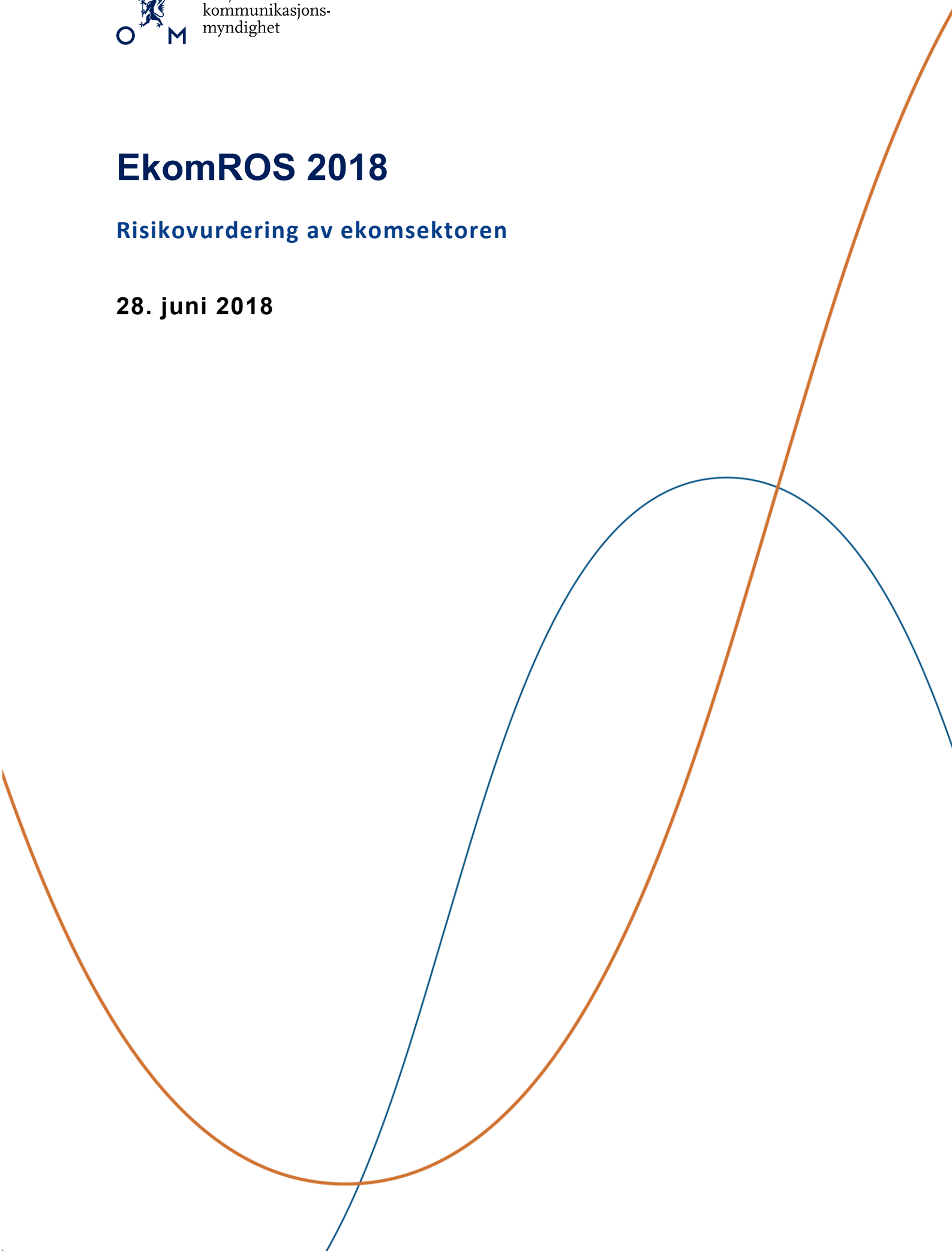
Nasjonal kommunikasjons-myndighet

EkomROS 2018

Risikovurdering av ekomsektoren

28. juni 2018



Forord

De nordiske statsministrene signerte nylig en intensjonsavtale om at Norden skal bli den første og beste sammenkoblede 5G-regionen i verden. En slik ambisjon er et viktig bidrag for å nå målene som er beskrevet i stortingsmeldingen *Digital Agenda for Norge (2016).*

Høsten 2018 er Norge vertsnasjon for den store NATO-øvelsen Trident Juncture. I tillegg til omfattende militær aktivitet med fysiske styrker, fly og fartøyer, vil øvelsen involvere store deler av totalforsvaret, som dermed får anledning til å teste sitt planverk. Bransjen for og myndigheter innen elektronisk kommunikasjon (ekom) er en viktig del av totalforsvaret og vil bli øvd sammen med andre sivile og militære aktører.

