en række instrumenter til at beskytte elektroniske kommunikationsnet, herunder EU's telekommunikationsramme[5], NIS-direktivet (direktivet om sikkerhed for net- og informationssystemer)[6] og forordningen om cybersikkerhed[78].

Inden for EU's telekommunikationsramme kan telekommunikationsoperatørerne pålægges forpligtelser af de medlemsstater, hvori de udbyder tjenester. Medlemsstaterne skal sikre, at de offentlige kommunikationsnets integritet og sikkerhed opretholdes, og at de virksomheder, der udbyder offentlige kommunikationsnet eller offentligt tilgængelige elektroniske kommunikationstjenester, træffer tekniske og organisatoriske foranstaltninger for på passende vis at styre risiciene for sikkerheden i deres net og tjenester[9]. Reglerne fastsætter desuden, at de kompetente nationale tilsynsmyndigheder skal have en række beføjelser til at udstede bindende instruktioner og sikre overholdelse af disse. Inden for rammerne af direktiv 2002/20/EF[10] kan medlemsstaterne desuden knytte vilkår vedrørende sikring af offentlige net mod ulovlig adgang i

[5] Direktiv 2002/21/EF som ændret ved direktiv 2009/140/EF af 25. november 2009 om fælles rammebestemmelser for elektroniske kommunikationsnet og -tjenester og direktiv 2018/1972 af 11. december 2018 om oprettelse af en europæisk kodeks for elektronisk kommunikation.

[6] Direktiv (EU) 2016/1148 af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen.

[7] Forordning (EU) 2019/881 af 17. april 2019 om ENISA (Den Europæiske Unions Agentur for Cybersikkerhed), om cybersikkerhedscertificering af informations- og kommunikationsteknologi.

[8] EU har oprettet en række samarbejdsorganer med henblik på at understøtte gennemførelsen af disse forpligtelser og instrumenter. Det primære er NIS-samarbejdsgruppen, som blev oprettet ved NIS-direktivet, og som samler kompetente myndigheder for at støtte og lette samarbejdet, navnlig ved at udstikke strategiske retningslinjer. CSIRT-netværket – et netværk af nationale CSIRT'er fra medlemsstaterne – fremmer udvekslingen af operationelle oplysninger. Den Europæiske Unions Agentur for Cybersikkerhed (ENISA), Kommissionen, medlemsstaterne og de nationale tilsynsmyndigheder har udviklet tekniske retningslinjer for nationale tilsynsmyndigheder om indberetning af hændelser, sikkerhedsforanstaltninger, trusler og aktiver.

[9] Artikel 13a om sikkerhed og integritet i net og tjenester i direktiv 2002/21/EF senest ændret ved direktiv 2009/140/EF og artikel 40 og 41 i direktiv 2018/1972.

[10] Direktiv 2002/20/EF af 7. marts 2002 om tilladelser til elektroniske kommunikationsnet og -tjenester (tilladelsesdirektivet).

overensstemmelse med direktiv 2002/58/EF til generelle tilladelser med det formål at sikre kommunikationshemmeligheden[11].

Den **europæiske kodeks for elektronisk kommunikation (EECC),** som erstatter den nuværende ramme fra den 21. december 2020, opretholder den nuværende rammes sikkerhedsbestemmelser (i afsnit V, artikel 40 og 41) og indfører også definitioner af sikkerhed i net og tjenester[12] og sikkerhedshændelser. Herudover fastsættes det i den europæiske kodeks for elektronisk kommunikation, at der som led i sikkerhedsforanstaltningerne som minimum bør tages hensyn til alle relevante aspekter af visse elementer inden for f.eks. sikkerhed i net og faciliteter, håndtering af sikkerhedshændelser, styring af driftskontinuitet, monitorering, audit og testning samt overholdelse af internationale standarder[13].

Hverken den nuværende ramme eller kodeksen for elektronisk kommunikation indeholder bestemmelser, som finder direkte anvendelse på producenter af netudstyr og andre tjenesteudbydere i forsyningskæden for elektronisk kommunikation, da disse udbydere ikke er omfattet af deres anvendelsesområde.

I henhold til **NIS-direktivet** skal operatører af væsentlige tjenester på andre områder (energi, finans, sundhedspleje, transport, udbydere af digitale tjenester osv.) træffe passende sikkerhedsforanstaltninger og indberette alvorlige hændelser til den kompetente nationale myndighed. NIS-direktivet indeholder også bestemmelser om koordinering mellem medlemsstaterne i tilfælde af grænseoverskridende hændelser, der berører operatører inden for direktivets anvendelsesområde.

Forordningen om cybersikkerhed, der trådte i kraft i juni 2019, indfører en ramme for europæiske ordninger for cybersikkerhedscertificering for produkter, processer og tjenester. Når certificeringsordningerne er indført, vil det i hele EU desuden være muligt for producenterne at påvise, at de i de tidlige faser af produkternes design har medtaget særlige sikkerhedsforanstaltninger, og for brugerne at fastslå tillidsniveauet for sikkerheden. Rammen er et vigtigt støtteværktøj til at fremme et ensartet sikkerhedsniveau. Den vil give mulighed for udviklingen af ordninger for cybersikkerhedscertificering for at kunne tackle behovet hos brugerne af 5G-udstyr og -software.

3.1.2 Andre relevante instrumenter på EU-plan:

På det handelspolitiske område vil EU's **forordning om screening af udenlandske direkte investeringer**[14] fra den 11. oktober 2020 danne grundlag for at koordinere detekteringen af og imødegå potentielle sikkerhedsrisici i forbindelse med udenlandske direkte investeringer i EU inden

[11] Direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor.

[12] I artikel 2, nr. 21), defineres "sikkerhed i net og tjenester" specifikt som "elektroniske kommunikationsnets og -tjenesters evne til på et givet fortrolighedsniveau at modstå handlinger, der er til skade for tilgængeligheden, autenticiteten, integriteten eller fortroligheden af disse net og tjenester, lagrede eller overførte eller behandlede data eller de dermed forbundne tjenester, der tilbydes af eller er tilgængelige via disse elektroniske kommunikationsnet eller -tjenester".

[13] Betragtning 94: …"vedrørende nets og faciliteters sikkerhed: fysisk og miljømæssig sikkerhed, forsyningssikkerhed, kontrol af adgang til net og netintegritet; vedrørende håndtering af sikkerhedshændelser: procedurer for håndtering af sikkerhedshændelser, kapacitet til detektering af sikkerhedshændelser, underretning om og meddelelse af sikkerhedshændelser; vedrørende styring af driftskontinuitet: strategi for tjenesters kontinuitet og beredskabsplaner, katastrofeberedskabskapacitet; vedrørende monitorering, audit og testning: monitorerings- og logningspolitikker, øvelsesberedskabsplaner, testning af net og tjenester, sikkerhedsvurdering og kontrol med overholdelse; samt overholdelse af internationale standarder."

[14] Forordning (EU) 2019/452 af 19. marts 2019 om et regelsæt for screening af udenlandske direkte investeringer i Unionen.

for bl.a. følsomme områder såsom kritiske teknologier og kritisk infrastruktur. Screeningmekanismen for direkte udenlandske investeringer kan, når den anvendes på 5G-værktøjskassen med henblik på at beskytte centrale 5G-aktiver og undgå afhængighed, være et vigtigt instrument til regelmæssig og bedre overvågning af udviklingen i udenlandske direkte investeringer i EU i 5G-værdikæden. Hvis specifikke tendenser i udenlandske direkte investeringer falder ind under forordningens anvendelsesområde, kan disse imødegås, og medlemsstaterne kan iværksætte hensigtsmæssige afbødende foranstaltninger.

EU anvender også **handelspolitiske beskyttelsesinstrumenter** til at genoprette et konkurrencepræget miljø for EU's industri, når den skades gennem dumpingimport eller subsidieret import. Nærmere bestemt har Europa-Kommissionen ansvaret for at undersøge påstande om dumping fra eksporterende tredjelandsproducenter eller i tilfælde af handelsforvridende støtte. Kommissionen indleder sædvanligvis en undersøgelse efter at have modtaget en klage fra de berørte EU-producenter, men den kan også undtagelsesvis gøre dette på eget initiativ[15].

I de eksisterende regler om **offentlige udbud**[16,] opfordres medlemsstaterne til ikke at tildele kontrakter udelukkende på grundlag af den laveste pris, men også til at tage hensyn til kvalitet på områder såsom sikkerheds-, arbejdskraft- og miljøkrav. De er desuden ikke til hinder for, at medlemsstaterne pålægger eller håndhæver de foranstaltninger, der kræves for at beskytte den offentlige sikkerhed eller væsentlige sikkerhedsinteresser. Tilbud fra tilbudsgivere, som ikke har sikret adgang til EU's marked for offentlige indkøb (baseret på bindende internationale eller bilaterale frihandelsaftaler, der omfatter offentlige indkøb), kan udelukkes. Medlemsstaterne kan også på visse betingelser udelukke en økonomisk aktør, der kan udgøre en risiko for væsentlige nationale sikkerhedsinteresser. På forsvars- og sikkerhedsområdet har offentlige indkøbere endvidere ikke pligt til at give operatører fra tredjelande adgang til udbudsprocedurer.

Opretholdelse og videreudvikling af den europæiske kapacitet på området for 5G og navnlig i kritiske dele af værdikæden ved at udnytte **EU's forsknings- og innovationsprogrammer og industripolitiske værktøjer** er en strategisk risikobegrænsende foranstaltning mod risikoen for afhængighed. Ved at støtte disruptive og ambitiøse forsknings-, innovations- og udrulningsprogrammer, f.eks. Horisont Europa, programmet for et digitalt Europa og Connecting Europe-faciliteten, kan udviklingen af europæiske konkurrencedygtige indkøbsmuligheder, især med hensyn til processorer og kritisk software, fremmes. Disse programmer indeholder også sikkerhedsrelaterede bestemmelser.

I tilknytning til EU's statsstøtteregler gør **vigtige projekter af fælleseuropæisk interesse** det muligt at samle viden, ekspertise, finansielle ressourcer og økonomiske aktører i hele EU[17,] med henblik på at overvinde betydelige markedssvigt eller systemiske mangler og samfundsmæssige udfordringer, som ikke kan håndteres på anden vis. De er beregnet på at samle den offentlige og private sektor, således at der kan iværksættes store projekter, som giver EU og dens borgere betydelige fordele.

[15] Forordning (EU) 2016/1036) om beskyttelse mod dumpingimport, forordning (EU) 2016/1037 om beskyttelse mod subsidieret indførsel og forordning (EU) 2015/478 om fælles ordninger for indførsel.

[16] F.eks. direktiv 2014/24/EU af 26. februar 2014 om offentlige udbud, direktiv 2009/81/EF af 13. juli 2009 på forsvars- og sikkerhedsområdet og meddelelse C(2019)5494 fra Kommissionen af 24. juli 2019 "Vejledning om deltagelse af tredjelandes tilbudsgivere og varer på EU's marked for offentlige udbud".

[17] Jf. artikel 107, stk. 3, litra b), i traktaten om Den Europæiske Unions funktionsmåde (TEUF) og C(2014)188/02 Kriterier for analysen af, hvorvidt statsstøtte til fremme af gennemførelsen af vigtige projekter af fælleseuropæisk interesse er forenelig med det indre marked.

Endelig omfatter **andre relevante eller potentielt relevante værktøjer og rammer på EU-plan og nationalt plan** regler om databeskyttelse og beskyttelse af privatlivets fred (navnlig den generelle forordning om databeskyttelse og e-databeskyttelsesdirektivet)[18], direktivet om radioudstyr[19], EU-reglerne om eksportkontrol[20], krav til kritiske infrastrukturer og rammebestemmelser, der har til formål at imødegå cyberhændelser eller -kriser, navnlig planen for en koordineret reaktion på væsentlige cybersikkerhedshændelser og kriser og EU's cyberdiplomatiske værktøjskasse[21].

3.2. National gennemførelse af EU's telekommunikationsregler

I henhold til EU's nuværende telekommunikationsregler[22] fører EU's medlemsstater tilsyn med et sæt sikkerhedskrav til telekommunikationsudbydere. Som beskrevet i punkt 3.1.1 ovenfor skal medlemsstaterne i henhold til artikel 13a sikre, at:

- telekommunikationsudbydere vurderer risici og træffer passende sikkerhedsforanstaltninger
- telekommunikationsudbydere træffer sikringsforanstaltninger for at afbøde virkningen af forstyrrelser i deres net og/eller tjenester, og
- telekommunikationsudbydere anmelder væsentlige hændelser til de relevante myndigheder.

De fleste nationale love til gennemførelse af EU's nuværende retlige rammer blev vedtaget omkring 2011. Med hensyn til tilsynsmetode og -forpligtelser har medlemsstaterne benyttet forskellige tilgange. Hvis bindende regler finder anvendelse på mobilnetoperatører, kan de f.eks. omfatte forskellige typer tekniske og organisatoriske foranstaltninger. I de medlemsstater, hvor sikkerhedsforanstaltningerne præciseres i yderligere tekniske og praktiske detaljer (ofte via afledt ret), henviser de ofte til sikkerhedsforanstaltningerne i sikkerhedsrammens artikel 13a[23].

På nuværende tidspunkt omhandler nationale foranstaltninger på dette område med meget få undtagelser ikke udtrykkeligt avancerede sikkerhedskrav, som specifikt vedrører udrulningen af 5G-net. De omhandler ligeledes ikke udtrykkeligt beføjelser til forhåndstilsyn eller forpligtelser vedrørende sikkerhed i forbindelse med operatørers indkøb og implementering af netudstyr, og de indeholder ikke bestemmelser, der har til formål at fremme sikkerhed og robusthed gennem en passende grad af leverandørdiversificering eller at afhjælpe risici og sårbarheder i forbindelse med de enkelte leverandørers risikoprofil.

[18] Forordning (EU) 2016/679 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og direktiv 2002/58/EF om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor.

[19] Direktiv 2014/53/EU af 16. april 2014 om harmonisering af medlemsstaternes love om tilgængeliggørelse af radioudstyr på markedet.

[20] Forordning (EF) nr. 428/2009 af 5. maj 2009 om en fællesskabsordning for kontrol med udførsel, overførsel, mæglervirksomhed og transit i forbindelse med produkter med dobbelt anvendelse og forslag til forordning af 28.9.2016 (COM(2016) 616).

