EUROPEISKA
KOMMISSIONEN

Bryssel den 29.1.2020
COM(2020) 50 final

MEDDELANDE FRÅN KOMMISSIONEN TILL EUROPAPARLAMENTET, RÅDET, EUROPEISKA EKONOMISKA OCH SOCIALA KOMMITTÉN SAMT REGIONKOMMITTÉN

Säker 5G-utbyggnad i EU – Genomförande av EU:s verktygslåda

1. *Inledning*

Femte generationens (5G) telenät kommer att ha en avgörande betydelse för den samhälleliga och ekonomiska utvecklingen i Europa. Tekniken väntas erbjuda enorma ekonomiska möjligheter och utgöra en viktig grund för den digitala och gröna omvandlingen inom sådana områden som transport, energi, tillverkning, hälsa, jordbruk och media.

5G kommer med andra ord att kunna påverka nästan alla aspekter av EU-medborgarnas liv. Cybersäkerheten i 5G-nät är därmed en mycket viktig fråga, inte bara för att skydda våra ekonomier, samhällen och demokratiska processer, utan även för att säkerställa en förtroendebaserad digital omvandling till gagn för alla EU-medborgare.

Många kritiska tjänster är beroende av 5G-nät och därmed skulle en systemisk och omfattande störning få väldigt allvarliga konsekvenser, och eftersom de digitala ekosystemen är sammankopplade skulle de gränsöverskridande effekterna kunna bli stora. Säkerställandet av cybersäkerheten i 5G-näten är därför en fråga av strategisk vikt för unionen, vid en tidpunkt då cyberattackerna är fler och mer sofistikerade än någonsin och initieras av många olika fientliga aktörer, i synnerhet aktörer som är tredjeländer eller understöds av stater. När det gäller säkerheten för sådana kritiska infrastrukturer som 5G väljer vi för första gången en gemensam europeisk strategi. Denna strategi är helt i enlighet med öppenheten på EU:s inre marknad så länge som EU:s riskbaserade säkerhetskrav uppfylls.

Den 22 mars 2019 efterlyste Europeiska rådet en samordnad strategi i fråga om 5G-nätens säkerhet. Den 26 mars 2019 antog kommissionen rekommendation (EU) 2019/534 om it-säkerhet i 5G-nät[1]. Rekommendationen uppmanade medlemsstaterna att genomföra nationella riskbedömningar och se över nationella åtgärder samt att arbeta tillsammans på EU-nivå med en samordnad riskbedömning och en gemensam verktygslåda med riskreducerande åtgärder. Detta meddelande är ett led i kommissionens övergripande europeiska digitala strategi, i enlighet med Europeiska rådets uppmaning.

2. *5G-utbyggnaden i EU*

Utbyggnaden av 5G-nätinfrastraktur i Europa är avgörande för den europeiska industristrategin och konkurrenskraften. Kommissionen har konstaterat att införandet av 5G-nätteknik är en viktig faktor för framtidens digitala tjänster. År 2016 antog kommissionen en 5G-handlingsplan för att se till att unionen har den konnektivitetsinfrastruktur som behövs för den digitala omvandlingen fram till 2020 och en omfattande 5G-användning i tätorter och på viktiga transportleder fram till 2025[2]. I meddelandet om ett europeiskt gigabitsamhälle sätter man upp målet att det ska finnas tillgång till mobil datakonnektivitet överallt[3], även på landsbygden och i avlägset belägna områden.

När det gäller frekvenstilldelning har medlemsstaterna tilldelat 16 % av 5G-pionjärfrekvensbanden[4]. Samråd om ett antal tilldelningsförfaranden kommer att genomföras

[1] Rekommendation (EU) 2019/534 om it-säkerhet i 5G-nät, EUT L 88, 29.3.2019, s. 42.
[2] 5G för Europa: en handlingsplan, COM(2016) 588 av den 14 september 2016.
[3] Konnektivitet för en konkurrenskraftig digital inre marknad - mot ett europeiskt gigabitsamhälle, COM(2016) 587.
[4] http://www.5GObservatory.eu.

de närmaste månaderna mot bakgrund av den rättsliga skyldigheten att tillåta användning av samtliga 5G-pionjärband före årets utgång.

Europa är en av de regioner i världen som har kommit längst när det gäller kommersiell lansering av 5G-tjänster[5]. De första 5G-tjänsterna väntas finnas tillgängliga i 138 europeiska städer före utgången av 2020. Tidiga 5G-nät bygger på den nuvarande fjärde generationen (4G) av nätteknik, och 5G-tjänster tillhandahålls i huvudsak åt allmänheten, antingen som en förbättring av 4G i fråga om kapacitet och hastighet, eller som ett kostnadseffektivt trådlöst alternativ till fasta nät[6].