Digitalisering for en enklere hverdag og ekomsektorens rolle i den nasjonale forsvarsevnen illustrerer viktigheten av ekomlovens krav til forsvarlig sikkerhet i nett og tjenester i fred, krise og krig.

I desember 2017 besluttet regjeringen at neste generasjon nødnett skal realiseres i de kommersielle mobilnettene. Denne beslutningen medfører at budskapet i fjorårets EkomROS om samfunnets økende avhengighet av mobilnettene, får enda sterkere betydning. Ved å inkludere nødetatenes fremtidige kommunikasjonsbehov i de kommersielle nettene, får disse spesielt viktige brukerne dra nytte av innovasjonen og den raske endringstakten i nettene.

Under et seminar om neste generasjon nødnett i november 2017, uttrykte avdelingsdirektør for IKT-sikkerhet i NSM, Hans Christian Pretorius, at *hastighet* er helt grunnleggende når det gjelder sikkerhet. Historisk sett dreide sikkerhet seg om å tenke de lange tankene og om å gå litt sakte fremover. I fremtiden vil sikkerhetsgevinsten i mye større grad dreie seg om å være delaktig i et utviklingsløp, og å raskt kunne endre seg. Dette oppnår man best ved å benytte de kommersielle nettene.

Ekomsektoren er i kontinuerlig endring. Samtidig som teknologiutviklingen har stor påvirkning på samfunnsutviklingen blant annet gjennom digitalisering, er også samfunns- og markedsutviklingen med å påvirke fremtidige teknologivalg. I tillegg endrer risiko- og trusselbildet seg dynamisk. Å identifisere relevante utviklingstrekk i sektoren er derfor en viktig del av Nkoms overordnede risikovurdering. Nkoms årlige risiko- og sårbarhetsvurdering er et ledd i vårt arbeid med sikkerhet i nett og tjenester der vi ønsker å bidra til høy bevissthet omkring sikkerhet og risiko.

Lillesand, juni 2018
Elisabeth Aarsæther
direktør, Nasjonal kommunikasjonsmyndighet

Sammendrag

Dette er det tredje året Nasjonal kommunikasjonsmyndighet (Nkom) publiserer en risikovurdering av ekomsektoren. Vurderingen bygger på erfaringer fra faktiske hendelser de siste årene, og mer generelle utviklingstrekk av betydning for sektoren.

I perioden som omfatter 2017 og frem til midten av mai 2018 har Nkom registrert 69 hendelser av en viss alvorlighetsgrad. Fiberbrudd er den klart hyppigste feilårsaken, etterfulgt av programvarefeil og utfall av strøm. Agderfylkene hadde store utfall av strøm i forbindelse med kraftig snøvær i januar 2018. For øvrig var det feil i sentrale komponenter i nettene som hadde de største kundekonsekvensene.

Det har vært to alvorlige feilsituasjoner som ikke ble fanget opp av tilbydernes driftsovervåkning, men som først ble avdekket da kundeklagene tok seg opp neste dag. En annen alvorlig hendelse hadde sammenheng med organisatorisk avstand mellom de med ekomteknisk systemkunnskap og IT-driftsmiljøet, med avhengigheter på tvers. Flere alvorlige hendelser hadde med endringshåndtering å gjøre.

Nkom har avdekket flere tilfeller av forstyrrelser av GPS-signaler. Ved to tilfeller har flytrafikken i Finnmark blitt forstyrret av støy østfra. Tidspunktene sammenfaller med kjent militær øvingsaktivitet på russisk side.

Innenfor cybersikkerhet har vi konstatert flere sårbarheter. Én knytter seg til en viktig rutingprotokoll for IP-rutere som knytter nettene sammen globalt. Sårbarheten gjør det mulig å manipulere nettet til å omdirigere trafikk til steder den kan bli avlyttet. Det er en lang og krevende prosess å bøte på sårbarheten og det kan forventes flere forsøk på å utnytte denne.

Et annet fenomen er såkalte «reflective amplification»-angrep som er en teknikk for å øke effekten av tjenestenektangrep med en faktor på mange tusen. Vi har sett eksempler på slike angrep i utlandet som er av en størrelsesordenen som ville påvirke all normaltrafikk hos en typisk norsk ISP.

Årets rapport drøfter tre utviklingstrekk av betydning for de kommende årene:

1) Fremtidens nødnett vil bli realisert i de kommersielle mobilnettene. Arbeidet med tilrettelegging for nød- og beredskapsbrukere i kommersielle nett i Norge vil legge viktige premisser for utviklingen av sikre og robuste mobilnett i fremtiden. Det vil fortsatt være nødvendig med en risikobasert forsterkning av reservestrømkapasiteten i de kommersielle nettene. Samtidig må man vurdere på hvilket nivå det vil være mer kost-/nyttesvarende å rette statlige investeringer direkte mot tiltak i kraftsektoren for å sikre strømforsynings-sikkerheten.