[21] Ramme for EU's fælles diplomatiske reaktion på ondsindede cyberaktiviteter (Rådets konklusioner af 20.11.2017, 9916/17) og Kommissionens henstilling om en koordineret reaktion på væsentlige cybersikkerhedshændelser og -kriser (EU 2017/1584). En arbejdsstrøm under NIS-samarbejdsgruppen har fået til opgave at gennemføre det operationelle lag, der er fastsat i planen.

[22] Direktiv 2002/21/EF som ændret ved direktiv 2009/140/EF af 25. november 2009 om fælles rammebestemmelser for elektroniske kommunikationsnet og -tjenester og direktiv 2018/1972 af 11. december 2018 om oprettelse af en europæisk kodeks for elektronisk kommunikation.

[23] Technical guidance on the security measures in Article 13a (https://resilience.enisa.europa.eu/article-13/guideline-for-minimum-security-measures) er en detaljeret sikkerhedsramme, der er udviklet i fællesskab af medlemsstaternes eksperter for at fremme en fælles tilgang til tilsyn og/eller god praksis for tilsynet med sektorens sikkerhed i hele EU. Rammen dækker en lang række sikkerhedsforanstaltninger på et højt niveau og finder anvendelse på forskellige typer telekommunikationsudbydere.

3.3. Standardisering (baseline-arbejde i 3GPP)

Flere og flere standardiseringsorganer arbejder med 5G-sikkerhedsspørgsmål, herunder arbejdsgruppen om Service and System Aspects 3 (SA3)[24] under 3rd Generation Partnership Project (3GPP)[25]. Bortset fra standarder kan den sikkerhedsarkitektur, der er defineret af 5G-OPP (baseret på resultaterne af 5G-Ensure), som fremhæver betydningen af forvaltningsområder, også anvendes.

5G-teknologier og -standarder kan forbedre sikkerheden sammenlignet med tidligere generationer af mobilnet takket være indførelsen af flere nye sikkerhedsrelaterede funktioner, f.eks. strengere autentifikation i radiogrænsefladen. Disse nye sikkerhedsfunktioner vil imidlertid ikke som standard blive aktiveret i netudstyret, da leverandører og operatører selv kan vælge, om de vil implementere dem. Disse sikkerhedsfunktioners overordnede effektivitet vil derfor i høj grad afhænge af, hvordan operatørerne implementerer og styrer deres net.

Som anført i rapporten om EU's koordinerede risikovurdering arbejder SA3-arbejdsgruppen også med kravene til lovlig aflytning i 5G-systemer og har planer om at udarbejde alle de specifikationer, der er nødvendige for at opfylde disse krav[26].

4. Foranstaltninger og risikobegrænsningsplaner

De foranstaltninger, der præsenteres i denne værktøjskasse, er henvendt til og skal gennemføres af ansvarlige nationale og europæiske myndigheder og agenturer inden for deres respektive kapacitets- og ansvarsområder, som kan spænde fra myndighedstilsyn til en national sikkerhedsrolle.

I overensstemmelse med rapporten om EU's koordinerede risikovurdering vedrører foranstaltningerne de relevante interessenter på sikkerhedsområdet i 5G-økosystemet[27], dvs. primært **mobilnetoperatører**[28] **og deres leverandører, navnlig producenter af telekommunikationsudstyr**.

På den ene side indtager mobilnetoperatører en vigtig rolle i beslutningstagningen, som giver dem indflydelse på den overordnede sikkerhed i deres net. På den anden side er producenter af telekommunikationsudstyr ansvarlige for at levere den software og hardware, der er nødvendig for at drive nettene.

[24] Arbejdsgruppen vedrørende Service and System Aspects 3 (SA3) er ansvarlig for sikkerhed og beskyttelse af privatlivets fred i 5G-standarder.

[25] 3GPP er det vigtigste globale organ for udvikling af standarder for mobilkommunikation, et samarbejde mellem syv organisationspartnere fra Europa (ETSI), USA (ATIS), Kina (CCSA), Japan (ARIB og TTC), Korea (TTA) og Indien (TSDSI). 3GPP's tekniske specifikationer omfatter industristandarder for sikkerhedsfunktioner i 3G, 4G og nu 5G.

[26] I sine konklusioner af 3.12.2019 (14517/19) understreger Rådet "behovet for at tackle og afbøde potentielle udfordringer som følge af etableringen af 5G-net og -tjenester inden for retshåndhævelse, f.eks. lovlig aflytning".

[27] Disse interessenter er udpeget i rapporten om EU's koordinerede risikovurdering og omfatter: mobilnetoperatører, mobilnetoperatørers leverandører (herunder producenter af telekommunikationsudstyr og andre tredjepartsleverandører som f.eks. cloudinfrastrukturudbydere, systemintegratorer, sikkerheds- og vedligeholdelsesleverandører og producenter af transmissionsudstyr), producenter af tilsluttede enheder og relaterede tjenesteudbydere samt andre interessenter (herunder tjeneste- og indholdsudbydere samt slutbrugere af 5G-mobilnet).

[28] Virtuelle mobilnetoperatører og operatører af kritisk infrastruktur fra en anden sektor end telekommunikationssektoren, som driver 5G-net til deres egne aktiviteter eller på vegne af tredjeparter, vil være omfattet af en tilsvarende kategori af interessenter.

De foranstaltninger, der præsenteres nedenfor, og deres beskrivelse er baseret på de relevante oplysninger i rapporten om EU's koordinerede risikovurdering. I den forbindelse gælder navnlig følgende:

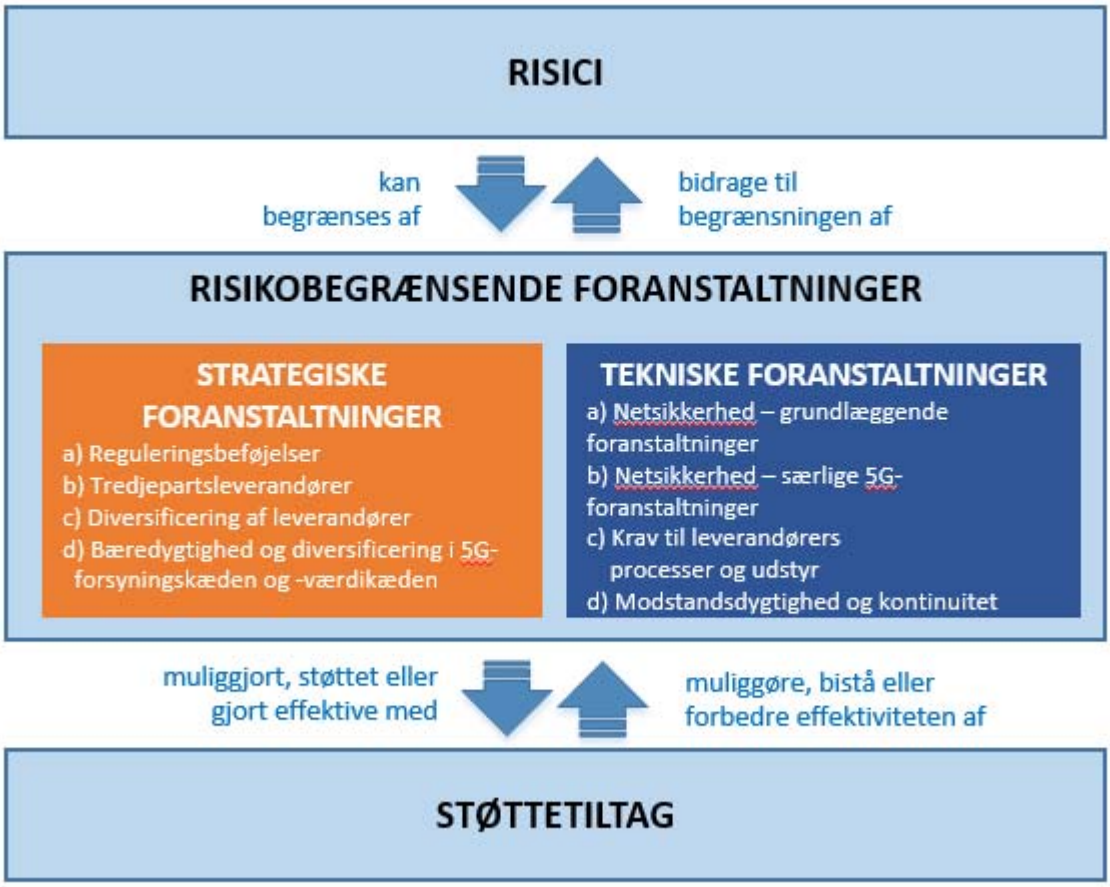
- Når der i foranstaltninger henvises til **kritiske eller følsomme netkomponenter eller funktioner**, bør identifikationen af disse komponenter eller funktioner baseres på og være i overensstemmelse med den **overordnede kategorisering af aktivers følsomhed, der er defineret i rapporten om EU's koordinerede risikovurdering** (se bilag 2 til denne værktøjskasse og afsnit 2.21 i rapporten om EU's koordinerede risikovurdering).

- Når der i foranstaltninger henvises til **enkelte leverandørers risikoprofil**, bør der ved vurderingen af risikoprofilen tages hensyn til de **faktorer, der er defineret i EU's koordinerede risikovurdering**[29] (se bilag 2 til denne værktøjskasse og afsnit 2.37 i rapporten om EU's koordinerede risikovurdering).

[29] I rapporten om EU's koordinerede risikovurdering identificeres en række risikofaktorer i forbindelse med vurderingen af leverandørens risikoprofil, herunder: sandsynligheden for, at leverandøren udsættes for indgriben fra et tredjeland (dette kan fremmes ved, men ikke begrænses til tilstedeværelsen af visse faktorer, som også er opført i rapporten om EU's koordinerede risikovurdering), leverandørens evne til at sikre leveringen og den generelle kvalitet af leverandørens produkter og cybersikkerhedspraksis, herunder graden af kontrol over vedkommendes egen forsyningskæde, og om sikkerhedspraksis prioriteres tilstrækkeligt.

4.1. Foranstaltninger og støttetiltag

Tabel 2 – Værktøjskassens foranstaltninger og støttetiltag



De risikobegrænsende foranstaltninger er opdelt i to overordnede kategorier: **strategiske og tekniske.**

Disse foranstaltninger (se bilag 1, tabel 1, for detaljer) kan bruges til at begrænse de **risici**, der er identificeret i rapporten om EU's koordinerede risikovurdering. De kan suppleres af støttetiltag, som kan forstærke deres effektivitet.

4.1.1 Strategiske foranstaltninger omfatter foranstaltninger om øgede reguleringsbeføjelser til myndighederne, således at de kan føre nøje kontrol med netudbud og -udrulning, specifikke foranstaltninger til at imødegå risici ved ikketekniske sårbarheder (f.eks. risiko for indblanding fra tredjeland eller risiko for afhængighed) samt mulige initiativer til at fremme en bæredygtig og diversificeret 5G-forsynings- og -værdikæde med henblik på at undgå langsigtede systemiske afhængighedsrisici. Strategiske foranstaltninger kan potentielt være yderst effektive til at imødegå visse 5G-cybersikkerhedsrisici, der er identificeret i rapporten om EU's koordinerede risikovurdering.

Følgende otte strategiske foranstaltninger er blevet identificeret:

- SF01 Styrkelse af de nationale myndigheders rolle
- SF02 Audit af operatører og krav om oplysninger
- SF03 Vurdering af leverandørernes risikoprofil og anvendelse af restriktioner over for leverandører, der vurderes at udgøre en høj risiko – herunder nødvendige udelukkelser for effektivt at begrænse risiciene – i forbindelse med centrale aktiver
- SF04 Kontrol med brugen af tjenesteudbydere og udstyrsleverandørers tredjelinjesupport
- SF05 Sikring af de enkelte mobilnetoperatørers leverandørdiversificering gennem hensigtsmæssige flerleverandørstrategier
- SF06 Styrkelse af modstandsdygtigheden på nationalt plan
- SF07 Identifikation af centrale aktiver og fremme af et diversificeret og bæredygtigt 5G-økosystem i EU
- SF08 Opretholdelse og opbygning af diversificering og EU-kapacitet i fremtidige netteknologier.

4.1.2 Tekniske foranstaltninger omfatter foranstaltninger til at styrke sikkerheden i 5G-net og -udstyr ved at forstærke sikkerheden i teknologier, processer, mennesker og fysiske faktorer. Effektiviteten af de tekniske foranstaltninger med hensyn til risikobegrænsning vil variere afhængigt af foranstaltningernes omfang og de typer risici, der skal imødegås. Tekniske foranstaltninger alene kan navnlig ikke anvendes til at imødegå ikketekniske sårbarheder (f.eks. risiko for indblanding fra tredjeland eller risiko for afhængighed).

Følgende 11 tekniske foranstaltninger er blevet identificeret:

- TF01 Sikring af, at der anvendes grundlæggende sikkerhedskrav (sikkert netdesign og sikker netarkitektur)
- TF02 Sikring og evaluering af gennemførelsen af sikkerhedsforanstaltninger i eksisterende 5G-standarder
- TF03 Sikring af strenge adgangskontroller
- TF04 Forøgelse af sikkerheden af virtualiserede netfunktioner

- TF05 Sikring af sikker styring, drift og overvågning af 5G-net
- TF06 Styrkelse af den fysiske sikkerhed
- TF07 Styrkelse af softwareintegritet og -opdatering samt styring af rettelser
- TF08 Forbedring af sikkerhedsstandarderne i leverandørernes processer gennem robuste indkøbsbetingelser
- TF09 Anvendelse af EU-certificering for 5G-netkomponenter, kundeudstyr og/eller leverandørers processer
- TF10 Anvendelse af EU-certificering for andre ikke-5G-specifikke IKT-produkter og -tjenester (tilsluttede enheder og cloudtjenester)
- TF11 Styrkelse af planer for modstandsdygtighed og kontinuitet.

4.1.3 En række målrettede støttetiltag kan desuden potentielt muliggøre og støtte de strategiske og tekniske foranstaltninger og derved øge deres effektivitet:

- ST01 Revision eller udarbejdelse af retningslinjer og bedste praksis for netsikkerhed
- ST02 Styrkelse af test- og auditkapaciteten på nationalt plan og EU-plan
- ST03 Støtte til og udformning af 5G-standarder
- ST04 Udvikling af retningslinjer for gennemførelsen af sikkerhedsforanstaltninger i eksisterende 5G-standarder
- ST05 Sikring af, at der anvendes tekniske og organisatoriske standardsikkerhedsforanstaltninger gennem en specifik EU-certificeringsordning
- ST06 Udveksling af bedste praksis for gennemførelsen af strategiske foranstaltninger, navnlig nationale rammer for vurdering af leverandørernes risikoprofil
- ST07 Forbedring af koordineringen af beredskabs- og krisestyring
- ST08 Gennemførelse af audit af indbyrdes afhængighed mellem 5G-net og andre kritiske tjenester
- ST09 Styrkelse af mekanismerne for samarbejde, koordinering og informationsudveksling
- ST10 Sikring af 5G-udrulningsprojekter, der modtager offentlig støtte, under hensyntagen til cybersikkerhedsrisici.

