# Föreskrift om kommunikationsnätets kritiska delar

Innehållsförteckning

## 1. Föreskriftens bakgrund och rättsgrund

I 244 a § (lagen 1207/2020; RP 98/2020 rd) i lagen om tjänster inom elektronisk kommunikation (917/2014, LTEK) föreskrivs om den nätverksutrustning som används i kommunikationsnätens kritiska delar. Enligt 1 mom. i paragrafen får nätverksutrustning inte användas i ett allmänt kommunikationsnäts kritiska delar, om det finns vägande skäl att misstänka att användningen av utrustningen äventyrar den nationella säkerheten eller försvaret på så sätt att det möjliggör utländsk underrättelseverksamhet eller sådan verksamhet som stör, lamslår eller på något annat skadligt sätt påverkar Finlands viktiga intressen, grundläggande samhällsfunktioner eller den demokratiska samhällsordningen. Som ett kommunikationsnäts kritiska delar betraktas enligt momentet dess centrala faciliteter och åtgärder med hjälp av vilka tillgången till nätet och trafiken på det kontrolleras eller styrs på ett väsentligt sätt.

Enligt 6 mom. i LTEK 244 a § får Transport- och kommunikationsverket (härefter också Traficom) meddela närmare föreskrifter om den tekniska definitionen av kommunikationsnät, särskilt av nätens kritiska delar, med beaktande av rekommendationerna från den delegation för nätsäkerhet som avses i 244 b §.

När man tillämpar 244 a § 1 mom. i LTEK kan man skilja på utredandet om huruvida det finns vägande skäl att misstänka att användningen av utrustningen äventyrar den nationella säkerheten eller försvaret och bedömningen av huruvida en del är kritisk för kommunikationsnätet. Denna föreskrift hanterar inte överhuvudtaget bedömningen av den s.k. *förutsättningen för fara* eftersom Traficoms rätt att meddela föreskrifter enligt 6 mom. enbart gäller det tekniska fastställandet av de kritiska delarna av kommunikationsnät.

EU:s medlemsstater publicerade den 29 januari 2020 en gemensam verktygslåda för att hantera och lösa säkerhetsriskerna. Genom föreskriften genomförs den åtgärd i EU:s gemensamma verktygslåda för 5G-säkerhet som gäller skyddet av kritiska delar av nätet.

Utöver 244 a § mom. 6 i LTEK grundar sig Transport- och kommunikationsverkets rätt att meddela föreskrifter på punkt 1, 3 och 12 i 244 § i LTEK. Enligt punkt 1 i paragrafen kan Transport- och kommunikationsverkets föreskrifter gälla bland annat klassificering i viktighetsordning, enligt punkt 3 informationssäkerhet och störningsfrihet, underhåll och uppföljning av dessa samt nätverksadministration, samt enligt punkt 12 teknisk dokumentation och statistik samt utformning av tillhörande dokument och lagring av uppgifter.

## 2. Övriga föreskrifter av Transport- och kommunikationsverket i frågan

Föreskriften om *televerksamhetens informationssäkerhet* (föreskrift 67) fastställer minimikraven på tillämpandet av informationssäkerhet. Avsikten med föreskriften är att beaktandet av informationssäkerhet i teleföretag blir en del av den dagliga verksamheten. Genom föreskriften försöker man garantera att möjliga informationssäkerhetsfaktorer beaktas i rutinen och genom effektiva processer som en del av tillhandahållandet av kommunikationsnätverk och dess tjänster.

Föreskriften om *säkerställande av kommunikationsnät och kommunikationstjänster samt om synkronisering av kommunikationsnät* (föreskrift 54) ställer minimikrav på teleföretag om bl.a. säkerställandet av effektmatning till utrustning som används för att tillhandahålla kommunikationsnätverk eller -tjänster, säkerställandet av utrustning och anslutningar samt fysiskt skydd av utrustning.

I föreskriften *om störningar i televerksamheten* (föreskrift 66) hanteras olika störningar i televerksamheten. Föreskriften gäller både situationer där teleföretagets tjänster utsätts för en betydande kränkning av informationssäkerheten eller hot om densamma (*informationssäkerhetsstörning*) och händelser som förhindrar eller på ett väsentligt sätt stör kommunikationstjänstens funktion (*funktionsstörning*). Föreskriften ålägger teleföretag skyldigheter som gäller såväl observation och hantering av störningar i informationssäkerheten och i funktionen som att anmäla och föra statistik över dem.

*Rekommendationen till teleföretag om beredskap* (rekommendation 311) ger teleföretag råd om hur beredskapskraven i lagen kan uppfyllas. Rekommendationen, som är delvis sekretessbelagd, är inte en allmän och allmäntäckande anvisning om förberedelse-, kontinuitets eller beredskapsplanering och genomförandet av dessa, utan i den har man lyft fram frågor som Transport- och kommunikationsverket rekommenderar att teleföretagen tar i beaktande som en del av deras beredskapsskyldighet och befintlig beredskapspraxis.

Föreskriften *om kommunikationsnätens och -tjänsternas kvalitet* (föreskrift 58) gäller mätning och kontroll av kommunikationsnäten och -tjänsternas driftssäkerhet, prestanda, tillförlitlighet och kvalitet. Föreskriften omfattar allmänna skyldigheter som tillämpas på alla kommunikationsnät och -tjänster samt speciella krav som gäller telefonitjänster, internetförbindelsetjänster och televisionstjänster.

Föreskriften om *tekniskt genomförande och säkerställande av nödtrafik* (föreskrift 33) innehåller krav med vilka det säkerställs att nödsamtal och nödtextmeddelanden samt därtill relaterad, för nödtjänsten väsentlig information överförs från de allmänna kommunikationsnäten till nödcentralerna. Föreskriftens krav säkerställer också att nödsamtalen har bättre möjligheter att lyckas än normala samtal vid olika slags belastningar och störningar i kommunikationsnätet.

## 3. Föreskriftens syfte

Syftet med föreskriften är att fastställa de kritiska delarna i kommunikationsnätet. I föreskriften kommer man i enlighet med motiveringarna i regeringens proposition och kommunikationsutskottets betänkanden att tekniskt beskriva nätets kritiska delar, dvs. de faciliteter och åtgärder med hjälp av vilka tillgången till nätet och trafiken på det kontrolleras eller styrs på ett väsentligt sätt.

Föreskriften kommer att styra teleföretag och separata nätverksaktörer inom sitt tillämpningsområde i planeringen av nät, anskaffning av nätverksutrustning, byggande, upprätthållande och hantering av nät. Genom föreskriften främjas nationell säkerhet och dataskyddet i kommunikationsnäten.

Föreskriften preciserar de delar av kommunikationsnätet på vilka skyldigheten att låta bli att använda nätverksutrustning som anges i 244 a § i lagen om tjänster inom elektronisk kommunikation kunde riktas. På så sätt förtydligar föreskriften de tillämpningsobjekt som nämns i paragrafen.

## 4. Andra alternativ för verkställandet

### 4.1. Nätverk och nätverkstekniker som föreskriften omfattar

244 a § i LTEK omfattar alla allmänna kommunikationsnät samt sådana till ett allmänt kommunikationsnät anslutna separata nät som hör till aktörer som är viktiga med tanke på samhällets vitala funktioner.

I beredningen av föreskriften bedömde man vilka nät som det i första hand var viktigt att se till att de omfattas av föreskriften, då det är möjligt att vid behov senare utvidga föreskriftens tillämpningsområde. Traficom fäste i sin bedömning uppmärksamhet vid brådskan av att fastställa kritiskheten hos nätverkets delar, effekten hos dessa samt vid arbetsbördan som fastställandet orsakar.

Frågan om föreskriftens exakta tillämpningsområde är av central betydelse för de nätverk vars delar inte omfattas av föreskriften, i vilket fall deras kritiskhet direkt fastställs av lagens generalklausul (244 a § 1 mom. i LTEK). Med andra ord innebär det att även om föreskriften inte fastställde de kritiska delarna för vissa nätverk eller nätverksteknik skulle det inte betyda att man inte även för deras del vid behov kan fastställa deras kritiska delar. I fråga om teknik som redan är etablerad och som redan länge varit i bruk kan man anta att det är relativt enkelt för nätverkets ägare eller innehavare att bedöma vilka de kritiska delarna av nätverket är. Föreskriften i sin tur är till nytta främst i situationer där det kan vara utmanande att tillämpa generalklausulen, till exempel i samband med nya nätverkstekniker.

#### 4.1.1. Fastställandet av kritiska delar som är gemensamma för alla kommunikationsnät

Traficom bedömer behovet och möjligheten att fastställa kritiska delar gemensamt för kommunikationsnät. Ifall ett dylikt fastställande kan genomföras skulle en fördel vara att man genom en rimlig mängd arbete kunde öka på klarheten om hur lagens generalklausul direkt kan tillämpas. Men å andra sidan förblir ett sådant fastställande nödvändigtvis på en klart mer allmän nivå än om man istället fastställer de kritiska delarna utgående från nätverksteknologi. Med beaktande att föreskriften i detta fall skulle göra det lättare att tillämpa lagen även på sådana nätverk vars kritiska delar inte fastställs skilt, anser Traficom att det är motiverat att noggrant utreda om huruvida en dylik fastställning kan utföras med tillräcklig noggrannhet för en föreskrift. I det här fallen skulle man alltså inte skilt behöva fastställa till exempel kritiska delar av fasta nätverk.

Dessutom kompletterar fastställandet av gemensamma kritiska delar de nätverksteknikssspecifika fastställningarna genom att undvika repetition i fastställningen av kritiska delar. Fastställandet av gemensamma kritiska delar kompletterar också brister i sådana funktioner som inte skilt fastställts i de tekniska specifikationer som hänvisas till i de nätverksteknikssspecifika definitionerna.

Under beredningen av föreskriften hörde Traficom åsikter om huruvida fastställandet av de gemensamma kritiska delarna borde begränsas till enbart IP-baserade kommunikationsnät. En del av aktörerna ansåg att det inte fanns orsak att exkludera kretskopplade nät ur tillämpningsområdet, eftersom de gemensamma definitionerna i stor grad även gäller för dem. Andra aktörer ansåg för sin del att en begränsning till IP-baserade nät kunde leda till problem med tillämpningen. Även fastställningsmetoden som används i Tyskland är teknologineutral (se kapitel 4.3.1).

Traficom bedömer att fastställandet av kommunikationsnätets kritiska delar kan utföras tillräckligt noggrant för att kunna tillämpas på den största delen av olika kommunikationsnät. Särskilt IP-nät är inbördes på många sätt såpass likadana att gemensamt fastställande av kommunikationsnätets kritiska delar lämpar sig väl på dem. Fastställandet kan dock inte enbart begränsas till IP-baserade paketförmedlande nät, eftersom den gemensamma fastställningen kan göras upp teknologineutralt. Till den del som det gemensamma fastställandet av kommunikationsnätets kritiska delar inte i enskilda fall kan tillämpas på något visst nät, skulle de kritiska delarna i kommunikationsnätet fastställas direkt utgående från definitionen i lagen,

om de inte skilt fastställs. Frågan behandlas noggrannare nedan i punkten om de olika fastställningsalternativen för kritiska delar och i punkten om detaljmotiveringar.

#### 4.1.2. 2G- och 3G-nät

Till den andra generationens (2G) mobilnätstekniker räknas till exempel GSM, GPRS och EDGE som etablerade. Den tredje generationens (3G) mobilnätstekniker är till exempel UMTS och HSPA. 2G- och 3G-nätverken utnyttjar både det kretskopplade och paketförmedlande stamnätet. Traditionell samtalstrafik förmedlas genom det kretskopplade nätet och datatrafik genom det paketförmedlande nätet.

Man håller på att slopa 3G-tekniken, och i regel anskaffas inga nya komponenter. Komponenterna utnyttjas inte i någon större utsträckning i de mer moderna generationernas tjänster, och inga särskilt kritiska användningsfall är kända. 3G-tekniken används inte heller i separata nät.

2G-tekniken kan fortsättningsvis vara i bruk i en längre tid, vilket innebär att komponenterna når slutet av sina livscykler och måste ersättas. Dessutom kommer det även i framtiden att finnas kritiska användningsfall (t.ex. 2G IoT, nödtrafik, eCall) för 2G-tekniken. Det handlar visserligen om en mycket mogen teknologi som är avsevärt mindre komplicerad än de senare generationerna.

Traficom antar att för dessa tekniker kan teleföretagen tillräckligt tydligt fastställa kommunikationsnätets kritiska delar på basis av specificeringen av gemensamma kritiska delar för olika nät som ingår i föreskriften och på basis av generalklausulen i 244 a § i LTEK. Därför finns det inte något särskilt behov av att meddela mer detaljerade föreskrifter för denna del.

#### 4.1.3. 4G-nät och 5G Non-Standalone-nät (5G NSA-nät)

Traficom har i sin bedömning av föreskriftens tillämpningsområde särskilt fäst uppmärksamhet vid teknik som används i 4G- och 5G-mobilnät. Med 4G-nät avses här nätverk som verkställs med LTE-teknik.

Det främsta användningsfallet för 5G NSA-nätet är att höja på radionätets dataöverföringskapacitet. 5G NSA-nätet baserar sig på 4G-nätets EPC-kärna (Evolved Packet Core). 5G NSA-näten har inte genomgått samma paradigmskifte som 5G-nätet, och trots senare uppdaterade versioner motsvarar nätets användningsfall inte 5G-nätets i någon vidare bemärkelse. 5G NSA-nätets funktionaliteter uppdateras under sin livscykel till ett 5G Standalone-, dvs. 5G SA-nät, i vilket skede det går att fastställa samma kritiska delar för det som för 5G-nät.

Traficom bedömer alternativa sätt att tillämpa föreskriften på 4G-nät. Om 4G-nätets kritiska delar fastställs, omfattar föreskriften för det första helt alla 4G-nät som grundar sig på LTE-teknologi. För det andra kunde föreskriften samtidigt också omfatta 5G NSA-näten till de delar som de baserar sig på LTE-teknologi (4G-nätets kärna, dvs. EPC).

Att fastställa nätverkets kärna och därigenom de kritiska delarna i nätet även utan en föreskrift är lättare för tidigare generationer jämfört med 5G, vilket i och för sig minskar på behovet av särskild fastställning. Tidigare nätens teknik är tämligen mogen och arkitekturen etablerad. Det här innebär dock också att arbetsmängden som krävs av myndigheterna för att fastställa nätverkens kritiska delar är tämligen liten. I avgörande ställning är därmed huruvida det har en stor effekt att genomföra fastställningen.

Det set ut som att man kommer att fortsätta använda 4G-näten i kritiska funktioner, såsom i den nya myndighetskommunikationstjänsten Virve 2.0 och i kritiska separata nät, vilket är ett starkt argument för fastställningen av deras kritiska delar. Dessutom är 4G-nätets livscykel kommer att fortsätta länge, och 5G-näten kommer inte inom den närmaste tiden att kunna ersätta det stora täckningsområdet som erbjuds av nationella mobilnät genomförda med LTE-teknik. 4G-näten kommer ännu långt in i framtiden att vara en ytterst viktig del av de finska kommunikationsnäten. Dessutom bör anmärkas att radionätet i 5G NSA-näten som grundar sig på 5G-teknologi stöder sig på 4G-nätets kärna, vilket innebär att 4G-teknologin spelar en kritisk roll även i 5G NSA-nät. Det bör också observeras att det existerar flera gränssnitt mellan 4G- och 5G-näten som är till för att garantera kompatibilitet (EPC-5GC interworking), vilket innebär att det kan finnas inbördes beroendeförhållanden mellan näten.

Som ett internationellt jämförelseobjekt kan det konstateras att man i Storbritannien har velat fästa teleföretagens uppmärksamhet vid både 5G-nätens och 4G-nätens särskilt utsatta delar.[1]

5G NSA-nätets 5G-komponenter skulle, vad gäller tillämpningsområde, höra till fastställningen av de kritiska delarna av 5G-nätet. Om man till exempel fastställer att en del är kritisk i 5G-nätet är delen också kritisk inom ett 5G NSA-nät. På motsvarande sätt skulle man vad gäller 4G-delarna som används i 5G NSA-nät bedöma deras kritiskhet utgående från vad som föreskrivs om delar i ett 4G-nät.

Utgående från ovannämnda kan det anses grundat att man mer noggrant fastställer kritiska delar som baserar sig på LTE-teknik i både 4G-nät och 5G NSA-nät i föreskriften. Noggrannare fastställning av 4G- och 5G-nätens kritiska delar fick också stort understöd i de åsikter som Traficom fick i samband med beredandet av föreskriften.

#### 4.1.4. Nät som baserar sig på 5G-teknologin

Det är viktigt att nätverk som använder 5G-teknik omfattas av föreskriften, åtminstone till den utsträckning som det är möjligt att fastställa deras kritiska delar med tanke på teknikens utveckling. Enligt förberedelsearbetet verkställer den nya LTEK 244 a § åtgärderna för 5G-nätens säkerhet i EU:s gemensamma verktygslåda gällande skyddet av nätets kritiska delar. Att fastställa de kritiska delarna i 5G-nät är därmed centralt med tanke på målen i den nya bestämmelsen.

För att göra det lättare att tillämpa den nya regleringen är det uttryckligen viktigt att närmare fastställa de kritiska delarna av 5G-nät. Man har precis börjat bygga 5G-näten, och de stora investeringar som kommer att göras inom en snar framtid och valet av komponenter kommer att vara avgörande för nätets säkerhet långt in i framtiden. Där det i tidigare mobilnätsgenerationer varit relativt enkelt att definiera nätets s.k. kärna (core) finns det mer rum för tolkning i fastställandet av kärnan eller nätets övriga kritiska delar med 5G-teknologi.

En av de centrala skillnaderna mellan 5G-nätet och dess föregångare är den nya nätverkskärnan som baserar sig på service bussar och mjukvarukomponenter. Trafiken mellan funktionerna i nätverkets kärna sker via standardiserade service bussar. En

[1] NCSC advice on the use of equipment from high risk vendors in UK telecoms networks, punkt 11.a.iii. 28.1.2020. https://www.ncsc.gov.uk/guidance/ncsc-advice-on-the-use-of-equipment-from-high-risk-vendors-in-uk-telecoms-networks

etablerad service buss gör det möjligt för serviceproducenter att fast integreras i 5G-nätets kärna. Det här gör det möjligt att anpassa nätet och optimera det utgående från de tjänster användarna använder. Det kommer att vara möjligt att lägga till nya komponenter till service bussen utan att ändra på den.

De nya funktionerna som är kritiska för samhället och användarnas säkerhet som kan genomföras genom 5G-teknologi kommer att ändra på hela nätets grundväsen. Ett system som tidigare i stor grad baserade sig på dataöverföring och fysiska nätelement kommer i stor grad att förvandlas till en mjukvarubaserad molntjänst som processerar data. För att kunna garantera säkerheten måste tillräckliga kontroller fastställas. Med hjälp av 5G-teknologin kommer man att kunna genomföra tidskritiska tjänster och andra tjänster för särskilda användningsfall. Till skillnad från tidigare system kan man i själva nätet verkställa informationshantering, särskilt sådan som baserar sig på kantberäkning, vilket gör att nätet skiljer sig från tidigare nät.

Utgående från det som konstaterats ovan är det motiverat att fastställa de kritiska delarna i 5G-nätet. I samband med fastställningsarbetet måste man dock vara beredd på att de tekniska specifikationer och teknologin ständigt utvecklas och att den praktiska implementationen av nätverken fortfarande i stor grad är oklar. I fastställningsarbetet måste man också bedöma den tidsspann inom vilken olika 5G-teknologier i framtiden kommer att tas i bruk i kommersiella nät.

Traficom inleder ett skilt arbetsprojekt för referensarkitektur med avsikt att fastställa de gemensamma verksamhetsmodeller, processer och bästa praxis för att se till att mobilnät, främst 5G-nät, säkert kan tas i bruk och hur de kan administreras. Arbetet utförs i samarbete med utrustningens tillverkare och mobilnätets teleföretag.

#### 4.1.5. Mobilnätets basstationer

Basstationerna innehåller en basstationsenhet samt en antennenhet som används för att ta emot och sända datakommunikation från och till terminaler. I 4G- och 5G-teknologierna förmedlar basstationen användarnas trafik direkt från operatörens (teleföretaget eller innehavaren av ett separat nät, dvs. en separat nätverksaktör) nätgränssnitt till andra datanät. I tidigare generationers teknologi förmedlas trafiken via en separat kontrollenhet för basstation eller kontrollenhet för radionät.

4G- och 5G-nätens basstationer utför delvis motsvarande faciliteter (t.ex. hantering av radioresurser) som de tidigare generationernas kontrollenheter för basstationer eller kontrollenheter för radionät (Base Station Controller, BSC i 2G, Radio Network Controller, RNC i 3G. För en enskild 4G- eller 5G-basstation påverkar dessa överförda faciliteter dock ett relativt litet antal användare jämfört till exempel med att i 3G-nätet kan en RNC kontrollera upp till ett tusen basstationer.

Grunden för 5G-nätets säkerhetsarkitektur är att nätet konfigureras och segmenteras i olika säkerhetszoner och att man kontrollerar och övervakar trafiken mellan säkerhetszonerna. Basstationerna kan på grund av riskerna kring dem konfigureras att behandlas av nätet som en komponent som hör till den lägsta säkerhetszonen.

Traficom anser att de särskilda dragen för basstationer i 5G-SA-nätet (gNodeB, också ng-eNodeB[2]) inte ännu kan utvärderas eftersom deras tekniska utveckling fortfarande är på hälft. Basstationernas arkitektur och användningsfall utvecklas fortfarande till väsentliga delar. Funktioner eller komponenter som hör till nätets kärna som har att göra med beslutsfattande, datakraft och intelligens kan överföras till basstationen. Dessa aspekter bör särskilt beaktas när man bedömer hur kritisk basstationen är. Frågan är ännu öppen om hur basstationens komponentarkitektur kommer att se ut och hur komponenterna eller funktionerna kan indelas och virtualiseras (se Open RAN). Även nätverksskivning (slicing) och kantberäkning (edge computing) håller på att utvecklas och deras användningssyften är fortfarande oklara, så det ännu för tidigt att meddela föreskrifter om dem åtminstone i samband med allmänna kommunikationsnätverk.

5G-basstationer (gNodeB/e-gNodeB) används också i 5G NSA-nät som baserar sig på 4G-nätets kärna, i vilket fall 5G-basstationernas viktigaste användningsfall är att öka på radionätets dataöverföringskapacitet. Utgångspunkten är att tjänsterna som beskrivits ovan i punkt 4.1.4 som är nya för 5G-nätet inte verkställs i dessa nät.

För separata nät kan betydelsen av en enskild basstation som en del av nätet avvika betydligt från situationen i allmänna kommunikationsnät. Traficom uppskattar att på grund av de separata nätens specialegenskaper måste man bedöma deras basstationer som en skild fråga. Frågan behandlas närmare i avsnitten för detaljmotiveringar.

Denna föreskrift har inte som avsikt att särskilt bedöma kritiskheten hos 4G- eller 5G-nätens basstationer vad gäller allmän televerksamhet. Därför kan deras kritiskhet som en del av nätet vid behov bedömas direkt utgående från definitionen i 244 a § 1 mom. i LTEK på kommunikationsnätets kritiska delar. Vid behov återkommer vi till bedömningen av basstationernas kritiskhet i uppföljningen av föreskriften.

Av samma orsak bedömer Traficom att det är för tidigt att ta ställning till funktionernas kritiskhet vad gäller sådana pålitliga anslutningar till Wi-Fi-nät eller fasta nät som möjliggörs av 5G-nät (Wireline Access) som i framtiden kan komplettera accessnät som baserar sig på 5G-basstationer. Därtill hörande funktioner definierade av 3GPP är åtminstone Wireline Access Gateway Function (W-AGF),) Trusted Non-3GPP Gateway Function (TNGF) och Trusted WLAN Interworking Function (TWIF). Det är för tidigt att här bedöma omfattningen av deras användning i framtiden och hur funktionerna kommer att verkställas, så vi återvänder vid behov till bedömningen av dem i föreskriftens uppföljning.

#### 4.1.6. Övrig kommunikationsnätsteknologi

Traficom bedömde i föreskriftens beredningsskede behovet av att skilt fastställa de kritiska delarna av vissa andra vanligaste kommunikationsnätsteknologier i föreskriften. Ovan har fastställandet av kritiska delar som är gemensamma för alla kommunikationsnät behandlats och resultatet av bedömningen har en inverkan på behovet av att skilt fastställa de kritiska delarna för enskilda nätverkstekniker.

[2] ng-eNodeB är en eNodeB som definierats i Rel-15, och som fungerar tillsammans med gNodeB när core-nätet är 5GC (3GPP TS 37.340, p. 4.1.3.1 och 4.1.3.2). Detta gör det möjligt att genomföra de nya funktionerna som 5G-core tillhandahåller (t.ex. QoS, nätverksskivning) med hjälp av LTE-radioteknologi. Se även 3GPP TS 36.300 p. 24.1 och 3GPP TS 38.300 p. 4.1 och 4.2.

Traficom bedömer att det inte finns något särskilt behov av att fastställa masskommunikationsnätens kritiska delar. Det kan antas att det är relativt enkelt för teleföretagen att fastställa dem utan stöd av föreskriften. Behovet av att fastställa dem minskas delvis av att man inte i masskommunikationsnäten förmedlar konfidentiella meddelanden och att utgångspunkten är att det inte är nödvändigt att kontrollera användarnas tillgång till nätet, även om det är av stor vikt att näten är fungerande.