2) Femte generasjon mobilteknologi nærmer seg lansering og vil åpne for mange nye anvendelser. Tingenes internett, IoT, forventes å få en stor vekst i forbindelse med 5G. For å håndtere den økende kompleksiteten i ekomnettene vil kunstig intelligens tas i bruk i økende grad. Siste års hendelser viser at kompleksiteten i ekomnettene og det å klare å detektere og tolke sammensatte feil, er en reell utfordring. For hver generasjon mobilnett oppnås det forbedringer i sikkerhet, men samtidig medfører en mer åpen arkitektur og nye og uforutsette bruksmønstre i 5G nye sårbarheter.

3) Tilbydere av elektronisk kommunikasjon blir i stadig større grad avhengig av utstyrsleverandører og andre underleverandører av tjenester. I en slik setting blir det viktig å sørge for tilstrekkelig kompetanse i egen organisasjon og den nye sikkerhetsloven vil legge føringer for hvordan tilbyderne skal sikre dette.

Vi setter nærmere søkelys på fire risikoområder i rapporten:

- Økt avhengighet til infrastruktur i verdensrommet
- Ekomsektorens betydning for totalforsvaret
- Nødnett i kommersielle nett
- Økt omfang av IoT

Ut fra vurderingen av disse risikoområdene ser Nkom det som viktig å understøtte arbeidet med sikkerhetsspørsmål som gjelder rombasert infrastruktur. Arbeidet koordineres blant annet i romsikkerhetsutvalget, deriblant avklaringene om ansvar og roller i i de delene av romvirksomhetens verdikjeder som angår ekomsektoren.

Når det gjelder risikoer knyttet til den øvre delen av krisespekteret, som krise, konflikt og krig, vil Nkom vise til høstens NATO-øvelse, Trident Juncture. Foruten å øve samhandling på myndighetsnivå, blir det viktig å erfare hvordan overordnede planverk og tiltak for totalforsvaret kan omsettes til treffsikre tiltak i ekomsektoren.

Den stadig økende kompleksiteten i ekomnettene og innføring av kunstig intelligens for å håndtere denne kompleksiteten, vil kreve et høyt nivå av systemkompetanse og sikkerhetsforståelse hos ekomtilbyderne. Dette vil være viktig for å kunne tilby brukerne tjenester med forsvarlig sikkerhet både i normalsituasjoner og i ekstraordinære situasjoner.

Scenarioene vi beskriver som ekstraordinære hendelser i tilknytning til neste generasjon nødnett i kommersielle nett vurderer vi til å representere moderat risiko. Det er imidlertid viktig å understreke at dette forutsetter at de viktigste sikkerhets- og robusthetsutfordringene blir utredet og påbegynt så tidlig som mulig. Den kommende konseptvalgutredningen blir viktig i så måte.

Innholdsfortegnelse

1 Innledning

Tilbydere av elektronisk kommunikasjon (ekom) er pålagt å utarbeide beredskapsplaner og tiltak for å opprettholde forsvarlig sikkerhet i sine nett og -tjenester. Som bakgrunn for slike planer og tiltak skal det gjøres risiko- og sårbarhetsanalyser (ROS). Tilbydernes ROS-vurderinger tar utgangspunkt i egen virksomhet, tjenesteproduksjon og infrastruktur, og gir ikke et overordnet sektorperspektiv. Nkom har derfor behov for å gjennomføre overordnede vurderinger av risiko og sårbarhet for å gi et helhetlig risikobilde av sektoren.

Gjennom året mottar Nkom mange varsler om hendelser i ekomnettene. Når det er behov for nærmere redegjørelse, innhentes mer utførlige rapporter som gir Nkom innsikt i sårbarheter og årsakssammenhenger. Gjennom det løpende forvaltningsarbeidet, samarbeidet med aktørene i sektoren og i tilsynsarbeidet, opparbeider Nkom oversikt over de ulike tilbydernes nett- og tjenestetopologi og utviklingsplaner. Dette skaper et viktig fundament for Nkoms risikovurderinger.

1. juli 2017 ble EkomCERT etablert hos Nkom. Dette responsmiljøet er først og fremst etablert for å bidra til deling av informasjon i sektoren, gi råd og koordinere tiltak. Gjennom nettverket til EkomCERT, får Nkom informasjon om sårbarheter, trusler og hendelser i det digitale domenet, noe som er et vikitg bidrag ut over den informasjonen vi tidligere hadde tilgang til i ROS-vurderingen.