4.2. Risikobegrænsningsplaner

For hvert af de ni risikoområder, der afdækkes i rapporten om EU's koordinerede risikovurdering, indeholder værktøjskassen **planer for risikobegrænsning**[30]. De består af mulige kombinationer af strategiske og/eller tekniske foranstaltninger (sammen med passende støttetiltag), der har til formål at mindske en sikkerhedsrisiko.

Risikobegrænsningsplanerne har til formål at udstikke retningslinjer for de **mest relevante/mest effektive risikobegrænsende foranstaltninger** med udgangspunkt i en evaluering af den forventede effektivitet af de individuelle foranstaltninger, der er anført i afsnit 4.1., med hensyn til begrænsning af en bestemt risiko. Det bør imidlertid bemærkes, at den forventede effektivitet af de fleste foranstaltninger i høj grad afhænger af deres omfang og den måde, hvorpå de gennemføres (øgede reguleringsbeføjelser kan f.eks. være meget effektive, hvis de har et passende omfang og anvendes effektivt).

Risikobegrænsningsplaner afspejler desuden betydningen af at kombinere foranstaltninger på en passende måde for at sikre, at de bliver så effektive som muligt, og at de kan håndhæves. Mange af foranstaltningerne, f.eks. anvendelsen af skærpede sikkerhedsforpligtelser for

[30] I denne forbindelse beskriver en *risikobegrænsningsplan* en mulig tilgang, der kan benyttes for at begrænse en risiko.

mobilnetoperatører, forudsætter, at tilsynsmyndighederne har de fornødne beføjelser til at definere og pålægge sådanne forpligtelser og til at overvåge og kontrollere deres gennemførelse.

Disse risikobegrænsningsplaner fremlægges i detaljer i bilag 1 (tabel 2). Der gives også en vejledende identifikation på højt niveau af andre potentielle effektfaktorer.

I den anslåede grad af **forventet effektivitet** tages der også højde for den oprindelige risiko og den forventede resterende risiko efter anvendelse af foranstaltningen, og følgende skala benyttes:

- Meget høj: Foranstaltningen anses for at være effektiv i meget høj grad, dvs. at den forventes at kunne begrænse de tilknyttede risici næsten fuldstændigt.
- Høj: Foranstaltningen anses for at være effektiv i høj grad, dvs. at den forventes at kunne begrænse de tilknyttede risici betydeligt.
- Middel: Foranstaltningen anses for at være delvist effektiv, dvs. at den forventes at kunne begrænse de tilknyttede risici i en vis grad.
- Lav: Foranstaltningen anses ikke for at være særlig effektiv, dvs. at den forventes kun at kunne begrænse de tilknyttede risici marginalt.

For hver foranstaltning angiver tabellen om risikobegrænsningsplaner (bilag 1, tabel 2) andre mulige parametre og karakteristika med det formål at hjælpe medlemsstaterne med at udvælge og gennemføre foranstaltninger:

- potentielle **gennemførelsesfaktorer** (kan være positive og/eller negative):
    - ressourceomkostninger
    - sektorspecifikke økonomiske virkninger (for operatører eller for leverandører)
    - bredere økonomiske og/eller samfundsmæssige virkninger

- vejledende **tidsrammer** for iværksættelse af de nødvendige tiltag for at gennemføre foranstaltningerne ved brug af følgende skala:
    - Kort sigt: 0-2 år
    - Mellemlang sigt: 2-5 år
    - Lang sigt: > 5 år

Af hensyn til overskueligheden vises en forenklet udgave af bilag 1, tabel 2, på næste side. Alle angivelser vedrørende den forventede effektivitet, de potentielle effektfaktorer og de vejledende tidsrammer nedenfor er med forbehold af de bemærkninger og betingelser, der er anført i tabel 2 i bilag 1. Se bilag 1 for mere detaljerede oplysninger.

Tabel 3: Forenklet oversigt over foranstaltninger i risikobegrænsningsplaner *(se bilag 1, tabel 2, for flere detaljer)*

FORANSTALTNINGER	Vejledende tidsramme			Potentielle gennemførelsesfaktorer				SPECIFIKKE FORANSTALTNINGER	RISICI								
	Kort sigt	Mellemlang sigt	Lang sigt	Ressourceomkostninger	Sektorspecifik økonomisk virkning	Sektorspecifik økonomisk virkning	Bredere økonomisk/samfundsmæssig		R1: Fejlkonfigurering af net	R2: Manglende adgangskontrol	R3: Dårlig kvalitet af produkterne	R4: Afhængighed af en enkelt leverandør	R5: Statslig indblanding via 5G-forsyningskæden	R6: Organiserede kriminelle gruppers udnyttelse af 5G-net	R7: Væsentlige forstyrrelser af kritiske infrastrukturer/tjenester	R8: Massive netnedbrud som følge af strømafbrydelse	R9: Udnyttelse af IoT
STRATEGISKE FORANSTALTNINGER																	
a) Reguleringsbeføjelser	✓			✓	✓	✓	✓	SF01									
								SF02									
b) Tredjepartsleverandører	✓			✓	✓	✓	✓	SF03									
								SF04									
c) Diversificering af leverandører	✓	✓		✓	✓	✓	✓	SF05									
								SF06									
d) Bæredygtighed og diversificering i 5G-forsyningskæden og -værdikæden	✓	✓	✓	✓	✓	✓	✓	SF07									
								SF08									
TEKNISKE FORANSTALTNINGER																	
a) Netsikkerhed – grundlæggende foranstaltninger	✓			✓	✓			TF01									
								TF02									
b) Netsikkerhed – særlige 5G-foranstaltninger	✓			✓	✓			TF03									
								TF04									
								TF05									
								TF06									
								TF07									
c) Krav til leverandørers processer og udstyr		✓	✓	✓	✓	✓		TF08									
								TF09									
								TF10									
d) Modstandsdygtighe	✓			✓	✓			TF11									

Forventet effektivitet:

Meget lav  Meget høj

5. Anvendelse og indførelse af værktøjskassen

5.1. Indsats på nationalt plan og/eller EU-plan

Som skitseret ovenfor er der behov for en passende kombination af forskellige typer foranstaltninger for effektivt at mindske de risici, der er afdækket. Medlemsstaterne skal træffe en række afbødende foranstaltninger for effektivt at imødegå den risiko, der er forbundet med 5G. Foranstaltningerne kan gennemføres ved hjælp af nationale tiltag og/eller EU-tiltag, afhængigt af de specifikke foranstaltninger og tiltag. Nogle foranstaltninger kan indføres eller gøres stærkere direkte på nationalt plan, mens andre måske kræver yderligere eller fælles tiltag på EU-plan i overensstemmelse med de respektive kompetencer.

Gennemførelsen af de **strategiske foranstaltninger** kan kræve specifik lovgivning på nationalt plan for at opnå den fulde virkning af foranstaltningerne. Nogle medlemsstater har allerede gennemført lovgivning vedrørende disse strategiske foranstaltninger, mens andre er ved at udarbejde lignende lovgivning. I fremtiden vil koordinering mellem medlemsstaterne eller på EU-plan kunne medvirke til at fremme konvergerende tilgange.

Foranstaltninger til fremme af bæredygtigheden og diversificeringen i 5G-forsyningskæden og -værdikæden med henblik på at forhindre afhængighed på lang sigt kræver en samordnet strategisk tilgang understøttet af politikker og lovgivning på EU-plan og/eller en effektiv gennemførelse af eksisterende EU-instrumenter i sammenhæng med 5G (f.eks. inden for forskning og innovation eller handel).

Mange af de **tekniske foranstaltninger** kan implementeres i forbindelse med gennemførelsen af den europæiske kodeks for elektronisk kommunikation. Med hensyn til gennemførelse og overvågning af disse foranstaltninger skal medlemsstaterne sandsynligvis samarbejde om kapacitetsopbygning, og de vil bevare et vist niveau af skøn med hensyn til tilsynsmetode og -forpligtelser. Da nogle af disse foranstaltninger vil være relevante for alle 5G-net på næsten samme måde, kan der med fordel etableres yderligere samarbejde og vidensdeling på EU-plan, navnlig gennem revision og udarbejdelse af retningslinjer og bedste praksis, ligesom der med fordel kan ske yderligere koordinering på EU-plan.

Støttetiltagene vil sandsynligvis ikke kræve lovgivningsmæssig støtte. De skal imidlertid koordineres på samme måde.

5.2. Gennemførelse af risikobegrænsningsplaner på nationalt plan

Når de enkelt medlemsstater udvælger, hvilke foranstaltninger de vil gennemføre, træffer de afgørelse om foranstaltningens egnethed. Medlemsstaten skal også vurdere, om den har ressourcer til at håndhæve foranstaltningen, eller om der er behov for at samarbejde med andre medlemsstater eller på EU-plan.

Medlemsstaternes gennemførelse af foranstaltningerne vil variere afhængigt af en række faktorer, f.eks. kendetegnene ved det nationale telekommunikationsmarked (herunder tidsrammen for etablering af 5G-net, tilstedeværelsen af leverandører i net og graden af afhængighed af individuelle leverandører, de nationale ressourcer og kapaciteter samt de retlige rammer og sikkerhedskrav, der

allerede gælder). Gennemførelsesplanerne kan også omfatte overgangsfaser eller trin, navnlig hvis en foranstaltning vil føre til en væsentlig ændring af den nuværende praksis.

En række fælles overordnede parametre gør sig imidlertid gældende på tværs af medlemsstaterne, som kan lægges til grund for udvælgelsen og prioriteringen af foranstaltninger. Disse parametre fastlægges gennem en vurdering på højt niveau af foranstaltningernes effektivitet og gennem en indikation af de forskellige typer effektfaktorer og den mulige/ønskede tidsramme for gennemførelsen af foranstaltningerne, som skitseret i bilag 1 (tabel 2).

Tabel 4: Sådan anvendes værktøjskassen

Trin 1	Medlemsstaten prioriterer risiciene ud fra den nationale risikovurdering og den EU-koordinerede risikovurdering.
Trin 1a	Medlemsstaten vurderer, hvor effektive de eksisterende foranstaltninger er til at mindske risiciene i risikovurderingen, og kortlægger mangler.
Trin 2	Medlemsstaten afdækker prioriterede risici i tabel 2 (bilag 1) for at imødegå de mangler, der er blevet kortlagt på trin 1a.
Trin 3	Medlemsstaten gennemgår de tilhørende anbefalede foranstaltninger og begrænsningsplaner, udvælger de(n) foranstaltning(er), der vil have størst virkning, og afvejer potentielle gennemførelsesfaktorer, enten alene eller sammen med en eller flere medlemsstater i samme situation.
Trin 5	Medlemsstaten gennemfører foranstaltningen/-erne eller dele heraf, enten alene eller sammen med en eller flere medlemsstater i samme situation.

6. Konklusioner og det videre forløb

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 følgende:

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. streng adgangskontrol, regler for sikker drift og overvågning, begrænsning af outsourcing af specifikke funktioner osv.)

- vurdere leverandørernes risikoprofil og følgelig **anvende relevante begrænsninger for leverandører, der anses for at udgøre en høj risiko – herunder nødvendige udelukkelser for på effektiv vis at begrænse risici – for vigtige aktiver**, der defineres som kritiske og følsomme (f.eks. kernenetfunktioner, netforvaltnings- og netstyringsfunktioner og netadgangsfunktioner)

- sikre, at hver operatør har en passende flerleverandørstrategi for at **undgå eller begrænse enhver større afhængighed** af en enkelt leverandør (eller leverandører med en tilsvarende risikoprofil), sikre en passende balance mellem leverandører på nationalt plan og **undgå afhængighed af leverandører, der vurderes at udgøre en høj risiko**, hvilket også kræver, at man undgår situationer med fastlåsning med en enkelt leverandør, herunder ved at fremme øget interoperabilitet af udstyr.

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

- opretholde en **diversificeret og bæredygtig 5G-forsyningskæde** for at undgå langvarig afhængighed, herunder ved at:

    - udnytte de eksisterende EU-værktøjer og -instrumenter fuldt ud, navnlig ved screening af potentielle udenlandske direkte investeringer, der påvirker 5G-nøgleaktiverne, og undgå forvridning på 5G-forsyningsmarkedet som følge af potentiel dumping eller subsidier og

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

- fremme koordineringen mellem medlemsstaterne med hensyn til **standardisering** for at nå specifikke sikkerhedsmål og **udvikle relevante EU-omfattende certificeringsordninger** for at fremme produkter og processer, der er mere sikre.

3. For at sikre, at denne 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**.

Bilag 1 til Cybersikkerhed i 5G-net – EU-værktøjskasse med risikobegrænsende foranstaltninger

- **Tabel 1: Strategiske foranstaltninger, tekniske foranstaltninger og støttetiltag**

STRATEGISKE FORANSTALTNINGER					
a) Reguleringsbeføjelser					
Ref.	**Foranstaltning**	**Beskrivelse**	**Tilknyttede risici**	**Relevante aktører**[31]	**Støttetiltag**
SF01	**Styrkelse af de nationale myndigheders rolle**	Dette bør omfatte reguleringsbeføjelser til nationale myndigheder, så de kan: – pålægge operatører skærpede forpligtelser, f.eks. vedrørende sikkerheden i signal-/styringsplanet – benytte beføjelser til på forhånd ud fra en risikobaseret tilgang at begrænse, forbyde og/eller pålægge specifikke krav eller betingelser for levering, udrulning og drift af 5G-netudstyr under hensyntagen til bl.a.: ▪ sikkerheden i kritiske og følsomme dele af 5G-net ▪ sikkerheden i selve udstyret eller miljøet (udrulning, sammenkoblinger osv.) ▪ risiko for indblanding fra tredjeland i 5G-forsyningskæden ▪ risiko for større afhængighed af en enkelt leverandør for enkelte mobilnetoperatører eller nationalt ▪ risici for den nationale sikkerhed.	R1 R2 R3 R4 R5 R6 R7	▪ Relevante myndigheder ▪ Operatører	ST01 ST04 ST06
SF02	**Audit af operatører og krav om oplysninger**	Når de kompetente myndigheder udøver deres beføjelser i henhold til artikel 41, stk. 2, i kodeksen for elektronisk kommunikation[32], bør de: - udføre audit eller kræve audit af mobilnetoperatører, om nødvendigt på et tilbundsgående teknisk niveau, f.eks. af kritiske komponenter og/eller følsomme dele af 5G-nettet - kræve, at operatørerne giver detaljerede og ajourførte oplysninger om deres planer om indkøb af 5G-udstyr og for inddragelse af tredjepartsleverandører	R1 R2 R3 R4 R5 R6 R7	▪ Relevante myndigheder ▪ Operatører	ST02

[31] I denne kolonne angives de primære ejere af foranstaltningerne, dvs. de aktører, der er ansvarlige for at udvikle, håndhæve og/eller gennemføre en foranstaltning.