Vid beredningen bedömdes också behovet av att fastställa de kritiska delarna av fasta bredbandsnät särskilt på basen av att deras komponenter också utnyttjas i 5G-näten som transmissions- och stamlänkar. Basstationernas funktion är baserad på accessnätets och regionnätens anslutningar. Verkställandet av 5G-näten ändrar dock inte på de fasta nätverkens roll vad gäller verkställandet av mobilnäten förutom eventuellt angående de allt mer kritiska tjänsterna som överförs till 5G-nätet. Vad gäller överföringsanslutningarna kan man kryptera tal- och annan trafik, vilket kan minska på riskerna. För regionnätens och accessnätens komponenters del ansågs det inte finnas generellt behov av att fastställa deras kritiskhet, eftersom deras inverkan är tämligen lokal. Fastställning av de kritiska komponenterna för det fasta nätets del kan bedömas vara relativt klart även utan stöd av en föreskrift.

För fasta trådlösa nät, såsom Wi-Fi nät, bedömer Traficom att behovet av fastställning inte är akut. Med hjälp av Wi-Fi-tekniken (IEEE 802.11 WLAN, Wi-Fi) genomförs i huvudsaken lokala nät. Dessutom möjliggörs inom 5G och 4G till exempel kopplingar till nätets kärna med hjälp av nätverksteknologier utanför 3GPP-arbetet. I det här fallet möjliggör operatorn till exempel en koppling direkt till 5G-tjänsterna via ett trådlöst lokalt Wi-Fi-nät.[3] Även om man kan utnyttja till exempel Wi-Fi nätverk för att förbättra inomhustäckningen genom ett utomstående gränssnitt (Non-3GPP Access) måste nätets kärna trots det inte lita på dylika nät. Wi-Fi-teknologin är inte heller något som allmänt används inom kritiska nät. Också LoRa-nätet kan omfattas av lagen, och det kan ha användningsfall som är viktiga för samhällets funktion. Traficom bedömer i detta skede att inga betydliga fördelar skulle fås av att föreskriva särskilt om dessa nät, med tanke på att fastställningen av deras kritiska delar antingen kan ske genom lagens generalklausul eller kan omfattas av fastställningen som berör samtliga kommunikationsnät (se kapitel 4.1.1).

4.2. Hur lösningar kring nätverksarkitekturen, säkerhetsarkitekturen eller informationssäkerhetskontroller påverkar fastställandet eller bedömningen av kritiskheten hos en del av ett kommunikationsnät

För tillämpandet av 244 a § i LTEK kan man fundera på i vilket skede man borde bedöma hur tillämpningen genomförs vad gäller lösningar kring nätverksarkitektur, säkerhetsarkitektur, informationssäkerhetskontroller eller motsvarande. Angående tillämpningen av paragrafen måste man särskilt bedöma vilka kommunikationsnätets kritiska delar är och om huruvida det finns vägande skäl att misstänka att användningen av utrustningen äventyrar den nationella säkerheten eller försvaret, det vill säga om användningen av nätverksutrustningen uppfyller den så kallade förutsättningen för fara enligt den första meningen i 244 a § 1 mom. i LTEK.

Det bör anmärkas att paragrafen och dess motiveringar visar att det är möjligt att en brist i säkerheten hos nätverksutrustning som används i en kritisk del av nätet eventuellt kan, beroende på situationen, repareras på andra sätt än genom att avlägsna

[3] Selvitys 5G:n kyberturvallisuudesta. Yhteenveto. Transport- och kommunikationsverket. Traficoms publikationer 14.05.2019, s. 5.

utrustningen ur nätet, till exempel genom en uppdatering[4]. Detta kan innebära att åtminstone konkreta informationssäkerhetskontroller bör bedömas i samband med bedömningen av förutsättningarna för fara istället för i det tidigare skedet då man bedömer om delen av nätverket eller nätverksutrustningen som används av den är en kritisk del av nätet. Å andra sidan kan man också tänka sig att åtminstone frågor kring nätverksarkitekturen kunde påverka hur två kritiska delar som i övrigt realiseras med samma teknik i vissa situationer i någon mån skiljer sig från varandra.

Om frågor kring arkitekturen eller informationssäkerhetskontroller togs i beaktande i föreskriften redan i det skede då kommunikationsnätets kritiska delar fastställs skulle det leda till att föreskriften blir betydligt mer komplex. Det skulle inte heller hjälpa till att främja det jämlika tillämpandet av föreskriften bland olika företag, och skulle öka på behovet av tillsyn. Ifall det dock uppdagas en klart avgränsad situation där dessa frågor är av avgörande betydelse finns det dock grunder för att föreskriva på ett sätt som tar i beaktande nätverksarkitektur eller informationssäkerhetskontroller. Av denna orsak används i föreskriften i första hand en fastställningsmetod enligt vilken kritiskheten hos kommunikationsnätets delar inte kopplas till någon viss lösning utförd av specifika teleföretag. Istället har Traficom bedömt att en fastställningsmetod utgående från dessa frågor kan utnyttjas i punkt 7 i föreskriften, där man fastställer möjligheten till ett undantag vad gäller fastställningen av kritiskheten hos kommunikationsnätens delar när det är fråga om funktioner som stöder tjänster som verkställs i kantnätet.

En fråga som skiljer sig aningen från föregående har att göra med användningen av samma nätverksutrustning i olika delar av kommunikationsnätet. En viss konkret nätverksutrustning kan användas både i kritiska och icke-kritiska delar av kommunikationsnätet.

## 4.3. Metoden för fastställning av kommunikationsnätets kritiska delar som används i föreskriften

### 4.3.1. Vald fastställningsmetod

Förberedelsearbetet för 244 a § i LTEK förutsätter tekniska definitioner av föreskriften, som tar i beaktande kommunikationsnätens standarder. Till exempel fastställer 3GPP:s definitioner i regel nätets delar ur en logisk synvinkel, det vill säga beroende på deras funktioner eller faciliteter. Enligt motiveringen (RP 98/2020 rd, s. 268) till LTEK 244 a § ska ”[i en föreskrift om nätets kritiska delar] de kritiska delar av nätet som avses och definieras i paragrafen beskrivas tekniskt, det vill säga de faciliteter och åtgärder med hjälp av vilka nätet och trafiken på det administreras på ett centralt sätt. [...] I de tekniska definitionerna i föreskriften ska de internationella standarder på basis av vilka kommunikationsnäten planeras och byggs beaktas.”

På grund av ovan sagda har Traficom fört fram som första alternativ för verkställandet det att man i föreskriften ska precisera de funktioner eller faciliteter som (åtminstone) anses vara kommunikationsnätets kritiska delar till de delar som fastställandet sker nätverksteknologispecifikt. Fastställande enligt 3GPP:s funktionsbaserade

[4] RP 98/2020 rd, s. 267: ”Före beslut fattas ska Transport-och kommunikationsverket höra kommunikationsnätets ägare eller andra innehavare och ge denna möjlighet att avhjälpa upptäckta säkerhetsbrister. Syftet med detta är att framhäva särskilt förverkligandet av proportionalitetsprincipen i tillsynsåtgärderna. Ägaren eller en annan innehavare av ett kommunikationsnät kan avhjälpa säkerhetsbristen t.ex. genom att uppdatera nätverksutrustningen, om det är tillräckligt för att avhjälpa situationen.”

definitioner har också varit den metod som valts i de länder där Traficom är medveten om att man försökt att tekniskt precisera omfattningen av 5G- eller 4G-nätens kritiska delar, dvs. Frankrike och Storbritannien.[5]

Fastställning av de kritiska delarna för 5G- och 4G-nät skulle i så fall ske skilt för sig, eftersom faciliteternas (funktionernas) namn och funktionalitet skiljer sig mellan dem. Funktionerna är logiska och splittrade i flera olika applikationer, och kan inte nödvändigtvis entydigt avgränsas från deras verksamhetsmiljöer i det verkliga livet. Sättet att fastställa dem skulle dock innebära att när man kan påvisa att en enskild programvarukomponent genomför ens en del av en sådan 3GPP-funktion som fastställts som en kritisk del av nätet, så skulle komponenten räknas som en kritisk del av nätet, även om komponenten inte i sig själv utför hela funktionen.

Ett mer noggrant fastställande gör det lättare att tillämpa regleringen på enskilda nät och främjar en rättvis tillämpning av reglerna inom olika företag. Ett mer noggrant fastställande gör det också möjligt att utnyttja tidigare utländska exempel. Ett mer noggrant fastställande skulle för sin del också sänka kostnaderna orsakad av myndighetsverksamhet i samband med tillämpandet av föreskrifterna på företagsnivå och i det skede då tolkningarna ska verkställas, samt risken att tillsynsmyndigheten inte anser att företagets tolkning är korrekt.

Vad gäller en förteckning över gemensamma kritiska delar som strävar att vara teknologineutral kan den inte basera sig på tekniska standarder, eftersom de är bundna till specifika teknologier. Även i EU:s gemensamma verktygslåda har man försökt fastställa viktighetsgraden för nätets olika delar genom de funktioner de genomför, även om de inte direkt hänvisar till de 3GPP:s definitioner av 5G-nätets funktioner.[6] Dessutom har man i Tyskland och Storbritannien på olika sätt försökt fastställa allmänna kritiska funktioner som kan tillämpas på olika nät, av vilka Traficom anser att Tysklands lösning är en mycket användbar jämförelsepunkt både till sin struktur och till sitt innehåll för denna föreskrift.

I Tyskland har den förbundsstatliga tillsynsmyndigheten för telebranschen (Bundesnetzagentur, BnetzA) och informationssäkerhetsmyndigheten (Bundesamt für Sicherheit in der Informationstechnik, BSI) gjort upp ett utkast om nätets kritiska funktioner.[7] Listan är inte enligt utkastet avsedd att vara uttömmande, och är teknologineutral. På listan nämns användarhantering, kryptografiska mekanismer, gränssnitt mellan nät, nättjänster, NFV och MANO samt virtualisering, administrations- och andra stödsystem, styrning av nättrafik och lawful interception (teleavlyssning och teleövervakning). Närmare specifikationer för listans punkter ges i utkastet per punkt.

I Storbritannien har man i en anvisning från det nationella cybersäkerhetscentret gjort teleföretagen medvetna om vissa funktioner som är gemensamma för alla nät

[5] Se För Förenade kungarikets del fotnot 1 och för Frankrikes del Arrêté du 6 décembre 2019 fixant la liste des appareils prévue par l'article L. 34-11 du code des postes et des communications électroniques. https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000039455672.
[6] Cybersecurity of 5G networks EU Toolbox of risk mitigating measures. CG Publication 01/2020. Bilaga 2, s. 39. https://ec.europa.eu/digital-single-market/en/nis-cooperation-group.
[7] Liste der kritischen Funktionen für öffentliche Telekommunikationsnetze und -dienste mit erhöhtem Gefährdungspotenzial, utkastet tillgängligt: https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/KatalogSicherheitsanforderungen/Listekritische-Funktionen.pdf.

och som anses vara särskilt utsatta för risker.[8] I anvisningsbrevet har dessa definierats enligt följande: "IP Core, Security Functions, Operational Support Systems (OSS), Management and Authentication, Authorisation and Audit (AAA) functions, Virtualisation infrastructure (including Network Function Virtualisation Infrastructure (NFVI)), Orchestrator and controller functions (including Management and Network Orchestration (MANO) and Software Defined Networks (SDN) orchestrators/controllers), Network monitoring and optimization, Interconnection equipment, Internet gateway functions, Lawful Intercept related functions."

#### 4.3.2. Utvärdering av andra alternativ till fastställningsmetoden för kommunikationsnätets kritiska delar

Under beredningen försökte vi också identifiera andra än de ovan nämnda metoderna för att fastställa kommunikationsnätets kritiska delar. Risken med en funktionsbaserad definition baserad på publicerade tekniska specifikationer är att ifall den genomförs i form av en sluten förteckning kan den vara så styv att vissa kritiska komponenter inte omfattas av definitionerna. Detta kan leda till att de redan fastställda funktionerna inte på grund av ändringar i 3GPP:s definitioner eller nyutvecklade funktionaliteter längre omfattar alla kritiska komponenter. Man kan dock minska på den här risken genom att använda jämförelser, se till att förteckningens utformning inte är uttömmande, genom att undvika att hänvisa till vissa versioner av standarderna, och genom att följa utvecklingen av standarder. Detta ökar visserligen på myndighetsarbetet som övervakningen av regleringen kräver.

Noggranna, funktionsbaserade definitioner kan visa sig vara styva ifall graden av kritiskhet för till och med samma komponenter som delar av olika aktörers nät visar sig variera kraftig till exempel på grund av den nätverks- eller säkerhetsarkitektur som teleföretaget valt. 5G-nätens informationssäkerhet påverkas väsentligen av de specifika lösningarna som tillämpats i näten i fråga, utrustningens fysiska skydd och säkerhetslösningarna i kantberäkningsmiljön, som inte diskuteras i 5G-standarden.[9] Noggrannare definitioner kräver sannolikt också oftare att man gör ändringar än ifall en mer generell definition används.

Å andra sidan skulle en mer generell definition vara mer arbetsdrygt för nätets ägare att tillämpa, eftersom resultatet kan bero på nätverkets särdrag och bedömningen måste uppdateras varje gång ändringar sker. Ifall definitionen däremot inte på något betydande vis är beroende av enskilda teleföretags lösningar är övervakningen enklare och det är lättare att se till att regleringen tillämpas jämlikt.

En mer generell definition kan dock genomföras på flera olika nivåer, och fördelarna och nackdelarna med den är fast i detaljerna.

**Till att börja med** kan man lyfta fram att klassificering i viktighetsordning och störningsklassificering av kommunikationsnätverkens och -tjänsternas komponenter i Traficoms föreskrifter 54 och 66 baserar sig på typen av kommunikationstjänst, antalet användare och arealen på det geografiska påverkningsområdet. Fördelen med en *definitionsmetod som baserar sig på tjänstens typ och inverkan på användarna*

[8] NCSC advice on the use of equipment from high risk vendors in UK telecoms networks, punkt 11.a. https://www.ncsc.gov.uk/guidance/ncsc-advice-on-the-use-of-equipment-from-high-risk-vendors-in-uk-telecoms-networks. Se också punkt 12.
[9] Selvitys 5G:n kyberturvallisuudesta. Yhteenveto. Transport- och kommunikationsverket. Traficoms publikationer 14.5.2019, s. 9.

vore att man inte i själva föreskriften skulle behöva en noggrannare teknisk specifikation som snabbt blir föråldrad. Om man väljer detta alternativ skulle man dock mer noggrant tvingas analysera om huruvida fastställningsmetoden omfattas av bemyndigandet att meddela föreskrifter; den här frågan diskuteras senare i denna punkt och i punkt 4.5.

Fördelen med en definitionsmetod som baserar sig på den effekt som funktions- eller informationssäkerhetsstörningar skulle ha är att man kan klassificera kommunikationsnätet komponenter utgående från deras effekt på användarna. Dessutom finns det tidigare erfarenhet av att använda en dylik definitionsmetod. Nackdelen med denna definitionsmetod är att den inte lämpar sig för att till exempel ange kritiskhet av separata näts delar som sådana, vilket innebär att dessa nät kräver sina egna kriterier. Definitionsmetoden lämpar sig också dåligt på situationer där komponentens kritiskhet grundar sig på dess förmåga att säkerställa kommunikationstrafikens sekretess, eller situationer där funktionaliteten kan ha distribuerats i flera apparater, i vilket fall en enskild apparats antal användare eventuellt inte når upp till minimiantalet användare för att den ska klassas som kritisk. De kriterier som används i de existerande föreskrifterna lämpar sig alltså inte som sådana för att fastställa kritiska komponenter, eftersom målen med fastställandet av kritiska delar skiljer sig från målen med klassificeringen i viktighetsordning från de tidigare föreskrifterna. Faktum är att det är svårt att komma på vilka kriterier för negativa effekter på användare som kunde ligga som grund för fastställandet av kritiska delar i nätet.

Att utföra fastställandet på basis av effekten på användare skulle i princip ur en regleringsteknisk synvinkel vara möjligt ifall man använder typen av service som grund, såsom görs i existerande Traficoms föreskrifter. Med detta avses att klassificeringen i viktighetsordning är kopplad till händelser som förhindrar till exempel att den allmänna telefonitjänsten, internetaccesstjänsten eller textmeddelandetjänsten fungerar för en grupp användare i en viss storleksklass. Nackdelen med denna fastställningsmetod är dock att den inte nödvändigtvis gör det lättare att definiera separata näts kritiska delar eftersom nätverkets innehavare som ska tillämpa föreskriften själv måste besluta vilka komponenter har den effekt på användarna som föreskriften förutsätter. Traficom bedömer dock att en definition som utgår från kommunikationstjänstens typ lämpar sig för att komplettera andra definitionsmetoder, till exempel för 4G- och 5G-nätens taltjänsters (Voice over LTE dvs VoLTE och Voice over New Radio, VoNR / 5G Voice) del, eftersom man i så fall kunde undvika att skilt tvingas definiera komponenterna i föreskriften: det är alltså fråga om IMS (IP Multimedia Core Network Subsystem)-komponenternas definition. Detta diskuteras senare i detaljmotiveringsavsnittet.

**Ett andra** alternativ kunde vara att inte använda de direkta funktionerna i nätets kärna som 3GPP fastställt utan istället på en *mer abstrakt nivå* beskriva funktioner som, ifall de genomförs av en komponent innebär det att komponenten klassas som kritisk. Detta innebär en fastställningsnivå som baserar sig på begrepp såsom trafikstyrning och -routning, identifiering och auktorisering av användare samt hantering av kryptografiska nycklar. Fördelen med dylika definitioner är att de inte påverkas av ändringar i lika stor grad som fastställningsmetoder som använder direkta hänvisningar till nätens delar eller funktioner som beskrivs i standarder eller i tekniska specifikationer. Nackdelen är dock att det i praktiken innebär att tillämpandet är mindre entydigt. Om man direkt får hänvisa till funktioner som fastställts i en specifikation kunde man använda den mer generella nivån för att komplettera den noggrannare förteckningen, vilket skulle minimera de olägenheter som diskuterats ovan ifall man använder enbart funktionsspecifika definitioner. En dylik aningen mer generell definitionsmetod som grundar sig på nätets funktioner passar däremot bra i en situation där man försöker att gemensamt fastställa de kritiska delarna för olika nät, och där

det inte kommer på fråga att hänvisa till de mer noggranna funktionerna som fastställts i standarder på grund av de stora skillnaderna mellan näten.

**Som tredje** alternativ är att teleföretagen eller andra ägare eller innehavare av nät som omfattas av regleringen *själva ska kunna identifiera och beskriva* vilka komponenter i nätet de har konstaterat vara kritiska delar av nätet enligt regleringen. Det noggrannare fastställandet av nätets kritiska delar skulle alltså utföras av de olika nätens ägare eller innehavare, utgående från kriterierna i föreskrifterna. Detta alternativ skulle beakta tolkningar där bedömningen av kritiskheten hos en del av nätverket kunde variera beroende på den nätverks- eller säkerhetsarkitektur som operatören av ett enskilt nätverk valt eller de konkreta informationssäkerhetskontroller operatören genomför. Ett dylikt krav kunde för det första åtminstone användas för att komplettera definitionerna genom att förutsätta att operatörerna uttryckligen identifierar de (i föreskriften angivna) kritiska delarna i sina kommunikationsnät och dokumentera dem. Å den andra sidan kunde ett dylikt sätt att föreskriva vara en del av en fastställningsmetod där operatören själv skulle fastställa sitt eget näts kritiska delar utgående från föreskriftens mer allmänna men tekniska bedömningskriterier.

Under beredningen bedömde man också möjligheten till att Traficom skulle meddela en föreskrift om fastställningsprocessen för kritiska delar. Rätten att meddela föreskrifter i 244 a § 6 mom. i LTEK kan tolkas som att man med detta avser eller i alla fall möjliggör att verkets föreskrift gäller själva definitionen, det vill säga processen genom vilken de kritiska delarna fastställs. Den egentliga fastställning för det egna nätets del skulle utföras av teleföretaget eller den separata nätverksaktören. I motiveringarna till 244 a § i LTEK konstateras dock att ”i en föreskrift om nätets kritiska delar ska de kritiska delar av nätet som avses och definieras i paragrafen beskrivas tekniskt”. Avsikten med bestämmelsen verkar därmed vara att utgångspunkten är att Traficom fastställer kommunikationsnätets kritiska delar. Detta stöds av omnämnandet i motiveringarna att Traficom regelbundet skulle bedöma behovet att uppdatera föreskrifter som utfärdats med stöd av regleringen i takt med att tekniken för kommunikationsnät utvecklas. 244 a § i LTEK verkar därmed inte enbart kräva att verksamhetsidkarna görs delaktiga i fastställningsprocessen av de kritiska delarna i deras egna kommunikationsnät. Men å andra sidan verkar bestämmelsen inte heller förutsätta att verkets föreskrift uttömmande fastställer alla kritiska delar i ett kommunikationsnät.

Under beredningen bedömdes också om huruvida LTEKs övriga bestämmelser kunde fungera som grund för att förplikta kommunikationsnätets ägare eller annan innehavare att delta i fastställningsprocessen och i dokumenteringen av den. I motiveringen till den nya 244 a § konstateras att ”den föreslagna regleringen kompletterar de övriga åtgärderna och skyldigheterna i lagen”. Därmed kan verkets mer allmänna befogenheter att meddela föreskrifter enligt 244 § i lagen tillämpas vid sidan om den särskilda befogenheten att meddela föreskrifter i den nya 244 a § 6 mom. För fastställning och dokumentering av kommunikationsnätets kritiska delar lämpar sig särskilt punkter 1, 3 och 12 i 244 § enligt vilken Transport- och kommunikationsverkets föreskrifter kan gälla bland annat klassificering i viktighetsordning, informationssäkerhet och störningsfrihet, underhåll och uppföljning av dessa samt nätverksadministration, samt teknisk dokumentation och statistik samt utformning av tillhörande dokument och lagring av uppgifter.

Som en internationell jämförelsepunkt kan vi ta fram *Norges modell.* I den kan ministerierna inom sina egna ansvarsområden utgående från en lag om nationell säkerhet identifiera samhällets grundläggande funktioner samt sådana betydande företag som är kritiska för att kunna verkställa en eller flera av samhällets grundläggande funktioner. Dessa företag utför utgående från en föreskrift som försvarsministeriet

gett om företagssäkerhet en bedömning av sin egen verksamhets skadegrad som de sedan skickar till det egna verksamhetsfältets ministerium. Ministeriet i sin tur klassificerar objektet eller infrastrukturen som ska skyddas utgående från den skadebedömning företaget gjort och meddelar säkerhetsmyndigheterna om klassificeringen. Företaget ansvarar för att skydda objekten och infrastrukturen i fråga.[10]

> Skadebedömningen förpliktas i företagssäkerhetsföreskriften, där man även ger motiveringar för utförandet av bedömningen. Närmare anvisningar om uppgörandet av skadebedömningen och dokumenteringen av den finns i en handbok som den nationella säkerhetsmyndigheten har gjort för företagen.[11]Handboken delar in bedömningsprocessen i fyra olika skeden, i vilka företaget 1) utreder betydelsen av sin företagsverksamhet för samhällets grundläggande funktioner 2) kartlägger objekt och infrastruktur 3) utför en skadebedömning av objekten och infrastrukturen samt 4) dokumenterar skadebedömningen de utfört.
>
> Varje skede i bedömningsprocessen beskrivs närmare i handboken. Till exempel i punkt 3 ges anvisningar om hur man stegvis kan fastställa vilka skadliga följder för de nationella grundläggande funktionerna kan orsakas ifall de objekt eller den infrastruktur som identifierats utsätts för skador, blir förstörd eller tas över olagligen.[12]

I Norges modell är det bedömningsarbete företagen gör själva en etablerad och väsentlig del av myndighetsprocessen genom vilken aktörer som är kritiska för samhällets funktion och de objekt som är kritiska för deras verksamhet identifieras, utvärderas och klassificeras. Modellen är baserad på lag, föreskrift samt anvisningar och handböcker som beskriver processen. I definitionsarbetet framhävs växelverkan och att företagen själva är de största experterna på sina egna objekt och på att bedöma sårbarheten i dem.

En regleringslösning i norsk stil kunde delvis genomföras i Finland genom att man genom föreskrift från verket först ger alla aktörer gemensamma kriterier åtminstone för vad som kan anses vara kritiska delar. Till näst kunde man förutsätta av aktörerna att själv utvärdera om huruvida deras nät använder sådana delar vars funktion är kritisk antingen utgående från föreskriften eller från lagens generalklausul (244 a § mom. 1). Aktören skulle sedan dokumentera vilka delar av sitt kommunikationsnät fastställts som kritisk. Traficom skulle ha rätt att få denna dokumentation utgående från myndigheternas allmänna rätt att få information enligt 315 § i LTEK. Genom Traficoms föreskrift är det dock inte möjligt att ålägga nya skyldigheter för aktörer att regelbundet eller i förväg lämna in dokument till myndigheten när nya komponenter tas i drift, utan detta behöver en begäran av myndigheten.

Det kan antas att det inte hittats några totalersättande alternativ för en funktionsbaserad förteckning ifall man vill fastställa kritiska delar för en specifik nätverksteknologi. Andra identifierade alternativ vore inte lika klara, och hade inga tydliga fördelar jämfört med en funktionsbaserad definition. Ett fastställande på mer allmän nivå

---

[10] Lov om nasjonal sikkerhet (sikkerhetsloven; https://lovdata.no/dokument/NL/lov/2018-06-01-24); Forskrift om virksomheters arbeid med forebyggende sikkerhet (virksomhetsikkerhetsforskriften, 57 §; https://lovdata.no/dokument/LTI/forskrift/2018-12-20-2053). Med objekt som ska skyddas avses t.ex. en byggnad, ett utrymme, ett transportmedel eller annat material eller del av dylikt objekt; med infrastruktur avses utrymmen eller system, som ofta innehåller två eller flera komponenter och anslutningar mellan dem.