När det gäller möjligheter inom nya företagstjänster, t.ex. inom energi, livsmedel och jordbruk, hälso- och sjukvård, tillverkning och transport, ligger Europa långt framme med investeringar som uppgår till en miljard euro, inklusive 300 miljoner euro i EU-finansiering inom ramen för det offentlig-privata 5G-partnerskapet inom Horisont 2020. Investeringarna avser bl.a. över 160 storskaliga 5G-försök som identifierats i Europa, inbegripet tio gränsöverskridande motorvägskorridorer för storskalig testning av 5G-baserade uppkopplade och automatiserade mobilitetstjänster. Försöken omfattar 5G-baserade tillämpningar inom olika områden från hållbar hälso- och sjukvård och automatiserad mobilitet till resurseffektivt jordbruk, smarta elnät och industri 4.0. Dessutom har EIB, med stöd av Europeiska fonden för strategiska investeringar, tillhandahållit lån för att accelerera forsknings- och utvecklingsarbetet avseende 5G-teknik.

Den europeiska kodexen för elektronisk kommunikation (nedan kallad *kodexen*)[7], som tillämpas från och med den 21 december 2020, utgör en viktig grund för att skapa en investeringsvänlig miljö för 5G-nät och för den fortsatta utvecklingen. Offentliga finansieringsprogram, som Fonden för ett sammanlänkat Europa – Digitalt[8] eller europeiska struktur- och investeringsfonder, kommer också att vara viktiga för att stödja den framtida utbyggnaden av 5G-nät, i synnerhet genom att koppla samman olika delar av samhället med 5G-baserade tjänster som skolor, sjukhus, städer och lokal förvaltning.

Med tanke på Europas strategiska möjligheter inom 5G-tjänster för olika branscher kommer det att vara mycket viktigt att operatörer och tjänsteleverantörer investerar i avancerade nät- och tjänstelösningar för 5G. Dessa kommer inte bara att kräva nya 5G-radionät utan också s.k. självständiga 5G-stomnät, för att tillhandahålla avancerade 5G-funktioner som nätverksskivning[9] och edge computing[10].

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

[6] Några av de nya 5G-funktionerna kommer att fasas in. I en första fas (kort eller väldigt kort sikt) kommer 5G-utbyggnaden i första hand att bestå av nät som inte är självständiga (*non stand-alone networks*), där endast radioaccessnätet uppgraderas till 5G-teknik. Det kommer att ge slutanvändarna förbättrad mobil bredbandskapacitet, men bygger fortfarande på befintliga 4G-stomnät. I nästa fas (kort/medellång till lång sikt) kommer utbyggnaden av självständiga 5G-nät, inklusive 5G-stomnätsfunktioner att kräva – och på sikt resultera i – betydligt mer omfattande förändringar av nätarkitekturen.

[7] Europaparlamentets och rådets direktiv (EU) 2018/1972 om inrättande av en europeisk kodex för elektronisk kommunikation (omarbetning).

[8] Förslag till förordning om inrättande av Fonden för ett sammanlänkat Europa och om upphävande av förordningarna (EU) nr 1316/2013 och (EU) nr 283/2014, COM(2018)438 av den 6 juni 2018.

[9] 5G-nätverksskivning möjliggör en hög grad av separation mellan olika tjänsteskikt på samma fysiska nät, vilket ökar möjligheterna att erbjuda differentierade tjänster på hela nätet.

[10] Edge computing är ett distribuerat beräkningsparadigm som utför beräkningar och datalagring närmare den plats där de behövs, för att förbättra responstiden och spara bandbredd.

Kommissionen kommer att fortsätta att ge sitt fulla stöd åt en framgångsrik 5G-utbyggnad i EU, bl.a. genom kontakter med medlemsstaterna och intressenterna för att tillvarata 5G-teknikens möjligheter. Relevanta hälsoaspekter kommer att beaktas baserat på försiktighetsprincipen[11], i samarbete med berörda internationella organisationer och vetenskapssamhället.

3. EU:s samordnade riskbedömning av cybersäkerheten i 5G-nät

Inom ramen för det kollektiva arbetet i samarbetsgruppen för nät- och informationssäkerhet[12] genomförde varje medlemsstat sin egen nationella riskbedömning av sina 5G-nätinfrastrukturer och sände resultaten till kommissionen och Enisa (Europeiska unionens cybersäkerhetsbyrå) i början av juli 2019.

Baserat på dessa nationella riskbedömningar offentliggjorde samarbetsgruppen, som består av medlemsstaternas företrädare, kommissionen och Enisa, den 9 oktober 2019 en rapport om EU:s samordnade riskbedömning av cybersäkerheten i 5G-nät[13]. I rapporten redogörs för de största hoten, de huvudsakliga fientliga aktörerna, de känsligaste tillgångarna och de främsta sårbarheterna (både tekniska och andra typer av sårbarheter) som påverkar 5G-nät. På denna grundval identifierades också ett antal riskkategorier av strategisk betydelse ur ett EU-perspektiv, illustrerade med konkreta riskscenarier, vilka speglar relevanta kombinationer av olika parametrar (sårbarheter, hot och fientliga aktörer) med avseende på de olika tillgångarna (se bilagan).

Som komplement till den här rapporten, och som ytterligare underlag för verktygslådan, utförde Enisa en särskild kartläggning av hotbilden[14]. Den omfattade en detaljerad analys av vissa tekniska aspekter, i synnerhet en kartläggning av nättillgångar och de hot som påverkar dessa.