[32] For specifikke nye anvendelser i 5G (f.eks. små lukkede 5G-net med kritiske funktioner som f.eks. et havne- eller et hospitalsnet) bør det vurderes, om reguleringsbeføjelser finder anvendelse på disse nye typer mobilnetoperatører, og hvis ikke, bør behovet for at regulere dem vurderes.

		- kræve, at operatørerne dokumenterer og vedligeholder en beskrivelse af, hvordan de grundlæggende tekniske netsikkerhedsforanstaltninger gennemføres[33].			
b) Tredjepartsleverandører					
SF03	**Vurdering af leverandørernes risikoprofil og anvendelse af restriktioner over for leverandører, der vurderes at udgøre en høj risiko – herunder nødvendige udelukkelser for effektivt at begrænse risiciene – i forbindelse med centrale aktiver**	– Fastlægge en ramme med klare kriterier under hensyntagen til de risikofaktorer, der er identificeret i punkt 2.37 i EU's koordinerede risikovurdering[34], og med tilføjelse af landespecifikke oplysninger (f.eks. trusselsvurdering fra de nationale sikkerhedstjenester osv.), således at de nationale kompetente myndigheder og mobilnetoperatører kan: – udføre strenge vurderinger af risikoprofilen for alle relevante leverandører på nationalt plan og/eller EU-plan (f.eks. sammen med andre medlemsstater eller andre mobilnetoperatører) – anvende restriktioner – herunder nødvendige udelukkelser for effektivt at begrænse risiciene – i forbindelse med centrale aktiver, der er udpeget som kritiske og følsomme i EU's koordinerede risikovurdering (f.eks. kernenetfunktioner, netforvaltnings- og netorkestreringsfunktioner og adgangsnetfunktioner), på grundlag af vurderingen af risikoprofilen – træffe foranstaltninger for at sikre, at mobilnetoperatører har indført hensigtsmæssige kontroller og processer til at håndtere potentielle restrisici, f.eks. regelmæssig audit af forsyningskæden og regelmæssige risikovurderinger, robust risikostyring og/eller specifikke krav til leverandører på grundlag af deres risikoprofil.	R2 R5	▪ Relevante myndigheder ▪ Operatører	ST06, ST10
SF04	**Kontrol med brugen af tjenesteudbydere og udstyrsleverandørers tredjelinjesupport**	Fastlægge en retlig/lovgivningsmæssig ramme, som begrænser aktivitetstyper og betingelser, hvorunder mobilnetoperatører kan outsource bestemte funktioner til tjenesteudbydere, for både fysisk og virtuel infrastruktur, herunder: – anvende restriktioner, især i følsomme dele af 5G-net, f.eks. sikkerheds- og netdriftsfunktioner, og når tjenesteudbydere anses for at udgøre en høj risiko som defineret i SF03	R2 R5	▪ Relevante myndigheder ▪ Operatører	ST06, ST10

[33] Dette kan omfatte sikkerhedsområder som f.eks. administrative oplysningers sikkerhed, personalesikkerhed, hardware-, software- og telekommunikationssikkerhed, sikkerhed i informationsmateriale og anvendelse, fysisk sikkerhed mv.

[34] I rapporten om EU's koordinerede risikovurdering identificeres en række risikofaktorer i forbindelse med vurderingen af leverandørens risikoprofil, herunder: sandsynligheden for, at leverandøren udsættes for indgriben fra et tredjeland (dette kan fremmes ved, men ikke begrænses til tilstedeværelsen af visse faktorer, som også er opført i rapporten om EU's koordinerede risikovurdering), leverandørens evne til at sikre leveringen og den generelle kvalitet af leverandørens produkter og cybersikkerhedspraksis, herunder graden af kontrol over vedkommendes egen forsyningskæde, og om sikkerhedspraksis prioriteres tilstrækkeligt.

		– indføre udvidede sikkerhedsbestemmelser i forbindelse med funktioner, der outsources til tjenesteudbydere, for den adgang, som tjenesteudbydere får til at udføre disse funktioner. Indføre streng adgangskontrol, især til kritisk følsomme komponenter og/eller følsomme dele af nettet, for udstyrsproducenters tredjelinjesupport under design, udrulning og/eller drift af net, og især for leverandører, der anses for at udgøre en høj risiko som defineret i SF03.			
c) Diversificering af leverandører					
SF05	**Sikring af de enkelte mobilnetoperatørers leverandørdiversificering gennem hensigtsmæssige flerleverandørstrategier**	Sikre, at hver mobilnetoperatør har en passende multileverandørstrategi under hensyntagen til de tekniske begrænsninger og interoperabilitetskrav i de forskellige dele af et 5G-net, med henblik på at: - undgå eller begrænse større afhængighed af en enkelt leverandør (eller flere leverandører med en tilsvarende risikoprofil) - undgå afhængighed af leverandører, der anses for at udgøre en høj risiko som defineret i SF03.	R4	▪ Relevante myndigheder ▪ Operatører	ST03, ST10
SF06	**Styrkelse af modstandsdygtigheden på nationalt plan**	Sikre, at der er en passende balance mellem leverandører på nationalt plan, således at der opnås modstandsdygtighed, hvis der opstår en hændelse med en operatør og/eller en leverandør, under hensyntagen til de geografiske og befolkningsmæssige forhold i de enkelte medlemsstater.	R4	▪ Relevante myndigheder ▪ Operatører	ST03, ST10
d) Bæredygtighed og diversificering i 5G-forsyningskæden og –værdikæden					
SF07	**Identifikation af centrale aktiver og fremme af et diversificeret og bæredygtigt 5G-økosystem i EU**	– Forbedre overvågningen af udenlandske direkte investeringer i 5G-værdikæden på grundlag af EU's screeningmekanisme for direkte udenlandske investeringer (f.eks. gennem en kortlægning af centrale 5G-aktiver, anvendelse af overvågningsværktøjer og undersøgelse af specifikke retningslinjer) for bedre at kunne spore udenlandske investeringer i 5G-værdikæden, som kan udgøre en trussel for sikkerheden eller den offentlige orden i mere end én medlemsstat. Kritisk infrastruktur, offentlig sikkerhed, adgang til og kontrol med oplysninger og cybersikkerhed indgår i anvendelsesområdet for forordningen om direkte udenlandske investeringer, således at investeringer kan evalueres under hensyntagen til faktorer såsom køberes/virksomheders risikoprofil.	R4	▪ Kommissionen og medlemsstaterne	ST10

		– Hvis der opstår afhængighed i 5G-værdikæden som følge af producenters handelsfordrejende markedsadfærd, som er omfattet af anvendelsesområdet og betingelserne for EU's relevante antidumping- og antisubsidieregler – og hvis disse anmeldes via en ad hoc-klage eller under særlige omstændigheder via Kommissionens eget initiativ – kan en sådan adfærd undersøges og håndteres gennem EU's handelsbeskyttelsesforanstaltninger.			
SF08	**Opretholdelse og opbygning af diversificering og EU-kapacitet i fremtidige netteknologier.**	Udvikle politikker, der skaber optimale betingelser for europæiske teknologivirksomheder og styrker innovation inden for centrale teknologiområder med henblik på at fremme et diversificeret, bæredygtigt og sikkert europæisk 5G-økosystem, herunder ved at: – udvikle det foreslåede institutionaliserede EU-partnerskab på området for NGI/6G ("intelligente net og tjenester")[35] med det formål at sikre, at der er en tilstrækkelig grad af leverandørdiversificering og tilstrækkelig viden og leveringskapacitet i EU på tværs af telekommunikationsværdikæden – udvikle EU's kapacitet og dermed også undgå afhængighed ved at støtte disruptiv og ambitiøs forskning og innovation. Dette vedrører gennemførelsen af de forskellige EU-finansieringsprogrammer, herunder navnlig Horisont Europa, programmet for et digitalt Europa og Connecting Europe-faciliteten (f.eks. gennem initiativer såsom 5G-korridorer til opkoblet og automatiseret mobilitet) – samle viden, ekspertise, finansielle ressourcer og økonomiske aktører i hele EU med henblik på at overvinde betydelige markedssvigt eller systemiske mangler i værdikæden (IPCEI) og yderligere specifikke initiativer fra erhvervslivets side.	R4	▪ Kommissionen og medlemsstaterne ▪ Alle 5G-interessenter	ST10

[35] Forslag til europæisk partnerskab om intelligente net og tjenester (Horisont Europa-programmet). Link til indledende konsekvensanalyse: https://EF.europa.eu/info/law/better-regulation/initiatives/ares-2019-4972300_en.

TEKNISKE FORANSTALTNINGER					
a) Netsikkerhed – grundlæggende foranstaltninger					
Ref.	**Foranstaltninger**	**Beskrivelse**	**Tilknyttede risici**	**Relevante aktører**	**Støttetiltag**
TF01	**Sikring af, at der anvendes grundlæggende sikkerhedskrav (sikkert netdesign og sikker netarkitektur)**	Sikre, at mobilnetoperatørerne gennemfører eksisterende bedste praksisser og anbefalinger for sikkerhed, som ikke er specifikke for 5G-net, i f.eks. produktudvikling, daglig netstyring, hændelsesstyring og sikkerhedsopdateringer[36], f.eks. ved at indføre og revidere risikovurderingsplaner for mobilnetoperatører. Sikre, at mobilnetoperatører ajourfører oplysninger om sikkerhedspolitik, herunder operationelle oplysninger, som også omfatter procedurer for ændrings- og hændelsesstyring af centrale net- og informationssystemer.	R1 R2 R3 R6 R7 R8 R9	▪ Relevante myndigheder ▪ Operatører	ST01, ST05, ST09, ST10
TF02	**Sikring og evaluering af gennemførelsen af sikkerhedsforanstaltninger i eksisterende 5G-standarder**	Sikre, at mobilnetoperatører og deres leverandører gennemfører de eksisterende sikkerhedsforanstaltninger i de relevante 5G-teknologistandarder (f.eks. 3GPP) og bruger dem som en sikkerhedsmæssig minimumsbasislinje for mobilnetoperatører med henblik på at sikre, at også de fakultative dele af disse standarder, som er relevante for sikkerheden, gennemføres i tilstrækkelig grad	R1 R2 R3 R6 R7 R9	▪ Relevante myndigheder ▪ Operatører ▪ Leverandører	ST03, ST04, ST05, ST10
b) Netsikkerhed – særlige 5G-foranstaltninger					

[36] Disse foranstaltninger bør baseres på internationale eller europæiske standarder eller tekniske retningslinjer, f.eks. artikel 13a-ekspertgruppens retningslinjer for minimumssikkerhedsforanstaltninger (https://resilience.enisa.europa.eu/article-13/guideline-for-minimum-security-measures/Article_13a_ENISA_Technical_Guideline_On_Security_Measures_v2_0.pdf).

TF03	**Sikring af strenge adgangskontroller**	Sikre, at mobilnetoperatører gennemfører tilstrækkelige, fleksible og verificerbare tekniske foranstaltninger, som sikrer, at: – der anvendes strenge adgangskontroller – princippet om det mindste privilegium anvendes, således at de forskellige rettigheder i nettet (f.eks. adgangsrettigheder mellem netfunktioner, netadministratorers rettigheder og virtualiseringskonfiguration) minimeres – princippet om adskillelse af opgaver finder anvendelse – der er indført procedurer for at sikre, at disse regler altid er i kraft og udvikler sig med nettet. Ved fastsættelsen af politikker for adgangskontroller bør det særligt sikres, at tredjeparters fjernadgang så vidt muligt minimeres og/eller undgås. Det gælder navnlig leverandører, der anses for at udgøre en høj risiko. Når fjernadgang er nødvendig, f.eks. for at afhjælpe tjenesteafbrydelser, bør mobilnetoperatøren anvende passende autentificering[37], tilladelser, logning og audit for at synliggøre adgangen til data og konfigurationsændringer eller ændringer af nettet.	R1 R2 R3 R5 R6 R7	▪ Relevante myndigheder ▪ Operatører	ST05, ST10
TF04	**Forøgelse af sikkerheden af virtualiserede netfunktioner**	Sikre, at mobilnetoperatører overholder bedste praksis for virtualisering af netfunktioner. Bemærk, at der kan være situationer, f.eks. når en netfunktion er meget kritisk, eller når den håndterer meget følsomme oplysninger, hvor virtualisering ikke bør anvendes, og at fysisk adskillelse kan være nødvendig i sådanne situationer.	R1 R3 R6 R7	▪ Relevante myndigheder ▪ Operatører	ST01, ST05, ST10
TF05	**Sikring af sikker styring, drift og overvågning af 5G-net**	Sikre, at mobilnetoperatører driver deres netdriftscentre og/eller sikkerhedsdriftscentre på stedet, i landet og/eller i EU. Netdriftscentre og sikkerhedsdriftscentre er en del af mobilnetoperatørens infrastruktur til gennemførelse og overvågning af foranstaltningerne til sikker netforvaltning og -drift. De bør sørge for klar synlighed og gennemføre effektiv netovervågning af som minimum alle kritiske komponenter og følsomme dele af 5G-nettet for at opdage uregelmæssigheder og for at identificere og undgå trusler, f.eks. trusler mod kernenettet fra kompromitterede brugerenheder og IoT. De bør også sikre, at mobilnetoperatører beskytter kommunikationsnettets eller -tjenestens styringstrafik for at undgå	R1 R2 R3 R5 R6 R7 R9	▪ Relevante myndigheder ▪ Operatører	ST05, ST09, ST10