[11] Nasjonal sikkerhetsmyndiget: Håndbok i skadevurdering. https://nsm.no/regelverk-og-hjelp/veiledere-og-handboker-til-sikkerhetsloven/handbok-i-skadevurdering/om-denne-handboken/.

[12] I skede 3 ska företaget utreda (i) vilka skadliga följder orsakas åt de nationella grundläggande funktionerna ifall de identifierade objekten eller infrastrukturen försvinner helt eller delvis (ii) hur länge objekten eller infrastrukturen kan vara ur funktion helt eller delvis innan de nationella grundläggande funktionerna påverkas, (iii) hur objekten eller infrastrukturen kan ersättas eller repareras inom en rimlig tid samt (iv) hur olagligt övertagande av objekten eller infrastrukturen kan påverka befolkningens grundläggande säkerhet.

uppskattas dock vara lämpligt om man kompletterar en mer detaljerad, nätverksteknikspecifik fastställning.

### 4.4. Styrsystem för basstationer och andra komponenter

Med basstationernas styrsystem är det möjligt att påverka användarnas tillgång till nätet eller till och med helt förhindra den samt trafiken som basstationerna förmedlar, till exempel genom att göra den långsammare. Man kan bedöma att basstationernas styrsystem är kritiska delar av kommunikationsnätet även i situationer där den enskilda basstationen som systemet styr inte i sig självt kan betraktas som en kritisk del av ett kommunikationsnät. Detsamma kan gälla styrsystem för andra element.

Det är typiskt att basstationens apparatleverantör också levererar styrsystemet. Gränssnitten mellan radionätet och styrsystemet är i de flesta fall slutna, även om olika apparatleverantörers styrsystem eventuellt kan ha begränsad förmåga att styra basstationselement som tillverkats av andra tillverkare. Inom området pågår ett utvecklingsprojekt, Open RAN, med avsikt att göra systemen och deras gränssnitt öppna.

I beredningen bedömdes särskilt kritiskheten hos basstationernas styrsystem och det mest ändamålsenliga sättet att fastställa dem i föreskriften. Olika alternativ som bedömdes var A) basstationens styrsystem fastställs som kritiskt som sådant, B) bedömning från fall till fall om kritiskheten hos ett styrsystem och C) att en basstations styrsystems icke-kritiskhet skulle bindas till vissa kriterier.

Alternativ C förkastades på den grund att det troligen skulle förutsätta att man i föreskriften fastställer kriterier för nödvändiga dataskyddskontroller och andra saker som påverkar ärendet på förhand. Traficom anser att det inte finns några lämpliga på förhand kända kriterier med vilka man med säkerhet kunde utesluta att ett system är kritiskt. Betydelsen av konkreta informationssäkerhetskontroller kan bäst bedömas i det skede när man bestämmer om huruvida de så kallade förutsättningarna för fara som beskrivs i 1 mom. i 244 a § i LTEK uppfylls.

Alternativ A förkastades eftersom man inte ansåg det möjligt att utan undantag fastställa basstationernas styrsystem som en kritisk del av kommunikationsnätet. I föreskriften är det ändamålsenligt att fastställa som kommunikationsnätets kritiska delar åtminstone de nätverksadministrationssystem som har att göra med hantering av kommunikationsnätets kritiska delar. Komponenterna som är föremål för styrningen, det vill säga basstationerna, vore inte nödvändigtvis i sig själva kritiska delar av kommunikationsnätet, utan deras kritiskhet bedöms direkt utgående från definitionen i 1 mom. i 244 a § i LTEK, eftersom man inte ännu i denna föreskrift föreskriver om bedömningen av basstationernas kritiskhet. Av denna orsak ska kritiskheten hos basstationernas styrsystem bedömas på skilda grunder i de situationer när basstationerna i sig själva inte är kritiska. Bedömningen av kritiskheten hos basstationernas styrsystem beror i sista hand på om de enskilt uppfyller definitionen på en kritisk del i kommunikationsnätet. Det här kan påverkas av situationens konkreta särdrag, till exempel antalet basstationer som styrsystemet i fråga hanterar.

Alternativ B blev därmed det mest genomförbara alternativet. I detta fall anses styr- och övervakningsanordningar för andra delar av nätet än kritiska delar av kommunikationsnätet i sådana fall där de väsentligen påverkar tillgången till nätet och trafiken på nätet. Att utföra bedömningen orsakar i viss grad en administrativ börda på teleföretag och separata nätverksaktörer, men som motvikt betyder det att basstationernas styrsystem från fall till fall kan betraktas som icke-kritiska.

## 4.5. Telefonitjänster i mobilnät

I IP-baserade 4G- och i framtiden 5G-mobilnät genomförs paketförmedlad allmän telefonitjänst med hjälp av IMS (IP Multimedia Core Network Subsystem) i nätets kärna. I den tidigare generationens nät är den allmänna telefonitjänsten kretskopplad.

Enligt åsikterna som mottogs i samband med beredningen av Traficoms föreskrift ansågs IP-baserade telefonitjänster i regel som kritiska, och man ansåg att kommunikationsnätens delar som ansluter sig till dem skilt ska fastställas som kritiska. Tillgången till telefonitjänster liksom samtalens sekretess var ytterst viktiga. I anknytning till tillgången till mobilnätets allmänna telefonitjänster kan det anmärkas att tills vidare kan samtalen också normalt genomföras i 2G- eller 3G-nätet. En del av de aktörer som deltog i beredningen ansåg att 2G- eller 3G-nätets tjänster tills vidare tryggar ljudsamtal. Traficom anser att det trots det är motiverat att fastställa IMS Core till nödvändiga delar som en kritisk del av kommunikationsnätet. I telefonitjänster som genomförts med nyare nätverksteknik har den mycket stor betydelse med tanke på kommunikationens konfidentialitet, eftersom den kan användas för att få tillgång till icke-krypterad telefontrafik och användarnas lokaliseringsuppgifter. Det är inte heller möjligt att i alla situationer använda kretskopplade tjänster istället, så även med tanke på tillgång är IMS Core viktig.

Traficom anser att, med tanke på hur viktig den allmänna telefonitjänsten är, det är motiverat att separat fastställa kritiskheten hos därtill hörande IP-baserade funktioner. Faciliteternas och åtgärdernas kritiskhet för kretskopplade telefonitjänster skulle fastställas utgående från förteckningen över de gemensamma kritiska delarna i olika nät som ingår i föreskriften, samt vid behov direkt utgående från 1 mom. i 244 a § i LTEK.

Liksom konstaterades ovan i kapitlet 4.3.2 om fastställningsmetoden för kommunikationsnätets kritiska delar, kunde en fastställningsmetod som baserar sig på kommunikationstjänstens typ vara lämplig för att komplettera de övriga fastställningsmetoderna. En dylik fastställningsmetod kunde betyda att man inte separat skulle behöva definiera de kritiska komponenterna för IMS i föreskriften.

Traficom bedömer att det också är ändamålsenligt att utnyttja 3GPP:s specifikationer för IMS Core, eftersom detta formar en gemensam grund för olika teleföretag. På denna grund förkastades det alternativ där man enbart skulle ha fastställt som kritiska de faciliteter i mobilnätet som har att göra med verkställandet av IP-baserad allmän telefonitjänst, eftersom en dylik fastställning leder till problem med avgränsning. De åsikter som Traficom mottagit understödde i frågan om hur IMS ska fastställas en fastställning som utgår från 3GPP:s funktioner, även om en del av respondenterna upplevde att de kritiska delarna också kan fastställas som helhet. Traficom anser att fastställandet av IMS Core:s kritiska funktioner på ett detaljerat och funktionsbaserat sätt betydligt och onödigt skulle göra föreskriften för detaljerad, eftersom den tekniska specifikationen av IP Multimedia Core Network Subsystem omfattar en väldigt komplicerad funktionshelhet. Därför bestämde sig Traficom för en lösning där man kombinerar en fastställningsmetod som utgår från typen av kommunikationstjänst med en metod som grundar sig på 3GPP:s tekniska definitioner. Det uppskattas att en dylik fastställningsmetod trots allt är tillräckligt klar för att tillämpas i teleföretagen.

## 4.6. Kritiska separata nät

Enligt 244 a § 2 mom. i LTEK, ”Vad som föreskrivs i 1 mom. tillämpas också på ett sådant till ett allmänt kommunikationsnät anslutet separat nät som hör till ett kärnkraftverk, en hamn, en flygplats eller någon motsvarande aktör som är viktig med tanke på samhällets vitala funktioner.”. Dessa nätverk hänvisas till med termen ”kritiska separata nät” och nätens ägare eller innehavare med ”separata nätverksaktörer”. I 244 a § i LTEK tar man inte ställning till teknologin som använts för det kritiska separata nätet, utan ett kritiskt separat nät kan vara fast eller trådlöst.

4G- och 5G-näten kan verkställas i anpassad form för lokala ändamål som separata nät. Dylika objekt kan vara till exempel läroanstalter, sjukhus, köpcentrum, evenemangscentrum och fabriker. Lokala, skräddarsydda nätlösningar kan i princip utnyttja frekvenser som har hyrts av nationella operatörer eller eventuellt skilt inriktats för detta användningsändamål i sina nät , eller använda frekvensband som inte är tillståndspliktiga. Kantberäkningsmiljöer som används i den lokala aktörens utrymmen och miljöer kan spela en central roll i verkställandet av specialtjänsterna och beräkningsfunktionerna.[13]

Lokala 4G- eller 5G-nät kan i princip verkställas med hjälp av mycket olika modeller (deployment models) inom de arkitekturer som 3GPP definierat.[14] Dessa nätverk kan hänvisas till i de tekniska specifikationer med begreppet non-public network, NPN. I Standalone NPN-fall kommer nätets funktioner att verkställas helt lokalt. Nätet kan ha en anslutning till det allmänna kommunikationsnätet via en brandvägg. Dessutom är olika kombinationer av allmänna kommunikationsnät och NPN möjliga, där vissa funktioner verkställs lokalt och vissa i det allmänna kommunikationsnätet. NPN är i dessa fall beroende av det allmänna kommunikationsnätet. Till exempel kan enbart radionätet vara delat, men control plane (styrtrafiken) kan också ha verkställts inom det allmänna kommunikationsnätet. Detta kan genomföras bl.a. genom att styra trafiken till ett lokalt datanät (local breakout), genom nätverksskivning eller genom att använda en egen APN (access point name).

Traficom utvärderade i förberedelseskedet följande alternativ:

A) De kritiska delarna i kritiska separata nät fastställs inte skilt, utan de fastställs enligt samma principer som delar i allmänna kommunikationsnät

B) De kritiska delarna av kritiska separata nät fastställs självständigt

C) Definitionen av de allmänna kritiska delarna kompletteras vid behov med preciseringar för kritiska separata nät.

Alternativ B förkastades på den grunden att det skulle leda till att man onödigt skapar överlappande definitioner, eftersom näten utnyttjar samma teknologier som i allmänna kommunikationsnät. Traficom anser att definitionen på kritiska delar i vilket fall som helst inte kan vara snävare än för allmänna kommunikationsnät, vilket lämnar alternativ A och C.

[13] Selvitys 5G:n kyberturvallisuudesta. Yhteenveto. Transport- och kommunikationsverket. Traficoms publikationer 14.05.2019, s. 8.
[14] Se t.ex. 5G-ACIA: 5G Non-Public Networks for Industrial Scenarios; GSA: Private LTE & 5G Networks Report; och Ericsson: Critical capabilities for private 5G networks.

Traficom anser också att utgångspunkten är att föreskriften tillämpas som sådan även för att fastställa de kritiska delarna av kritiska separata nät. Inga stora skillnader i principerna bakom arkitekturen eller funktionaliteten bedöms existera mellan allmänna kommunikationsnät och separata nät. På grund av de separata nätverkens egenart ska man dock för basstationernas del bedöma om det finns behov av kompletterande reglering (se kapitel 4.1.5 om nätets basstationer och punkt 3 i detaljmotiveringarna). Inga andra särskilda behov av precisering för fastställandet av de separata nätens kritiska delar framkom i samband med beredningen av föreskriften. Därmed beslutade vi att välja alternativ C.

## 4.7. Funktioner som stöder tjänster på kantnätet

Med hjälp av kantberäkning kan man tillhandahålla informationshanteringstjänster i kanten av 5G-nätet till exempel i situationer där det krävs mycket låg latens. Kantberäkning möjliggör att flera olika servicehelheter verkställs på samma plattform. Servicehelheten kan bestå av en eller flera arbetsskeden, som utförs virtualiserat på plattformen.[15]

Gränssnitt mellan kantberäkningen och nätets kärna kan ses som särskilt utsatta för attacker, och deras inverkan på hela nätets funktion kan vara stor. Den största risken med kantberäkning är att plattformen som den körs på utnyttjas när man försöker bryta in i resten av nätet eller i andra workloads, eller i form av överbelastningsattacker på resten av nätet. De vanligaste sätten som riskerna realiseras kan vara att genom programvara bryta sig in i en annan workload eller ett internet- eller radiogränssnitt eller i form av ett fysiskt inbrott genom utrustning.

För att verkställa kantberäkningen kan funktioner i nätets kärna föras ut till nätets kant eller i övrigt närmare nätets användare. För kantberäkning kan man på nätets kant genomföra kärnans funktioner, till exempel 5G-nätets UPF-funktion (User Plane Function) eller en lokal kopia av den, eller andra av kärnans funktioner som enligt punkt 6 i föreskriften har fastställts som en på förhand antagen kritisk del av nätet. När man vill styra eller avlasta användartrafiken på nätets kant för kantberäkning, måste UPF genomföras där. Det här förutsätter ett gränssnitt till nätets egentliga kärna. Därför bedöms till nästa särskilt UPF, och motiveringar framförs varför UPF alltid kan betraktas som en kritisk del av kommunikationsnätet, även när den genomförs på kantnätet.

UPF:s centrala roll i hanteringen och övervakningen av användarnas trafik på kantnätet betyder att man kan utgå från att den är en kritisk del av 5G-nätet även på kantnätet. UPF genomför också andra kritiska tjänster, såsom styrning av användartrafik, filtrering, övervakning eller vidareroutning vid behov till ett lokalt datanät eller internet med hjälp av N6-gränssnittet. UPF producerar tjänster och styr trafiken från RAN-nätet och från användare från andra mobilnät än 3GPP-nät. UPF spelar också en central roll i teleavlyssningen av användarnas trafik och i insamlingen av faktureringsuppgifter. UPF kan vara en funktion som är allmänt använd i all datatrafik, sessionsspecifik, eller skivspecifik. Den kan också verkställas inom kantberäkningen på sin egen plattform, dit användarnas trafik styrs genom N6-gränssnittet.

Samtidigt beslutar UPF om styrningen och övervakningen av användartrafiken och vid behov om att terminera trafiken i ett lokalt nät eller datanät, varför det är viktigt hur UPF:s säkerhet i sig självt har tryggats. UPF:s centrala säkerhetsfunktioner med

[15] Komponenter som har att göra med kantberäkning har beskrivits till exempel i dokumentet ENISA Threat Landscape for 5G Networks, punkt 3.9.

tanke på användartrafiken är bl.a. DPI (deep packet inspection), krypteringsfunktioner samt möjliggörandet av teleavlyssning av trafik på kantnätet.

Å andra sidan växelverkar UPF även med Session Management Function (SMF)-funktionen i nätets kärna som hanterar användarnas sessioner, som är i direktkontakt med SBA-service bussen, vars säkerhet är kritisk med tanke på hela nätets säkerhet. UPF växelverkar även med nätets övriga funktioner, och användarfallen för dessa kan variera beroende på session, skiva eller applikation. UPF behöver en anslutning till nätets gemensamma SMF, så att användarnas trafik kan överföras från en UPF till en annan, om användaren till exempel rör sig mellan flera olika funktioner med olika geografiska placeringar. Frågan är alltså om nätets egentliga kärna kan skyddas från nätets kärnfunktioner som verkställts lokalt.

Eftersom UPF:s betydelse som en del av nätet potentiellt är så stor, ska man i föreskriften ha en mycket hög tröskel för att anse att den är icke-kritisk, även om den verkställs på kantnätet. Faktorer som påverkar bedömningen är åtminstone det, att funktionen enbart betjänar vissa användare, och att man inte genom den kan erbjuda tillgång till allmänna kommunikationsnät såsom internet. Bedömningen påverkas också av hur de lokala funktionernas resursbegäran hanteras och hur de övervakas, samt huruvida man behandlar den lokala funktionen som icke-tillförlitlig för kärnnätets informationssäkerhet. Traficom har utvärderat följande alternativ.

A) UPF och övriga core-funktioner fastställs alltid som kritiska delar av nätet, alltså också när de används för tjänster på kantnätet.

Fördelen med denna fastställningsmetod är klarhet och att föreskriften tillämpas entydigt. Det finns dock orsak att fundera på om huruvida man genom att fastställa dessa funktioner som kritiska delar i kommunikationsnätet försvårar i någon grad ibruktagandet av dem och påverkar teleföretagens beslut om valet av utrustningsleverantör. Antalet leverantörer som till exempel erbjuder UPF-funktioner för kantnätet är dock stor, och begränsas inte till bara de mest kända utrustningstillverkarna.

Denna fastställningsmetod vore säkrare i förhållande till osäkerheten kring hur betydande styrningen som sker på kantnätet kommer att vara sist och slutligen i 5G-nätet, och vad kantberäkning i praktiken kommer att användas för. Det är möjligt att överföringen av nätets funktioner till kantnätet blir väldigt vanligt, eftersom snabb responstid och optimering av kapaciteten som finns tillgänglig är väsentligt, varför denna fastställningsmetod kommer att garantera att dessa funktioner inte utesluts ur tillämpningsområdet för 244 a § i LTEK.

B) Ett undantag definieras, enligt vilket tjänster som verkställs på kantnätet inte betraktas som kritiska delar av kommunikationsnätet på vissa förutsättningar

Detta alternativ förutsätter att man i föreskriften beskriver åtminstone i allmänna drag de kriterier enligt vilka funktionen kan betraktas som icke-kritisk. Utmaningen med detta alternativ är att man lyckas definiera kriterier som garanterar att funktionen inte trots allt måste fastställas som en kritisk del av kommunikationsnätet. Konkreta metoder för hur skyddsmekanismen genomförs kan inte fastställas på förhand, utan det skulle bli på teleföretagens ansvar. De skyddsmekanismer som kommer att behövas kommer också att bero på hur dessa funktioner kommer att använ-

das och hur tekniken utvecklas till exempel angående hur dessa funktioners gränssnitt gentemot resten av kärnnätets funktioner kommer att ordnas i framtiden.[16] Det är också inte känt om den nuvarande nivån på tekniken gör det möjligt att få till stånd skyddsmekanismer som kan garantera detta. Tröskeln för att räkna en skyddsmekanism som tillräcklig vore hög.

Fastställandet av undantaget blir problematiskt om, i och med att nätet utvecklas, stora delar av nätets funktioner på grund av undantaget i föreskriften på lång sikt inte trots allt skulle komma att betraktas som kritiska delar av kommunikationsnätet. Risken med att fastställa ett undantag är alltså att en stor del av de av 5G-nätets funktioner som stöder nya användningssyften eventuellt kunde komma att betraktas som icke-kritiska.

Riskerna med att fastställa dessa undantag minskas dock betydligt av att man regelbundet kommer att uppdatera föreskriften. I uppföljningen kommer man redan under de kommande åren att granska hur föreskriften tillämpas och vilken effekt teknikens utveckling och det praktiska ibruktagandet av kantberäkningen kommer att ha. Det innebär att man kan bedöma på nytt om det fortfarande är motiverat att ha undantaget, samt även i större utsträckning hur kritiska funktionerna kring kantberäkning eventuellt är.

## 5. Beredande av föreskriften

I föreskriftens tekniska definitioner bör man enligt regeringspropositionen (RP 98/2020 rd) beakta internationella standarder som används för att planera och bygga kommunikationsnät. I beredningen av föreskriften har man särskilt använt sig av ETSI:s standarder och 3GPP:s tekniska specifikationer, som har tagits i beaktande vid fastställandet av de kritiska delarna av 4G- och 5G-nät.

Föreskriften har förberetts i samarbete med branschen och olika myndigheter. I beredningen har deltagit parter som ansvarar för den nationella säkerheten och från försvarsmakten.

### 5.1. Hörande

Traficom skickade i september 2020 en inbjudan till alla teleföretag, de största tillverkarna av nätutrustning samt relevanta myndigheter att delta i beredningen av föreskriften. Från det tidigaste utkastskedet deltog i beredningen följande parter antingen genom att kommentera eller genom att följa med arbetet: DNA, Cinia, Digita, Elisa, Ericsson, FiCom ry, Finnet-förbundet rf, FNE-Finland, Huawei, Luoteis-Kuhmon kyläverkko-osuuskunta, Länsilinkki, NDC Networks, Nokia, Suomen Erillisverkot, Telia Finland och Ålands Telekommunikation samt Försörjningsberedskapscentralen, försvarsministeriet, försvarsmakten, inrikesministeriet, utrikesministeriet och finansministeriet. I september-november ordnades fem distansmöten för parterna som deltog i beredningen (beredningsgruppen), utöver vilket en stor del av deltagarna svarade på Traficoms skriftliga frågor som stödde beredningen mellan mötena. Deltagarna hade möjligheten att kommentera på Traficoms utkast av föreskriften och motiveringspromemorian.

[16] Det är till exempel möjligt att framtida versioner av de tekniska specifikationer av 5G-nätet möjliggör öppnandet av service bussen för användartrafik och därmed för UPF, istället för att den indirekt är i kontakt med kärnan genom Session Management Function (SMF)-funktionen som hanterar användarsessioner.

De som deltog i beredningsgruppen fick en ytterligare möjlighet att kommentera utkasten till föreskrift och motiveringspromemoria innan de blev färdiga att skickas på remiss för perioden 21.1–3.2.2021. Nedan beskrivs de centrala kommentarer och preciseringar som gjordes på grund av dem.

I en del kommentarer framfördes att till föreskriften fogas en skyldighet att överlåta dokumenten till myndigheten regelbundet eller på förhand när nya komponenter tas i drift. Traficom konstaterar att det saknar befogenhet att genom föreskrift uppställa nya skyldigheter för utlämnande av uppgifter eller rätt att få information, och därför ska man tillämpa existerande bestämmelser om saken, vilka för Traficom är bland annat 315 §, 320 §, 244 a § 5 mom. och 244 b § 3 mom. i LTEK. I kommentarerna föreslog man också att 4G- och 5G-basstationerna alltid ska vara kritiska, vilket inte genomfördes. Till den delen hänvisas till det som konstaterats ovan i **Error! Reference source not found.**, vilket preciserades på basis av respons.

Utifrån de kommentarer som kommit in preciserades ett exempel som beskriver för kommunikationsnätets och -tjänsters funktion nödvändiga infrastrukturtjänster som stöder funktionen (punkt **Error! Reference source not found.**, underpunkt **Error! Reference source not found.** i detaljmotiveringen i motiveringspromemorian). Det kan gälla till exempel ett koncentrerat system för tidsinformation som förmedlar och säkerställer basstationernas tids- och fassynkroniseringssignaler.

Vad gäller specificering av kritiska delar som hänför sig till sammankoppling önskade man få preciserad att den mottagande parten inte är ansvarig för kommunikationsnätets kritiska delar (för den andra partens del). Traficom konstaterar därför att förbudet enligt 244 a § 1 mom. i LTEK att använda nätverksutrustning i ett allmänt kommunikationsnäts kritiska delar gäller uttryckligen kommunikationsnätets (i.e. nätverksutrustningens) ägare eller annan innehavare, dvs. de instanser som skyldigheten att avlägsna nätverksutrustningen ur nätet kan riktas till på basis av 244 a § 3 mom. i LTEK.

I flera kommentarer föreslogs att punkt 1 underpunkt i) i förteckningen i punkten 4 i föreskriften inte skulle gälla kontrollenheter för 2G- och 3G-nätets basstationer, oberoende av deras viktighetsklass. Traficom ansåg att förslaget inte var motiverat ifall en kontrollenhet för basstation ändå, på basis av antalet användare eller verkningsområdets areal, skulle höra till viktighetsklass 1 eller 2. Traficom preciserade dock att kontrollenheterna för basstationen ska inte bli kommunikationsnätets kritiska delar endast därför att de i föreskrift 54 automatiskt anges höra minst till viktighetsklass 2. Konsekvensbedömningen kompletterades till den delen.

*[Kompletteras efter remissbehandlingen.]*

### 5.2. Remissrespons

*[Kompletteras efter remissbehandlingen.]*

## 6. En bedömning av föreskriftens inverkan

Föreskriften är ny. Ingen föreskrift har tidigare funnits om fastställandet av kommunikationsnätets kritiska delar. Föreskriften kommer att på förhand styra teleföretag och separata nätverksaktörer inom sitt tillämpningsområde i planeringen av nät, anskaffning av nätverksutrustning samt i byggande, upprätthållande och hantering av nät. Genom föreskriften främjas nationell säkerhet och dataskyddet i kommunikationsnäten. Föreskriften preciserar de delar av kommunikationsnätet på vilka förbudet mot användning av nätverksutrustning enligt 244 a § i lagen om tjänster inom

elektronisk kommunikation kan riktas. På så sätt förtydligar föreskriften de tillämpningsobjekt som nämns i paragrafen.