I den EU-samordnade riskbedömningsrapporten lyfter man fram följande aspekter som är viktiga för 5G-nät:

a) De tekniska förändringar som införs genom 5G kommer att öka den totala attackytan och antalet potentiella ingångar för attacker:

– Förbättrade funktioner i nätets periferi och en mindre centraliserad arkitektur än i tidigare generationers mobilnät. Det innebär att vissa av stomnätets funktioner kan vara integrerade i andra delar av nätet vilket medför att den motsvarande utrustningen blir känsligare (t.ex. basstationer eller manofunktioner).

– Det ökade beroendet av programvara i 5G-utrustningen medför ökade risker förbundna med utvecklings- och uppdateringsprocesserna för programvara. Det ger också upphov till

[11] Rådets rekommendation av den 12 juli 1999 om begränsning av allmänhetens exponering för elektromagnetiska fält (0 Hz–300 GHz) (1999/519/EG).

[12] Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen. Samarbetsgruppen för nät- och informationssäkerhet inrättades genom direktivet om nät- och informationssäkerhet och ska säkerställa ett strategiskt samarbete och informationsutbyte mellan EU:s medlemsstater när det gäller cybersäkerhet.

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

[14] Enisa, *Threat landscape for 5G networks*: https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks.

nya risker för konfigurationsfel och innebär att val som görs av varje mobilnätsoperatör i nätets utbyggnadsfas får större betydelse i säkerhetsanalysen.

b) Dessa nya tekniska funktioner kommer att öka betydelsen av mobilnätoperatörernas beroende av tredjepartsleverantörer och deras roll i 5G-försörjningskedjan.

Det kommer i sin tur att öka antalet angreppsvägar som skulle kunna utnyttjas av fientliga aktörer, i synnerhet aktörer som är tredjeländer eller understöds av stater, på grund av deras kapacitet (avsikt och resurser) att utföra attacker mot EU-medlemsstaters telenät, samt de potentiellt allvarliga konsekvenserna av sådana attacker.

Med tanke på den ökade exponeringen för attacker som underlättas av tredjepartsleverantörer kommer leverantörernas individuella riskprofiler att vara särskilt viktiga, i synnerhet i de fall då en leverantör har en betydande närvaro inom ett nät eller område.

c) Ett stort beroende av en enskild leverantör ökar exponeringen för och konsekvenserna av potentiella fel hos den leverantören. Ett sådant beroende förvärrar också de potentiella konsekvenserna av svagheter och sårbarheter och risken för att de kan utnyttjas av fientliga aktörer, i synnerhet när beroendet gäller en leverantör som är förknippade med en hög risknivå.

d) Om några av de nya användningsfall som planeras för 5G förverkligas kommer 5G-näten att bli en viktig del av försörjningskedjan för många kritiska it-tillämpningar. Därmed kommer inte bara konfidentialitets- och integritetskrav att påverkas, utan nätens integritet och tillgänglighet kommer att bli en viktig nationell säkerhetsfråga och en stor säkerhetsutmaning ur ett EU-perspektiv.

Källa: EU:s samordnade riskbedömning

En slutsats av EU:s samordnade riskbedömningsrapport är att dessa utmaningar skapar ett nytt säkerhetsparadigm som gör det nödvändigt att ompröva den nuvarande politik- och säkerhetsramen för 5G-sektorn och dess ekosystem och gör att medlemsstaterna måste vidta de riskreducerande åtgärder som krävs.

För att på ett effektivt sätt hantera de identifierade riskerna och stärka 5G-nätens säkerhet och resiliens krävs en övergripande strategi, som omfattar ett antal nyckelåtgärder och stödåtgärder som kan angripa riskerna samtidigt. EU:s samordnade riskbedömning ger ett underlag för framtagandet av riskreducerande åtgärder som kan tillämpas på nationell och europeisk nivå.

Rådets slutsatser av den 3 december 2019 stödde resultaten av den samordnade riskbedömningen och betonade ”vikten av en samordnad strategi och ett effektivt genomförande av rekommendationen i syfte att undvika fragmentering på den inre marknaden”[15]. Därför uppmanade rådet medlemsstaterna, kommissionen och Enisa att vidta ”alla nödvändiga åtgärder inom ramen för sina behörigheter för att säkerställa säkerhet och

[15] Rådets slutsatser om 5G:s betydelse för den europeiska ekonomin och behovet av att minska säkerhetsriskerna i samband med 5G, den 3 december 2019, 14517/19 https://www.consilium.europa.eu/media/41595/st14517-en19.pdf.

integritet i elektroniska kommunikationsnät, särskilt 5G-nät, och att fortsätta att konsolidera en samordnad strategi för hantering av säkerhetsutmaningarna i samband med 5G-teknik".

4. EU:s verktygslåda för 5G-cybersäkerhet

Den 29 januari 2020 offentliggjorde samarbetsgruppen för nät- och informationssäkerhet EU:s verktygslåda med riskreducerande åtgärder[16]. Den behandlar alla risker som identifierats i den samordnade riskbedömningsrapporten.