[37] Med hensyn til autentificering finder generel god praksis anvendelse, og relevante mekanismer bør anvendes, f.eks. i forbindelse med tredjeparters midlertidige adgang og/eller fjernadgang (f.eks. ingen permanente ID'er og alene anvendelse af midlertidige (engangs-)adgangskoder, som kun kan bruges til specifikke opgaver). Disse foranstaltninger kan f.eks. håndhæves ved brug af hensigtsmæssig PAM-platforme (Privileged Access Management).

		uautoriserede ændringer af kommunikationsnettet eller tjenestekomponenterne.			
TF06	**Styrkelse af den fysiske sikkerhed**	Sikre, at mobilnetoperatører styrker den fysiske beskyttelse af kritiske komponenter og følsomme dele af 5G-nettet ved brug af en risikobaseret tilgang til Multi-access Edge Computing (MEC) og basisstationer[38], f.eks. kortlægning af, hvor komponenterne er installeret og anvendes, f.eks. MEC-anvendelse på hospitaler. Når de fysiske adgangskontroller styrkes, er det vigtigt at sikre, at der kun gives adgang til et begrænset antal sikkerhedstjekkede, uddannede og kvalificerede medarbejdere. Adgangen for tredjeparter, kontrahenter og leverandørers ansatte og integratorer bør begrænses og overvåges, især når der er tale om kritiske komponenter og følsomme dele af 5G-nettet.	R6 R7	▪ Relevante myndigheder ▪ Operatører	ST05, ST10
TF07	**Styrkelse af softwareintegritet og -opdatering samt styring af rettelser**	Sikre, at mobilnetoperatører implementerer hensigtsmæssige værktøjer og processer til at sikre softwareintegritet, som pålideligt kan identificere og spore ændringer og status for rettelser, når der foretages softwareopdateringer og sikkerhedsrettelser i 5G-nettet.	R1 R3 R5 R6 R7	▪ Relevante myndigheder ▪ Operatører	ST02, ST10

[38] Når mobilnetoperatørerne udfører risikoanalysen, bør de tage komponenterne og tjenesten i betragtning (f.eks. en kritisk MEC-tjeneste på et hospital).

c) Krav til leverandørers processer og udstyr					
TF08	**Forbedring af sikkerhedsstandarderne i leverandørernes processer gennem robuste indkøbsbetingelser**	Sikre, at mobilnetoperatører kræver, at udstyrsleverandører opfylder specifikke sikkerhedsstandarder, i indkøbsprocessen (f.eks. vedrørende specifikke sikkerhedsforbedringer og kvalitetsniveauer, sikkerhedsvedligeholdelse af udstyret i hele dets levetid og indbygget sikkerhed i produktudviklingsprocesserne).	R3 R6 R7	▪ Relevante myndigheder ▪ Operatører ▪ Leverandører	ST02, ST10
TF09	**Anvendelse af EU-certificering for 5G-netkomponenter, kundeudstyr og/eller leverandørers processer**	Kommissionen bør overveje at medtage relevante EU-ordninger for kritiske netkomponenter, der anvendes i 5G-net og/eller 5G-kundeudstyr i EU's rullende arbejdsprogram[39] (f.eks. eSIM og relateret kryptografisk materiale), inden for EU's certificeringsramme. Det bør også på et senere tidspunkt undersøges, om certificeringsprocessen eller leverandørens proces også kan føjes til EU's rullende arbejdsprogram.	R3 R6 R7	▪ Relevante myndigheder ▪ Kommissionen ▪ ENISA ▪ Interessenter	ST02, ST03, ST09, ST10
TF10	**Anvendelse af EU-certificering for andre ikke-5G-specifikke IKT-produkter og -tjenester (tilsluttede enheder og cloudtjenester)**	Kommissionen bør overveje at medtage EU-ordninger inden for EU's certificeringsramme for ikke-5G-specifikke IKT-produkter og -tjenester i EU's rullende arbejdsprogram, f.eks. med hensyn til: – sikkerheden i cloudtjenester og relaterede teknologier, som er en vigtig del af udrulningen af 5G[40] – sikkerheden i forbundne (slutbruger-)enheder, herunder IoT.	R9	▪ Relevante myndigheder ▪ Kommissionen ▪ ENISA ▪ Interessenter	ST02, ST03, ST09, ST10

[39] Inden for EU's ramme for cybersikkerhedscertificering bør Kommissionen offentliggøre EU's rullende arbejdsprogram for udvikling af EU-certificeringsordninger inden juli 2020.

[40] I henhold til artikel 48, stk. 2, i forordningen om cybersikkerhed, anmodede Kommissionen den 21.11.2019 ENISA om at udarbejde et forslag til ordning for cybersikkerhedscertificering af cloudtjenester.

d) Modstandsdygtighed og kontinuitet					
TF11	**Styrkelse af planer for modstandsdygtighed og kontinuitet**	Sikre, at mobilnetoperatører styrker deres planer for modstandsdygtighed og kontinuitet. Mobilnetoperatører bør sikre, at de har fastlagt tilstrækkelige planer, hvis en katastrofe påvirker den igangværende drift af deres net, og sikre, at enhver kritisk afhængighedssituation kortlægges og afbødes efter behov. Mobilnetoperatører bør kræve, at deres leverandører anvender lignende ordninger, og kun anvende leverandører, der kan påvise et tilstrækkeligt niveau af langsigtet modstandsdygtighed.	R7 R8	▪ Relevante myndigheder ▪ Operatører ▪ Leverandører ▪ Operatører af kritisk infrastruktur	ST07, ST08, ST10

STØTTETILTAG

a) Netsikkerhed				
Ref.	**Støttetiltag**	**Beskrivelse**	**Relevante aktører**	**Relaterede foranstaltninger**
ST01	**Revision eller udarbejdelse af retningslinjer og bedste praksis for netsikkerhed**	Ajourføre de eksisterende tekniske retningslinjer for sikkerhedsforanstaltninger for telekommunikationsudbydere baseret på artikel 13a i direktiv 2002/21/EF om fælles rammebestemmelser for elektroniske kommunikationsnet og -tjenester og tilpasse dem artikel 40 i den europæiske kodeks for elektronisk kommunikation, under hensyntagen til behovet for at udvikle bedste praksis med hensyn til ny teknologi og udvikling, f.eks. virtualisering af netfunktioner (NFV).	▪ Relevante myndigheder ▪ ENISA ▪ Operatører	SF01, TF01, TF04
ST02	**Styrkelse af test- og auditkapaciteten på nationalt plan og EU-plan**	Styrke kompetencer samt test- og auditkapaciteten på nationalt plan og EU-plan, herunder navnlig – støtte udviklingen af ekspertise hos udbydere af audittjenester til informationssystemer til at foretage sikkerhedsaudit af telekommunikation gennem kapacitetsopbygning og EU-investeringer i uddannelse – Kommissionen bør overveje at medtage udviklingen af en EU-certificeringsramme for udbydere af tjenester til audit af cybersikkerhed i EU's rullende arbejdsprogram med henblik på navnlig at støtte udviklingen af kapacitet til at foretage tilbundsgående teknisk audit og sikkerhedsevaluering i samarbejde med medlemsstaterne og fremme udvekslingen af oplysninger om benchmarks for certificerede udbydere af audittjenester. En EU-ramme for teknisk audit og sikkerhedsevaluering vil sikre et bedre udgangspunkt for at kræve sikkerhed fra leverandører.	▪ Relevante myndigheder ▪ Kommissionen ▪ ENISA	SF02, TF07, TF08, TF09, TF10

b) Standardisering				
ST03	**Støtte til og udformning af 5G-standarder**	Øge engagementet i relevante standardiseringsorganer, navnlig gennem styrket koordinering på EU-plan, med det formål at øge kapaciteten til at udforme standarder i overensstemmelse med de konstaterede behov ved at oprette et forum eller en gruppe af nationale regulerende myndigheder og andre kompetente myndigheder i medlemsstaterne, som skal rapportere til NIS-samarbejdsgruppen og ECCG[41], og som specifikt får til opgave at: – bidrage til at opnå en passende grad af konvergens med hensyn til tekniske foranstaltninger baseret på standardisering og certificering i overensstemmelse med gældende lovgivning, herunder bl.a. forordningen om cybersikkerhed – fremme standardisering af grænseflader for at fremme leverandørdiversificeringen – sikre forbindelsen mellem NIS-samarbejdsgruppen og relevante europæiske og/eller internationale standardiseringsorganer – sikre, at EU's industri deltager fuldt ud i og bidrager til dialogen mellem industrien og medlemsstaterne.	▪ Relevante myndigheder ▪ Kommissionen ▪ Operatører ▪ Leverandører ▪ ENISA	SF05, SF06, TF02, TF09, TF10
ST04	**Udvikling af retningslinjer for gennemførelsen af sikkerhedsforanstaltninger i eksisterende 5G-standarder**	Udvikle specifikke EU-retningslinjer for gennemførelsen af sikkerhedsforanstaltninger i eksisterende 5G-standarder (f.eks. 3GPP), herunder navnlig: – at udstede anbefalinger vedrørende de fakultative elementer af standardisering og aspekter, der ikke er omfattet af en særlig standard[42] – at identificere eksisterende mangler inden for standardisering af telekommunikationsarkitekturer/-funktioner med henblik på at mindske de identificerede risici.	▪ Relevante myndigheder ▪ ENISA	SF01, TF02
ST05	**Sikring af, at der anvendes tekniske og organisatoriske standardsikkerhedsforanstaltninger gennem en specifik EU-certificeringsordning**	Overveje at udvikle en EU-certificeringsordning inden for EU's certificeringsramme for informationssikkerhedsstyringssystemer (ISMS) for telekommunikationsudbydere.	▪ Relevante myndigheder ▪ ENISA ▪ Interessenter	TF01-06
c) Tredjepartsleverandører				

[41] Den Europæiske Cybersikkerhedscertificeringsgruppe (ECCG), som er etableret i medfør af forordningen om cybersikkerhed, er sammensat af repræsentanter for de nationale cybersikkerhedscertificeringsmyndigheder eller repræsentanter for andre relevante nationale myndigheder.

[42] Dette kan f.eks. omfatte implementering/hosting, anbefalet kommercielt tilgængelige software- og hardwarearkitekturer og -konfigurationer, overvågningsprocedurer og andre aspekter.

ST06	**Udveksling af bedste praksis for gennemførelsen af strategiske foranstaltninger, navnlig nationale rammer for vurdering af leverandørernes risikoprofil**	Udveksle god praksis for gennemførelse af strategiske foranstaltninger, navnlig vedrørende de risikofaktorer, der skal tages i betragtning (se afsnit 2.37 i rapporten om EU's koordinerede risikovurdering), når leverandørernes risikoprofil vurderes, med det formål at fremme en koordineret tilgang. Ud over de faktorer, der er anført i rapporten om EU's koordinerede risikovurdering, kan disse faktorer omfatte oplysninger, der er specifikke for den enkelte medlemsstat, f.eks. leverandørernes markedsudbredelse, nationale sikkerhedstjenesters efterretninger om trusler osv.	▪ Relevante myndigheder	SF01, SF03, SF04
d) Modstandsdygtighed og kontinuitet				
ST07	**Forbedring af koordineringen af beredskabs- og krisestyring**	Sikre, at der er gode samarbejds- og koordineringsmekanismer mellem de relevante nationale myndigheder og på EU-plan, gennem det løbende arbejde i den særlige NIS-arbejdsstrøm, i forbindelse med håndteringen af store grænseoverskridende cybersikkerhedshændelser og -kriser på grundlag af Kommissionens plan[43]. For at forberede sig på omfattende hændelser, der involverer 5G-net, kan medlemsstaterne desuden overveje at medtage 5G-scenarier i nationale og EU-dækkende cyberøvelser, hvis det er relevant.	▪ Relevante myndigheder ▪ ENISA	TF11
ST08	**Gennemførelse af audit af indbyrdes afhængighed mellem 5G-net og andre kritiske tjenester**	Analysere kritisk afhængighed mellem 5G-net og andre kritiske sektorer, f.eks. elforsyning, og sektorafhængighed for 5G, f.eks. vandforsyning og transport. Dette bør også omfatte cirkulær afhængighed (f.eks. 5G-net, der er afhængigt af elforsyning, hvor elforsyningen samtidig er afhængig af 5G-net).	▪ Relevante myndigheder	TF11
e) Samarbejde og koordinering				
ST09	**Styrkelse af mekanismerne for samarbejde, koordinering og informationsudveksling**	Overveje anvendelsen af eksisterende mekanismer for samarbejde, koordinering og informationsudveksling, herunder tiltag og støtte fra ENISA, navnlig gennem regelmæssige trusselsvurderinger.	▪ Relevante myndigheder ▪ ENISA	TF01, TF05, TF09, TF10

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

f) Offentlige udbud				
ST10	**Sikring af 5G-projekter, der modtager offentlig støtte, under hensyntagen til cybersikkerhedsrisici**	Udvikle detaljerede retningslinjer for 5G-relaterede sikkerhedsbestemmelser i offentlige udbud og EU-finansieringsprogrammer (Horisont Europa, programmet for et digitalt Europa og Connecting Europe-faciliteten). Disse retningslinjer kan udarbejdes inden for komitologiproceduren af udvalgsmedlemmer, der er udpeget af medlemsstaterne, i forbindelse med udarbejdelsen af de årlige arbejdsprogrammer under de forskellige finansieringsprogrammer. Offentlige finansieringsprogrammer, f.eks. Connecting Europe-facilitetens digitale område, forventes at få afgørende indflydelse på, hvordan 5G-nettet vil blive udrullet i Europe, f.eks. 5G-korridorer til opkoblet og automatiseret mobilitet og 5G-konnektivitet hos de socioøkonomiske drivkræfter. Ovennævnte retningslinjer bør derfor anvendes ved gennemførelsen af disse programmer. Når der etableres konsortier for sådanne projekter med deltagelse af eller administrativ støtte fra offentlige myndigheder, og der er konstateret cybersikkerhedsrisici (især risici, der er identificeret i rapporten om EU's koordinerede risikovurdering, og de risikobegrænsende foranstaltninger, der er beskrevet i denne værktøjskasse), bør de tages i betragtning ved udvælgelsen af leverandører eller andre projektdeltagere. I EU-direktiverne og EU's politikker opfordres medlemsstaterne i forbindelse med offentlige udbud til ikke at tildele kontrakter udelukkende på grundlag af den laveste pris, men også til at tage hensyn til kvalitet på områder såsom sikkerheds-, arbejdskraft- og miljøkrav. I sin henstilling af 26. marts 2019 henviser Kommissionen endvidere specifikt til den mulige udvikling og gennemførelse af europæiske cybersikkerhedscertificeringsordninger i forbindelse med offentlige udbud, der vedrører 5G-net.	▪ Relevante myndigheder ▪ Kommissionen	SF03-08 TF01-11

- # Tabel 2: Risikobegrænsningsplaner

I tabel 2 nedenfor præsenteres risikobegrænsningsplaner for hvert af de risikoområder, der er identificeret i rapporten om EU's koordinerede risikovurdering.