*Identifikations- och dokumentationsplikt*

*Företagspåverkan.* Identifikations- och dokumentationsplikten av kommunikationsnätets kritiska delar som förslagits i punkt 3 av föreskriften uppskattas orsaka teleföretagen och separata nätverksaktörer som plikten berör ekonomiska kostnader i någon grad då de fastställer och dokumenterar sina näts kritiska delar och de komponenter som används i dem. Plikten riktar sig i samma utsträckning till alla teleföretag och separata nätverksaktörer som omfattas av 244 a § i LTEK. Arbetsmängden som förutsätts av dokumenteringen är för ägare eller innehavare av små och tekniskt okomplicerade nät dock i praktiken mindre än för ägare och innehavare av stora och komplicerade nät. Identifikations- och dokumenteringsplikten kan också bedömas ha positiva företagspåverkan, eftersom plikten för sin del främjar iakttagandet av de nya reglerna i teleföretag och separata nätverksaktörer. Därmed skulle kraven i de nya reglerna troligen med större säkerhet att beaktas även när man planerar ändringar i kommunikationsnätet. Plikten kan dessutom antas i någon mån minska på – dock inte helt eliminera – risken att aktören skulle bli tvungen att avlägsna nätverksutrustning från kritiska delar av sitt nät enligt 244 a § i LTEK. I de åsikter som Traficom fick under beredningen understödde inte majoriteten att identifikations- och dokumenteringsplikten skulle begränsas för att minska på den administrativa bördan till bara en viss del av de allmänna kommunikationsnäten eller kritiska separata näten.

*Inverkan på myndighetsverksamhet.* Identifikations- och dokumenteringsplikten bedöms ha betydande positiva effekter på genomförandet av tillsynsuppgifterna som åläggs den regelövervakande myndigheten. En uppdaterad dokumentation fungerar som underlag för övervakningen av att reglerna följs samt för att påbörja eventuella fortsatta åtgärder.

*Övriga samhälleliga effekter.* Identifikations- och dokumenteringsplikten bedöms för sin del trygga de kritiska delarna som avses i 244 a § i LTEK samt därigenom genomförandet av avsikten med de nya reglerna och kommunikationsnätens säkerhet.

*Fastställandet av olika näts gemensamma kritiska delar samt fastställandet av 4G- och 5G-nätets kritiska delar*

- Virtualisering och nätets virtualiserade funktioner

*Företagspåverkan.* I föreskriften definieras virtualisering som en kritisk del av kommunikationsnätet när det används för genomförandet av en facilitet eller åtgärd som är en kritisk del av nätverket. Dessutom fastställs som kritisk del av kommunikationsnätet vad som helst för funktion eller åtgärd när den verkställs med hjälp av virtualisering som betraktas som kommunikationsnätets kritiska del. Föreskriften förbjuder i princip inte att man verkställer både kritiska och i regel icke-kritiska funktioner på samma virtualiseringsplattform, men risken för att nätverksutrustningen tas ur bruk enligt 244 a § i LTEK kan leda till att teleföretaget för säkerhets skull istället verkställer flera skilda virtualiseringsplattformer för att skilja på kritiska och icke-kritiska funktioner. Teleföretagen har dock ur en regelmässig synvinkel möjligheten att verkställa funktionerna även på samma plattform, om de trots det kan sörja för sina förpliktelser. Man har strävat efter att minimera omfattningen på kommunikationsnätens kritiska delar till det absolut nödvändiga, och föreskriften räknar inte vad som helst för virtualiseringsplattform som en kritisk del av nätet.

- Funktioner som stöder tjänster på kantnätet

*Företagspåverkan.* Föreskriften skulle beskriva de kriterier enligt vilka en funktion som fungerar på 4G- eller 5G-nätets kant och som producerar tjänster som stöder nätets styrning och som i princip hör till kommunikationsnätets kärnfunktioner trots det undantagsvis kan betraktas som annat än en kritisk del av kommunikationsnätet. Undantaget skulle göra det möjligt att föreskriften inte i onödan skulle tillämpas på funktioner för vilkas del man kan garantera att funktionen inte kan anses kontrollera eller styra tillgången till nätet eller trafiken på det. I detta fall skulle 244 a § i LTEK inte begränsa teleföretagens verksamhet. Å andra sidan skulle teleföretagen förorsakas kostnader av att påvisa rätten till undantaget och av att ta i bruk de skyddsmekanismer som undantaget förutsätter. Dessa åtgärder uppskattas dock vara nödvändiga för att det ska vara möjligt att betrakta dessa funktioner som något annat än kommunikationsnätets kritiska delar.

*Inverkan på myndighetsverksamhet.* För att teleföretaget eller den separata nätverksaktören ska kunna be om ett undantag, måste Traficom kunna bedöma tillräckligheten hos skyddsmekanismerna som krävs för tillämpandet av 244 a § i LTEK, vilket kan behöva betydlig expertkunskap. Att reda ut dessa frågor kan dock vara nödvändigt i vilket fall som helst som en del av bedömning av om huruvida de s.k. förutsättningarna för fara uppfylls på grund av de åtgärder som teleföretagen eller separata nätverksaktörerna genomför. Därför uppskattar man inte att undantagets existens skulle öka på Traficoms arbetsbörda i betydande grad.

- Delar av radioaccessnätet och basstationernas styrsystem

*Företagspåverkan.* Traficom anser att det är för tidigt att i denna föreskrift ange huruvida basstationer är kommunikationsnätets kritiska delar eller inte. Teleföretaget och separata nätverksaktörer bör själv bedöma hur kritiska de är i förhållande till teknikivån och bland annat i förhållande till de funktioner och åtgärder som basstationerna genomför. Detta medför i viss mål osäkerhet för aktörerna, men Traficom anser att det inte går att undvika detta i den här situationen. Föreskriften tar dock ställning till bedömningen av kritiskheten som en del av nätet hos vissa basstationer oberoende av om basstationerna i sig är kommunikationsnätets kritiska delar. Hanteringssystem och kontrollenheter för basstationer är sådana.

Basstationernas styrsystem och andra styr- och övervakningsanordningar för icke-kritiska delar av kommunikationsnätet anses enligt denna föreskrift som kritiska delar av kommunikationsnätet även i sådana fall där de väsentligen påverkar tillgången till nätet och trafiken på nätet även när de väsentligt kan påverka tillgång till nätet eller trafiken på nätet även om det element som administreras inte i sig är en kritisk del av kommunikationsnätet. Att utföra bedömningen av en dels kritiskhet orsakar i viss grad en administrativ börda på teleföretag och separata nätverksaktörer, men som motvikt betyder det att basstationernas styrsystem från fall till fall kan betraktas som icke-kritiska.

Eftersom basstationernas utrustningsleverantörer också är typiskt leverantörer av deras styrsystem, är det knappast i detta skede ekonomiskt eller tekniskt motiverat att anskaffa ett styrsystem för basstationerna från en annan leverantör eller själv utveckla ett. Av den här orsaken kan man anta att basstationernas styrsystems eventuella kritiskhet som del av nätet också indirekt kan påverkas av teleföretagets eller den separata nätverksaktörens val av leverantören av basstationerna i deras nät. Administrationssystemen kan dock möjliggöra administrationen av en annan tillverkares basstationer men då kan det finnas restriktioner i funktioner.

Även om basstationernas styrsystem skulle anses vara en kritisk del av kommunikationsnätet skulle teleföretaget trots det välja nätverksutrustning där det ingår en större risk av att användningsförbudet i 244 a § i LTEK skulle tillämpas på användningen av dessa nätverksutrustningen. I detta fall kan operatören försöka visa att även om man i nätet använder ett sådant styrsystem för basstationer som betraktas som kritiska delar av kommunikationsnätet, äventyrar det trots det inte den nationella säkerheten eller försvaret. Det här kan man försöka visa till exempel genom att genomföra ytterligare kontroller för att trygga informationssäkerheten (se punkt 4.3); detta kan leda till att styrmiljön har segment med olika säkerhetsnivåer, där det är av central betydelse att de är separerade och att deras säkerhet tryggas. Eftersom 244 a § i LTEK grundar sig på tillsyn i efterhand, har operatörerna inte möjligheten att på förhand helt avlägsna risken för att man i framtiden skulle tvingas avlägsna basstationerna styrsystem. Dessutom bör man observera att basstationernas styrsystem inte nödvändigtvis, beroende på situationens unika särdrag, kan definieras enligt föreskriften som en kritisk del i kommunikationsnätet i sådana fall där de basstationer som styrsystemen styr inte betraktas som kommunikationsnätets kritiska delar.

Men å andra sidan, även när nätets basstationer inte betraktas som kommunikationsnätets kritiska delar, kan teleföretagen efter att de bedömt riskerna komma fram till att det inte är förnuftigt att skaffa basstationer utan styrsystem från samma utrustningsleverantör, även om själva basstationerna inte betraktas som kritiska delar i kommunikationsnätet, ifall deras styrsystem skulle komma att betraktas som en kritisk del av kommunikationsnätet. Detta är möjligt om det inte finns ett styrsystem för basstationselement som är oberoende av leverantör på marknaden och vars anskaffning är ekonomiskt och funktionellt förnuftigt, eller om en sådan inte kan utvecklas, och om teleföretaget uppskattar att risken för att styrsystemet skulle tvingas avlägsnas utan full ersättning under basstationens livscykel är för hög. Detta kan leda till att operatörernas möjliga utbud av basstationsleverantörer i praktiken blir mindre, om man antar att leverantören av basstationernas styrsystem är samma som basstationernas. Det här kunde påverka operatörernas förhandlingsställning och konkurrensen mellan utrustningsleverantörer. Denna effekt kan dock uppskattas vara begränsad med tanke på att hur man kommer att bedöma själva basstationernas kritiskhet i sig själv och för övrigt är en risk för operatören, eftersom man inte i denna föreskrift fastställer huruvida basstationer är kritiska delar av kommunikationsnäten.

I 2G- och 3G-näten används särskilda kontrollenheter för basstationer och radionät som enligt denna föreskrift skulle vara kommunikationsnätets kritiska delar åtminstone när de på basis av användartalet eller verkningsområdet hör till viktighetsklass 1 eller 2. Enligt de kommentarer som Traficom fått är basstationerna i praktiken beroende av samma tillverkare av kontrollenheter för basstationer, även om de, enligt Traficoms uppgifter, har samband med ett gränssnitt som kan möjliggöra användning av olika tillverkares utrustning. Att kontrollenheter för basstationer anses vara kommunikationsnätets kritiska delar kan bedömas ha likadana konsekvenser som när basstationernas administrationssystem är kommunikationsnätets kritiska del, och det inte är ekonomiskt eller funktionellt sett möjligt att använda basstationer utan samma tillverkares kontrollenheter för basstationer. Olika nättekniker kan vara integrerade i en och samma basstationsenhet, vilket innebär att den integrerade basstationens 2G- och 3G-funktionalitet inte kunde användas i detta fall även om 4G- och 5G-funktionaliteten bevaras. Man håller emellertid att avstå från 3G-tekniken.

På lång sikt kan bedömningen av att basstationernas styrsystem eller basstationerna är kommunikationsnätets kritiska delar påverka arkitekturval för radionätet och till

exempel leda till att man tar i bruk OpenRAN-lösningen, vilket skulle leda till att kopplingen mellan styrsystemet och basstationerna samt deras leverantörer minskar betydligt. I detta fall kan radionätets arkitektur förändras mot ett mer utrustningsleverantörsneutralt håll, och det kan vara praktiskt lättare att byta ut styrsystemet. De tekniska lösningarna är dock veterligen fortfarande i utvecklings- och experimentskedet när denna föreskrift meddelas.

# Detaljmotivering

## 1. Tillämpningsområde

Enligt punkt 1 i föreskriften tillämpas föreskriften på allmän televerksamhet och på sådant till ett allmänt kommunikationsnät anslutet separat nät som hör till aktörer som är viktiga med tanke på samhällets vitala funktioner enligt 244 a § 2 mom. i lagen om tjänster inom elektronisk kommunikation (917/2014, LTEK).

Föreskriftens tillämpningsområde omfattar alla aktörer som 244 a § i LTEK tillämpas på, det vill säga både teleföretag och separata nätverksaktörer.

Föreskriften är inte uttömmande. Utöver de delar som i föreskriften fastställts som kritiska delar av kommunikationsnät tillämpas 244 a § i LTEK, vilket innebär att kommunikationsnätets kritiska delar också direkt kan fastställas utgående från definitionen i 1 mom. i paragrafen på kommunikationsnätets kritiska delar.

## 2. Definitioner

I denna punkt definieras de centrala begreppen som används i föreskriften.

**Kommunikationsnätets kritiska del**

Definitionen på kommunikationsnätets kritiska del motsvarar definitionen i 1 mom. i 244 a § i LTEK. Som ett kommunikationsnäts kritiska delar betraktas enligt den dess centrala faciliteter och åtgärder med hjälp av vilka tillgången till nätet och trafiken på det kontrolleras eller styrs på ett väsentligt sätt. Ur denna definition kan härledas att utgångspunkten är att varje kommunikationsnät har delar som är kritiska för nätets funktion.

Det bör anmärkas att man skilt från bedömningen av hur kritisk en del är i ett kommunikationsnätverk måste fråga sig om huruvida användningen av någon viss nätverksutrustning i en kritisk del av nätet uppfyller den s.k. förutsättningen för fara i 244 a § 1 mom. av LTEK. För att den ska uppfyllas förutsätts det att, ”det finns vägande skäl att misstänka att användningen av utrustningen äventyrar den nationella säkerheten eller försvaret på så sätt att det möjliggör utländsk underrättelseverksamhet eller sådan verksamhet som stör, lamslår eller på något annat skadligt sätt påverkar Finlands viktiga intressen, grundläggande samhällsfunktioner eller den demokratiska samhällsordningen”. Denna föreskrift hanterar inte överhuvudtaget bedömningen av förutsättningen för fara eftersom Traficoms rätt att meddela föreskrifter enligt 6 mom. enbart gäller det tekniska fastställandet av de kritiska delarna av kommunikationsnäten.

I regeringspropositionen preciseras begreppet kommunikationsnätets kritiska delar på följande vis (s. 265):

> *Som ett kommunikationsnäts kritiska delar betraktas nätets kärna, i synnerhet sådana faciliteter och åtgärder med hjälp av vilka nätet och trafiken på det styrs och administreras på ett centralt sätt. I den nuvarande nättekniken är den kritiska kärnan till exempel den del av stamnätet där olika användares tillträde till nätet administreras och status för användarnas anslutningar upprätthålls. Kommunikationsnätets kritiska delar säkerställer tillgången till tjänster och kommunikationens konfidentialitet. Till kommunikationsnätets kritiska delar hör också de delar av nätet som säkerställer informationssäkerheten i hela kommunikationsnätet. När det gäller de nuvarande näten har dessa arrangemang och åtgärder genomförts i stamnätet.*

*Också i fråga om 5G-nät är det möjligt att särskilja de kritiska delarna av nätet, även om 5G-nätets struktur är mer komplicerad än tidigare nätgenerationers. I framtida nät, såsom 5G-nät och 6G-nät, bör de kritiska delarna definieras i enlighet med den aktuella tekniska utvecklingen. Det väsentliga vid definitionen av ett kommunikationsnäts kritiska delar är också att bedöma vem som har faktiska möjligheter att påverka funktionen och egenskaperna hos en del av kommunikationsnätet eller den nätverksutrustning som finns i där.*

I Kommunikationsutskottets betänkanden (KoUB 16/2020 rd, s. 16) har definitionen på kommunikationsnätets kritiska delar definierats noggrannare enligt det som förutsatts i grundlagsutskottets utlåtande (GrUU 35/2020 rd). Enligt betänkandet ”som en kritisk del av kommunikationsnätet betraktas endast de centrala funktioner och åtgärder genom vilka tillgången till nätet och trafiken på nätet kontrolleras eller styrs på ett väsentligt sätt. Enligt uppgift har preciseringen gjorts efter diskussion mellan olika ministerier. Utskottet har dock fogat ordet ”centrala” till ändringen på grund av grundlagsutskottets utlåtande. De kritiska delarna av kommunikationsnätet har en central betydelse med tanke på nätets funktion, upprätthållandet av nätet samt kommunikationens konfidentialitet och nätets informationssäkerhet.”

När man bedömer betydelsen av åsikterna som framförts om de funktioner som enligt regeringspropositionen ska betraktas som kritiska delar av kommunikationsnät ska man alltså uppmärksamma att i enlighet med utskottsbetänkandena har definitionen på kritiska delar gjorts noggrannare, och gäller nu istället kontroll och styrning av *tillgången till nätet* istället för hur nätet kontrolleras och styrs. Begreppet tillgång till nätet har dock inte avgränsats enbart till att gälla tillgången till nätet för de användare som nämns i regeringspropositionen, utan kommunikationsnätets kritiska delar kan också vara sådana som kontrollerar eller styr annan tillgång till nätets funktioner och utrustning, till exempel på basen av administrativa anslutningar som sammankopplar nät eller används för att underhålla dem. Dessutom kan begreppet kontroll eller styrning av tillgången till nätet till exempel innehålla kommunikationens konfidentialitet och funktioner som har att göra med tryggandet av tillgången till tjänster på nätet, med den förutsättningen att de också har att göra med kontroll eller styrning av tillgången till nätet. Utgående från betänkandet från Kommunikationsutskottet kan man förmoda att en funktion blir mer central och mer väsentlig, om den påverkar nätets funktion, upprätthållandet av nätet, nätets konfidentialitet eller nätets informationssäkerhet. Därtill bör man märka att funktionerna som har att göra med kontroll eller styrning av trafiken på nätet har fastställts som kritiska delar av kommunikationsnätet i enlighet med regeringspropositionen, förutom att begreppet ’administreras’ har ersatts med begreppet ’kontrolleras’.

**Kritiskt separat nät och separat nätverksaktör**

Det som i den nya 244 a § 2 mom. definieras som ett sådant till ett allmänt kommunikationsnät anslutet separat nät som hör till ett kärnkraftverk, en hamn, en flygplats eller någon motsvarande aktör som är viktiga med tanke på samhällets vitala funktioner. Dessa nät hänvisas i föreskriften till med begreppet ”kritiskt separat nät” och den som äger eller innehar ett dylikt nät med begreppet ”separat nätverksaktör”.[17] Om till exempel en mikrooperatör tillhandahåller ett kritiskt separat nät som tjänst för en aktör som med tanke på samhällets vitala funktioner är central, anses

[17] Enligt beredningsarbetet (RP 98/2020 rd, s. 266) har samhällets kritiska tjänster identifierats bland annat i statsrådets beslut om målen med försörjningsberedskapen (SRb 1048/2018) som utfärdats med stöd av 2 § i lagen om tryggande av försörjningsberedskap (1390/1992) samt som en del av det nationella genomförandet av direktivet om nät- och informationssäkerhet (RP 192/2017 rd).

mikrooperatören till den delen också vara en aktör som är viktig med tanke på samhällets vitala funktioner. Föreskriftens skyldigheter gäller då ägaren av det kritiska separata nätet eller en annan innehavare.

Föreskriften och 244 a § i LTEK tillämpas enbart på separata nät *anslutna till allmänna kommunikationsnät.* Till tillämpningsområdet hör alltså bara icke-ordinarie separata nät, skilt från sådana ordinarie separata nätverk som inte alls har sammankopplats till det allmänna kommunikationsnätet och därmed inte hör till tillämpningsområdet för 244 a § i LTEK.[18] 244 a § i LTEK tillämpas inte på sådana kommunikationsnät som inte är allmänna kommunikationsnät och inte heller kritiska separata nät, t.ex. på vanliga inomhusnät i fastigheter eller företag. Däremot i sådana fall där kommunikationsnätet används för att erbjuda kommunikationstjänster åt en användarkrets som inte har avgränsats på förhand, det vill säga när man idkar allmän televerksamhet, tillämpas 1 mom. i 244 a § i LTEK och punkterna i föreskriften som gäller teleföretag[19].

Med sammankoppling avses till exempel att ett separat nätverk som verkställs med mobilnätsteknik har en anslutning till internet genom en fast nätuppkoppling eller erbjuder möjligheten att ringa samtal utanför det separata nätet. Tillämpningsförutsättningen för 244 a § 2 mom. i LTEK är alltså inte till exempel att man kopplar samman mobilnät eller erbjuder roaming.

Ett kritiskt separat nät kan vara ett kommunikationsnät som verkställts med vad som helst för teknologi och som inte är ett allmänt kommunikationsnät. Enligt motiveringarna till 244 a § i LTEK är det väsentligt med tanke på tillämpningen enligt 2 mom. att kommunikationsnätet i fråga är verksamt i en ur samhällets synvinkel sett såpass kritisk miljö att äventyrandet av nätets kärnfunktion kunde leda till att den nationella säkerheten eller försvaret äventyras (RP 98/2020 rd, s. 266).

**Kommunikationsnätets eller -tjänstens komponent**

Med kommunikationsnätets eller -tjänstens komponent avses i denna föreskrift ett nätelement, instrument eller datasystem som kommunikationsnätet eller -tjänsten består av eller som det utnyttjar. Begreppet används i flera av Traficoms föreskrifter. Kommunikationsnätets eller -tjänstens komponenter är till exempel mobiltelefonväxel, basstationsstyrenhet, basstation, meddelandecentral, nätverksnav för bredband, namnserver, server som ansvarar för nätets åtkomsthantering, switch, router, SIP-applikationsserver, komponent i intelligentnät, DVB-T-nätets huvud- och slavsändare eller DVB-T2-nätets sändare. Med kommunikationsnätets eller -tjänstens komponent avses *inte* kanaler eller apparatens eller nätelementets delar, såsom till exempel mobiltelefonväxelns processorenheter. Ifall någon funktion (till exempel namnserverprogramvaran) har distribuerats över flera olika apparater, anses varje apparat vara en egen komponent.

[18] Begreppet separat nät används på ett annorlunda sätt i den nya 244 a § än i den upphävda kommunikationsmarknadslagen (393/2003). I kommunikationsmarknadslagen avses med separata nät kommunikationsnät som inte har kopplats samman med allmänt kommunikationsnät (130 §).
[19] Enligt föreskriftens motiveringar tillämpas 1 mom. i 244 a § i LTEK, vilken gäller allmänna kommunikationsnät, även på tillhandahållande av myndighetsnät och nät- och kommunikationstjänster med anknytning till den myndighetskommunikation som avses i LTEK i de fall där teleföretagens allmänna kommunikationsnät används för att erbjuda dem (RP 98/2020 rd, s. 265).

**4G-nät**

I denna föreskrift avses med 4G-nät ett mobilnät (dess kärna eller radioaccessnät) som använder LTE-teknik och som baserar sig enligt 3GPP:s tekniska specifikationer på EPS-arkitekturen (Evolved Packet System). EPS består av en kärna som optimerats för paketförmedlad trafik (Evolved Packet Core, EPC) och ett radioaccessnät (Evolved UTRAN dvs. E-UTRAN)[20].

**5G-nät**

Med 5G-nät avses i denna föreskrift ett mobilnät som verkställts med femte generationens teknik, som enligt 3GPP:s tekniska specifikationer baserar sig på ett femte generationens kärnnät (5GC Fifth Generation Core Network, TS 21.905) eller ett femte generationens radioaccessnät (New Radio, NR, Fifth Generation radio access technology).

Begreppet 5G-nät omfattar även med tanke på föreskriftens tillämpning komponenter från 5G Non-Standalone dvs. 5G NSA-nätets 5G-generation, som alltså i föreskriften räknas bland de kritiska komponenterna för 5G-nätet. Till exempel ifall en komponent som används i någon viss del av 5G-nätet i föreskriften har fastställts som kritisk, tillämpas denna definition även i situationer där komponenten används som del av ett 5G NSA-nät. 5G NSA-nätet uppdateras under sin livscykel till ett 5G Standalone-, dvs. 5G SA-nät, i vilket skede det går att tillämpa samma definitioner på kritiska delar för det som för 5G-nät.5G NSA-nät behöver inte skilt definieras i föreskriften, eftersom de använder sig av 4G- och 5G-nätens funktioner. Inga nya komponenter eller av 3GPP fastställda funktioner kommer att läggas till 4G-nätets kärna, dvs. till EPC-nätet på grund av 5G NSA, utan de utvecklade funktionaliteterna genomförs genom redan existerande komponenter.

**Övriga definierade begrepp**

I övrigt tillämpas begreppen enligt 3 § i LTEK. I paragrafen har definierats bland annat teleföretag, kommunikationstjänst, kommunikationsnät, nätverksutrustning och allmänt kommunikationsnät.

## 3. Fastställande av kritiska delar och dokumentering

### 3.1. Identifikation av kommunikationsnätets kritiska delar och dokumentering

I punktens första underpunkt förpliktas teleföretag och separata nätverksaktörer att identifiera de kritiska delarna i sina kommunikationsnät och de komponenter som används i kommunikationsnätet och -tjänsten. De måste alltså för sitt eget näts del fastställa vilka delar av nätet och vilka av de komponenter som används i det enligt lagen och föreskriften kan fastställas som kritiska delar av nätet. Dessutom måste teleföretag och separata nätverksaktörer göra upp och upprätthålla uppdaterad dokumentation om de kritiska delar de identifierat i sina kommunikationsnätverk och de komponenter de använder i sina kommunikationsnätverk och -tjänster. Komponentens tillverkare och modellnummer eller en annan identifieringsuppgift ska framgå av dokumentationen. För virtualisering till exempel bör man åtminstone do-

[20] TS 21.905 Vocabulary for 3GPP Specifications: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=558.

kumentera komponenter som används för att genomföra den virtuella fysiska plattformen, virtuella infrastrukturen, nätets virtuella funktioner och virtualiseringshantering (jfr punkt 11 i förteckningen i punkt 4 i föreskriften).