Nkom har også utstrakt samarbeid med andre sektormyndigheter, med regionale myndigheter, og andre totalforsvarsaktører. Dette samarbeidet bidrar til å skape en forståelse av rollen som elektronisk kommunikasjon spiller både for samfunnssikkerheten og statssikkerheten, og hvilke samfunnskonsekvenser brudd på nett og -tjenesters tilgjengelighet, konfidensialitet og integritet kan ha.

I kapittel 2 omtales hendelser og sårbarheter vi har fått kunnskap om i året som har gått, mens vi i kapittel 3 ser fremover og drøfter betydningen av relevante utviklingstrekk i sektoren. Sammen med det generelle trusselbildet i samfunnet, danner dette grunnlag for å identifisere viktige risikoområder. I første del av kapittel 4 gjengir vi trekk fra de nasjonale trusselvurderingene, før vi i andre del utforsker potensielle uønskede hendelser (scenarioer) innenfor de identifiserte risikoområdene.

2 Erfaringer fra 2017

2.1 Hendelsesstatistikk

Ekomtilbyderne varsler rutinemessig Nkoms beredskapsvakt ved utfall, systemsvikt eller andre hendelser som påvirker elektroniske kommunikasjonsnett og -tjenester. Nkom videreformidler relevant informasjon til andre etater og beredskapsaktører på regionalt og nasjonalt nivå, og vurderer eventuelle tiltak basert på omfang og alvorlighetsgrad. Nkom registrerer uønskede hendelser for å sikre sporbarhet og oppfølging. Følgende oversikt tar utgangspunkt i hendelser over en viss alvorlighetsgrad registrert av Nkom i perioden 1. januar 2017 - 16. mai 2018. Metoden i årets utgave av EkomROS skiller seg fra metoden benyttet i tidligere utgaver, og antall hendelser er nå noe lavere. Det tilgjengelige datagrunnlaget gir nå en samlet oversikt over antall registrerte hendelser, alvorlighetsgrad, tidspunkt for hendelsen, og type feil/årsak, samt en beskrivelse av hendelsen.

2.1.1 Antall hendelser og alvorlighetsgrad for hele perioden

For perioden 1. januar 2017 – 16. mai 2018 har Nkom registrert 69 uønskede hendelser av en slik alvorlighetsgrad at de har medført oppfølging fra Nkom. Alvorlighetsgraden ved uønskede hendelser kategoriseres etter beredskapsnivå. Ved NORMAL overvåker Nkom situasjonen. Nivået GRØNN krever økt beredskap og tettere oppfølging. Nivåene ORANSJE og RØD krever høyere beredskap og aktiv krisehåndtering. For hele perioden har Nkom registrert 25 hendelser som NORMAL, 43 hendelser som GRØNN og én hendelse som ORANSJE. Ingen hendelser ble registrert som RØD.

Hendelser fordelt på alvorlighetsgrad for hele perioden 1. januar 2017 – 16. mai 2018		
År	**Alvorlighetsgrad**	**Antall uønskede hendelser**
2017	NORMAL	21
	GRØNN	25
	ORANSJE	0
	RØD	0
Første halvår 2018	NORMAL	4
	GRØNN	18
	ORANSJE	1
	RØD	0
	Totalt	**69**

Tabell 1. Antall hendelser fordelt på alvorlighetsgrad.