EU:s verktygslåda omfattar identifiering och beskrivning av ett antal strategiska och tekniska åtgärder samt motsvarande stödåtgärder som ska stärka åtgärdernas effektivitet. Dessa åtgärder kan vidtas för att reducera identifierade risker. **Strategiska åtgärder** innefattar åtgärder som rör ökade regleringsbefogenheter för myndigheter att granska upphandling och utbyggnad av nät, särskilda åtgärder för att hantera risker kopplade till icke-tekniska sårbarheter, samt tänkbara initiativ för att främja en hållbar och diversifierad 5G-försörjningskedja och 5G-värdekedja, så att man kan undvika systemiska långsiktiga beroenderisker. **Tekniska åtgärder** omfattar åtgärder för att stärka säkerheten för 5G-nät och 5G-utrustning genom att angripa de risker som orsakas av teknik, processer och mänskliga och fysiska faktorer. För varje riskområde som identifieras i EU:s samordnade riskbedömning tillhandahålls också **riskreduceringsplaner** som baseras på de effektivaste åtgärderna.

I slutsatserna om EU:s verktygslåda, som antagits av samarbetsgruppen för nät- och informationssäkerhet, rekommenderas därför bland annat ett antal **nyckelåtgärder** som ska genomföras av alla medlemsstater och av kommissionen enligt följande:

Slutsatser om EU:s verktygslåda

EU:s verktygslåda omfattar ett antal olika åtgärder som – om de kombineras på lämpligt sätt och genomförs effektivt – ger en grund för en samordnad strategi på detta område. Med tanke på de många olika riskområden som identifieras i EU:s samordnade riskbedömning och det faktum att de är så olika, finns det ingen enskild typ av åtgärd som kommer att vara tillräcklig. I stället krävs det flera olika åtgärder som kombineras på lämpligt sätt för att täcka alla de viktigaste riskområdena.

Baserat på bedömningen av tänkbara riskreduceringsplaner och identifieringen av de effektivaste åtgärderna, rekommenderas följande enligt verktygslådan:

1. Alla medlemsstater bör säkerställa att de vidtagit åtgärder (inklusive gett de nationella myndigheterna befogenheter) som gör att de på ett ändamålsenligt och proportionerligt sätt kan reagera på nu identifierade och framtida risker och i synnerhet att de kan begränsa, förhindra och/eller införa särskilda krav eller villkor enligt en riskbaserad strategi när det gäller försörjning, utbyggnad och drift av 5G-nätutrustning på grundval av ett antal säkerhetsrelaterade skäl.

De bör i synnerhet göra följande:

- *Stärka **säkerhetskraven** för operatörer av mobilnät (bl.a. strikta tillträdeskontroller, bestämmelser om säker drift och övervakning och begränsning av möjligheterna att lägga ut specifika funktioner på entreprenad).*

- *Bedöma leverantörers riskprofil och till följd av detta **tillämpa relevanta begränsningar på leverantörer som anses utgöra hög risk – inbegripet uteslutande när så krävs för en effektiv***

[16] Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures, den 29 januari 2020. https://ec.europa.eu/digital-single-market/en/nis-cooperation-group.

riskreducering – när det gäller nyckeltillgångar *som definieras som kritiska och känsliga i EU:s samordnade riskbedömning (t.ex. stomnätsfunktioner, nätförvaltnings- och orkestreringsfunktioner samt accessnätsfunktioner).*

 Säkerställa att varje operatör har en lämplig flerleverantörsstrategi, så att man kan ***undvika eller begränsa mer omfattande beroenden*** *av en enda leverantör (eller leverantörer med liknande riskprofil), säkerställa en lämplig balans av leverantörer på nationell nivå och* ***undvika ett beroende av leverantörer som anses förknippade med hög risk****. Detta kräver också att man undviker alla inlåsningssituationer där man binds till en enda leverantör, inklusive genom att främja mer interoperabel utrustning.*

2. Europeiska kommissionen bör tillsammans med medlemsstaterna bidra till följande:

 Upprätthållande av en ***diversifierad och hållbar 5G-försörjningskedja*** *för att undvika långsiktiga beroenden, t.ex. genom följande:*

o Fullständigt utnyttjande av befintliga EU-verktyg och EU-instrument, i synnerhet genom screening av potentiella ***utländska direktinvesteringar*** *som påverkar 5G-nyckeltillgångar och motverkande av* ***snedvridning*** *på försörjningsmarknaden för 5G till följd av dumpning eller subventioner.*

o Fortsatt stärkande av ***EU:s kapacitet inom 5G-teknik och post-5G-teknik*** *genom användning av relevanta EU-program och EU-medel.*

 Främjande av samordningen mellan medlemsstater på ***standardiseringsområdet*** *för att uppnå specifika säkerhetsmål och utveckling av* ***relevanta EU-certifieringssystem*** *för att främja säkrare produkter och processer.*

3. För att säkerställa att denna samordnade strategi fungerar över tid bör mandatet förlängas för samarbetsgruppen för nät- och informationssäkerhet, liksom samarbetet med andra berörda organ och enheter, för att i synnerhet göra följande:

 Periodisk översyn (med stöd av kommissionen och Enisa) av de ***nationella riskbedömningarna och EU:s riskbedömning*** *av säkerheten för 5G-nät och post-5G-nät, för att vidareutveckla och justera bedömningsmetoden och anpassa den till 5G-teknikens snabba utveckling.*

 Detaljerad och regelbunden ***övervakning och utvärdering av genomförandet*** *av verktygslådan baserat på strukturerad rapportering från medlemsstaterna.*

 Samordning av och stöd till genomförandet av ***stödåtgärder****, som kräver samarbete på EU-nivå, i synnerhet när det gäller utarbetandet av riktlinjer och utbyte av bästa praxis för de olika åtgärderna.*

 Stöd till ytterligare möjlig samordning på EU-nivå där så är lämpligt, i synnerhet för ytterligare konvergens ***i fråga om tekniska och organisatoriska säkerhetskrav för nätoperatörer****.*

Källa: EU:s verktygslåda.