Föreskriften förutsätter att teleföretaget och de separata nätverksaktörerna för det första identifierar den konkreta nätverksutrustningen som de använder i sina kommunikationsnäts kritiska delar. För det andra ska de kritiska delarna identifieras även i relation till nätverksarkitekturen så att företaget identifierar och fastställer vissa delar av sina nät som kritiska redan när nätverksarkitekturen planeras, i vilket skede regleringen skulle uppmana företaget att beakta kraven i 244 a § i LTEK redan när företaget planerar anskaffningen av nätverksenheter. Bedömningen ska hållas aktuell i samband med ändringar eller planerade ändringar i nätverksarkitekturen, säkerhetsarkitekturen eller utrustningen.

Identifieringen av de kritiska delarna i nätet förpliktar inte teleföretagen eller separata nätverksaktörer att bedöma deras betydelse för den nationella säkerheten. Utöver föreskriften ska aktören tillämpa definitionen direkt ur 1 mom. i 244 a § i LTEK, enligt vilken ”som en kritisk del av kommunikationsnätet betraktas endast de centrala funktioner och åtgärder genom vilka tillgången till nätet och trafiken på nätet kontrolleras eller styrs på ett väsentligt sätt.

Genom förpliktelsen strävar man efter att främja verkställandet av 244 a § i LTEK samt garantera att den och föreskriften tillämpas jämlikt. Utan dokumenteringsplikten i fråga kunde Traficom inte lika effektivt övervaka hur teleföretagen och de separata nätverksaktörerna tillämpar de nya reglerna. Traficom kan som del av sin tillsynsverksamhet be om den dokumentation som punkten förutsätter, på basen av myndigheternas allmänna rätt att få information enligt 315 § i LTEK.

Teleföretaget och separata nätaktörer ska själv bedöma hur kritiska deras kommunikationsnäts delar är med stöd av skyldigheten att identifiera och dokumentera nät enligt punkt 3 i föreskriften. I sista hand är det Traficom som i samband med ett enskilt tillsynsärende avgör, oberoende av teleföretagets eller separata nätaktörers självbedömning, huruvida en viss del av nätet ska anses vara kritisk.

### 3.2. Bedömningen av kritiskheten hos tjänster på kantnätet

I punktens andra underpunkt föreskrivs att teleföretag och separata nätverksaktörer ska dokumentera motiveringarna till sina bedömningar, om de, utgående från punkt 7 i föreskriften, bedömer att de funktioner eller åtgärder för ett 4G- eller 5G-nätverk som avses i tabell 1 och 2 (i punkt 5 och 6 i föreskriften) inte räknas som kritiska delar av deras kommunikationsnät. I punkt 7 i föreskriften möjliggör man att en funktion som i övriga fall skulle betraktas som en kritisk del av kommunikationsnätet under vissa förutsättningar kan betraktas som icke-kritisk, om man genom den stöder tjänster på kantnätet och om den effektivt har separerats från kommunikationsnätets kritiska delar.

I dokumentationen ska man beskriva de grunder som operatören har baserat sin utvärdering på, till exempel informationssäkerhetskontroller. Dokumenteringsplikten riktar sig enbart till de delar som antas vara kommunikationsnätets kritiska delar och som fastställts specifikt i tabell 1 eller 2.

### 3.3. Bedömning av kritiskheten hos de separata nätverkets basstationer

I punktens tredje underpunkt fastställs en särskild plikt för separata nätverksaktörer att göra upp och upprätthålla en bedömning av huruvida det separata nätverkets basstationer ska betraktas som kommunikationsnätets kritiska delar. I utvärderingen

ska aktören ta i beaktande åtminstone det separata nätverkets geografiska omfattning, en enskild basstations andel av den totala nätverkstrafiken samt de funktioner och åtgärder som basstationen tillhandahåller i det separata nätverket. Utöver de skilt nämnda kriterierna ska man bedöma eventuella andra frågor som kan vara relevanta i frågan om basstationen kontrollerar eller styr tillgången till nätet eller trafiken på nätet på ett väsentligt sätt. Plikten att upprätthålla bedömningen innebär att man ska uppdatera den regelbundet och vid behov ändra på den om betydande ändringar sker i nätet eller i hur det används.

Traficom anser det motiverat att för de separata nätverkens del ge dem en större förpliktelse gällande basstationerna, eftersom dess basstationer kan tjänstgöra ett litet område och tjänsten kan vara av stor betydelse för användarna, och basstationens funktioner oftare hittas på samma plattform som nätets kärnfunktioner. Traficom ansåg det dock inte som nödvändigt att alltid fastställa alla de separata nätverkens basstationer som kritiska delar av kommunikationsnätet, eller försöka fastställa bindande kriterier för denna bedömning.

I underpunkten ges dessutom en särskild förpliktelse åt separata nätverksaktörer att dokumentera hur de kommit fram till sin bedömning. Förpliktelsen tillämpas också i sådana fall där aktören bestämmer sig för att en basstation inte ska betraktas som en kritisk del av det separata nätverket.

Skyldigheten för separata nätverksaktörer att identifiera och dokumentera nät gäller inte basstationer eller andra delar av kommunikationsnätet eller kommunikationsnätets eller -tjänstens komponenter som används i dem till den delen de används för *allmän televerksamhet*. På det allmänna kommunikationsnätets delar tillämpas skyldigheter som ålagts teleföretag i föreskriften.

## 4. Kommunikationsnäts kritiska delar

### 4.1. Fastställandet av kritiska delar

I punkten fastställs de av nätets funktioner som åtminstone ska betraktas som kommunikationsnätets kritiska delar. Förteckningen är inte uttömmande, och utöver den måste teleföretagen eller de enskilda nätverksaktörerna bedöma om det i deras egna nät finns kritiska delar som inte är en del av förteckningen i punkten. Föreskriften begränsar alltså inte den direkta tillämpningen av definitionen på kommunikationsnätets kritiska delar enligt 244 a § 1 mom.. Förteckningen i denna punkt och föreskriftens nätverkstekniskt specifika punkter kompletterar varandra.

Förteckningen är teknologineutral. Punkten gäller i princip alla kommunikationsnät, som till exempel kretskopplade och paketförmedlande mobilnät samt fasta bredbandsnät. Förteckningen har i första hand gjorts upp för målkommunikationsnäten, men den kan till de delar som är tillämpbara också användas i fastställningen av masskommunikationsnätens kritiska delar. Enligt punkten är nätets del kritisk även om den enbart verkställer en del av den funktionalitet som fastställts som kritisk. Detta och sättet att fastställa dem utgående från funktion skulle dock innebära att när man kan påvisa att en enskild komponent genomför ens en del av en sådan funktion som fastställts som en kritisk del av nätet, så skulle komponenten betraktas som en kritisk del av nätet, även om komponenten inte i sig själv utför hela funktionen. En enskild programvarukomponent eller nätverksutrustning kan också verkställa mer än en funktion.

När förteckningen har gjorts upp har man använt som jämförelseobjekt andra motsvarande förteckningar som gjorts upp i Tyskland och Storbritannien (se närmare kapitel 4.3 i detaljmotiveringarna).[21] Därtill ingår utöver de av kärnnätets funktioner (Core network functions) som i EU:s gemensamma verktygslåda beskrivits som kritiska, också hantering av virtualiseringen av nätets funktioner (NFV management) och orkestrering av nätverk (Management and Network Orchestration, MANO), som också ingår i föreskriftens förteckning. Med vissa specifikationer ingår det i förteckningen också som delar utöver MANO de fakturerings-, styr- och stödsystem som i verktygslådan getts kritiskheten moderate/high (måttlig/hög), transport- och transmissionsfunktioner och anslutningspunkter mellan näten.

4.2. Kommunikationsnäts kritiska funktioner

1) Routning och övrig kontroll eller styrning av slutanvändarnas trafik

Enligt denna underpunkt är de centrala funktionerna som har att göra med routning och övrig kontroll eller styrning av slutanvändarnas trafik i kommunikationsnätet, som väsentligt kan påverka den trafik som går genom kommunikationsnätet, kommunikationsnätets kritiska delar. I underpunkten preciseras därtill att kommunikationsnätets kritiska delar utgående från detta åtminstone är:

- komponenter i allmänna kommunikationsnät eller -tjänster när de hör till viktighetsklass 1 eller 2 enligt föreskriften om säkerställande av kommunikationsnät och kommunikationstjänster samt om synkronisering av kommunikationsnät, dvs. föreskrift 54 enligt deras användarantal eller verkningsområde,

- komponenter i kommunikationsnät eller -tjänster när de i övrigt kontrollerar en väsentlig del av hela nätets trafik, samt

- komponenter i ett kommunikationsnät eller -tjänst i en datacentral; när de är nödvändiga för funktionen av kommunikationsnätets kritiska del;

Denna underpunkt omfattar alltså de centrala funktioner genom vilka man sörjer för routningen eller övrig styrning av slutanvändarnas trafik i nätet till terminaler och mellan nät. Underpunkten innehåller på motsvarande vis också funktioner som har att göra med M2M-trafiken. Underpunkten innehåller också system som kan analysera användartrafiken, som används för att hitta skadlig trafik och som delvis också kan höra till den nedanstående punkten om informationssäkerhetsfunktioner. Vanligtvis verkställs dessa funktioner i mobilnätets kärna eller i stamnätet.

Denna underpunkt täcker i mobilnät särskilt funktioner som har att göra med routning av användartrafiken (user plane) eller som används för att kontrollera trafiken på nätet genom styrningstrafik (control plane). Underpunkten täcker också delvis hantering av rörlighet i mobilnät (mobility management). I mobilnät räknas också meddelandecentralen (SMSC) och nätslussarna som är kopplade till den som delar som styr användartrafiken på det sätt som avses i denna underpunkt.

Till underpunkten hör också funktioner som har att göra med nätverksskivning (network slicing) till de delar som de verkställer funktionerna enligt punkten. Med nätverksskivning avses indelning och separering av trafik inom mobilnäten för att

[21] Cybersecurity of 5G networks EU Toolbox of risk mitigating measures. CG Publication 01/2020. Bilaga 2, s. 39. https://ec.europa.eu/digital-single-market/en/nis-cooperation-group. Se också EU coordinated risk assessment of the cybersecurity of 5G networks. Report. 9 October 2019, k. 2.21. https://ec.europa.eu/digital-single-market/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security.

kunna garantera vissa önskade kvalitetsparametrar. En nätverksskiva formar en logisk helhet (ett logiskt nät) inom en fysisk nätverksinfrastruktur. En nätverksskiva kan ha gemensamma och särskilda dedikerade resurser. I mobilnätet stöder fjärde och femte generationens teknologi nätverksskivning i olika grad, och i 5G-nät deltar flera olika av nätets funktioner i skivningen.

Genom dessa funktioner kontrolleras och styrs trafiken på nätet, varför de ska betraktas som kommunikationsnätets kritiska delar. Funktionerna har också en väsentlig betydelse i tillgången till tjänsterna, kommunikationens konfidentialitet och i att trygga informationssäkerheten i hela kommunikationsnätet.

Stamnätet är centralt särskilt med tanke på styrningen av nätets trafik och tjänsternas tillgänglighet, eftersom trafiken från nätet förmedlas genom det (genom routning). Stamnätet är av samma orsak central också med tanke på kommunikationens konfidentialitet. Också region- och överföringsnätens komponenter är på motsvarande sätt centrala då de är tillräckligt betydelsefulla.

I underpunkten preciseras dessutom att de kritiska delarna i ett kommunikationsnät är kommunikationsnätets eller -tjänstens komponenter som hör till viktighetsklass 1 eller 2 enligt användarantalet eller verkningsområde, inklusive sådana gränsrouters som uppfyller detta kriterium, oberoende av om de enligt operatörens arkitektur är en del av stam-, region- eller överföringsnätet. Viktighetsklasserna föreskrivs för ögonblicket i Kommunikationsverkets föreskrift 54 B/2014 M om säkerställande av kommunikationsnät och kommunikationstjänster samt om synkronisering av kommunikationsnät. Föreskriftens förpliktande om viktighetsklassificering tillämpas inte på separata nätverk. Nätverksutrustning som hör till dessa viktighetsklasser betraktas alltid som kommunikationsnätets kritiska delar, eftersom de påverkar en såpass betydande mängd användare att man alltid måste anse att de väsentligen kontrollerar eller styr trafiken på nätet.

Enligt föreskrift 54 är viktighetsklassen för mobilnätets kontrollenhet för basstation alltid minst 2, men med tanke på denna föreskrift skulle de anses vara kommunikationsnätets kritiska delar bara om de på basis av föreskrift 54 skulle höra till viktighetsklass 1 eller 2 även på basis av deras användarantal eller verkningsområde. Det betyder att bedömningen av deras kritiskhet skulle basera sig på samma kriterier som kommunikationsnätets övriga delar.

Kommunikationsnätets kritiska delar är dessutom i enlighet med preciseringen också komponenter som styr en väsentlig del av hela kommunikationsnätets trafik. Det tillämpas också på separata nät. Dylika är till exempel komponenter som sammanför stamnätet. I stamnätet kan man förmedla både trafik från mobilnätet och det fasta nätet. I stamnätet förmedlas all eller majoriteten av trafiken mellan basstationer och mobilnätets kärna eller kärnans interna trafik eller det fasta nätets trafik. Med stamnätet sammankopplas de regionala näten med varandra. Ett exempel på nätverksdelar som omfattas av denna underpunkt är IP/MPLS-nätet som sammankopplar operatörens regionnät. Tillämpningen av underpunkten är dock inte begränsad till stamnätet eller kärnnätet, eftersom dessa inte kan definieras entydigt.

Baserat på den andra preciseringen hör till denna underpunkt också datacentraler till exempel när man genom den sammankopplar kommunikationsnätets kritiska delar som verkställts i datacentralen, såsom mobilnätets kärnas centrala funktioner, med stamnätet.

2) Åtkomsthantering, verifiering och auktorisering av slutanvändare, allokering av nätverksresurser till slutanvändare samt administrering av slutanvändarnas anslutningar och sessioner

Denna underpunkt omfattar funktioner genom vilka man styr slutanvändarnas och därmed deras terminalers tillgång till nätet, upprätthåller användarnas sessioner och anslutningars läge, samt autentiserar och auktoriserar slutanvändarna (terminalerna) och ser till att nätets resurser allokeras till dem. Auktorisering av användare, allokering av nätverksresurser till användare och administrering av användarsessioner är centrala förutom vad gäller tjänstens tillgänglighet också för att säkerställa kommunikationens sekretess.

Denna underpunkt omfattar bland annat funktioner som i mobilnätet ansvarar för autentiseringen av användarens terminal och förmedlingen av autentiseringen mellan nät samt administrering av bärarförbindelser (bearer) mellan terminalen och nätet. Punkten täcker också delvis hantering av rörlighet i mobilnät (mobility management).

I mobilnät täcker denna underpunkt bland annat för sin del den centraliserade autentiseringen av anslutningar från olika nät i en komponent (Non-3GPP Access) samt Authentication, Authorisation and Accounting (AAA)-funktionerna till de delar som de har att göra med autentiseringen och auktoriseringen av slutanvändarna.

I underpunkten ingår vad gäller allokering av resurser bland annat distribuering av IP-adresser till användarnas terminaler och DNS-servrar som tjänstgör användarna, som är centrala med tanke på tillgången till tjänsten.

Till underpunkten hör också funktioner som har att göra med nätverksskivning (network slicing) till de delar som de verkställer funktionerna enligt punkten, till exempel anvisning av terminaler i nätverksskivor. I 5G deltar flera olika av nätets funktioner i skivningen. Centrala säkerhetsrisker som har att göra med skivningen är att skivorna inte är tillräckligt separerade samt åtkomsthantering, vilket riskerar dataläckage mellan skivor eller att skivornas delade datakraft reserveras.

Genom dessa funktioner kontrolleras och styrs särskilt användarnas tillgång till nätet, varför de ska betraktas som kommunikationsnätets kritiska delar. Funktionerna har också en väsentlig betydelse i kontroll av nätverkets trafik, upprätthållande av anslutningar samt tillgången till tjänsterna, kommunikationens konfidentialitet och i att trygga informationssäkerheten i hela kommunikationsnätet.

3) Registrering, verifiering och auktorisering av nätverkets tjänster eller funktioner

Enligt denna underpunkt är kommunikationsnätets kritiska delar registrering och auktorisering samt inbördes autentiseringen och auktorisering av olika funktioner. Som kommunikationsnätets kritiska delar betraktas till exempel olika register i nätet med vilka man upprätthåller uppgifter om nätets funktioner, och de av nätets funktioner som ansvarar för auktoriseringen av andra funktioner (Authentication, Authorisation and Accounting (AAA)).

Genom dessa funktioner kontrolleras och styrs tillgång till nätet, såsom nätets olika funktioners tillgång till nätets andra funktioner, varför de ska betraktas som kommunikationsnätets kritiska delar. Funktionerna har också en väsentlig betydelse i kontroll av nätverket, hantering av användarnas tillgång till nätet, upprätthållande av anslutningar samt tillgången till tjänsterna, kommunikationens konfidentialitet och i att trygga informationssäkerheten i hela kommunikationsnätet.

4) Kommunikationsnätets och -tjänstens kritiska infrastrukturtjänster som är nödvändiga och stöder dess funktion

Enligt denna underpunkt är kommunikationsnätets kritiska delar kommunikationsnätets och -tjänstens kritiska infrastrukturtjänster som är nödvändiga och stöder dess funktion. Dylika funktioner är bland annat:

- databaser som innehåller uppgifter om nätverkets kritiska funktioner och användaruppgifter
- nätverkets komponenter som används för att konfigurera nätverkskärnans interna IP-adresser och domännamn, såsom DNS- och DHCP-tjänster
- tidstjänster som utnyttjas för att synkronisera tid i nätverkets kritiska delar (påverkar bland annat nyckelhantering och loggning)
- centraliserat system som förmedlar och verifierar basstationernas tids- och fassynkroniseringssignaler[22].

Genom dessa funktioner kontrolleras och styrs nätets olika funktioners tillgång till nätets olika funktioner samt synkroniseringstrafiken i nätet, varför de ska betraktas som kommunikationsnätets kritiska delar. Funktionerna har också en väsentlig betydelse i kontroll av nätverket, hantering av användarnas tillgång till nätet, upprätthållande av anslutningar samt tillgången till tjänsterna, kommunikationens konfidentialitet och i att trygga informationssäkerheten i hela kommunikationsnätet.

5) Funktioner för kommunikationsnätens eller -tjänsternas gränssnitt, inklusive roaming

Enligt denna underpunkt hör till kommunikationsnätets kritiska delar funktioner som verkställer gränssnitt för kommunikationsnätens eller -tjänsterna till utomstående applikationer. Med detta avses särskilt gränssnitt utanför nätets kärna, genom vilka tillgången till nätets tjänster öppnas åt andra nätverk eller tjänster, som antingen kan bestå av teleföretagets eller den separata nätverksaktörens egna eller som producerats av utomstående leverantörer.

Kommunikationsnätets kritiska delar är också gränssnitt som har att göra med roaming, som öppnas åt till exempel IPX-aktörer och som möjliggör anslutningar mellan nät. Gränssnitten som avses här kan också användas för att möjliggöra tillgång till nätets funktioner till exempel genom ett trådlöst lokalt nät. Som kommunikationsnätets kritiska delar betraktas också nätverkets användares internetslussar samt gränssnitt till teleföretagens eller de separata nätverksaktörernas övriga interna system, såsom IMS-nätet.

Det är möjligt att använda externa gränssnitt för att tränga sig in i kärnnätets funktioner, försvaga nätets funktioner eller få tillgång till konfidentiell information om nätets funktioner och dess användare. Det finns flera olika gränssnittslösningar, och deras säkerhetsegenskaper är i stor grad utanför standardiseringsarbetet.

[22] Åtminstone ePRTC (Enhanced Primary Reference Time Clock), T-GM (Telecom Grandmaster) och atomur inbegripet. Eventuellt kan samma system, utöver säkerställandet, förmedla synkroniseringssignalen via satellitpositioneringssystemet till basstationer koncentrerat i normala förhållanden. Med detta system avses inte transmissionsnätets komponenter som används för överföring av signaler och som typiskt är samma som för annan telekommunikation och som kan vara kommunikationsnätets kritiska delar på basis av andra punkter i denna föreskrift.

Genom dessa funktioner kontrolleras och styrs trafiken på nätet samt tjänsternas tillgång till nätet, varför de ska betraktas som kommunikationsnätets kritiska delar. Funktionerna har också en väsentlig betydelse i kontroll av nätverket, hantering av användarnas tillgång till nätet, upprätthållande av anslutningar samt tillgången till tjänsterna, kommunikationens konfidentialitet och i att trygga informationssäkerheten i hela kommunikationsnätet.

6) Funktioner som sammankopplar kommunikationsnät eller -tjänster i sådana fall där funktionen väsentligen kan påverka tillgången till kommunikationsnätet eller dess trafik

Denna underpunkt täcker internetknutpunkter och direkt anslutning till andra nät och tjänster, i vilket fall trafiken förmedlas mellan kommunikationsnät. Utöver IP-stamnätets är för kommunikationsnätets och dess tjänsters verksamhet centrala IP-transit och sammankopplingspunkter till andra operatörers nätverk och internetnätverket. Sammankopplingens väsentliga effekter på kommunikationsnätets trafik skulle bedömas i relation till det ifrågavarande trafikslaget på nätet.

Underpunkten innehåller till exempel internetknutpunkten (IXP) och mobiloperatörernas knutpunkt (DIX). Kanalen till internetknutpunkten kan vara en del av operatörens stamnät, vars komponenter enligt kriterierna i underpunkt 1 är kommunikationsnätets kritiska delar.

Genom dessa funktioner kontrolleras och styrs trafiken på nätet, varför de ska betraktas som kommunikationsnätets kritiska delar. Funktionerna är av väsentlig betydelse för trafiken mellan näten och tillgången till tjänster samt för kommunikationens konfidentialitet och för säkrandet av hela kommunikationsnätets informationssäkerhet.

7) Centraliserad kryptering och nyckelhantering för kommunikationsnätet, dess funktioner och slutanvändarnas trafik

Denna underpunkt täcker skapandet, lagrandet och förmedlandet av krypteringsnycklar för kommunikationsnätets utrustning, programvara och användare, säkrandet av deras integritet samt andra centrala funktioner under deras livscykel. Funktionen kan anses vara centraliserad, även om den är fysiskt distribuerad till exempel i flera olika utrymmen för utrustning. Punkten innehåller också funktioner som deltar i certifikathierarkin och/eller som används för att skapa och förmedla nycklar samt förmedla information om deras giltighet (CRL, dvs. certificate revocation list eller motsvarande).

Underpunkten gäller autentisering och kryptering mellan både användare och nätverket och mellan nätverkets komponenter och funktioner.

Underpunkten täcker särskilt följande områden: kryptering av trafiken mellan nätets basstationer och nätets kärna (inklusive basstationernas trådlösa överföringsanslutningar), kryptering som används av stamnätets komponenter och kryptering av funktioner i nätets kärna. Den täcker också kryptering av databaser som kommunikationsnätets kritiska delar använder. Underpunkten täcker inte till exempel krypteringen av radiotrafiken i radiogränssnittet mellan användaren och basstationen.

Genom dessa funktioner kontrolleras och styrs användartrafiken på nätet samt användarnas tillgång till nätet, varför de ska betraktas som kommunikationsnätets kritiska delar. Funktionerna har en väsentlig betydelse med tanke på kommunikationens konfidentialitet och i att trygga informationssäkerheten i hela kommunikationsnätet.

8) Informationssäkerhetsfunktioner som påverkar kommunikationsnätets kritiska delar

Underpunkten omfattar funktioner vars uppgift är att övervaka, styra, begränsa eller filtrera nätverkets trafik eller hantera logguppgifter från system som har att göra med kommunikationsnätets kritiska delar. Underpunkten täcker också funktioner vars uppgift det är att sköta om och övervaka åtgärder som har att göra med underhåll eller administration av nätet.

Informationssäkerhetsfunktioner skyddar till exempel kärnnätet mot hot från radionätet och från utomstående nät, men även kärnnätets funktioner mot interna hot. Informationssäkerhetsfunktioner, såsom informationssäkerhetsprogramvara på servrarna, gör det möjligt att administrera de kritiska systemens plattformar eller deras operativsystem. Underpunkten täcker också informationssäkerhetsfunktioner som riktar sig till andra än kommunikationsnätets kritiska delar, såsom administrativa anslutningar.

En informationssäkerhetsfunktion som skyddar nätets kärna som avses i denna underpunkt kan beroende på nätverksarkitekturen också ha verkställts utanför kärnnätet. Underpunkten innehåller också informationssäkerhetsfunktioner som påverkar andra funktioner som fastställts som kommunikationsnätets kritiska delar, till exempel styrsystem.

Informationssäkerhetsfunktionerna särskiljer nätets olika säkerhetszoner och nätverkssegment samt filtrerar och övervakar datatrafiken mellan dem. Till dessa hör bland annat:

- segment mellan nätets kärna och överföringsnätet samt radionätet och
- Ömsesidiga gränssnitt för OSS- och BSS-systemen och deras gränssnitt gentemot kommunikationsnätet, samt
- funktioner som är avsedda för att övervaka eller kontrollera trafiken mellan eller inom ovan nämnda, såsom brandväggar, Security Gateway och Border Gateway-funktionerna som terminerar tunneltrafiken mellan de olika säkerhetszonerna (security domain) i operatörens nät, som används för att kontrollera och styra trafiken mellan en operatörs olika nät eller mellan flera operatörers nät.

Informationssäkerhetsfunktionerna kan också handla om nätverkets virtualiserade funktioner (NVF) som virtuellt producerar tjänster och programvara för nätet. De kan dela samma plattform med andra motsvarande program.