I den anslåede grad af **forventet effektivitet** tages der også højde for den oprindelige risiko og den forventede resterende risiko efter anvendelse af foranstaltningen, og følgende skala benyttes:

- Meget høj: Foranstaltningen anses for at være effektiv i meget høj grad, dvs. at den forventes at kunne begrænse de tilknyttede risici næsten fuldstændigt.
- Høj: Foranstaltningen anses for at være effektiv i høj grad, dvs. at den forventes at kunne begrænse de tilknyttede risici betydeligt.
- Middel: Foranstaltningen anses for at være delvist effektiv, dvs. at den forventes at kunne begrænse de tilknyttede risici i en vis grad.
- Lav: Foranstaltningen anses ikke for at være særlig effektiv, dvs. at den forventes kun at kunne begrænse de tilknyttede risici marginalt.

For hver foranstaltning angiver tabellen om risikobegrænsningsplaner (bilag 1, tabel 2) andre mulige parametre og karakteristika med det formål at hjælpe medlemsstaterne med at udvælge og gennemføre foranstaltninger:

- potentielle **gennemførelsesfaktorer** (både positive og/eller negative):
  - ressourceomkostninger
  - sektorspecifikke økonomiske virkninger (for operatører eller for leverandører)
  - bredere økonomiske og/eller samfundsmæssige virkninger

- vejledende **tidsrammer** for iværksættelse af de nødvendige tiltag for at gennemføre foranstaltningerne ved brug af følgende skala:
  - Kort sigt: 0-2 år
  - Mellemlang sigt: 2-5 år
  - Lang sigt: > 5 år

Risiko 1: **Fejlkonfigurering af net** Risikobegrænsningsplan: Øge nettets sikkerhed og modstandsdygtighed			
Mest relevante/virkningsfulde foranstaltninger	**Forventet effektivitet**	**Potentielle gennemførelsesfaktorer**	**Vejledende tidsramme**
Reguleringsbeføjelser: SF01: Styrkelse af de nationale myndigheders rolle SF02: Audit af operatører og krav om oplysninger	Afhænger af gennemførelsen af foranstaltninger, men kan være **MEGET HØJ.**	▪ Ressourceomkostninger ▪ Sektorspecifikke økonomiske virkninger (for operatører og leverandører) ▪ (Potentielt) bredere økonomiske og/eller samfundsmæssige virkninger	**KORT** sigt
Netsikkerhed – grundlæggende foranstaltninger TF01: Sikring af, at der anvendes grundlæggende sikkerhedskrav (sikkert netdesign og sikker netarkitektur) TF02: Sikring og evaluering af gennemførelsen af sikkerhedsforanstaltninger i eksisterende 5G-standarder	Afhænger af foranstaltningernes omfang, men kan være **MIDDEL** til **HØJ**.	▪ Ressourceomkostninger ▪ Sektorspecifikke økonomiske virkninger	**KORT** sigt
Netsikkerhed – særlige 5G-foranstaltninger TF03: Sikring af strenge adgangskontroller TF04: Forøgelse af sikkerheden af virtualiserede netfunktioner TF05: Sikring af sikker styring, drift og overvågning af 5G-net TF07: Styrkelse af softwareintegritet og -opdatering samt styring af rettelser	Afhænger af foranstaltningernes omfang, men kan være **HØJ**.	▪ Ressourceomkostninger ▪ Sektorspecifikke økonomiske virkninger	**KORT** sigt. Afhænger af tidsplanen for 5G-udrulningen.
Risiko 2: **Manglende adgangskontrol** Risikobegrænsningsplan: Øge nettets sikkerhed, herunder navnlig ved at **styrke reglerne for leverandørers adgang og for anvendelsen af tjenesteudbydere og tredjelinjesupport**			
Mest relevante/virkningsfulde foranstaltninger	**Forventet effektivitet**	**Potentielle gennemførelsesfaktorer**	**Vejledende tidsramme**
Reguleringsbeføjelser: SF01: Styrkelse af de nationale myndigheders rolle SF02: Audit af operatører og krav om oplysninger	Afhænger af gennemførelsen af foranstaltninger, men kan være **MEGET HØJ.**	▪ Ressourceomkostninger ▪ Sektorspecifikke økonomiske virkninger (operatører) ▪ (Potentielt) bredere økonomiske og/eller samfundsmæssige virkninger	**KORT** sigt

Tredjepartsleverandører SF03: Vurdering af leverandørernes risikoprofil og anvendelse af restriktioner over for leverandører, der vurderes at udgøre en høj risiko, i forbindelse med centrale aktiver SF04: Kontrol med brugen af tjenesteudbydere og udstyrsleverandørers tredjelinjesupport	Afhænger af foranstaltningernes omfang, men kan være **HØJ**.	▪ Ressourceomkostninger ▪ Sektorspecifikke økonomiske virkninger (for operatører og leverandører) ▪ (Potentielt) bredere økonomiske og/eller samfundsmæssige virkninger	**KORT** sigt. Afhænger af tidsplanen for 5G-udrulningen.
Netsikkerhed – grundlæggende foranstaltninger TF01: Sikring af, at der anvendes grundlæggende sikkerhedskrav (sikkert netdesign og sikker netarkitektur) TF02: Sikring og evaluering af gennemførelsen af sikkerhedsforanstaltninger i eksisterende 5G-standarder	Afhænger af foranstaltningernes omfang, men kan være **MIDDEL**.	▪ Ressourceomkostninger ▪ Sektorspecifikke økonomiske virkninger	**KORT** sigt
Netsikkerhed – særlige 5G-foranstaltninger TF03: Sikring af strenge adgangskontroller TF05: Sikring af sikker styring, drift og overvågning af 5G-net	Afhænger af foranstaltningernes omfang, men kan være **HØJ**.	▪ Ressourceomkostninger ▪ Sektorspecifikke økonomiske virkninger (operatører)	**KORT** sigt. Afhænger af tidsplanen for 5G-udrulningen.
Risiko 3: **Dårlig udstyrskvalitet** Risikobegrænsningsplan: **Lægge pres på eller anvende incitamenter over for leverandører med det formål at øge produktkvaliteten og nettets sikkerhed og modstandsdygtighed**			
Mest relevante/virkningsfulde foranstaltninger	**Forventet effektivitet**	**Potentielle gennemførelsesfaktorer**	**Vejledende tidsramme**
Reguleringsbeføjelser: SF01: Styrkelse af de nationale myndigheders rolle SF02: Audit af operatører og krav om oplysninger	Afhænger af foranstaltningernes omfang, men kan være HØJ eller **MEGET HØJ.**	▪ Ressourceomkostninger ▪ Sektorspecifikke økonomiske virkninger (operatører) ▪ (Potentielt) bredere økonomiske og/eller samfundsmæssige virkninger	**KORT** sigt
Netsikkerhed – grundlæggende foranstaltninger TF01: Sikring af, at der anvendes grundlæggende sikkerhedskrav (sikkert netdesign og sikker netarkitektur) TF02: Sikring og evaluering af gennemførelsen af sikkerhedsforanstaltninger i eksisterende 5G-standarder	Afhænger af foranstaltningernes omfang, men kan være **MIDDEL**.	▪ Ressourceomkostninger ▪ Sektorspecifikke økonomiske virkninger	**KORT** sigt

Netsikkerhed – særlige 5G-foranstaltninger TF03: Sikring af strenge adgangskontroller TF04: Forøgelse af sikkerheden af virtualiserede netfunktioner TF05: Sikring af sikker styring, drift og overvågning af 5G-net TF07: Styrkelse af softwareintegritet og -opdatering samt styring af rettelser	Afhænger af foranstaltningernes omfang, men kan være **HØJ**.	▪ Ressourceomkostninger ▪ Sektorspecifikke økonomiske virkninger (for operatører og leverandører)	**KORT** sigt. Afhænger af tidsplanen for 5G-udrulningen.
Krav til leverandørers processer og udstyr TF08: Forbedring af sikkerhedsstandarderne i leverandørernes processer gennem robuste indkøbsbetingelser TF09: Anvendelse af EU-certificering for 5G-netkomponenter og/eller leverandørers processer	**MIDDEL** (muligvis HØJ på lang sigt)	▪ Ressourceomkostninger ▪ Sektorspecifikke økonomiske virkninger (for operatører og leverandører)	**MELLEMLANG og LANG** sigt
Risiko 4: **Afhængighed af en enkelt leverandør** Risikobegrænsningsplan: **Sikre leverandørdiversificering for hver operatør og hvert geografisk område på nationalt plan og fremme langsigtet bæredygtighed for 5G-forsyningskæden**			
Mest relevante/virkningsfulde foranstaltninger	**Forventet effektivitet**	**Potentielle gennemførelsesfaktorer**	**Vejledende tidsramme**
Reguleringsbeføjelser: SF01: Styrkelse af de nationale myndigheders rolle SF02: Audit af operatører og krav om oplysninger	Afhænger af foranstaltningernes omfang, men kan være **HØJ eller MEGET HØJ**	▪ Ressourceomkostninger ▪ Sektorspecifikke økonomiske virkninger (operatører) (Potentielt) bredere økonomiske og/eller samfundsmæssige virkninger	**KORT** sigt
Diversificering af leverandører: SF05: Sikring af de enkelte mobilnetoperatørers leverandørdiversificering gennem hensigtsmæssige flerleverandørstrategier SF06: Styrkelse af modstandsdygtigheden på nationalt plan	Afhænger af foranstaltningens omfang, men kan være **MEGET HØJ**	▪ Ressourceomkostninger ▪ Sektorspecifikke økonomiske virkninger (for operatører og leverandører)[44] ▪ (Potentielt) bredere økonomiske og/eller samfundsmæssige virkninger	**KORT til MELLEMLANG** sigt. Afhænger af tidsplanen for 5G-udrulningen.

[44] Med hensyn til foranstaltningen SF05 afhænger den sektorspecifikke økonomiske virkning også af den eksisterende diversificering

Bæredygtighed og diversificering i 5G-forsyningskæden og -værdikæden: SF07: Identifikation af centrale aktiver og fremme af et diversificeret og bæredygtigt 5G-økosystem i EU SF08: Opretholdelse og opbygning af diversificering og EU-kapacitet i fremtidige netteknologier.	Afhænger af foranstaltningens omfang, men kan være **MEGET HØJ**	▪ Ressourceomkostninger ▪ Sektorspecifikke økonomiske virkninger (for operatører og leverandører) ▪ (Potentielt) bredere økonomiske virkninger	**KORT, MELLEMLANG og LANG** sigt
Risiko 5: **Statslig indblanding via 5G-forsyningskæden** Risikobegrænsningsplan: Begrænse brugen af **højrisikoleverandører og styrke processer for adgangskontrol, netovervågning og styring af rettelser**			
Mest relevante/virkningsfulde foranstaltninger	**Forventet effektivitet**	**Potentielle gennemførelsesfaktorer**	**Vejledende tidsramme**
Reguleringsbeføjelser: SF01: Styrkelse af de nationale myndigheders rolle SF02: Audit af operatører og krav om oplysninger	Afhænger af foranstaltningernes omfang, men kan være **HØJ** eller **MEGET HØJ**	▪ Ressourceomkostninger ▪ Sektorspecifikke økonomiske virkninger (operatører) ▪ (Potentielt) bredere økonomiske og/eller samfundsmæssige virkninger	**KORT** sigt
Tredjepartsleverandører SF03: Vurdering af leverandørernes risikoprofil og anvendelse af restriktioner over for leverandører, der vurderes at udgøre en høj risiko, i forbindelse med centrale aktiver SF04: Kontrol med brugen af tjenesteudbydere og leverandørers tredjelinjesupport	Afhænger af omfanget af foranstaltninger og eksponeringen for højrisikoleverandører, men kan være **MEGET HØJ**	▪ Ressourceomkostninger ▪ Sektorspecifikke økonomiske virkninger (for operatører og leverandører) ▪ (Potentielt) bredere økonomiske og/eller politiske virkninger	**KORT** sigt. Afhænger af tidsplanen for 5G-udrulningen
Netsikkerhed – særlige 5G-foranstaltninger TF03: Sikring af strenge adgangskontroller TF05: Sikring af sikker styring, drift og overvågning af 5G-net TF07: Styrkelse af softwareintegritet og -opdatering samt styring af rettelser	Hvis foranstaltningen gennemføres alene, kan den være **MIDDEL**	▪ Ressourceomkostninger ▪ Sektorspecifikke økonomiske virkninger	**KORT** sigt. Afhænger af tidsplanen for 5G-udrulningen.
Risiko 6: **Organiserede kriminelle gruppers udnyttelse af 5G-net** Risikobegrænsningsplan: **Øge nettets sikkerhed og forbedre kvaliteten af leverandørens processer og udstyr**			
Mest relevante/virkningsfulde foranstaltninger	**Forventet effektivitet**	**Potentielle gennemførelsesfaktorer**	**Vejledende tidsramme**