Slutsatserna om verktygslådan visar medlemsstaternas starka vilja att gemensamt hantera 5G-nätens säkerhetsutmaningar. Det är av grundläggande betydelse för säkerheten inom medlemsstater och EU som helhet, för nationella ekonomier, för EU:s inre marknad och för Europas tekniska suveränitet. Både EU:s samordnade riskbedömning och EU:s verktygslåda visar det stora värdet av det kollektiva arbete som gjorts i samarbetsgruppen för nät- och informationssäkerhet, med en intensiv samverkan mellan företrädare för alla medlemsstater och kommissionen och Enisa.

Verktygslådan möjliggör en gemensam EU-strategi för 5G-cybersäkerhet, vilket främjar konsekvens på hela den inre marknaden genom EU-politik och EU-samordning, liksom medlemsstaternas utövande av sina befogenheter när det gäller i synnerhet nationell säkerhet. De riskreducerande åtgärder och riskreduceringsplaner som verktygslådan omfattar möjliggör en ändamålsenlig, effektiv och proportionerlig EU-respons på gemensamma 5G-cybersäkerhetsutmaningar.

Kommissionen välkomnar offentliggörandet av EU-verktygslådan för 5G-cybersäkerhet och stöder helt alla ovannämnda slutsatser.

Kommissionen uppmanar medlemsstaterna och unionens berörda institutioner, byråer och organ att

i) säkerställa ett snabbt genomförande av effektiva och ändamålsenliga riskreduceringsstrategier i hela EU i linje med EU:s verktygslåda, och

ii) vidta alla ytterligare åtgärder som är nödvändiga för att säkerställa samordning på unionsnivå, bl.a. genom fortsatt arbete inom samarbetsgruppen för nät- och informationssäkerhet och inrättandet av en robust mekanism för att övervaka genomförandet av EU:s verktygslåda och för att säkerställa effektiva åtgärder och en välfungerande inre marknad.

5. Genomförandet av verktygslådan

Medlemsstaternas beslutsamhet att utnyttja verktygslådan fullt ut är nödvändig för en trovärdig och framgångsrik europeisk strategi för 5G-säkerhet. Det är medlemsstaterna som beslutar om en viss åtgärd är lämplig baserat på de nationella förhållandena. För att de identifierade riskerna ska kunna undanröjas är det dock avgörande att ett **antal nyckelåtgärder, enligt rekommendationerna från samarbetsgruppen för nät- och informationssäkerhet (se slutsatserna om verktygslådan ovan), vidtas i varje medlemsstat och, när det gäller några av åtgärderna, på EU-nivå**.

Kommissionen är redo att fortsätta ge sitt fulla stöd under de kommande faserna och uppmanar medlemsstaterna att

- **senast den 30 april 2020** vidta konkreta och mätbara åtgärder för att genomföra de nyckelåtgärder som rekommenderas i slutsatserna om EU:s verktygslåda, och

- **senast den 30 juni 2020,** inom ramen för samarbetsgruppen för nät- och informationssäkerhet, utarbeta en rapport om genomförandeläget i varje medlemsstat för dessa nyckelåtgärder, baserat på den regelbundna rapportering och tillsyn som görs i synnerhet inom samarbetsgruppen för nät- och informationssäkerhet, med stöd av kommissionen och Enisa.

5.1. Ett riskbaserat och samordnat tillvägagångssätt för hantering av 5G-leverantörer

Eftersom slutmålet är att säkerställa att 5G-näten är säkra, resilienta och hållbara har medlemsstaterna enats om att de enskilda leverantörernas riskprofiler måste bedömas. Som en följd av detta bör relevanta begränsningar tillämpas på leverantörer som anses utgöra en hög risk för nyckeltillgångar (även uteslutande om det krävs för att verkligen reducera riskerna),

såsom anges i verktygslådan. Kommissionen är redo att stödja medlemsstaterna i genomförandet av dessa åtgärder.

För att stödja genomförandet i hela EU omfattar EU:s samordnade riskbedömningar och EU:s verktygslåda riktlinjer för 1) bedömningen av leverantörers riskprofil[17] och 2) känslighetsgraden för nätelement och nätfunktioner[18], liksom andra tillgångar. Både EU:s samordnade riskbedömning och åtgärderna enligt verktygslådan täcker risker förknippade med leverantörer av 5G-nätutrustning och nättjänster. De täcker inte andra produkter eller tjänster som kan tillhandahållas av dessa eller andra leverantörer.

Såsom anges i punkt 2.37 i EU:s samordnade riskbedömning kan individuella leverantörers riskprofiler bedömas baserat på flera faktorer.