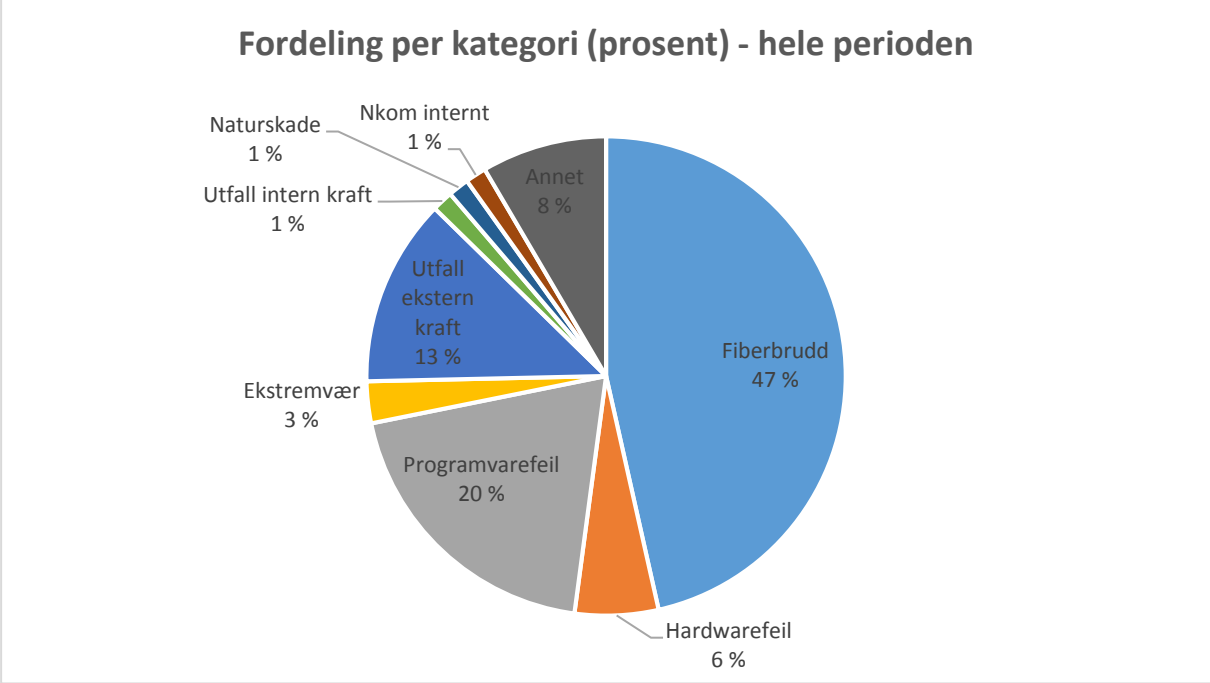
2.1.2 Hendelser fordelt per kategori

Hendelser er her inndelt i kategorier med hensyn til type feil/årsak. De ni kategoriene er som følger:

Kategori	Betydning
Fiberbrudd	Fysisk brudd på fiberoptiske kabler, for eksempel brudd i forbindelse med gravearbeid eller slitasje
Hardwarefeil	Feil i kritiske systemkomponenter, for eksempel gammelt utstyr, overbelastning eller fysiske skader i forbindelse med planlagt arbeid eller oppgraderinger
Programvarefeil	Logiske feil i kritisk programvare, for eksempel i forbindelse med programvareoppdateringer eller andre endringer
Ekstremvær	Utfall eller redusert redundans som følge av ekstremvær
Utfall ekstern kraft	Utfall eller redusert redundans som følger av svikt i ekstern kraftforsyning til kritiske komponenter, for eksempel strøm til basestasjoner
Utfall intern kraft	Utfall eller redusert redundans knyttet til feil i intern kraftforsyning, for eksempel svikt i batteribanker
Naturskade	Utfall eller redusert redundans som følge av naturskader på systemkomponenter som ikke karakteriseres som ekstremvær, for eksempel lynnedslag eller vårflom
Nkom internt	Uønskede hendelser internt i Nkom som påvirker Nkoms håndteringsevne, for eksempel svikt i interne informasjons- og kommunikasjonssystemer
Annet	Samlebetegnelse for uønskede hendelser som ikke faller inn under de øvrige kategoriene, for eksempel frekvensforstyrrelser eller tilsiktede hendelser

Datagrunnlaget for hele perioden viser at fiberbrudd og programvarefeil utgjør de vanligste årsakene til utfall totalt sett. Omtrent 67 % av tilfellene faller inn under disse to kategoriene. Fiberbrudd utgjør alene omtrent 47 % av tilfellene. Selv om fiberbrudd er en viktig årsak, er likevel programvarefeil ofte en mer alvorlig feil. Fiberbrudd medfører som regel lokale utfall som er begrenset i omfang, og rettetiden er med noen viktige unntak relativt kort. Alvorlige programvarefeil, på den annen side, kan gjerne forårsake landsdekkende utfall. Det samme gjelder hardwarefeil. Hardwarefeil er riktignok relativt sjeldne med kun fire tilfeller i hele perioden, men hardwarefeilene som oppstår får som regel store konsekvenser.