Reguleringsbeføjelser SF01: Styrkelse af de nationale myndigheders rolle SF02: Audit af operatører og krav om oplysninger	Afhænger af foranstaltningernes omfang, men kan være HØJ eller **MEGET HØJ**	▪ Ressourceomkostninger ▪ Sektorspecifikke økonomiske virkninger (operatører) ▪ (Potentielt) bredere økonomiske og/eller samfundsmæssige virkninger	**KORT** sigt
Netsikkerhed – grundlæggende foranstaltninger TF01: Sikring af, at der anvendes grundlæggende sikkerhedskrav (sikkert netdesign og sikker netarkitektur) TF02: Sikring og evaluering af gennemførelsen af sikkerhedsforanstaltninger i eksisterende 5G-standarder	Afhænger af foranstaltningernes omfang, men kan være **MIDDEL til HØJ**.	▪ Ressourceomkostninger ▪ Sektorspecifikke økonomiske virkninger	**KORT** sigt
Netsikkerhed – særlige 5G-foranstaltninger TF03: Sikring af strenge adgangskontroller TF04: Forøgelse af sikkerheden af virtualiserede netfunktioner TF05: Sikring af sikker styring, drift og overvågning af 5G-net TF06: Styrkelse af den fysiske sikkerhed TF07: Styrkelse af softwareintegritet og -opdatering samt styring af rettelser	Afhænger af foranstaltningernes omfang, men kan være **HØJ**.	▪ Ressourceomkostninger ▪ Sektorspecifikke økonomiske virkninger	**KORT** sigt. Afhænger af tidsplanen for 5G-udrulningen.
Krav til leverandørers processer og udstyr TF08: Forbedring af sikkerhedsstandarderne i leverandørernes processer gennem robuste indkøbsbetingelser TF09: Anvendelse af EU-certificering for 5G-netkomponenter og/eller leverandørers processer	**MIDDEL** (muligvis HØJ på lang sigt)	▪ Ressourceomkostninger ▪ Sektorspecifikke økonomiske virkninger (for operatører og leverandører)	**MELLEMLANG og LANG** sigt
Risiko 7: **Væsentlige forstyrrelser af kritiske infrastrukturer eller tjenester** Risikobegrænsningsplan: **Øge nettets sikkerhed, modstandsdygtighed og kontinuitet og forbedre kvaliteten af leverandørens processer og udstyr**			
Mest relevante/virkningsfulde foranstaltninger	**Forventet effektivitet**	**Potentielle gennemførelsesfaktorer**	**Vejledende tidsramme**
Reguleringsbeføjelser: SF01: Styrkelse af de nationale myndigheders rolle SF02: Audit af operatører og krav om oplysninger	Afhænger af foranstaltningernes omfang, men kan være HØJ eller **MEGET HØJ**	▪ Ressourceomkostninger ▪ Sektorspecifikke økonomiske virkninger (operatører) ▪ (Potentielt) bredere økonomiske og/eller samfundsmæssige virkninger	**KORT** sigt

Netsikkerhed – grundlæggende foranstaltninger TF01: Sikring af, at der anvendes grundlæggende sikkerhedskrav (sikkert netdesign og sikker netarkitektur) TF02: Sikring og evaluering af gennemførelsen af sikkerhedsforanstaltninger i eksisterende 5G-standarder	Afhænger af foranstaltningernes omfang, men kan være **MIDDEL til HØJ**.	▪ Ressourceomkostninger Sektorspecifikke økonomiske virkninger	**KORT** sigt
Netsikkerhed – særlige 5G-foranstaltninger TF03: Sikring af strenge adgangskontroller TF04: Forøgelse af sikkerheden af virtualiserede netfunktioner TF05: Sikring af sikker styring, drift og overvågning af 5G-net TF06: Styrkelse af den fysiske sikkerhed TF07: Styrkelse af softwareintegritet og -opdatering samt styring af rettelser	Afhænger af foranstaltningernes omfang, men kan være **HØJ**.	▪ Ressourceomkostninger Sektorspecifikke økonomiske virkninger	**KORT** sigt. Afhænger af tidsplanen for 5G-udrulningen.
Krav til leverandørers processer og udstyr TF08: Forbedring af sikkerhedsstandarderne i leverandørernes processer gennem robuste indkøbsbetingelser TF09: Anvendelse af EU-certificering for 5G-netkomponenter og/eller leverandørers processer	**MIDDEL** (muligvis HØJ på lang sigt)	▪ Ressourceomkostninger ▪ Sektorspecifikke økonomiske virkninger (for operatører og leverandører)	**MELLEMLANG og LANG** sigt
Modstandsdygtighed og kontinuitet: TF11: Styrkelse af planer for modstandsdygtighed og kontinuitet	Afhænger af foranstaltningernes omfang, men kan være **HØJ**.	▪ Ressourceomkostninger ▪ Sektorspecifikke økonomiske virkninger	**KORT** sigt. Afhænger af tidsplanen for 5G-udrulningen.
Risiko 8: **Massive netnedbrud som følge af afbrydelse af elforsyningen** Risikobegrænsningsplan: **Sikre modstandsdygtighed og kontinuitet og øge nettets sikkerhed**			
Mest relevante/virkningsfulde foranstaltninger	**Forventet effektivitet**	**Potentielle gennemførelsesfaktorer**	**Vejledende tidsramme**
Netsikkerhed – grundlæggende foranstaltninger TF01: Sikring af, at der anvendes grundlæggende sikkerhedskrav (sikkert netdesign og sikker netarkitektur)	Afhænger af gennemførelsen, men kan være **MEGET HØJ.**	▪ Ressourceomkostninger ▪ Sektorspecifikke økonomiske virkninger	**KORT** sigt
Modstandsdygtighed og kontinuitet: TF11: Styrkelse af planer for modstandsdygtighed og kontinuitet	Afhænger af foranstaltningernes omfang, men kan være **HØJ**.	▪ Ressourceomkostninger ▪ Sektorspecifikke økonomiske virkninger	**KORT** sigt. Afhænger af tidsplanen for 5G-udrulningen.
R9: **Udnyttelse af IoT** Risikobegrænsningsplan: **Øge nettets sikkerhed og forbedre sikkerheden i slutbrugernes IoT-enheder**			

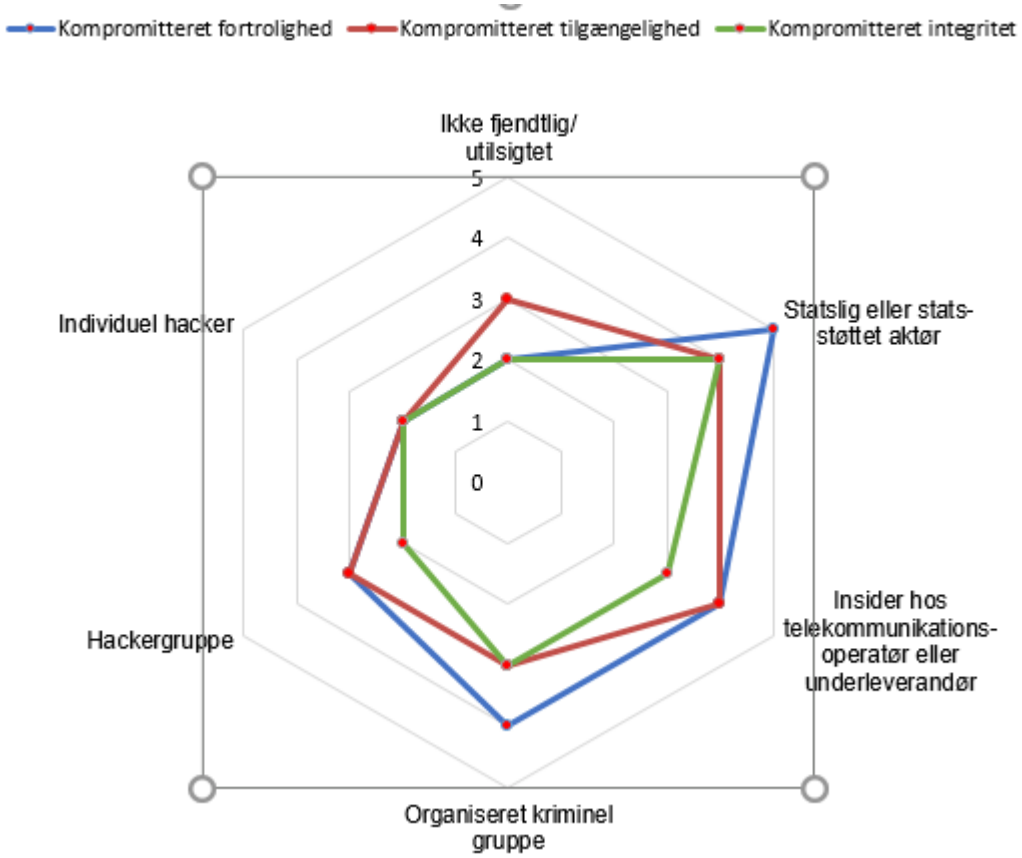
Mest relevante/virkningsfulde foranstaltninger	Forventet effektivitet	Potentielle gennemførelsesfaktorer	Vejledende tidsramme
Netsikkerhed – grundlæggende foranstaltninger TF01: Sikring af, at der anvendes grundlæggende sikkerhedskrav (sikkert netdesign og sikker netarkitektur) TF02: Sikring og evaluering af gennemførelsen af sikkerhedsforanstaltninger i eksisterende 5G-standarder	Afhænger af foranstaltningernes omfang, men kan være **MIDDEL**.	▪ Ressourceomkostninger ▪ Sektorspecifikke økonomiske virkninger	**KORT** sigt
Netsikkerhed – særlige 5G-foranstaltninger TF05: Sikring af sikker styring, drift og overvågning af 5G-net	Afhænger af foranstaltningernes omfang, men kan være **HØJ**.	▪ Ressourceomkostninger ▪ Sektorspecifikke økonomiske virkninger	**KORT** sigt. Afhænger af tidsplanen for 5G-udrulningen.
Krav til leverandørers processer og udstyr TF10: Anvendelse af certificering for andre ikke-5G-specifikke produkter og tjenester (tilsluttede enheder og cloudtjenester)	**HØJ**	▪ Ressourceomkostninger ▪ Sektorspecifikke økonomiske virkninger	**MELLEMLANG og LANG** sigt

Bilag 2 – Sammendrag af resultaterne af EU's koordinerede risikovurdering[45]

EU's koordinerede risikovurdering følger den tilgang, der er fastlagt i ISO/IEC: 27005 Risk Assessment Methodology. Den afspejler vurderingen af en række parametre:

- de vigtigste former for trusler mod 5G-net
- de vigtigste trusselsaktører
- de vigtigste aktiver og deres grad af følsomhed
- de vigtigste sårbarheder og
- de vigtigste risici og relaterede scenarier.

Trusler, aktiver og sårbarheder



Figur 1 – Oversigt over trusselskategorier efter trusselsaktører

[45] Hele rapporten: https://EF.europa.eu/digital-single-market/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security.

Trusler

Trusler fra stater eller statsstøttede aktører vurderes at være de mest relevante. De repræsenterer netop de alvorligste og samtidig de mest sandsynlige trusselsaktører, da de kan have den nødvendige motivation, hensigt og vigtigst kapacitet til at gennemføre vedvarende og sofistikerede angreb på 5G-nettenes sikkerhed.

Kombinationen af motivation, hensigt og kapacitet på højt niveau sætter stater i stand til at gennemføre angreb, som kan være meget komplekse og have stor indflydelse på væsentlige tjenester for offentligheden, hvilket vil forringe tilliden til mobile teknologier og operatører. Stater eller statsstøttede aktører kan f.eks. forårsage omfattende afbrydelser eller betydelige forstyrrelser af telekommunikationstjenester ved at udnytte udokumenterede funktioner eller angribe indbyrdes afhængige kritiske infrastrukturer (f.eks. elforsyningen).

Med hensyn til statslige og statsstøttede aktører kan der konstateres en særlig trussel fra tredjelandes cyberangreb. Flere medlemsstater har – baseret på visse enheders tidligere angreb eller eksistensen af et bestemt tredjelands offensive cyberprogram mod dem – konstateret, at visse tredjelande udgør en særlig cybertrussel for deres nationale interesser.

Det bemærkes også, at insidere eller underleverandører under visse omstændigheder også kan betragtes som potentielle trusselsaktører, især hvis de mobiliseres af stater, idet en stat kan bruge dem til at få adgang til kritiske målaktiver.

Yderligere kategorier af aktører kan også anses for at have en vigtig motivation til og interesse i at få adgang til 5G-net, f.eks. organiserede kriminelle grupper, virksomheder, der søger at opnå konkurrencefordele på det teknologiske område gennem tyveri af intellektuel ejendom, eller cyberterrorister.

Netaktiver

KATEGORIER AF ELEMENTER OG FUNKTIONER		EKSEMPLER PÅ CENTRALE ELEMENTER
Kernenetfunktioner	**KRITISK**	Autentificering af brugerudstyr, roaming og funktioner til sessionsstyring
		Funktioner til transport af brugerudstyrsdata
		Styring af adgangsregler
		Registrering og godkendelse af nettjenester
		Lagring af slutbruger- og netdata
		Link til tredjepartsmobilnet
		Kernenetfunktioners eksponering for eksterne applikationer
		Slutbrugerenheders attribution til network slices
Netforvaltnings- og netorkestreringsfunktioner (MANO-funktioner)	**KRITISK**	
	MODERAT/HØJ	Sikkerhedsstyringssystemer

Forvaltningssystemer og støttetjenester (ud over MANO-funktioner)		Fakturering og andre støttesystemer, f.eks. netpræstation
Radioadgangsnet	**HØJ**	Basisstationer
Transport- og transmissionsfunktioner	**MODERAT/HØJ**	Netudstyr på lavt niveau (routere, switches osv.)
		Filtreringsudstyr (firewalls, IPS osv.)
Udvekslinger mellem net	**MODERAT/HØJ**	IP-net uden for mobilnetoperatørens lokaler Nettjenester leveret af tredjeparter

Kernenetfunktioner i 5G-nettet anses generelt for at være kritiske. Påvirkning af kernenettet kan potentielt kompromittere fortroligheden, tilgængeligheden og integriteten af alle nettjenesterne (mens kompromittering af andre komponenter kan have en mere begrænset virkning og f.eks. kun påvirke en specifik funktion eller et bestemt område). De mest følsomme data overføres desuden via kernenetkomponenter.

Forvaltningssystemer og støttetjenester (MANO-funktioner mv.) anses for vigtige, selv om disse systemer ikke overfører data, da de kontrollerer vigtige netelementer og derfor kan anvendes til at udføre ondsindede handlinger, f.eks. sabotage og spionage med alvorlige konsekvenser. Tabet af disse systemers og tjenesters integritet kan desuden medføre alvorlige driftsforstyrrelser i 5G-nettet.

Blandt de centrale funktioner og forvaltningssystemer/støttetjenester vurderes en række elementer og funktioner at have særligt stor betydning, herunder navnlig: MANO-funktioner, centrale adgangs- og kontrolfunktioner, sikkerhedsfunktioner, funktioner til lovlig aflytning, krypteringsinfrastruktur, der er nødvendig for at konfigurere og drive 5G-net, og specifikke styringsfunktioner.

Netadgangsfunktioner anses også for at have relativt høj følsomhed. Vurderingen af specifikke elementers følsomhed i forbindelse med adgangsfunktionerne varierer imidlertid afhængigt af en række faktorer. I de kommende udviklingsfaser af 5G vil traditionelt mindre følsomme dele af nettet få større betydning og blive mere følsomme. Det gælder f.eks. visse elementer i nettets radioadgangsdel, afhængigt af det omfang, hvori de håndterer brugerdata eller udfører intelligente eller følsomme funktioner. Når edge computing indføres, forventes visse kernenetfunktioner desuden fysisk at blive flyttet længere ud i nettet, tættere på adgangsstederne.