Bedömningen av leverantörers riskprofiler bör endast utföras av säkerhetsskäl och baserat på objektiva kriterier. För att främja ett samordnat sätt att genomföra dessa åtgärder rekommenderas i verktygslådan att medlemsstaterna utbyter information om nationella tillvägagångssätt och bästa praxis. Kommissionen anser också att detta bör göras som en av de första prioriteringarna för nästa fas av arbetet i samarbetsgruppen för nät- och informationssäkerhet, tillsammans med kommissionen och Enisa.

Det är viktigt att begränsningarna i fråga om leverantörer som anses utgöra hög risk, inklusive uteslutande om det krävs för en effektiv riskreducering, liksom åtgärderna för att motverka ett beroende av sådana leverantörer, vidtas snabbt. Om detta görs i ett så tidigt stadium som möjligt, även i samband med licensförfarandet för 5G-frekvenser när så är möjligt, så ökar det förutsebarheten för marknadsaktörerna. Detta bidrar i sin tur till en snabb utbyggnad av 5G-näten och säkerställer den långsiktiga nätsäkerheten och resiliensen för 5G-försörjningskedjan.

Samtidigt kan man vid det nationella genomförandet av dessa åtgärder specificera andra tidsramar, när så är nödvändigt och motiverat, i synnerhet när det redan finns en hög grad av beroende av utrustning eller tjänster från leverantörer som bedöms utgöra hög risk (t.ex. genom beaktande av cyklerna för uppgradering av utrustning, i synnerhet migreringen från nät som inte är självständiga 5G-nät till självständiga sådana). Medlemsstaterna kan överväga att fastställa genomförandeplaner som inkluderar lämpliga övergångsperioder för berörda nätoperatörer. Dessa övergångsperioder bör i så fall definieras på ett sådant sätt att de bevarar eller till och med stärker incitamenten för investering i modern nätutrustning, inklusive att accelerera införandet av fullt utvecklade självständiga 5G-stomnät och ersätta befintlig 4G-utrustning i andra delar av näten (t.ex. i radioaccessnätet), i linje med målen för 5G-handlingsplanen[19].

Eftersom de programvarubaserade 5G-näten är så komplexa kan teleoperatörerna tänkas förlita sig allt mer på tredjeparter som utför vissa uppgifter, såsom underhåll och uppgradering av 5G-nät och programvara, liksom andra utkontrakterade tjänster, utöver leveranserna av nätutrustning. Såsom beskrivs i EU:s samordnade riskbedömning utgör detta

[17] Punkt 2.37 i EU:s samordnade riskbedömning.

[18] I punkt 2.21 i EU:s samordnade riskbedömning anges de viktigaste kategorierna av element och funktioner samt deras allmänna känslighetsgrad. Där anges också ett antal nyckelelement som identifierats av medlemsstaterna för varje kategori. I punkterna 2.28 och 2.29 identifieras ett antal andra typer av känsliga tillgångar eller områden (t.ex. specifika enheter eller geografiska områden).

[19] 5G för Europa: en handlingsplan, den 14 september 2016, COM(2016) 588.

en källa till allvarliga säkerhetsrisker. Särskild uppmärksamhet måste därför ägnas åt denna aspekt. Det är mycket viktigt att en grundlig säkerhetsbedömning också görs av riskprofilen för de leverantörer som utför dessa uppgifter, i synnerhet när uppgifterna inte utförs i EU. Ändamålsenliga åtgärder bör vidtas, inklusive begränsningar som tillämpas på i synnerhet känsliga delar av 5G-näten eller nödvändigt uteslutande av högriskenheter i linje med verktygslådans riskreducerande åtgärder, för att bevara 5G-infrastrukturens integritet på lång sikt.

5.2. Kommissionens roll för att stödja genomförandet av verktygslådan

Kommissionen kommer att fortsätta att stödja det allmänna genomförandet av EU:s strategi för 5G-cybersäkerhet och dessutom ta särskilda initiativ för de åtgärder och mål i verktygslådan där detta kan ge ett mervärde. Kommissionen kommer att utnyttja alla sina befogenheter och relevanta instrument i den mån som det är nödvändigt för att åtgärda identifierade säkerhetsaspekter. Genom att göra detta, och genom att agera tillsammans med medlemsstaterna och den privata sektorn, vill kommissionen stödja strategiska åtgärder som kommer att bidra till att säkerställa EU:s suveränitet på det tekniska området och ledarskap i den fortsatta utvecklingen av nätteknik, cyberteknik och alla de berörda byggstenar som vår hela ekonomi och säkerhet är beroende av.

Mer specifikt kommer kommissionen att göra följande för att säkerställa genomförandet av motsvarande riskreducerande åtgärder från verktygslådan inom sina behörighetsområden.

Skydda cybersäkerheten i 5G-nät och en diversifierad 5G-värdekedja:

-**Cybersäkerhetssamarbete**: Fortsätta att ge medlemsstaterna stöd till ett effektivt, samordnat och snabbt genomförande av nationella åtgärder genom samarbetsgruppen för nät- och informationssäkerhet.