Till underpunkten hör också informationssäkerhetsfunktioner som har som uppgift att styra och förmedla tjänster från nätverket till utomstående nätverk såsom roamingnätverk eller andra nätverk utanför mobilnätet. Som exempel kan nämnas Diameter Edge Agent och för 5G-nätets del SEPP-nätslussen, som fungerar som förmedlare för genomförandet av trafiken och tjänster mellan olika operatörers nät, och till vars uppgifter hör att skydda kommunikationen för nätets kärnas tjänster mot samtrafiknätet mellan operatörerna. Andra exempel på informationssäkerhetsfunktioner som också kan vara virtualiserade är nätverkets dataskyddsprogram såsom brandväggar och trafikfiltreringsprogram eller stödprogram som används i nätverksinfrastrukturen såsom DHCP- eller DNS-tjänster.

Genom dessa funktioner kontrolleras och styrs nätets interna trafik samt tillgången till nätet och därför ska de betraktas som kommunikationsnätets kritiska delar.

Funktionerna har en väsentlig betydelse med tanke på kommunikationens konfidentialitet och i att trygga informationssäkerheten i hela kommunikationsnätet.

9) Nätverksadministrations- och nätverksövervakningssystem samt vissa andra faktureringss-, stöd- och bakgrundssystem

Enligt denna underpunkt hör till kommunikationsnätets kritiska delar nätverksadministrations- och nätverksövervakningssystem som antingen direkt har att göra med administrationen eller övervakningen av kommunikationsnätets kritiska delar eller när de i övrigt väsentligen påverkar tillgången till nätet eller trafiken på nätet. Men även andra stöd- och bakgrundssystem räknas som kommunikationsnätets kritiska delar, när de väsentligen kan påverka tillgången till kommunikationsnätet eller trafiken på nätet.

Nätverksadministrations- och nätverksövervakningssystem är därmed för det första kritiska delar av kommunikationsnätet när de har att göra med administrering eller övervakning av en funktion som betraktas som en kritisk del av kommunikationsnätet av någon annan orsak. För det andra är funktionerna som avses här kritiska delar av kommunikationsnätet när de i övrigt väsentligen kan påverka tillgången till kommunikationsnätet eller trafiken i nätet, till exempel på grund av antalet element som administreras, även om till exempel ett enskilt administrerat element inte skulle betraktas som en kritisk del av kommunikationsnätet. Till exempel basstationernas styrsystem kan vara en kritisk del av kommunikationsnätet på basis av detta även i situationer där en enskild basstation inte i sig själv skulle betraktas som en kritisk del av kommunikationsnätet, eftersom basstationernas styrsystem kan påverka användarnas tillgång till nätet eller till och med helt blockera den, och också påverka trafiken som basstationen förmedlar till exempel genom att göra den långsammare.

Med nätverksadministrations- och nätverksövervakningssystem avses här programvara, instrument eller gränssnitt genom vilka man opererar, upprätthåller eller i övrigt administrerar och övervakar kommunikationsnätets olika resurser såsom basstationer, informationssäkerhetssystem, nätutrustning samt mjukvara för att underhålla dessa.

Nätverksadministrations- och nätverksövervakningssystem är till exempel s.k. OSS-system (Operations Support Systems) och MANO-system (Management and Orchestration) samt deras gränssnitt gentemot BSS-system (Business Support Systems). OSS- och BSS-systemen kan vara i kontakt med varandra beroende på nätverksarkitekturen genom en service buss som i så fall formar ett gränssnitt som anses vara en kritisk del. Även automatiska system som används för att optimera och styra nätet kan omfattas helt eller delvis av denna underpunkt utgående från ovan nämnda förutsättningar. Sådana kan till exempel vara system som samlar in information om nätets prestanda, och som styr nätet till exempel genom att förmedla analyserade data som används för att styra nätet tillbaka till en nätverksfunktion. Denna underpunkt omfattar också till exempel IPAM-system, som används för att administrera konfigurera IP-adresser på nätet samt de system som avses i Transport- och kommunikationsverkets föreskrift 66A 4.2. § för mottagande och analys av kommunikationsnätets eller -tjänstens övervakningsuppgifter.

Till MANO-funktionerna hör komponenter till mjukvarudefinierade nätverk, bl.a. komponenter som tillhandahåller NFV-orkestrering. Till deras huvuduppgifter hör att styra, fastställa och förenhetliga anslutningarna mellan nätverkskomponenter i mjukvarudefinierade nätverk. Funktionerna enligt denna underpunkt täcker även VIM och VNF-funktionerna vars uppgift är att administrera nätverkets virtuella infrastruktur jämte plattformar och de servicekomponenter som den brukar. Även administrering

av nätverksskivning omfattas av denna punkt. Även mjukvarudefinierade nätverk (Software Defined Networking, SDN) hör till denna underpunkt. Med SDN avses virtualiseringen av nätverksfunktioner och att de överförs till en förenhetligad kontrollplan, där nätets egenskaper kan administreras genom programvarugränssnitt. Till exempel för 5G-nätens del kan administrationen automatiseras och styras programmatiskt och dynamiskt enligt föränderliga behov.

Vad gäller andra fakturerings-, stöd- och bakgrundssystem (bl.a. BSS) täcker underpunkten system som väsentligen kan påverka tillgången till kommunikationsnätet eller trafiken på nätet, till exempel med tanke på tillgången till tjänster. Till exempel system som påverkar provisionering av anslutningar kan på grund av ett eventuellt missbruk eller programfel på samma gång utesluta en stor mängd anslutningar från nätet.

Med faktureringssystem avses här både funktioner som har att göra med det tekniska verkställandet av fakturering i nätets kärna samt system som stöder fakturering utanför kärnan. Även om nätet kan fungera utan ett faktureringssystem, kan fakturering betraktas som en kritisk del av kommunikationsnätet om den väsentligen kan påverka tillgången till tjänster eller kommunikationens konfidentialitet. Faktureringssystemets funktioner kan typiskt delas in i online- och offline-funktioner. För mobilnätens del har administreringen och arkitekturen för nätets fakturering fastställts i 3GPP:s tekniska specifikationen 32.240. Faktureringssystemet kan påverka tillgången till tjänsten i fall av online-fakturering då systemet kan förhindra i realtid att användaren får tillgång till nätet eller dess tjänster genom att genomföra en kvothanteringstjänst (quota management) genom vilken den kan bevilja eller förbjuda användarna tillgång till tjänsten utgående från tid eller data. Faktureringssystemet samlar in och hanterar faktureringsuppgifter, som kan innehålla konfidentiella uppgifter som beskriver kommunikationen, till exempel om kommunikationens parter. Faktureringssystemet möjliggör tillgång till förmedlingsuppgifter som behandlats på nätet, vilket kan äventyra kommunikationens konfidentialitet.

Genom dessa funktioner kontrolleras och styrs trafiken på nätet samt tillgången till nätet, varför de ska betraktas som kommunikationsnätets kritiska delar. Funktionerna har en väsentlig betydelse för styrningen och kontrollen av nätverket, hantering av användarnas tillgång till nätet samt tillgången till tjänsterna och kommunikationens konfidentialitet och i att trygga informationssäkerheten i hela kommunikationsnätet. Funktioner som hör till faktureringssystemet kan användas för att kontrollera och styra tillgången till nätet, varför de ska betraktas som kommunikationsnätets kritiska delar. Funktionerna har väsentlig betydelse för kontroll av trafiken på nätet samt på tryggandet av tillgången till tjänster, men även för kommunikationens konfidentialitet.

10) Verkställandet av teleavlyssning eller teleövervakning

Enligt denna underpunkt skulle kommunikationsnätets kritiska delar omfatta lawful interception, dvs. LI-funktioner. Denna underpunkt handlar både om komponenter som skilt anskaffats för LI och om andra av nätverkets komponenter som direkt har att göra med verkställandet av LI-funktionerna. I 3GPP:s tekniska specifikationer har fastställts funktioner som verkställer LI-funktioner.

Denna underpunkt innehåller de tekniska hjälpmedel och egenskaper i kommunikationsnätverket som förutsätts enligt 243.1 § punkt 16 och 245 § i lagen om tjänster inom elektronisk kommunikation genom vilka teleföretaget ser till att teleavlyssning och teleövervakning tekniskt och funktionellt kan genomföras (se RP 221/2013 rd, s.188-189 och 192).

Att dessa funktioner fungerar rätt är av central betydelse för att se till att kommunikationen förblir konfidentiell. Beroende på åtgärden har de åtminstone att göra med styrning av trafiken (lagring av teleavlyssningsuppgifter), administrering av användarnas tillgång (rätten enligt 10:6 § i tvångsmedelslagen (806/2011) att användningen av adressen eller utrustningen tillfälligt förhindras i samband med teleövervakning) eller övrig tillgång till nätet (tillgång till teleövervaknings- och teleavlyssningsuppgifterna).

11) Virtualisering av nätverket när detta är i bruk för genomförandet av faciliteten eller åtgärden som är kritisk del av nätverket

I denna underpunkt fastställs virtualisering som kritisk del av kommunikationsnätet när man virtualiserar funktioner som hör till kommunikationsnätets kritiska delar. Detta innebär att virtualiseringsplattformen (virtualiseringsinfrastrukturen och dess fysiska plattform) administrerar komponenter som i sin tur kontrollerar och styr nätet och trafiken på det, vilket gör dem till kommunikationsnätets kritiska delar. I ett virtualiserat kommunikationsnät är nätets funktioner beroende av virtualiseringsplattformen och dess styr- och orkestreringssystem.

De kritiska delar av kommunikationsnätet som virtualiseringen gäller har till största delen fastställts i de övriga delarna av denna föreskrift. Eftersom föreskriften inte är uttömmande kan man också betrakta andra av kommunikationsnätets delar än de som skilt fastställts som kritiska i denna föreskrift som kommunikationsnätets kritiska delar enligt 244 a § i LTEK. I föreskriftens punkt 3 förpliktas teleföretaget eller den separata nätverksaktören att identifiera de kritiska delarna i sina kommunikationsnät. Punkten om virtualisering innebär alltså som utgångspunkt att de kritiska delar som teleföretagen identifierat också i virtualiserad form betraktas som kommunikationsnätets kritiska delar.

I underpunkten fastställdes dock inte själva virtualiseringen som kritisk. I situationer när man enbart virtualiserar andra funktioner och åtgärder än de som betraktas som kommunikationsnätets kritiska delar betraktas virtualisering alltså inte vara en kritisk del av kommunikationsnätet.

5G-nätets kärna baserar sig på virtualiserade tjänster, som kan verkställas i en miljö som påminner om en typisk IT-infrastruktur, men det är också möjligt att virtualisera tidigare generationernas nätverksfunktioner. I 5G-nätet kan man virtualisera själva nätverksfunktionerna med programvara som styr näten, och det är möjligt att distribuera nätets kapacitet i olika virtuella skivor enligt behov. Med virtualiseringen av nätfunktioner (Network Function Virtualizaton, NFV) avser man att 5G-nätverksfunktionerna verkställs programmatiskt istället för genom traditionell nätverksutrustning. Virtualiseringsplattformarna delas mellan flera olika funktioner och programvara. Plattformarnas säkerhet blir en kritisk faktor i säkerställandet av hela nätets informationssäkerhet.[23]På virtualiseringsplattformen kan man verkställa en eller flera nätverksfunktioner.

Enligt underpunktens kriterier kunde som kommunikationsnätets kritiska delar betraktas i ett 5G-nät åtminstone nätets virtualiserade funktioner (Virtual Network Functions, VNF) virtualiseringsinfrastrukturen för nätverksfunktionerna (NFV Infrastructure, NFVI), hanteringen och orkestreringen av de virtualiserade funktionerna,

[23]Om virtualiseringens informationssäkerhetshot, se t.ex. 3GPP TR 33.848 V0.5.0 (2019-11). Study on Security Impacts of Virtualisation. https://www.3gpp.org/DynaReport/33848.htm.

samt virtualiseringens fysiska plattform. Hanteringen av de virtualiserade funktionerna och virtualiseringen sker genom MANO-systemet , till vilket hör åtminstone NFV Orchestrator (NFVO ansvarar bl.a. för att resurserna orkestreras mellan VIM:er), VNF Manager (VNFM som ansvarar för hanteringen av VNF-instanser) och Virtualised Infrastructure Manager (VIM, som styr virtualiseringsinfrastrukturens (NFVI):s verksamhet).[24]

12) Funktioner som verkställts genom virtualisering och som betraktas som kommunikationsnätets kritiska delar

Utgående från denna underpunkt kan man betrakta som kommunikationsnätets kritiska delar övriga funktioner eller åtgärder än ovan nämnda, eller som i övrigt anses vara en kritisk del, när den genomförs genom virtualisering som enligt ovan i punkt 11 betraktas som en kritisk del av kommunikationsnätet. I föregående underpunkt fastställer man själva virtualiseringen som en kritisk del i kommunikationsnätet i vissa situationer. I sådana fall där virtualiseringen betraktas som en kritisk del av kommunikationsnätverket fastställs i denna underpunkt även de andra funktioner som genomförts i samma virtualiseringsmiljö som kritiska delar av kommunikationsnätet.

När de virtualiserade funktionerna delar resurser, leder det till informationssäkerhetsrisker och beroendeförhållanden mellan de virtualiserade funktionerna, och det är möjligt för funktionerna att påverka de övriga virtualiserade funktionerna. Tillgången till plattformen från de virtualiserade funktionerna skulle äventyra de övriga funktionerna. Av den här orsaken är det befogat att räkna alla funktioner som verkställs på samma kritiska virtualiseringsplatform som kritiska delar av nätet och anta att de används i en kritisk del av kommunikationsnätet, även om vissa av dem om de skulle ha verkställts på en skild plattform inte skulle räknas som kritiska delar av kommunikationsnätet. Till exempel om basstationens centralenhet (central unit, CU) inte i övriga fall skulle räknas som kommunikationsnätets kritiska del, men om den skulle virtualiseras på samma plattform som nätets kärnfunktioner som betraktas som kommunikationsnätets kritiska funktioner, skulle det innebära att CU också betraktas som en kritisk del av kommunikationsnätet enligt denna underpunkt.

Denna underpunkt förhindrar inte i sig självt att man på samma plattform verkställer både kritiska och i övriga fall icke-kritiska funktioner, den innebär enbart all detta leder till att de virtualiserade funktionerna som annars skulle räknas som icke-kritiska nu omfattas av tillämpningen av 244 a §. Teleföretagen kan verkställa funktionerna på samma plattform, om de trots det kan sörja för sina andra förpliktelser enligt reglerna.

13) Centrala faciliteter och åtgärder genom vilka man möjliggör tillgång till uppgifter om abonnemang som hanteras i kommunikationsnätet eller uppgifter om terminalens geografiska läge, eller som tillåter lokalisering med hjälp av kommunikationsnätet.

Uppgifter som avslöjar abonnemanget eller terminalen och därigenom användarens geografiska läge (lokaliseringsuppgifter) riskerar potentiellt missbruk, och kan till och med utsätta användaren för fysiska hot. Det kan vara fråga om förmedlingsuppgifter som vanligen hanteras för att förmedla kommunikation och som samtidigt ger information om användarens plats med en viss precision, eller lokaliseringsuppgifter som hanteras för andra ändamål än för att förmedla kommunikationen. Tjänster/komponenter som har att göra med lokalisering på nätet har inte alltid direkt att

[24] Se gällande virtualisering i 5G-nät ENISA Threat Landscape for 5G Networks., k 3.7

göra med förmedling av kommunikation, utan de kan användas för s.k. mervärdestjänster som därför inte till alla delar omfattas av ovanstående underpunkter. Förmedlingsuppgifter, lokaliseringsuppgifter och mervärdestjänster har definierats i 3 § i LTEK.

Enligt underpunkten är kommunikationsnätets kritiska delar för det första funktioner och åtgärder som möjliggör tillgång till uppgifter om det geografiska läget för ett abonnemang eller en terminal som hanteras i kommunikationsnätet, såsom lagrade förmedlings- eller lokaliseringsuppgifter. Dessa funktioner kan anses kontrollera eller styra tillgången till nätet, varför de ska betraktas som kommunikationsnätets kritiska delar. För det andra är kommunikationsnätets kritiska delar faciliteter och åtgärder som gör det möjligt att ta reda på abonnemangets eller terminalens geografiska läge. Att ta reda på det geografiska läget kan anses basera sig på kontroll av nätet och trafiken på det.

Funktioner som underpunkten avser är till exempel:

- Gateway Mobile Location Centre (GMLC) som stöder erbjudandet av lokaliseringsbaserade tjänster och genom vilken man kan få tillgång till funktioner eller utomstående serviceproducenter som har rätt till uppgifterna, såsom leverantörer av mervärdestjänster som hanterar uppgifterna med användarens samtycke, förfrågningar om användarens geografiska läge och tillgång till lokaliseringsuppgifterna (3GPP TS 23.273, Rel. 16)

- Enhanced Serving Mobile Location Center (E-SMLC), som stöder utredning av terminalens geografiska läge i LTE-nät (3GPP TS 23.271)

- Location Management Function (LMF) som stöder utredningen av terminalens geografiska läge i 5G-nät (3GPP TS 23.273).

Ovan nämnda funktioner utnyttjas till exempel nödpositionering.[25] I nättjänster som har att göra med geografiskt läge deltar därtill flera andra funktioner, som har fastställts som kritiska antingen i tidigare underpunkter eller i senare punkter i denna föreskrift.

## 5. 4G-nätets kritiska delar

### 5.1. Fastställandet av 4G-nätets kritiska delar

I denna punkt fastställs de av nätets funktioner som åtminstone är 4G-nätets kritiska delar genom att hänvisa till funktioner av nätens kärna som nämns i 3rd Generation Partnership Project:s (3GPP) tekniska specifikation TS 23.002. Punktens första underpunkt är till största del klargörande till sin karaktär eftersom man i den för fram utgångspunkten att kärnans funktioner är kommunikationsnätets kritiska delar.

I den första underpunkten fastställs att de kritiska delarna av kommunikationsnätet för 4G-nätets del är de paketförmedlande funktioner som nämns i 3GPP:s tekniska specifikation TS 23.002 punkt 4.1.1, 4.1.4 och 4.1.5 till den del som de används för att kontrollera eller styra tillgången till nätet och trafiken på nätet på ett väsentligt sätt. Detta innebär dock att inte alla funktioner som ingår i de nämnda punkterna

[25] Network Induced Location Request (NI-LR). https://itectec.com/spec/6-10-procedures-dedicated-to-support-regulatory-services/.

nödvändigtvis betraktas som kommunikationsnätets kritiska delar. Den första underpunktens precision ”paketförmedlande” har som avsikt att exkludera de kretskopplade funktionerna som ingår i punkterna som förtecknats.[26] Funktionerna har på det sätt som avses i punkten kunnat fastställas i den tekniska specifikationen 23.002 genom att hänvisa till andra specifikationer i 3GPP.

I punktens andra underpunkt fastställs de av 4G-nätets funktioner som åtminstone ska betraktas som kommunikationsnätets kritiska delar. Vad gäller de funktioner som nämns i förteckning 1 i föreskriften behövs inte en noggrannare analys av delens kritiskhet i kommunikationsnätet, utan man kan utgå från att de alltid är kommunikationsnätets kritiska delar. I punkt 7 i föreskriften beskrivs dock ett möjligt undantag till detta. I punkt 7 i föreskriften möjliggör man att en funktionalitet som i övriga fall skulle betraktas som kommunikationsnätets kritiska del under vissa förutsättningar kan betraktas som icke-kritisk, om man genom den stöder tjänster på kantnätet och om man har upprättat mekanismer för att skydda kommunikationsnätets kritiska delar.

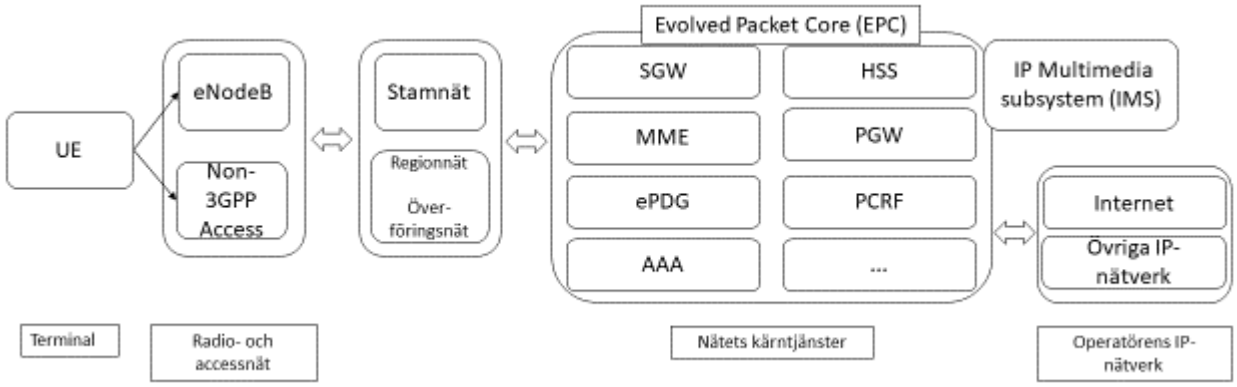
Den första underpunkten och tabellen som hänvisas till i den andra underpunkten om kritiska delar är under inga förhållanden uttömmande, utan teleföretagen och de separata nätverksaktörerna ska också bedöma om deras nät har kritiska delar som inte nämns i förteckningen. Utöver förteckningen skulle man alltså tillämpa inte enbart definitionerna för de för alla nät gemensamma kritiska delarna enligt punkt 4 i föreskriften, utan också definitionen som sådan på en kritisk del av ett kommunikationsnät enligt 244 a § 1 mom. i LTEK.

Funktionerna enligt 3GPP:s specifikationer är logiska och distribuerade över flera applikationer. Enligt punkten vore nätets del kritisk även om den enbart verkställer en del av den funktionalitet som fastställts som kritisk. Detta och sättet att fastställa dem utgående från funktion skulle dock innebära att när man kan påvisa att en enskild programvarukomponent genomför ens en del av en sådan funktion som fastställts som en kritisk del av nätet, så skulle komponenten betraktas som en kritisk del av nätet, även om komponenten inte i sig själv utför hela funktionen. En enskild programvarukomponent eller nätverksutrustning kan också verkställa mer än en funktion.

Det verkar självklart att vad gäller 4G-delar som används i 5G NSA-nät skulle man bedöma deras kritiskhet utgående från vad som föreskrivs om delar i ett 4G-nät i föreskriften. 5G NSA-nätet baserar sig på 4G-nätets EPC-kärna. För denna föreskrifts del gäller alltså förteckningen över 4G-nätets kritiska delar också de av 4G-nätets funktioner som 5G NSA-nätet utnyttjar.

I bild 1 har man på en allmän nivå beskrivit arkitekturen på ett kommunikationsnät som baserar sig på LTE-teknologi. IP Multimedia Subsystem som nämns på bilden behandlas i punkt 8 i föreskriften. Alla funktioner som beskrivs till nästa är en del av nätets kärntjänster enligt bilden.

[26] Till exempel har förmedlandet av textmeddelanden till basstationer eller från basstationer till meddelandecentraler att göra med SMS-GMSC (SMS Gateway MSC) och SMS Interworking MSC (SMS-IWMSC).




*Kuva 1* Exempel på 4G-nätets arkitektur på en allmän nivå

I samband med att förteckning 1 i föreskriften gjordes tog man som jämförelsepunkt i beaktande en motsvarande förteckning som gjorts upp i Storbritannien. Storbritannien har genom en anvisning från det nationella cybersäkerhetscentret gjort teleföretagen medvetna om funktioner som anses särskilt utsatta för risker i 5G-näten och vissa 4G-nät samt funktioner som är gemensamma för alla nät.[27]

## 5.2. 4G-nätets kritiska funktioner

### Home Subscriber Server (HSS)

Home Subscriber Server (HSS) är en central databas som innehåller uppgifter om användarens sessioner och anslutningar för hantering i ett kommunikationsnät som baserar sig på LTE-teknologi. I ett mobilnät kan finnas en eller flera centraldatabaser beroende på antalet användare i nätet och dess arkitektur.

HSS ansvarar för användarnas åtkomsthantering, identifiering av användare, användarprofiler samt hantering av rörlighet (till exempel genom att ge information om en MME som tjänstgör användaren). HSS ansvarar också för nyckelhantering och för att skapa verifieringsvektorer i kommunikationsnätet. HSS spelar också en roll i verkställandet av teleavlyssning eller teleövervakning (Lawful Interception, dvs. LI-funktioner).

HSS innehåller enligt 3GPP:s tekniska specifikation nuförtiden funktioner för ett hemregister (HLR, Home Location Register) och en autentiseringscentral (AuC, Authentication Centre).[28]

Med denna funktion kontrollerar man och styr användarnas tillgång till nätet, varför den ska betraktas som en kritisk del av kommunikationsnätet. Funktionerna har också en väsentlig betydelse i kontroll och styrning av nätverket och dess trafik, upprätthållande av anslutningar samt tillgången till tjänsterna, kommunikationens konfidentialitet och i att trygga informationssäkerheten i hela kommunikationsnätet.

[27] NCSC advice on the use of equipment from high risk vendors in UK telecoms networks, punkt 11.a. 28.1.2020. https://www.ncsc.gov.uk/guidance/ncsc-advice-on-the-use-of-equipment-from-high-risk-vendors-in-uk-telecoms-networks. Se också punkt 12. För 4G:s del är dessa funktioner: "mobile core functions, including Home Subscriber Server (HSS), Packet Gateway (PGW), Policy and Charging Rules Function (PCRF) and, in some cases, the Mobility Management Entity (MME) and Serving Gateway (SGW)."
[28] 3GPP TS 23.002, k. 4.1.1.1.1–4.1.1.1.2.