Transport- og transmissionsfunktioner anses for moderat til meget følsomme. Ligesom adgangsfunktionerne varierer vurderingen af specifikke elementers følsomhed i forbindelse med transport- og transmissionsfunktionerne imidlertid afhængigt af en række faktorer.

Funktioner til udveksling mellem net anses for moderat til meget følsomme, afhængigt af deres rolle i forbindelserne mellem mobilnetoperatører.

Andre aktiver

I forbindelse med centrale aktiver kræver en række enheder og kategorier af brugere særlig opmærksomhed. Det gælder navnlig:

- operatører af kritiske tjenester omhandlet i NIS-direktivet og operatører af kritisk infrastruktur
- offentlige enheder, retshåndhævende myndigheder, beredskabstjenesterne og militæret
- centrale sektorer/enheder, der ikke er omfattet af cybersikkerhedsbestemmelser
- strategiske private virksomheder og
- områder eller enheder, hvor der ikke findes en backupløsning, hvis 5G-nettet svigter.

En række medlemsstater har udpeget geografiske områder, som er særligt følsomme, på grundlag af en analyse af demografiske, økonomiske, samfundsmæssige og nationale sikkerhedsfaktorer. Nogle områder vil faktisk blive udsat for alvorligere forstyrrelser som følge af koncentrationen af økonomisk og samfundsmæssig afhængighed af net- og informationssystemer (f.eks. i tilfældet af intelligente byer), eller fordi de rummer følsomme enheder eller kategorier af brugere.

Sårbarheder

I rapporten vurderes tre primære typer sårbarheder:

1. ***Sårbarheder i forbindelse med hardware, software, processer og politikker***

Som enhver anden digital infrastruktur kan 5G-net være forbundet med en række generelle tekniske sårbarheder, som kan påvirke software og hardware eller være resultatet af potentielle mangler i de forskellige aktørers sikkerhedsprocesser[46]. I en tidlig udrulningsfase skal der desuden også tages behørigt hensyn til sårbarheder i den eksisterende 3G- og 4G-infrastruktur.

Mange af disse sårbarheder er ikke specifikke for 5G-net, men deres antal og betydning forventes at stige i forbindelse med 5G som følge af teknologiens øgede kompleksitet og økonomiernes og samfundenes stadig større afhængighed af denne infrastruktur.

Proces- eller konfigurationsrelaterede sårbarheder vurderes at være særligt vigtige i det fremtidige 5G-miljø:

For alle interessenter, navnlig mobilnetoperatører og deres leverandører:

- mangel på specialiseret og uddannet personale til at sikre, overvåge og vedligeholde 5G-net
- mangel på tilstrækkelige interne sikkerhedskontroller, overvågningspraksisser og sikkerhedsstyringssystemer og utilstrækkelige risikostyringspraksisser

[46] Praksis for en af de største leverandører af netudstyr til 4G-tjenester er f.eks. blevet undersøgt af Det Forenede Kongeriges Huawei Cybersecurity Evaluation Centre (HSCEC).

- manglende eller utilstrækkelige sikkerhedsprocedurer eller operationelle vedligeholdelsesprocedurer, f.eks. softwareopdatering/styring af rettelser og
- manglende overholdelse af 3GPP-standarder eller ukorrekt gennemførelse af standarder.

For mobilnetoperatører:

- dårligt netdesign og dårlig netarkitektur
- dårlig fysisk sikkerhed for net- og IT-infrastruktur
- dårlige politikker for lokal- og fjernadgang til netkomponenter
- manglende eller utilstrækkelige sikkerhedskrav i indkøbsprocessen og
- dårlig ændringsstyringsproces.

2. Leverandørspecifikke sårbarheder

Den øgede betydning af software og tjenester, der leveres af tredjepartsleverandører i 5G-net, medfører en større eksponering for en række sårbarheder, som kan skyldes enkelte leverandørers risikoprofil. Enkelte leverandørers risikoprofiler kan vurderes på grundlag af flere faktorer, herunder:

- sandsynligheden for, at leverandøren udsættes for indgriben fra et tredjeland. Dette er et af de centrale aspekter ved vurderingen af de ikketekniske svagheder i forbindelse med 5G-net[47]. Sådan indgriben kan fremmes ved, men ikke begrænses til tilstedeværelsen af følgende faktorer:
    - en stærk forbindelse mellem leverandøren og et bestemt tredjelands regering
    - tredjelandets lovgivning, navnlig hvis der ikke findes nogen lovgivningsmæssig eller demokratisk kontrol eller domstolsprøvelse, eller hvis der ikke findes aftaler om sikkerhed eller databeskyttelse mellem EU og det pågældende tredjeland[48]
    - leverandørens ejerforhold og
    - tredjelandets mulighed for at udøve enhver form for pression, herunder i forbindelse med produktionsstedet for udstyret.
- leverandørens evne til at sikre leveringen
- den generelle kvalitet af leverandørens produkter og cybersikkerhedspraksis, herunder graden af kontrol over vedkommendes egen forsyningskæde, og om sikkerhedspraksis prioriteres tilstrækkeligt.

Ved vurderingen af leverandørens risikoprofil kan der også tages hensyn til meddelelser udstedt af EU-myndigheder og/eller medlemsstaternes nationale myndigheder.

3. Sårbarheder som følge af afhængighed af enkelte leverandører

[47] En trusselsaktørs direkte adgang til eller indflydelse på forsyningskæden for telekommunikation kan gøre det betydeligt lettere for vedkommende at udføre ondsindede handlinger, og virkningen af sådanne handlinger kan derved blive betydeligt værre, men det bør også bemærkes, at aktører med målrettede hensigter og kapaciteter, f.eks. en statslig aktør, muligvis vil forsøge at udnytte sårbarheder på ethvert trin i livscyklussen for leverandørens produkter.

[48] I denne forbindelse tildeler flere medlemsstater leverandører, som hører under jurisdiktionen for tredjelande, der fører en offensiv cyberpolitik, en højere risikoprofil.

Inden for individuelle net skaber en stor afhængighed af en enkelt leverandør (monokultur) afhængighed af specifikke løsninger og gør det vanskeligere at indkøbe løsninger fra andre leverandører, især hvis løsningerne ikke er fuldt interoperable.

Følgelig eksponeres EU-baserede operatører, som bliver for afhængige af en enkelt leverandør, for en række risici, f.eks. fordi den pågældende leverandør udsættes for kommercielt pres, går ned, fusioneres eller overtages eller underlægges sanktioner.

På nationalt plan og EU-plan øges den generelle sårbarhed i 5G-infrastrukturen af manglende leverandørdiversificering, især hvis et stort antal operatører køber deres følsomme aktiver hos en leverandør med en høj risiko som beskrevet ovenfor. Afhængighed af et eller flere net har også stor betydning for modstandsdygtigheden på nationalt plan og EU-plan og skaber punkter, der kan forårsage nedbrud af hele systemet.

Tilstedeværelsen af et begrænset antal leverandører på markedet kan desuden mindske deres incitament til at udvikle sikrere produkter. Det kan også have en negativ indvirkning på de nationale myndigheders og operatørers muligheder for at kræve højere sikkerhedsgarantier, især for mindre medlemsstater eller operatører.

Primære risici og risikoscenarier

I EU's koordinerede risikovurdering udpeges en række risikokategorier, der illustreres ved konkrete risikoscenarier, som beskriver angrebsveje, som en trusselsaktør kan bruge til at nå sit mål:

I – Risikoscenarier ved utilstrækkelige sikkerhedsforanstaltninger	**R1 –** Fejlkonfigurering af net Ved at udnytte dårligt konfigurerede systemer og arkitekturer trænger en statslig aktør ind i 5G-nettet via dets eksterne grænseflader, og det medfører en kompromittering af nettets kernefunktioner, eller bruger edge computing-noder til at kompromittere fortroligheden og afbryde distribuerede tjenester. **R2 –** Manglende adgangskontrol En underleverandør med administratorrettigheder på nettet udfører en utilsigtet handling, som medfører et brud på systemets fortrolighed/integritet og/eller tilgængelighed. Underleverandørens handling kan skyldes et lovkrav, der er pålagt af et tredjeland, eller uansvarlig adfærd fra vedkommendes personales side.
II – Risikoscenarier i forbindelse med 5G-forsyningskæden	**R3 –** Dårlig kvalitet af produkterne Spionage fra statslige eller statsstøttede aktører, som anvender malware til at misbruge netkomponenter af dårlig kvalitet eller utilsigtede sårbarheder, som påvirker følsomme elementer i hovednettet, f.eks. virtualisering af netfunktioner. **R4 –** Afhængighed af en enkelt leverandør inden for de enkelte net eller manglende diversificering på landsplan En mobilnetoperatør indkøber en stor del af vedkommendes følsomme netkomponenter eller -tjenester hos en enkelt leverandør. Tilgængeligheden af udstyr og/eller opdateringer fra denne leverandør begrænses drastisk som følge af leverandørens manglende levering (f.eks. på grund af et tredjelands handelssanktioner eller andre

	kommercielle omstændigheder). Følgelig falder kvaliteten af leverandørens udstyr på grund af prioriteringen af forsyningssikkerheden i forhold til forbedringer af produktsikkerheden.
III – Risikoscenarier i forbindelse med de primære trusselsaktørers modus operandi	**R5 –** Statslig indblanding via 5G-forsyningskæden: En fjendtlig statslig aktør lægger pres på en leverandør under aktørens jurisdiktion for at få adgang til følsomme netaktiver gennem (bevidst eller utilsigtet) indbyggede sårbarheder. **R6 –** Organiserede kriminelle gruppers udnyttelse af 5G-net eller angreb på slutbrugere Ved at overtage kontrollen med en kritisk del af 5G-netarkitekturen afbryder en organiseret kriminel gruppe forskellige tjenester for at kræve løsepenge af virksomheder, der er afhængige af disse tjenester, eller af mobilnetoperatøren selv. Ved brug af en lignende angrebsmetode går en organiseret kriminel gruppe alternativt efter slutbrugere, f.eks. ved at sende falske meddelelser til nettets brugere som en del af et omfattende phishing-angreb eller onlinesvindel eller ved at bruge det kompromitterede net til at få adgang til fortrolige data om brugere (f.eks. tofaktorgodkendelseskoder) for at opnå yderligere fortjeneste.
IV – Risikoscenarier i forbindelse med de indbyrdes afhængigheder mellem 5G-net og andre kritiske systemer	**R7 –** Væsentlige forstyrrelser af kritiske infrastrukturer eller tjenester Ondsindede hackere kan kompromittere beredskabstjenester ved at overtage kontrollen med deres dedikerede net, og derved kan de kompromittere tilgængeligheden af tjenesten og integriteten af de oplysninger/data, der bruges til/i den pågældende tjeneste. **R8 –** Massive netnedbrud som følge af afbrydelse af elforsyningen eller andre støttesystemer Massive strømafbrydelser som følge af naturkatastrofer eller angreb på energinettet udført af en stat, en statsstøttet aktør eller en organiseret kriminel gruppe.
V – Risikoscenarier vedrørende slutbrugerudstyr	**R9 –** Udnyttelse af tingenes internet (IoT): En gruppe hackere eller en statsstøttet aktør overtager kontrollen med enheder med lav sikkerhed som f.eks. IoT (sensorer, husholdningsapparater osv.) med det formål at angribe nettet ved at overbelaste dets signalplan.

Konklusioner i EU's koordinerede risikovurdering

I EU's koordinerede risikovurdering understreges en række vigtige sikkerhedsudfordringer, som sandsynligvis vil opstå eller blive mere fremtrædende i 5G-net sammenlignet med situationen i eksisterende net. Disse sikkerhedsmæssige udfordringer er hovedsagelig knyttet til:

- centrale nyskabelser inden for 5G-teknologien (som også vil medføre en række specifikke sikkerhedsforbedringer), navnlig den vigtige software og den brede vifte af tjenester og applikationer, der muliggøres af 5G

- leverandørernes rolle i forbindelse med opbygning og drift af 5G-net og graden af afhængighed af de enkelte leverandører.

Udrulningen af 5G-net forventes især at få følgende virkninger:

- Øget eksponering for angreb og flere potentielle adgangssteder for angribere: Eftersom 5G-net i stigende grad baseres på software, er der stadig større risiko for alvorlige sikkerhedsbrister, bl.a. som følge af leverandørernes svage softwareudviklingsprocesser. Det kan også blive lettere for trusselsaktører at indsætte bagdøre i produkter og gøre dem sværere at opdage.

- På grund af ny funktioner og nye egenskaber i 5G-netarkitekturen bliver visse dele af netudstyret eller funktionerne mere følsomme, f.eks. basisstationer eller centrale tekniske netforvaltningsfunktioner.

- Øget risikoeksponering som følge af mobilnetoperatørernes afhængighed af deres leverandører . Det vil også kunne føre til et større antal angrebsveje, der kan udnyttes af trusselsaktører, og øge den potentielle alvor af sådanne angreb. Blandt de forskellige potentielle aktører betragtes lande uden for EU og statsfinansierede grupper som de groveste og mest tilbøjelige til at angribe 5G-net.

- På baggrund af den øgede eksponering for angreb, der skyldes leverandører, vil den enkelte leverandørs risikoprofil blive særlig vigtig, herunder sandsynligheden for, at leverandøren udsættes for interferens fra et ikke-EU-land.

- Øget risici som følge af større afhængighed af leverandører: En stor afhængighed af en enkelt leverandør øger risikoen for en potentiel forsyningsafbrydelse, f.eks. hvis virksomheden går ned, og det forværrer også konsekvenserne heraf. Det forværrer samtidig de mulige konsekvenser af svagheder eller sårbarheder og af deres mulige udnyttelse af trusselsaktører, især når afhængigheden vedrører en leverandør, der udgør en høj risiko.

- Trusler mod nettenes tilgængelighed og integritet vil blive et stort sikkerhedsproblem: Eftersom 5G-net ventes at blive rygraden i mange kritiske It-applikationer, vil nettenes integritet og tilgængelighed blive vigtige nationale sikkerhedsspørgsmål og en stor sikkerhedsmæssig udfordring set ud fra et EU-perspektiv. Dertil kommer spørgsmål som fortrolighed og trusler mod privatlivets fred.

I rapporten 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 sektoren og dens økosystem, og at det bliver af allerstørste vigtighed, at medlemsstaterne træffer de nødvendige risikobegrænsende foranstaltninger.