- **Tele- och cybersäkerhetsbestämmelser**: Stödja genomförandet av verktygslådans åtgärder med avseende på säkerhetskraven, i synnerhet vad gäller relevanta föreskrifter inom de europeiska bestämmelserna om elektronisk kommunikation, och ta ställning till mervärdet av eventuella genomförandeakter med tekniska och organisatoriska säkerhetsåtgärder som kompletterar de nationella bestämmelserna och gör de säkerhetsåtgärder som åläggs operatörerna effektivare och mer konsekventa.

- **Standardisering**: Vidta åtgärder för att bidra till att upprätthålla och vid behov utöka det europeiska deltagandet i respektive standardiseringsorgan, för att uppnå Europas säkerhets- och interoperabilitetsmål. Kommissionen kommer i synnerhet att tillsammans med medlemsstaterna bedöma och främja tekniska specifikationer och standarder som möjliggör interoperabilitet mellan leverantörer av 5G-utrustning i olika delar av nätet, inklusive befintliga nät, för att möjliggöra en verklig flerleverantörsmiljö, genom t.ex. öppna interoperabla gränssnitt.

- **Certifiering**: Stöd till utvecklingen av 5G-certifieringssystem som tillgodoser 5G-nätens behov inom EU:s cybersäkerhetscertifieringsram.

- **Screening av utländska direktinvesteringar**: Stödja genomförandet av EU:s screeningram genom att kartlägga 5G-värdekedjan, inklusive känsliga nättillgångar, och regelbundet övervaka utländska direktinvesteringar längs hela värdekedjan. I linje med screeningtidsplanen (från och med oktober 2020) kommer kommissionen att granska

utländska direktinvesteringar på 5G-området i enlighet med riktlinjerna i förordning (EU) 2019/452, med beaktande av EU:s samordnade riskbedömning och EU:s verktygslåda.

- **Handelspolitiska skyddsåtgärder**: Övervaka all relevant marknadsutveckling inom EU och tredjeländer och skydda EU-aktörer på den europeiska 5G-marknaden med handelspolitiska skyddsåtgärder för att motverka potentiell snedvridning av handeln (dumpning eller subventioner), även genom preliminära undersökningar.

- **Konkurrensregler:** Övervaka hur marknaderna för tillhandahållande av 5G-maskinvara och 5G-programvara fungerar för att säkerställa att de leder till konkurrenspräglade förhållanden, även när det gäller avtalsmässiga eller tekniska inlåsningssituationer.

- **EU:s finansieringsprogram**: Säkerställa att deltagandet i EU:s finansieringsprogram inom relevanta teknikområden kommer att förenas med villkor om uppfyllande av säkerhetskrav, genom att fullt ut utnyttja och fortsätta att införa säkerhetsvillkor i forsknings- och innovationsprogram, i synnerhet Horisont Europa, programmet för ett digitalt Europa och Fonden för ett sammanlänkat Europa 2, europeiska struktur- och investeringsfonder och andra relevanta program. Detta bör också göras i EU:s externa finansieringsprogram och finansieringsinstrument, även när det gäller finansiering som tillhandahålls genom internationella finansiella institutioner.

- **Offentlig upphandling:** Använda offentlig upphandling som en hävstång på området 5G-nät för att främja identifierade mål avseende säkerhet, diversifierad leverantörsbas och långsiktig hållbarhet för 5G-nät. I synnerhet försöka säkerställa att säkerhetsaspekter beaktas på vederbörligt sätt vid tilldelning av offentliga kontrakt relaterade till 5G-nät, i linje med EU:s regler för offentlig upphandling.

- **Incident- och krishantering (strategi) samt cyberövningar**: Maximalt utnyttja utvecklingen av EU:s strategi för samordnade insatser vid storskaliga cyberincidenter och cyberkriser[20]. Tillsammans med Enisa ta ställning till en eventuell 5G-cyberövning så snart marknaden blivit tillräckligt mogen.

Dessutom följande, under ansvar av unionens höga representant för utrikes frågor och säkerhetspolitik och Europeiska kommissionens vice ordförande samt rådet:

- **Ram för en gemensam diplomatisk respons från EU mot skadlig cyberverksamhet (verktygslåda för cyberdiplomati)[21]**: Vid skadlig cyberverksamhet som hotar EU:s integritet och säkerhet uppmuntras medlemsstaterna att utnyttja relevanta åtgärder inom den gemensamma utrikes- och säkerhetspolitiken som ingår i EU:s verktygslåda för cyberdiplomati (inklusive restriktiva åtgärder vid behov), för att främja samarbete, underlätta reducering av hot och påverka potentiella angripares beteende.

Ett antal program kommer också att bidra till målet att undvika eller begränsa risken för långsiktigt beroende, genom att främja en diversifierad och hållbar marknad för 5G, även genom att upprätthålla EU-kapacitet i 5G-värdekedjan och investera i innovation, i enlighet med EU:s internationella åtaganden.

[20] Kommissionens rekommendation (EU) 2017/1584 om samordnade insatser vid storskaliga cyberincidenter och cyberkriser.
[21] Rådets slutsatser av den 20 november 2017, 9916/17.