Equipment Identity Register (EIR)

EIR, eller enhetsidentifikationsregistret, är en databas för mobilnätet i vilken man lagrar internationella enhetsidentifikationsuppgifter (IMEI) och som innehåller mobilenhetens tillståndsuppgifter. Normal användning av terminaler på kommunikationsnätet som placerats på EIR:s svarta lista blockeras.

Med denna funktion kontrollerar man användarnas tillgång till nätet, varför den ska betraktas som en kritisk del av kommunikationsnätet. Funktionen har en väsentlig betydelse för att förhindra att enheter utan tillstånd får tillgång till nätet och därmed tryggandet av tillgången till nätets tjänster.

Subscription Locator Function (SLF)

SLF förmedlar namnet på centraldatabasen (HSS) som innehåller användardata till nätets funktioner (AAA, AAS, I-CSCF) när det finns fler än en av dem i mobilnätet.

Med denna funktion kontrollerar och styr man användarnas tillgång till nätets tjänster, varför den ska betraktas som en kritisk del av kommunikationsnätet. Funktionerna har också en väsentlig betydelse i kontroll och styrning av nätverket och dess trafik, upprätthållande av anslutningar samt tillgången till tjänsterna, kommunikationens konfidentialitet och i att trygga informationssäkerheten i hela kommunikationsnätet.

Mobile Management Entity (MME)

MME (rörlighetshanteringsenheten) ansvarar för terminering av terminalernas styrningstrafik, registrering av terminaler och hanteringen av förbindelser samt hantering av rörlighet. Den spelar också en roll i roaming. MME verkställer också LI-funktioner.

Med denna funktion kontrollerar man och styr användarnas tillgång till nätet, varför den ska betraktas som en kritisk del av kommunikationsnätet. Funktionerna har också en väsentlig betydelse i kontroll och styrning av nätverket och dess trafik, upprätthållande av anslutningar samt tillgången till tjänsterna, kommunikationens konfidentialitet och i att trygga informationssäkerheten i hela kommunikationsnätet.

Serving Gateway (SGW)

SGW (tjänstgörande nätsluss) ansvarar för routningen och hanteringen av trafik på användarnivå mellan basstationer och PDN-GW. MME styr tillsammans med SGW skapandet av nya anslutningar och modifieringen av existerande anslutningar mellan terminalen och nätet. SGW verkställer också LI-funktioner.

Med denna funktion kontrollerar man och styr trafiken på nätet, varför den ska betraktas som en kritisk del av kommunikationsnätet. Funktionen har också en väsentlig betydelse i att upprätthålla kommunikationsnätets anslutningar samt i att garantera tillgången till tjänster och kommunikationens konfidentialitet.

Packet Data Network Gateway (PDN GW)

PDN-GW (nätsluss för ett paketförmedlat nät) är en gränssnittsfunktion mellan operatörens interna IP-nät och ett utomstående IP-nät. PDW-GW ansvarar för att distribuera IP-adresser till terminaler. Den övervakar också användarpolicyn. Med PDN-GW utförs också filtrering och analys av trafiken, utgående från vilken man kan genomföra fakturering och kontrollera trafiken. PDN-GW verkställer också LI-funktioner.

Med denna funktion kontrollerar man och styr trafiken på nätet, varför den ska betraktas som en kritisk del av kommunikationsnätet. Funktionen har också en väsentlig betydelse i att upprätthålla kommunikationsnätets anslutningar samt i att garantera tillgången till tjänster och kommunikationens konfidentialitet.

Evolved Packet Data Gateway (ePDG)

Med ePDG verkställs anslutningen av användare utanför mobilnätet (non-3GPP-access) genom att routa trafiken mellan PDN-GW och användaren. Med eDPG verkställs allmänna VoWiFi-tjänster (Voice over WiFi, taltjänst som verkställs med hjälp av ett trådlöst lokalt nät).

ePDG aktiverar nyckelutbyte mellan användaren och ePDG samt skapar en IPSec-tunnel för att säkra kommunikationen som sker på gränssnittet. ePDG verkställer också autentiseringen och auktoriseringen av IPSec-tunneln. ePDG verkställer också LI-funktioner.

Med denna funktion kontrollerar man och styr trafiken på nätet, varför den ska betraktas som en kritisk del av kommunikationsnätet. Funktionen har också en väsentlig betydelse i att upprätthålla kommunikationsnätets anslutningar samt i att garantera tillgången till tjänster och kommunikationens konfidentialitet.

3GPP AAA Server och 3GPP AAA Proxy

AAA-servern (server) ansvarar för autentisering, auktorisering och rörlighetshantering för användare utanför mobilnätet (non-3GPP-access) samt innehåller de användaruppgifter som behövs för att verkställa åtkomsthanteringen. AAA-proxyservern (proxy) erbjuder motsvarande tjänster i roamingsituationer. AAA-proxyservern väljer också vid behov den nätsluss som tjänstgör under användarens session.

AAA-servern har särskilt att göra med verkställandet av VoWiFi-tjänsten. AAA verkställer också LI-funktioner.

Med denna funktion kontrollerar man användarnas tillgång till nätet och därför ska den betraktas som en kritisk del av kommunikationsnätet. Funktionen har också väsentlig betydelse för kommunikationens konfidentialitet, styrning och hantering av kommunikationsnätet och dess trafik samt upprätthållandet av anslutningar.

Access Network Discovery and Selection Function (ANDSF)

ANDSF ansvarar för styrningen av användarens trafik mellan mobilnätet och nät utanför mobilnätet (non-3GPP-access) såsom mellan WLAN-nät genom att ge information om routningen av trafiken och terminalernas rörlighet. Beroende på hur funktionen verkställs hämtas uppgifterna antingen från ANDSF-servern eller så distribuerar servern dem till målterminalerna.

Med denna funktion kontrollerar och styr man användarnas trafik på nätet och därför ska den betraktas som en kritisk del av kommunikationsnätet. Funktionen har också väsentlig betydelse för användarnas tillgång till nätet och tillgången till nätets tjänster.

Policy and Charging Rules Function (PCRF)

PCRF fungerar som en styrpunkt för användarpolicyn och faktureringen för användarnas anslutningar. PCRF ser till att trafiken på användarnivån överensstämmer med användarprofilen. PCRF har en central roll i kvaliteten på anslutningstjänsterna som

erbjuds åt användarna, faktureringen och i styrningen av VoLTE-taltjänsten och roaming.

Med denna funktion kontrollerar man och styr användarnas trafik och tillgång till nätet och därför ska den betraktas som en kritisk del av kommunikationsnätet. Funktionen har också väsentlig betydelse för upprätthållande av anslutningar och för att trygga tillgången till tjänster.

## 6. 5G-nätets kritiska delar

### 6.1. 5G-nätets särdrag och dess arkitektur

5G-nätets kärna omfattar vissa kärnfunktioner i nätet som krävs för att nätet ska fungera eller kunna producera vissa kritiska tjänster åt nätet. Den omfattar även gränssnitt till utomstående system och nät, kantnätet och till utomstående s.k. IPX- och datanäts funktioner. I nätverkets kärna fattas beslut om användarens tillgång till nätet och om trafikstyrningen, samt beslutas om huruvida information ska hanteras lokalt i nätet nära användaren. I nätets kärna styrs och fattas beslut samt säkerställs funktionen hos den infrastruktur som nätet och dess plattformar behöver.

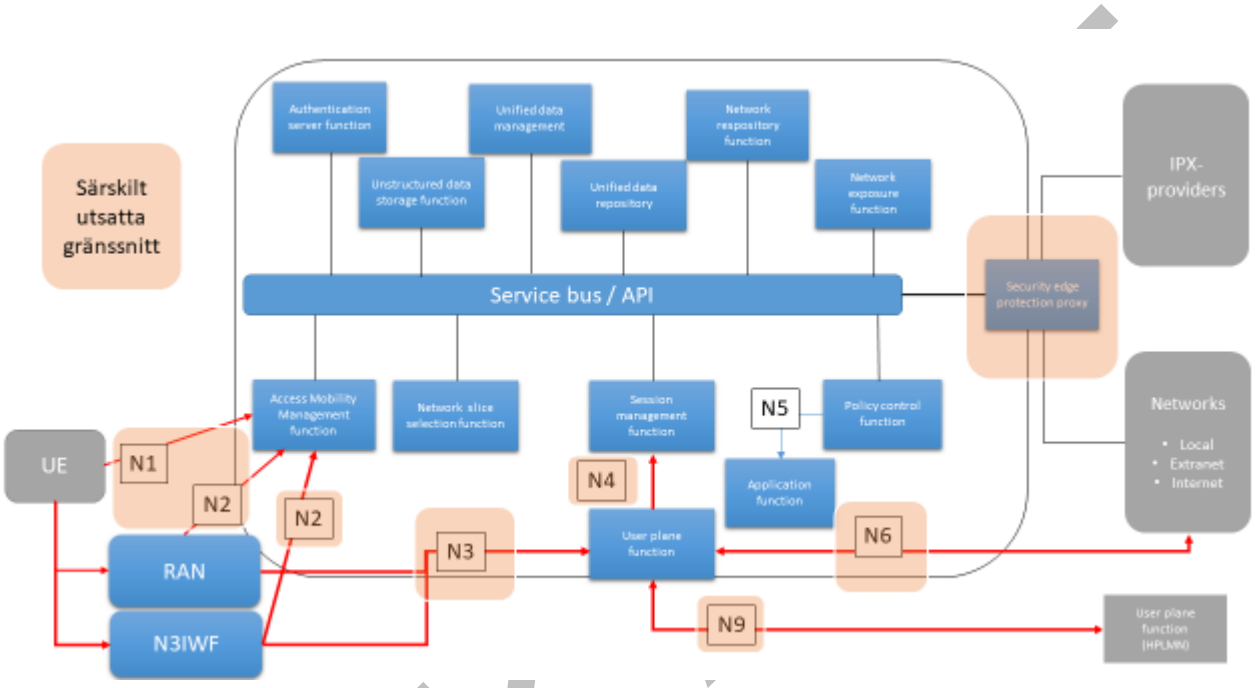
5G-nätets kärna består av en service buss och mjukvarukomponenter. I nätets kärna har man åtskilt plattformen och nätets mjukvarubaserade komponenter från varandra och de kan byggas oberoende av varandra. Flera funktioner eller programvara kan dela en plattform. Plattformarnas säkerhet är en kritisk faktor i säkerställandet av hela nätets informationssäkerhet. Hoten mot nätets kärnas funktioner inbegriper bland annat utomstående gränssnitt genom vilka man kan påverka eller bryta in i programvaran i nätets kärna, samt tvärgående trafik genom nätets kärna. 5G-servicearkitekturerns standardiserade service bussar gör det möjligt för serviceproducenter att fast integreras i 5G-kärnans viktiga bussar. Det här gör det möjligt att anpassa nätet och optimera det utgående från de tjänster användarna använder.

Komponenter som styr 5G-nätets verksamhet hanteras som funktioner i nätet, vilka kan bestå av flera olika mjukvaruprogram eller s.k. containrar som erbjuder en etablerad och färdig exekveringsmiljö för programvaran som behövs. Trafiken mellan funktionerna i nätverkets kärna sker via standardiserade service bussar. Nätets kärna bjuder också på gränssnitt som möjliggör roaming för användare från andra operatörers nät samt trafik till andra datanät såsom internet eller organisationernas intranät.

I 5G-näten ökar användningen av virtualisering, som kommer att spela en viktig roll, medan virtuella miljöer kommer att bli betydligt mer dynamiska. Virtualisering kan redan användas i 4G-teknologierna och även i IMS (IP multimedia subsystem). Vid plattformlösningar kan man övergå till molnbaserade virtualiseringslösningar för datatrafikplattformar och serverplattformar. Nätets olika komponenter såsom basstationernas mjukvara och funktionaliteterna i nätets kärna kan tillhandahållas med hjälp av virtualiserade plattformar.

Till 5G-nätets kärna kan man räkna komponenter som hör till nätets basstationer som sköter om styrningen och routningen av trafiken, identifiering och auktorisering av användare samt hantering och distribuering av krypteringsnycklar. Till kärnan hör också teleföretagens gränssnitt för sammankopplingen av mobilnät mellan olika aktörer. Funktioner som ansvarar för detta är enligt 3GPP:s specifikationer åtminstone UPF, AMF och SEPP samt till dem hörande komponenter i en servicebaserad arkitektur. 5G-nätets centrala funktioner enligt 3GPP:s arkitektur visas i bild 2.

5G-nätets huvudsakliga säkerhetszoner kan allmänt talat indelas i två olika nivåer: nätets kärna och dess gränssnitt samt kantnätet. Kantnätet omfattar nätets överföringsanslutningar oberoende av hur de verkställs, basstationer och eventuellt komponenter för kantberäkning. Avskiljandet mellan nätets kärna och nätets kant är inte entydigt, men det kan anses att gränsen i lika stor grad finns mellan terminalernas och basstationernas kontrollplan (control plane) och N1- och N2-gränssnitten mellan näten som i N3-gränssnittet mellan dataförbindelsen från basstationen och nätet (user plane). Gränssnitten N32 och N6 skiljer nätet från IPX- och databaserade nät, och N9-gränssnittet från besökarnätet.




*Kuva 2* 5G-kärnnätets centrala funktioner och gränssnitt

## 6.2. Fastställandet av 5G-nätets kritiska delar

I denna punkt fastställs de av nätets funktioner som åtminstone är 5G-nätets kritiska delar genom att hänvisa till funktioner av nätens kärna som nämns i 3GPP:s tekniska specifikation TS 23.501. Punktens första underpunkt är till största del klargörande till sin karaktär eftersom man i den för fram utgångspunkten att kärnans funktioner är kommunikationsnätets kritiska delar.

I den första underpunkten fastställs att de kritiska delarna av kommunikationsnätet funktioner i 5G-nätets kärna är liksom de definierats i 3GPP:s tekniska specifikation 23.501 punkt 6.2 till den del som de på ett väsentligt sätt kontrollerar eller styr tillgången till nätet och trafiken som går i nätet. Detta innebär dock att inte alla funktioner som ingår i de nämnda punkterna nödvändigtvis betraktas som kommunikationsnätets kritiska delar. Funktionerna har också eventuellt i punkten med avsikt fastställts i den tekniska specifikationen 23.501 genom att hänvisa till andra tekniska specifikationer i 3GPP.

I punktens andra underpunkt fastställs de av 5G-nätets funktioner som åtminstone ska betraktas som kommunikationsnätets kritiska delar. Vad gäller de funktioner som nämns i förteckning 2 i föreskriften behövs inte en noggrannare analys av delens kritiskhet i kommunikationsnätet, utan man kan utgå från att de alltid hör till

kommunikationsnätets kritiska delar. I punkt 7 i föreskriften beskrivs dock ett möjligt undantag till detta. I punkt 7 i föreskriften möjliggör man att en funktionalitet som i övriga fall skulle betraktas som kommunikationsnätets kritiska del under vissa förutsättningar kan betraktas som icke-kritisk, om man genom den stöder tjänster på kantnätet och om man har upprättat mekanismer för att skydda kommunikationsnätets kritiska delar.

Funktionerna enligt 3GPP:s specifikationer är logiska och distribuerade över flera applikationer. Enligt punkten vore nätets del kritisk även om den enbart verkställer en del av den funktionalitet som fastställts som kritisk. Detta och sättet att fastställa dem utgående från funktion skulle dock innebära att när man kan påvisa att en enskild programvarukomponent genomför ens en del av en sådan funktion som fastställts som en kritisk del av kommunikationsnätet, så skulle komponenten betraktas som en kritisk del av nätet, även om komponenten inte i sig själv utför hela funktionen. En enskild programvarukomponent eller nätverksutrustning kan också verkställa mer än en funktion.

5G-komponenterna i 5G NSA-nätet omfattas vad gäller tillämpningsområdet av de olika punkterna av fastställandet av de kritiska delarna av 5G-nätet. Om man till exempel fastställt någon viss del av 5G-nätet som kritisk, är delen också kritisk när den används i ett 5G NSA-nät. På motsvarande sätt vad gäller 4G-delarna som används i 5G NSA-nät bedöms deras kritiskhet utgående från vad som föreskrivs om delarna i ett 4G-nät.

Majoriteten av funktionerna som fastställts i punkten begränsar sig till kantnätet även i sådana fall där kärnnätet enligt beskrivningen ovan i punkt 6.1 anses vara en del av nätet som kan avskiljas genom vissa specifika gränssnitt från kantnätet. Ett undantag till detta är Non-3GPP InterWorking Function (N3IWF) som möjliggör anslutning genom WLAN till 5G-nätet.

Den första underpunkten och tabellen som hänvisas till i den andra underpunkten om kritiska delar är under inga förhållanden uttömmande, utan teleföretagen och de separata nätverksaktörerna ska också bedöma om deras nät har kritiska delar som inte nämns i förteckningen. Utöver förteckningen ska man alltså tillämpa inte enbart definitionerna för de för alla nät gemensamma kritiska delarna enligt punkt 4 i föreskriften, utan också definitionen som sådan på en kritisk del av ett kommunikationsnät enligt 244 a § 1 mom. i LTEK. Eftersom tabellen inte är uttömmande kan eventuella andra funktioner som fastställs i framtiden och som uppfyller liknande kritiska funktionaliteter antingen vara kritiska delar av kommunikationsnätet enligt punkt 4 i föreskriften eller enligt 244 a § 1 mom. i LTEK.

### 6.3. 5G-nätets kritiska funktioner

Access and Mobility Management Function (AMF)

AMF ansvarar för terminering av accessnätets och användarnas styrningstrafik, anslutningar till radionätets basstationer och terminaler och registrering till kärnnätet samt för rörlighetshantering.

AMF har en nyckelroll i nätverksskivningen och erbjuder terminaler tillgång till alla de skivor som erbjuds den. AMF ansvarar också för att skapa och hantera anslutningar utanför mobilnätet (non-3GPP-access, t.ex. WLAN). AMF spelar också en roll i verkställandet av teleavlyssning eller teleövervakning (Lawful Interception, dvs. LI-funktioner).

Med denna funktion kontrollerar man och styr användarnas tillgång till nätet, varför den ska betraktas som en kritisk del av kommunikationsnätet. Funktionen har också en väsentlig betydelse i kontroll av nätverkets trafik, upprätthållande av anslutningar samt tillgången till tjänsterna, kommunikationens konfidentialitet och i att trygga informationssäkerheten i hela kommunikationsnätet.

User Plane Function (UPF)

UPF ansvarar för routning, styrning och hantering av användartrafik liksom SGW/PGW i 4G-nät. UPF kan verkställas som en distribuerad eller lokal funktion i nätet, till exempel i samband med kantberäkning (MEC)[29]. Det är också på UPF:s ansvar att hantera kvaliteten på användartrafikens tjänster (QoS) samt upprätthållandet av sessioners och tjänsters kontinuitet som är särskilt väsentligt för URLLC. UPF verkställer också LI-funktioner.

Med denna funktion kontrollerar och styr man användarnas trafik och därför ska den betraktas som en kritisk del av kommunikationsnätet. Funktionen har också väsentlig betydelse för upprätthållande av anslutningar och för att trygga tillgången till tjänster och kommunikationens konfidentialitet.

Policy Control Function (PCF)

PCF ansvarar för trafikstyrning och verkställandet av åtkomstpolicyn. Funktionen använder parametrar från bl.a. UDR-registret som har att göra med styrningen av användartrafiken. PCF spelar en central roll i kvaliteten på nätets tjänster och i styrningen av fakturering. PCF har stöd för nätverksskivning, rörlighetspolicyn (mobility policies) och roaming.

Med denna funktion kontrollerar man och styr användarnas trafik och tillgång till nätet och därför ska den betraktas som en kritisk del av kommunikationsnätet. Funktionen har också väsentlig betydelse för upprätthållande av anslutningar och för att trygga tillgången till tjänster.

Authentication Server Function (AUSF)

AUSF ansvarar för tjänster och funktioner på nätet i anknytning till autentiseringen av användarnas terminaler och erbjuder en gemensam referensram för autentisering för både 3GPP- och icke-3GPP-anslutningar. AUSF verkställer för 5G delvis liknande funktioner som HSS i 4G.

Med denna funktion kontrollerar man och styr användarnas trafik och tillgång till nätet och därför ska den betraktas som en kritisk del av kommunikationsnätet. Funktionen har också en väsentlig betydelse i tillgången till tjänsterna, kommunikationens konfidentialitet och i att trygga informationssäkerheten i hela kommunikationsnätet.

Unified Data Management (UDM)

UDM ansvarar för identifiering av användare, åtkomsthantering, hantering av abonnemang, användarregister samt skapandet och hantering av krypteringsnycklar. UDM upprätthåller administrationsfunktioner för beställaruppgifter, såsom fastställandet och radering av 5G-beställare, bytet av SIM-kort, ändring av MSISDN-siffror

[29] MEC in 5G networks. First edition – June 2018, ETSI White Paper No. 28, s. 8. Tillgänglig: https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp28_mec_in_5G_FINAL.pdf.

samt ändringar och förfrågningar kring beställningsuppgifter. UDM verkställer för 5G delvis liknande funktioner som HSS i 4G. UDM verkställer också LI-funktioner.

Med denna funktion kontrollerar och styr man användarnas tillgång till nätets tjänster, varför den ska betraktas som en kritisk del av kommunikationsnätet. Funktionerna har också en väsentlig betydelse i kontrollen av nätverket och dess trafik, upprätthållandet av anslutningar samt tillgången till tjänsterna, kommunikationens konfidentialitet och i att trygga informationssäkerheten i hela kommunikationsnätet.

Application Function (AF)

AF stöder fattandet av routningsbeslut i nätet enligt de applikationer användarna använder. AF utnyttjar data som fastställts i NEF-funktionen och kan via NEF växelverka med kärnnätet. Nätets olika funktioner kan fungera i AF:s roll. Till exempel P-CSCF som har att göra med verkställandet av IMS-tjänster kan ta AF:s roll.

Med denna funktion kontrollerar man och styr trafiken på nätet och tillgång till nätet, varför den ska betraktas som en kritisk del av kommunikationsnätet. Funktionen har också väsentlig betydelse för upprätthållande av anslutningar och för att trygga tillgången till tjänster och hela kommunikationsnätets informationssäkerhet.

Network Exposure Function (NEF) och Intermediate NEF (I-NEF)

NEF gör det möjligt att erbjuda 5G-kärnnätets funktioner till tredje parters aktörer och utomstående applikationer. NEF ansvarar för att nätverkets tjänster marknadsförs bl.a. i 3GPP-nätverk, förmedlar information om applikationer utanför nätet till mobilnätet, och ansvarar för service bussens interna styrning.

NEF gör det möjligt för AF att säkert kommunicera med nätet. Den kan också lagra i UDR uppgifter den fått av andra funktioner. I-NEF fungerar som NEF i roamingsituationer.

Med denna funktion kontrollerar man användarnas tillgång till nätets funktioner, varför den ska betraktas som en kritisk del av kommunikationsnätet. Funktionen har också väsentlig betydelse för upprätthållande av anslutningar, tillgången till tjänster och för att trygga kommunikationens konfidentialitet och hela kommunikationsnätets informationssäkerhet.

Network Repository Function (NRF)

NRF ansvarar för tillgången till nätets tjänster, registrering och auktorisering. NRF upprätthåller en förteckning av nätets tjänster och komponenter och erbjuder därmed registrerings- och sökfunktioner, och möjliggör ömsesidig tillgång och kommunikation mellan nätets övriga funktioner och tjänster. Alla 5G-nätets funktioner växelverkar med NRF.

Med den här funktionen kontrollerar man tillgången till nätets resurser och tjänster genom att upprätthålla och förmedla information om dem, varför den ska betraktas som en kritisk del av kommunikationsnätet. Funktionen har också en väsentlig betydelse i tillgången till tjänsterna, och i att trygga informationssäkerheten i hela kommunikationsnätet.

Network Slice Selection Function (NSSF)

NSSF ansvarar för tjänster och definitioner i samband med nätverksskivning, styr och kontrollerar AMF-funktionen. NSSF fastställer den AMF som betjänar terminalen och beslutar om de nätverksskivor som är tillåtna och som erbjuds terminalen.

Med denna funktion kontrollerar man och styr trafiken på nätet och användarnas tillgång till nätet, varför den ska betraktas som en kritisk del av kommunikationsnätet. Funktionen har också betydelse för upprätthållande av anslutningar, tillgången till tjänster och för att trygga kommunikationens konfidentialitet och hela kommunikationsnätets informationssäkerhet.

Network Slice Specific Authentication and Authorization Function (NSSAAF)

NSSAAF ansvarar för skivspecifik autentisering och auktorisering tillsammans med AAA-servern och AAA-proxyservern.

Med denna funktion kontrollerar man och styr användarnas tillgång till nätet, varför den ska betraktas som en kritisk del av kommunikationsnätet. Funktionen har också en väsentlig betydelse i tillgången till tjänsterna, kommunikationens konfidentialitet och i att trygga informationssäkerheten i hela kommunikationsnätet.

Session Management Function (SMF)

I SMF har man sammankopplat funktioner som har att göra med sessionsadministrationens styrtrafik. SMF ansvarar bland annat för hantering av sessioner enligt nätpolicyn, allokeringen av IP-adresser samt styr sessionsspecifika UPF-funktioner. SFM verkställer också LI-funktioner.

Med denna funktion kontrollerar man och styr trafiken på nätet, varför den ska betraktas som en kritisk del av kommunikationsnätet. Funktionen har också väsentlig betydelse för upprätthållande av anslutningar, tillgången till tjänster och för att trygga kommunikationens konfidentialitet och hela kommunikationsnätets informationssäkerhet.