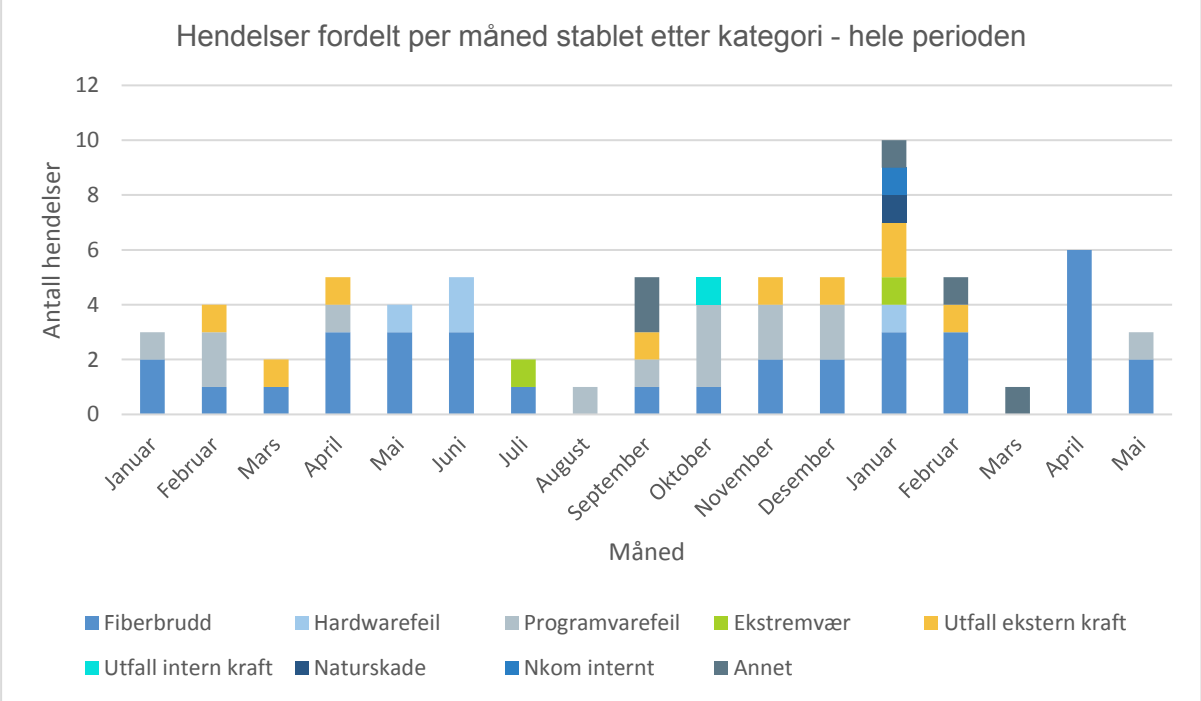
Ni tilfeller gjelder svikt i ekstern kraftforsyning. Nkom har de siste årene gjennomført tiltak for å øke reservestrømkapasiteten på basestasjoner gjennom programmet for forsterket ekom og vedtak om minstekrav til reservestrøm i mobilnett. Totalt fem hendelser er registrert under kategorien «*Annet*». To av disse gjelder forstyrrelser på GPS-signaler, ett tilfelle gjelder frekvensforstyrrelser/støy på maritim VHF kanal 16 for nødkommunikasjon til sjøs, ett tilfelle gjelder mangelfulle endringsrutiner i forbindelse med planlagt arbeid, og ett tilfelle gjelder økt beredskap i forbindelse med en mobiloperatørs flytting av kritiske kjernenettkomponenter (dette utløste ingen feilsituasjon).



Figur 1. Hendelser fordelt på type feil/årsak.

2.1.3 Månedsvis fordeling

Den månedlige oversikten viser hvordan ulike typer hendelser fordeler seg gjennom hele perioden fra januar 2017 og ut i første halvår 2018. Oversikten viser en relativt jevn fordeling, med i hovedsak mellom to og fem hendelser per måned gjennom 2017. Fiberbrudd og programvarefeil er også relativt jevnt fordelt gjennom året.



Figur 2. Hendelser fordelt per måned stablet etter kategori.

Oversikten viser samtidig en betydelig økning i antall registrerte hendelser i januar 2018. Dette er knyttet til en rekke sammenfallende hendelser. Snøværet i Agderfylkene i januar medførte store utfordringer for kraftforsyningen på Sørlandet, og ekom ble også påvirket. Det kraftige snøfallet medførte fiberbrudd og svikt i kraftforsyningen flere steder. Snøen medførte også relativt lang rettetid.

2.2 Hendelser rapportert til ENISA

Enkelte hendelser med betydning for nettverks- og informasjonssikkerhet rapporteres rutinemessig videre til EUs byrå for nettverks- og informasjonssikkerhet (European Union Agency for Network and Information Security - ENISA). ENISA har som hovedformål å styrke nettverks- og informasjonssikkerheten i EU. ENISA bistår blant annet Europakommisjonen, de øvrige EU-byråene og medlemsstatene i spørsmål knyttet til den videre utviklingen av europeisk regulering på nettverks- og informasjonssikkerhetsfeltet. Norge er tilknyttet byrået og har observatørstatus i byråets styre. For 2017 har Nkom rapportert tre hendelser til ENISA.

2.2.1 Hardwarefeil medførte bortfall av mobile datatjenester

I mai 2017 mistet kunder hos en norsk mobiltilbyder tilgang til datatjenester som følge av en hardware-feil. Feilen oppstod om kvelden 11. mai, men ble først oppdaget etter et større antall kundeklager om morgenen 12. mai. Systemovervåkningen viste at 20 % av mobil datatrafikk over 4G/LTE falt ut. Feilsøk viste at feilen var knyttet til en eldre ruter på en kjernenettlokasjon. Det var allerede planlagt å skifte ut den eldre ruteren, men dette var foreløpig ikke iverksatt.