Främja innovation och investera i teknik för cybersäkerhet och i nätinfrastruktur:

- EU:s **finansieringsprogram**: Öka investeringarna i forskning, innovation och användning av nätteknik och de relevanta underliggande byggstenarna. Kommissionen har föreslagit att nästan tre miljarder euro ska avsättas för cybersäkerhetsteknik i nästa EU-budget för perioden 2021–27. Detta innefattar forskning och innovation inom Horisont Europa och stöd till cybersäkerhetskapacitet inom programmet för ett digitalt Europa. InvestEU kan också lämna finansiellt stöd till forskning och utveckling inom 5G liksom stöd för utbyggnaden.

Inom nästa Horisont Europa-program[22] har kommissionen föreslagit att det ska inrättas ett institutionaliserat EU-partnerskap för NGI/6G (”smarta nät och tjänster”), i partnerskap med branschen och i samordning med medlemsstaterna för att slutföra 5G-utbyggnaden och framför allt för **att förbereda för 6G,** nästa generations mobilteknik. Det föreslogs att mer än 2,5 miljarder euro av EU-investeringar skulle avsättas från EU-budgeten (2021–27) och att dessa skulle matchas med minst 7,5 miljarder euro av privata investeringar för detta initiativ.

- **Industriell utveckling och utbyggnad**: Utvärdera potentiella marknadsluckor eller marknadsmisslyckanden längs 5G-värdekedjan som skulle motivera målinriktade insatser inom nästa långtidsbudget eller ett eventuellt ”viktigt projekt av gemensamt europeiskt intresse” på cybersäkerhetsområdet, i linje med förslagen från högnivåforumet för viktiga projekt av gemensamt europeiskt intresse. Beslut om att utarbeta och inrätta viktiga projekt av gemensamt europeiskt intresse ligger i medlemsstaternas och företagens händer. EU-bestämmelserna utgör en möjliggörande ram och kommissionen står beredd att underlätta de nödvändiga kontakterna och lämna vägledning.

[22] Finansiering kan också tillhandahållas genom fonden för ett sammanlänkat Europa 2.0 och programmet för ett digitalt Europa.

6. Slutsats

5G-nät kan erbjuda en mängd olika möjligheter för europeiska medborgare och det europeiska samhället och ekonomin. Det är därför nödvändigt att se till att 5G-näten är säkra och resilienta. Samtidigt utgör cybersäkerhetshoten (även risken för inblandning från tredjeländer eller statsstödda aktörer) en utmaning som snabbt utvecklas och blir allt viktigare i takt med det ökade beroendet av teknik och data. Om vi försummar cybersäkerheten kan det underminera förtroendet för den digitala ekonomins och det digitala samhällets utveckling och EU kommer därmed inte att kunna utnyttja alla fördelarna. Därför krävs en utvecklingsbar och stärkt respons.

Det behövs en samordnad och konsekvent strategi för cybersäkerhet i EU när det gäller kritisk teknik och kritiska nät för att EU ska kunna säkra sin tekniska suveränitet och upprätthålla och utveckla sin industriella kapacitet. Kommissionen kommer att ge sitt fulla stöd åt genomförandet av EU:s cybersäkerhetsstrategi för 5G-nät och samtidigt se till att EU-marknaderna förblir öppna för produkter och tjänster som uppfyller kraven för cybersäkerhet och förtroende, som ständigt utvecklas.

I detta avseende är det viktigt att alla intressenter på området 5G-säkerhet visar ett starkt engagemang, och det kräver ett fortsatt samarbete mellan medlemsstaterna, kommissionen och Enisa.

Som ett omedelbart nästa steg, såsom anges ovan, uppmanar kommissionen medlemsstaterna att snabbt agera för att på ett effektivt och objektivt sätt vidta de åtgärder som överenskommits inom ramen för verktygslådan och att fortsätta att arbeta tillsammans, med stöd av kommissionen och Enisa, för att säkra samordningen på EU-nivå. Samtidigt kommer kommissionen att vidta alla relevanta åtgärder inom sitt behörighetsområde för att stödja medlemsstaternas genomförande av verktygslådan och stärka dess effekter.

Tillägg: Riskkategorier (källa: EU:s samordnade riskbedömning)

	Riskkategorier
Riskscenarier kopplade till otillräckliga säkerhetsåtgärder	*R1: Felkonfigurering av nät*
	R2: Bristande tillträdeskontroll
Riskscenarier kopplade till 5G-försörjningskedjan	*R3: Låg kvalitet på produkter*
	R4: Beroende av en enda leverantör inom ett enskilt nät eller bristande diversifiering på nationell nivå
Riskscenarier kopplade till de viktigaste fientliga aktörernas arbetssätt	*R5: Statlig inblandning i 5G-försörjningskedjan*
	R6: Utnyttjande av 5G-näten från organiserad brottslighet eller organiserad kriminell grupp som inriktar sig på slutanvändare
Riskscenarier kopplade till ömsesidiga beroenden mellan 5G-nät och andra kritiska system	*R7: Betydande störningar av kritisk infrastruktur eller kritiska tjänster*
	R8: Omfattande nätfel på grund av avbrott i elförsörjningen eller andra stödsystem
Riskscenarier kopplade till slutanvändarnas enheter	*R9: Utnyttjande av sakernas internet*