Security Edge Protection Proxy (SEPP)

SEPP är en proxyserver som stöder döljandet av nätets topologi samt filtrering av meddelanden och övervakning av styrtrafikgränssnitt mellan mobilnät. SEPP fungerar som en tillförlitlig åtkomsthanteringsfunktion gentemot andra datanät (t.ex. IPX-nät i fall av roaming).

Med denna funktion kontrollerar man och styr trafiken på nätet och tillgång till nätet, varför den ska betraktas som en kritisk del av kommunikationsnätet. Funktionen har också väsentlig betydelse för upprätthållande av anslutningar, tillgången till tjänster och för att trygga kommunikationens konfidentialitet och hela kommunikationsnätets informationssäkerhet.

Unstructured Data Storage Function (UDSF)

UDSF är en valfri funktion som övriga nätverksfunktioner kan använda för att lagra och hämta ostrukturerade data. Dylik data kan vara uppgifter som har att göra med till exempel funktionens anslutningar, sessioner eller läge. UDSF kan vara funktionsspecifik eller så kan funktionerna använda en gemensam delad UDSF.

Med denna funktion kontrollerar man och styr trafiken på nätet, varför den ska betraktas som en kritisk del av kommunikationsnätet. Funktionen har också en väsentlig betydelse i tillgången till tjänsterna, kommunikationens konfidentialitet och i att trygga informationssäkerheten i hela kommunikationsnätet.

Unified Data Repository (UDR),

UDR är ett datalager som kan lagra och söka bland annat beställaruppgifter från UDM, policyrelaterade data från PCF samt strukturell data och applikationsdata från NEF. Nätet kan ha flera UDR-funktioner, och UDR kan betjäna antingen enskilda nätfunktioner eller en grupp av nätets funktioner. UDR kan också integreras i en enskild nätverksfunktion.

Med denna funktion kontrollerar man och styr trafiken på nätet, varför den ska betraktas som en kritisk del av kommunikationsnätet. Funktionen har också en väsentlig betydelse i tillgången till tjänsterna, kommunikationens konfidentialitet och i att trygga informationssäkerheten i hela kommunikationsnätet.

UE radio Capability Management Function (UCMF)

UCMF lagrar och förvarar terminalernas apparatidentifikationsspecifika radiokapabiliteter, som fastställs antingen av kommunikationsnätet eller terminaltillverkaren. Sådana radiokapabiliteter är bland annat information om understödda radioteknologier och frekvensband samt om andra radionätsegenskaper. UCMF kommunicerar med AMF genom att ge den dessa uppgifter. UCMF kan också fungera i ett 4G-nät, i vilket fall den kommunicerar med MME.

Uppgifterna i UCMF är inte i sig själva känsliga, men de styr nätets verksamhet. Hotet om att manipulera UCMF:s uppgifter är en så kallade downgrade attack, som man dock kan begränsa med hur nätet verkställs.

Med denna funktion kontrollerar och styr man tillgången till nätet, varför den ska betraktas som en kritisk del av kommunikationsnätet. Funktionen har också väsentlig betydelse för att trygga tillgången till tjänster.

Non-3GPP InterWorking Function (N3IWF)

N3IWF möjliggör tillgång till 5G-kärnnätet genom ett trådlöst lokalt nät (WLAN). N3IWF stöder skapandet av en Ipsec-tunnel med terminalen och auktoriserar användarens tillgång till 5G-kärnnätet. IPSec-tunneln samt N2- och N3-gränssnitten dvs. användar- och styrtrafiken termineras i N3IWF.

Med denna funktion kontrollerar man och styr trafiken på nätet och tillgång till nätet, varför den ska betraktas som en kritisk del av kommunikationsnätet. Funktionen har också väsentlig betydelse för upprätthållande av anslutningar, tillgången till tjänster och för att trygga kommunikationens konfidentialitet och hela kommunikationsnätets informationssäkerhet.

5G-Equipment Identity Register (5G-EIR)

5G-EIR, eller enhetsidentifikationsregistret, är en databas för mobilnätet i vilken man lagrar internationella enhetsidentifikationsuppgifter (IMEI) och som innehåller mobilenhetens tillståndsuppgifter. Normal användning av terminaler på kommunikationsnätet som placerats på 5G-EIR:s svarta lista blockeras.

Med denna funktion kontrollerar man och styr användarnas tillgång till nätet, varför den ska betraktas som en kritisk del av kommunikationsnätet. Funktionen har också väsentlig betydelse för att trygga tillgången till tjänster.

Service Communication Proxy (SCP)

SCP har en viktig roll i 5G genom att förmedla och routa meddelanden till nätets övriga funktioner. Till SCP:s uppgifter hör också bland annat förenklandet av topologin, lastutjämning- och fördelning, hantering av överbelastning och harmonisering av meddelandeparametrarna för att förenkla integreringen i en miljö med flera apparatleverantörer.

Med denna funktion kontrollerar man och styr trafiken på nätet, varför den ska betraktas som en kritisk del av kommunikationsnätet. Funktionen har också väsentlig betydelse för upprätthållande av anslutningar, tillgången till tjänster och för att trygga kommunikationens konfidentialitet och hela kommunikationsnätets informationssäkerhet.

Network Data Analytics Function (NWDAF)

NWDAF betraktas dock inte som en kritisk del av kommunikationsnätet gällande nätets distribuerade funktioner till de delar som de inte kontrollerar eller styr tillgången till nätet eller trafiken på nätet på ett väsentligt sätt.

NWDAF utnyttjar maskininlärning genom att samla in nätverksspecifika data från nätets funktioner och sedan skickar tillbaka data analyserad i realtid till funktionerna. Dessutom producerar NWDAF förutspående analyser, genom vilken man stöder en förebyggande styrning av 5G-nätet. Baserat på den data som NWDAF insamlat kan man till exempel automatiskt skala nätverksinfrastrukturen, välja nätverksskivor eller automatisera åtkomst- och rörlighetshanteringen.

NWDAF är en kritisk del av kommunikationsnätet till den del som den på ett väsentligt vis kontrollerar eller styr tillgången till nätet och trafiken på nätet. NWDAF verkställs distribuerat i nätet, varför data från analysen kan utnyttjas i realtid även på kantnätet.

En centraliserad funktion är även när den är distribuerad alltid en kritisk del av kommunikationsnätet. När den verkställs på ett icke-distribuerat sätt, det vill säga när nätet enbart har en eller flera centraliserade NWDAF, är funktionen alltid kritisk. I detta fall kontrollerar man och styr trafiken på nätet på ett väsentligt vis med funktionen, varför den ska betraktas som en kritisk del av kommunikationsnätet. Funktionen har också väsentlig betydelse för att trygga tillgången till tjänster.

Hur NWDAF verkställs är fortfarande i stor grad öppet och det finns många olika alternativ tillgängliga.[30] Därför kan man inte entydigt utesluta distribuerade NWDAF-funktioner på kantnätet, utan deras kritiskhet fastställs beroende på hur de verkställs och hur väsentlig den enskilda funktionen är. Beroende på hur distribueringen genomförs behöver man inte nödvändigtvis räkna en enskild funktionalitet på kantnätet som hör till NWDAF som en kritisk del av kommunikationsnätet. Det här är möjligt till de delar som den inte kontrollerar eller på ett väsentligt sätt styr tillgången till nätet och trafiken på nätet, till exempel då den enbart påverkar en liten mängd användare eller basstationer.

[30] Eventuella sätt som NWDAF kan genomföras har diskuterats i den tekniska redogörelsen 3GPP TR 23.700-91, Study on enablers for network automation for the 5G System (5GS); Phase 2 (Release 17).

### 6.4. Internationell jämförelse

Fastställning enligt 3GPP:s funktionsbaserade specifikationer har också varit den metod som valts i de länder där Traficom är medveten om att man försökt att tekniskt precisera omfattningen av 5G-nätens kritiska delar, dvs. Frankrike och Storbritannien. Funktionerna som Frankrike och Storbritannien avser är främst definierade i 3rd Generation Partnership Project (3GPP):s tekniska specifikation TS 23.501.

I EU:s gemensamma verktygslåda har man fastställt som kritiska alla kärnnätets funktioner (core network functions).[31] I Storbritannien däremot har man i den nationella cybersäkerhetsmyndighetens anvisning velat fästa teleföretagens uppmärksamhet vad gäller 5G-nätet på funktioner som anses särskilt utsatta för risker. Dessa har fastställts på ett icke-uttömmande vis så att de täcker alla funktioner i 5G-nätets kärna som fastställts i 3GPP TS 23.501. Dessa saker förordar för sin del utgångspunkten enligt denna punkts första underpunkt, enligt vilken funktioner av nätens kärna allmänt betraktas som kommunikationsnätets kritiska delar.

I Frankrike däremot har man genom föreskrift beslutat om tillståndskrav på programvara och utrustning som används för auktorisering av terminaler i femte generations mobilnät, allokering av radioresurser och routning av elektronisk trafik mellan dem eller till tredje parters nät, samt programvara och utrustning som kontrollerar nätens säkerhet, integritet och tillgänglighet. I föreskriften används en mer noggrann definition enligt vilken följande funktioner enligt 3GPP:s specifikationer hör till 5G-nätets kärna:[32] Access and Mobility management Function (AMF); Authentication Server Function (AUSF); User Plane Function (UPF); Session Management Function (SMF); Policy Control Function (PCF); Network Slice Selection Function (NSSF); Network Repository Function (NRF); Network Exposure Function (NEF); Unified Data Management (UDM); Security Edge Protection Proxy (SEPP). Alla de nämnda funktionerna fastställs också här i Traficoms föreskrift som kommunikationsnätets kritiska delar.

Jämfört med Storbritanniens förteckning, som i stor grad täcker alla funktioner som 3GPP fastställt för 5G-kärnnätet, hör åtminstone inte i det första skedet till denna föreskrift Wireline Access Gateway Function (W-AGF) eller Trusted Non-3GPP Gateway Function (TNGF) och Trusted WLAN Interworking Function (TWIF). Denna lösning har motiverats i slutet av punkt 4.1.5. Om teleföretaget eller den separata nätverksaktören tar dessa funktioner i bruk, ska de bedöma hur kritiska funktionerna är direkt utgående från 244 a § 1 mom. i LTEK och punkt 4 i föreskriften.

## 7. Funktioner som stöder tjänster på kantnätet

I den här punkten fastställs ett undantag som kan tillämpas på bedömningen av kritiskheten av funktioner som betjänar styrningen av nätet på kantnätet. Punkten har

[31] Cybersecurity of 5G networks EU Toolbox of risk mitigating measures. CG Publication 01/2020. Bilaga 2, s. 39. https://ec.europa.eu/digital-single-market/en/nis-cooperation-group. Se också EU coordinated risk assessment of the cybersecurity of 5G networks. Report. 9 October 2019, k. 2.21. https://ec.europa.eu/digital-single-market/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security.

[32] Arrêté du 6 décembre 2019 fixant la liste des appareils prévue par l'article L. 34-11 du code des postes et des communications électroniques. https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000039455672. Dessutom täcker föreskriften basstationen, New Radio Base Station (en-gNodeB och gNodeB). Se punkt 4.1.5. om basstationer i denna motiveringspromemoria.

som avsikt att möjliggöra att nätets kärnfunktioner som verkställs lokalt inte betraktas som en kritisk del av kommunikationsnätet, och teleföretaget eller den separata nätverksaktören kan visa att förutsättningarna för undantaget uppfylls.

Enligt denna punkt anses inte som kritiska delar av kommunikationsnätet sådana funktioner och åtgärder av 4G- eller 5G-nät enligt tabell 1 eller 2 om förutsättningarna i punkten uppfylls. Förutsättningarna för att undantaget ska kunna tillämpas är:

- funktionen stöder i huvudsak erbjudandet av andra tjänster än kommunikationstjänster på kantnätet
- funktionen påverkar enbart i liten grad slutanvändaren, terminalen eller basstationerna
- ingen annan trafik förmedlas genom funktionen (dvs. trafik som inte har att göra med erbjudandet av tjänsten som verkställs på kantnätet)
- att kommunikationsnätets kritiska delars funktion är skyddade mot eventuell skadlig trafik genom att tillhandahålla nätens pålitliga skyddsmekanismer.

Eftersom de nätverksfunktioner som här avses enligt föreskriften som utgångspunkt skulle betraktas som kommunikationsnätets kritiska delar, betyder det att teleföretaget eller den separata nätverksaktören som vill dra nytta av undantaget har en plikt att reda ut om huruvida förutsättningarna uppfylls. I punkt 3 av föreskriften förutsätts det att man dokumenterar bedömningen och de skyddsmekanismer som ligger som grund till den.

Enligt punkten skulle undantagsmöjligheten enbart riktas till de kritiska funktioner i 4G- och 5G-nät som fastställts i föreskriftens tabeller 1 och 2. Det skulle alltså inte göra det möjligt att avvika från de gemensamma kritiska delarna för olika nätverk som listats i punkt 4. Därmed är till exempel genomförandet av teleavlyssning och teleövervakning som funktion utan undantag en kritisk del av kommunikationsnätet.

Undantaget kunde tillämpas i olika situationer där man vill producera tjänster i närheten av användaren. Sådana vore åtminstone en kantberäkning som operatören verkställer, med vilket man i det här sammanhanget avser Multi-Access Edge Computing (MEC) samt local breakout, där 5G-nätets trafik styrs till exempel till teleföretagets kundföretags egna interna nätverk direkt på kantnätet. För dessa situationer kan man på kantnätet verkställa till exempel en lokal UPF eller andra av nätets kärnas funktioner. I undantaget handlar det om förutsättningar där funktionens (t.ex. UPF som enligt föreskriften som utgångspunkt ska antas vara kommunikationsnätets kritiska del) kritiskhet kan bedömas annorlunda om den verkställs på ett geografiskt distribuerat sätt utanför det egentliga kärnnätet.

I punkten förutsätts för det första att funktionen stöder i huvudsak erbjudandet av andra tjänster än kommunikationstjänster på kantnätet. Med stöda avser man att funktionen till exempel ska ha något att göra med MEC-verkställandet eller verkställandet av en tjänst som baserar sig på local breakout, på så sätt att funktionen inte hör till kantnätets egentliga funktioner, och alltså inte fungerar som en gemensam funktion för nätets olika funktioner. Tjänster som erbjuds på kantnätet måste handla om andra än kommunikationstjänster, det vill säga till exempel styrning av en fabrik, funktioner som har att göra med teleföretagets affärsverksamhet eller andra motsvarande tjänster som inte är kommunikationstjänster och som används av någon viss grupp användare, och inte gemensamt av alla användare i teleföretagets mobilnät.

Ett kriterium är att det är fråga om en tjänst som produceras i närheten av användaren, men själva nätets kärnfunktion behöver inte verkställas fysiskt i samband med kantberäkningen, förutsatt att den verkställs uttryckligen i detta syfte och alltså inte fungerar som en egentlig del av kärnan. Den kunde placeras till exempel i ett accessnät eller i överföringsnätets knutpunkt.

För det andra får funktionen enbart i liten grad påverka slutanvändaren, terminalen eller basstationerna Den kan alltså inte på det sätt som avses i 244 a § 1 mom. i LTEK på ett väsentligt sätt styra trafiken på nätet, vilket också nästa förutsättning har att göra med.

För det tredje förutsätts det att ingen annan trafik förmedlas genom funktionen, dvs. sådan trafik som inte har att göra med erbjudandet av tjänsten som verkställs på kantnätet, förutom när det gäller erbjudande av kommunikationstjänster. I så fall är det till exempel fråga om en situation där en UPF som omfattas av undantaget enbart styr sådan användartrafik som hanteras för tjänsten som verkställs på kantnätet. Om användaren därtill skulle ha tillgång till nätets övriga tjänster är undantaget inte möjligt, om detta inte verkställs med hjälp av en annan UPF. I praktiken kan det här innebära att de har getts en egen PDU-session, som betjänas av skilda UPF. Beroende på hur det verkställs är det möjligt att en UPF som betjänar användare styr trafiken vidare till en annan UPF och till andra datanät (verkställande av en PDU-session, 3GPP TS 23.501, bild 4.2.3-4), vilket innebär att undantaget inte kan tillämpas.

För det fjärde förutsätts det att kommunikationsnätets kritiska delars funktion är skyddade mot eventuell skadlig trafik genom att tillhandahålla nätens pålitliga skyddsmekanismer. Skyddsmekanismerna ska kunna identifiera och hantera skadlig trafik, t.ex. överbelastningsangrepp och otillåtna accessförsök samt säkerställa att det inte är möjligt att utan auktorisering omdirigera trafik. Skyddsmekanismerna ska alltså säkerställa att funktionerna som stöder tillhandahållandet av tjänster på kantnätet inte kan kontrollera eller styra tillgången till nätet och trafiken på nätet på ett väsentligt sätt.

Dessa skyddsmekanismer kan till exempel verkställas med hjälp av en brandvägg och nätverkssegmentering samt med beredskapen att koppla funktionen ur nätet. Genom dessa kan man garantera att funktioner som stöder tjänster på kantnätet inte trots ett gränssnitt som kommer från nätets egentliga kärna kan påverka den eller andra UPF-funktioner på ett skadligt sätt. Det är inte möjligt i föreskriften att fastställa de mekanismer som man i praktiken kunde garantera detta. Effektiviteten hos de informationssäkerhetskontroller och andra åtgärder som teleföretagen och de separata nätverksaktörerna genomför skulle bedömas som helhet. Med dem ska man kunna avlägsna risken för att man med en funktion på kantnätet kunde få tillgång till det övriga nätet eller kunde styra resten av nätets funktion (särskilt kärnans) på ett väsentligt vis. När man bedömer väsentlighet ska man fästa uppmärksamhet vid om huruvida funktionen har möjlighet att påverka annat än enbart till exempel de uppgifter som behandlas i kantberäkningstjänsten som är i fråga. Man förutsätter dock inte att man med skyddsmekanismerna helt isolerar den funktion som stöder tjänster på kantnätet, eftersom detta inte bedöms vara möjligt med tanke på styrandet av nätet.

## 8. IP-baserade telefonitjänster i mobilnät

Punkten kompletterar föreskriftens övriga delar. Enligt punkten räknas som kommunikationsnätets kritiska tjänster sådana faciliteter och åtgärder som hör till IP Multimedia Core Network Subsystem (IMS) enligt 3GPP:s tekniska specifikation 23.228 genom vilka en allmän IP-baserad telefonitjänst verkställs.

I punkten fastställs som kritiska delar av kommunikationsnätet (IMS) Core till de delar som den används för att verkställa en IP-baserad allmän telefonitjänst.[33] I IP-baserade 4G- och i framtiden 5G-mobilnät verkställs den allmänna taltjänsten med IMS. Den används också för att verkställa andra multimediatjänster i IP-baserade mobilnät. IMS Cores funktioner är i kontakt via gränssnitt med 4G- eller 5G-nätet, och de kan betraktas om en del av nätets kärna.

Enligt 3 § i LTEK avses med allmän telefonitjänst en kommunikationstjänst som gör det möjligt att ringa och ta emot inrikes- och utrikessamtal med nummer som finns i en nationell eller internationell nummerplan.

Utgående från denna punkt kunde IMS Cores kritiska funktioner till exempel vara Call Session Control Function (CSCF), Subscription Locator Function (SLF), Breakout Gateway Control Function (BGCF) och Media Gateway Control Function (MGCF).

Telefonitjänster som baserar sig på IMS Core och som erbjuds i mobilnät är åtminstone VoLTE och VoWifi i 4G-nät. Punkten förutsätter inte att uttryckligen 4G- eller 5G-radionätet skulle utnyttjas i telefonitjänsten, utan terminalen kan också användа till exempel en WiFi-anslutning, förutsatt att det är fråga om en allmän telefonitjänst som teleföretaget erbjuder.

Genom IP-baserade mobilnäts förmedling är det möjligt att verkställa även andra taltjänster, som inte baserar sig på IMS Cores funktioner. I denna punkt i föreskriften föreskrivs inte om dessa andra tjänster, och den eventuella kritiskheten hos deras tillhörande funktioner ska vid behov bedömas på andra grunder.

## Föreskriftens ikraftträdande och övergångstid

Föreskriften träder i kraft den xx månad 2021 och gäller tills vidare. [*Föreskriften ska träda i kraft så snart som möjligt efter remissbehandlingen*].

Identifierings- och dokumenteringsskyldigheten i punkt 3 i föreskriften har en övergångsperiod på 6 månader, inom vilken den förutsedda dokumentationen ska utfärdas. Föreskriftens punkt 3 förutsätter att teleföretag och separata nätverksaktörer ska identifiera och dokumentera sina kommunikationsnäts kritiska delar och de komponenter som används i dem samt att de ska dokumentera sina bedömningar. Det är nödvändigt att ge en tillräcklig övergångsperiod för att kommunikationsnätets kritiska delar och de komponenter som används i dem ska kunna dokumenteras på ett omsorgsfullt sätt. Speciellt i fråga om de största teleföretagen förutsätter skyldigheten att de ska bedöma en betydlig mängd nätverksutrustningar, och detta gäller teleföretagens och de separata nätverksaktörernas alla nät oberoende av teknik. För att kunna uppfylla skyldigheten kan det bli nödvändigt att utveckla informationssystemen, beroende på sättet att genomföra dokumentationen. Övergångsperioden gäller enbart dokumentationen.

[33] IMS Core Reference Architecture, 3GPP TS 23.228.

## Uppföljning

Transport- och kommunikationsverket kommer att regelbundet bedöma behovet att uppdatera föreskriften. Vid bedömningen beaktas eventuella framtida rekommendationer från delegationen för nätsäkerhet, utvecklingen av kommunikationsnätteknologin och genomförandet av näten. I uppföljningen är det möjligt att vid behov utreda om det är nödvändigt att närmare bedöma kritiskhet hos betrodda Wi-Fi-nät eller hos funktioner som möjliggör anslutningar på basis av fasta nät (se kapitel 4.1.5). Det är också möjligt att följa upp hur föreskriften och speciellt den undantagsmöjlighet som finns punkt 7 har tillämpats.

## Källor

### Inhemska myndighetskällor

RP 98/2020 rd. Regeringens proposition till riksdagen med förslag till lagar om ändring av lagen om tjänster inom elektronisk kommunikation och av vissa lagar som har samband med den

Selvitys 5G:n kyberturvallisuudesta. Yhteenveto. Transport- och kommunikationsverket. Traficoms publikationer 14.05.2019. https://www.traficom.fi/fi/ajankohtaista/liikenne-ja-viestintavirasto-julkaisi-selvityksen-5gn-kyberturvallisuudesta

Kommunikationsutskottets betänkande KoUB 16/2020 rd – RP 98/2020 rd

Grundlagsutskottets utlåtande GrUU 35/2020 rd – RP 98/2020 rd

### Europeiska unionens publikationer

Cybersecurity of 5G networks EU Toolbox of risk mitigating measures. CG Publication 01/2020. https://ec.europa.eu/digital-single-market/en/nis-cooperation-group

EU coordinated risk assessment of the cybersecurity of 5G networks. Report. 9 October 2019. https://ec.europa.eu/digital-single-market/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security

ENISA Threat Landscape for 5G Networks. Updated threat assessment for the fifth generation of mobile telecommunications networks (5G). December 2020. https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks

### Utländska myndighetskällor

Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahn. Liste der kritischen Funktionen für öffentliche Telekommunikationsnetze und -dienste mit erhöhtem Gefährdungspotenzial. Utkast 29.4.2020. https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/KatalogSicherheitsanforderungen/ListekritischeFunktionen.pdf

NCSC advice on the use of equipment from high risk vendors in UK telecoms networks. 28.1.2020, uppdaterad 14.7.2020. https://www.ncsc.gov.uk/guidance/ncsc-advice-on-the-use-of-equipment-from-high-risk-vendors-in-uk-telecoms-networks

Nasjonal sikkerhetsmyndiget: Håndbok i skadevurdering. https://nsm.no/regelverk-og-hjelp/veiledere-og-handboker-til-sikkerhetsloven/handbok-i-skadevurdering/om-denne-handboken/)

### Övrigt

3GPP TS 21.905. Vocabulary for 3GPP Specifications. https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=558

3GPP TS 23.002. 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Network architecture (Release 16)

3GPP TS 23.228. 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS); Stage 2 (Release 16)

3GPP TS 23.273. 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 5G System (5GS) Location Services (LCS); Stage 2 (Release 16)

3GPP TS 23.501. 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects System architecture for the 5G System (5GS); Stage 2 (Release 16)

3GPP TR 33.848 V0.5.0 (2019-11). Study on Security Impacts of Virtualisation. https://www.3gpp.org/DynaReport/33848.htm

3GPP TS 36.300. 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2 (Release 15)

3GPP TS 38.300. 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; NR; NR and NG-RAN Overall Description; Stage 2 (Release 15)5G-ACIA: 5G Non-Public Networks for Industrial Scenarios. White Paper. July 2019. 5G Alliance for Connected Industries and Automation. https://www.5g-acia.org/publications/5g-non-public-networks-for-industrial-scenarios-white-paper/

5G-ACIA: 5G Non-Public Networks for Industrial Scenarios. White Paper. July 2019. 5G Alliance for Connected Industries and Automation. https://www.5g-acia.org/publications/5g-non-public-networks-for-industrial-scenarios-white-paper/

GSA: Private LTE & 5G Networks Report. February 2020. Global mobile Suppliers Association. https://gsacom.com/paper/private-lte-5g-networks-report-february-2020/

Ericsson: Critical capabilities for private 5G networks. Ericsson White Paper. December 2019. https://www.ericsson.com/en/reports-and-papers/white-papers/private-5g-networks

Ericsson: 5G migration strategy from EPS to 5G system. 24 February, 2020. https://www.ericsson.com/en/reports-and-papers/ericsson-technology-review/articles/migration-from-eps-to-5gs