Hendelsen ble håndtert ved at trafikken ble rutet om via en alternativ ruter på en annen kjernenettlokasjon. Feilen ble rettet i løpet av en times tid, men kundene hadde på dette tidspunktet opplevd problemer i rundt 12 timer.

Nkom bemerket i etterkant av hendelsen at varsler og hendelsesrapport fra ekomtilbyderen var mangelfulle. Tekniske feil på kjernenettlokasjoner er blant de viktigste årsakene til de mest alvorlige utfallene. Nkom presiserte derfor viktigheten av å gi utfyllende og presis informasjon i varsler til myndighetene. Samtidig observerer Nkom at det er en stor utfordring å oppdage feilsituasjoner med uklare årsakssammenhenger i stadig mer komplekse systemer med vidtrekkende avhengigheter.

2.2.2 Utfall etter uautorisert endring av programvare

I november 2017 medførte en endring i programvare totalt utfall i tale- og meldingstjenester hos en norsk mobiltilbyder. Endringen ble utført av en underleverandør og var verken varslet eller godkjent hos driftsmiljøet i henhold til endringsrutinene. Endringen påvirket kritisk programvare på en kjernenettlokasjon. Programvaren det gjelder benyttes for å sette opp samtaler og sende meldinger ved å fastslå hvilken operatør et nummer tilhører. Dette er en sentral funksjon på serverne i tilbyderens kjernenettinfrastruktur. Endringen medførte utfall i

tale- og meldings-tjenester i et tidsrom på omtrent 3 timer og 15 minutter. Datatjenester fungerte i mellomtiden som normalt. Nødnummer ble ikke påvirket.

Nkoms undersøkelser av årsakssammenhengene viste at feilen var knyttet til ansvars-fordelingen mellom virksomhetens IT-miljø og det ekomtekniske driftsmiljøet. Enkelte applikasjoner håndteres av IT-miljøet, mens andre applikasjoner håndteres av det ekomtekniske driftsmiljøet. Enkelte virtualiserte produksjonssystemer er et delt ansvar. Endringen det her gjelder ble utført på oppdrag fra IT-miljøet, men programvaren som ble påvirket var driftsmiljøets ansvar. Endringen skulle dermed ha vært godkjent i driftsmiljøet gjennom en skriftlig forespørsel før iverksettelse i henhold til endringsrutinene. Virksomheten var kjent med avhengighetene mellom miljøene. I dette tilfellet ble rutinene ikke fulgt.

I etterkant av hendelsen har mobiloperatøren gjort en ny vurdering av endringsrutinene og iverksatt tiltak for å skille produksjonssystemene i større grad for å redusere risiko. I forbindelse med dette har man vurdert avhengighetene og ansvarsfordelingen på nytt. Generelt er avstanden og ansvarsfordelingen mellom systemkompetanse og driftsmiljø en utfordring som krever klare endringsrutiner og god oversikt over avhengigheter på tvers av organisasjonen.

2.2.3 Programvareoppdatering medførte ustabilitet i taletjenester via 2G og 3G

I november 2017 medførte en rutinemessig oppdatering på en kjernenettserver ustabilitet i 2G og 3G hos en norsk mobiltilbyder, da oppdateringsprosessen stoppet opp før den ble fullført. Som en konsekvens ble oppslag mot abonnentsdatabasen stoppet. Overvåkningssystemene fanget ikke opp feilsituasjonen. Om morgenen dagen etter mottok tilbyderen et større antall kundeklager. En gjennomgang viste at berørte kundene var geografisk spredt over hele landet.

Som en konsekvens av feilen mistet rundt 10 % av tilbyderens kunder mulighet til å opprette samtaler. Kundene kunne fortsatt motta samtaler. Tale via 4G/LTE og nødanrop var ikke berørt. Tilbyderen identifiserte feilen og omstartet oppdateringsprosessen på serveren. I etterkant har tilbyderen innført rutiner som gjør det mulig å oppdage tilsvarende feil på operasjonssenteret. Denne hendelsen viser igjen hvordan stadig mer komplekse systemer med vidtrekkende avhengigheter og komplekse årsakssammenhenger gjør det utfordrende å oppdage feilsituasjoner i tide.

2.3 Frekvensforstyrrelser

Nkom gjennomfører tilsyn og kontrollerer at frekvensbruk skjer i overenstemmelse med de forpliktelser som følger av frekvenstillatelser og annet regelverk, herunder deknings- og utbyggingskrav, krav til utstrålt effekt mv. Stedlige tilsyn gjennomføres som følge av klage fra aktører, ved planlagte målekampanjer og ved generell kontroll av frekvensspekteret via fjernstyrte målestasjoner og målebiler.

Blant annet håndterte Nkom 130 saker tilknyttet forstyrrelser av basestasjoner for mobiltelefoni. Sakene omfattet alt fra lette forstyrrelser til blokkering av basestasjoner hvorav alle kom fra utilsiktede støykilder. 120 av disse sakene ble identifisert som følge av klager fra operatører. Støykildene var typisk utstyr med feil eller mangler som danner forstyrrende støysignal. Nkom har sett flere eksempler på at slik støy kommer fra kilder som defekte elektroniske kjørebøker, fjernkontroller osv.

De siste årene har fokuset på samfunnets avhengighet av satelittnavigasjonstjenester økt. Dette har i løpet av 2017 og så langt i 2018 blitt eksemplifisert i fire hendelser. Nkom har målt støysignaler som har ført til bortfall eller forstyrrelser av GPS-signaler for flytrafikk i områder i Finnmark. Støysignaler kan være utilsiktet stråling ved feil på utsyr, men det kan også være at støyen er laget for å forstyrre signaler – det vil si jamming.

Figur 3. Nkom foretok målinger fra helikopter i Kirkenes i september 2017.

I september 2017 ble Nkom anmodet om å utføre målinger i Kirkenes grunnet forstyrrelser på GPS-signaler for fly på strekningen mellom Alta og Kirkenes. Nkom detekterte da støysignaler fra øst. I en artikkel publisert på NRKs nettsider 5. oktober, ble det langt på vei konkludert med at hendelsen hadde sammenheng med en øvelse gjennomført på russisk side av grensen[1]. Nkom ble også orientert om en liknende hendelse i mars 2018. På bakgrunn av informasjon fra Forsvaret besluttet Nkom å ikke utføre nye målinger. Dette var begrunnet i likhetstrekkene med hendelsen i september.

Ved de to andre hendelsene har defekte elektroniske kjørebøker skapt støysignaler som har medført forstyrrelser og nedetid på GPS-signaler. I den ene hendelsen fikk ikke ambulansehelikopteret med base i Ål avlest GPS-posisjon på sitt navigasjonsutstyr. Den elektroniske kjøreboken som forårsaket støyen var lokalisert 150 meter unna helikopterets base. Det samme skjedde også for ferjen mellom Sandvikvåg og Halhjem. I dette tilfellet ble den defekte kjøreboken lokalisert i et område omkring 500 meter unna ferjekaien.

[1] Kilde: NRK.no (https://www.nrk.no/finnmark/stoy-fra-russland-slo-ut-gps-signaler-for-norske-fly-1.13720305)

I løpet av året har Nkom i tillegg avdekket en rekke forstyrrelser på andre tjenester med samfunnskritisk betydning. For eksempel har både nødkanal 16 til sjøs, værradar tilhørende meteorologisk institutt, Nødnett og Sikringsradioen alle blitt utsatt for forstyrrelser.

2.4 Cybersikkerhet

Det har vært en jevn strøm av cyberhendelser i perioden som denne rapporten dekker. Noen av disse utgjør en trussel for ekominfrastruktur. Vi har valgt ut to eksempler under som har fått mye oppmerksomhet både nasjonalt og internasjonalt i 2017 og inn i første halvår 2018. Disse er BGP hijacking og Memcached-basert DDoS.

2.4.1 BGP hijacking

Border Gateway Control (BGP) er en viktig rutingprotokoll som sørger for at IP-adresser tilknyttet de forskjellige nettene som utgjør internett kan nå og kommunisere med hverandre. IP-adresser annonseres i et globalt nettverk av BGP-rutere med informasjon om hvordan IP-adresser kan nås. Dette utføres av IP-adressenes eier, for eksempel en ISP. BGP er med andre ord en helt grunnleggende rutingprotokoll som sørger for Internetts funksjonalitet.

Annonsering av IP-adresser har historisk sett vært bygget på tillit. Det finnes få mekanismer for å undersøke og bekrefte at en annonsering av IP-adresse samsvarer med eierskap. BGP hijacking går ut på at en aktør i det globale BGP-nettet annonserer IP-adresser de ikke eier, og som dermed kan omdirigere trafikk til disse adressene. Slik kan trafikken havne på feil hender. BGP hijacking kan skje både utilsiktet, ved feilkonfigurasjon av en BGP-ruter, eller tilsiktet, for eksempel med mål om å få tilgang til andres kommunikasjon. Denne formen for trafikkmanipulering kan utnyttes for å få innsikt i innholdet i trafikken, manipulere innholdet eller sørge for at den ikke når frem til riktig mottaker.

I 2017 og 2018 har man sett flere eksempler på at kriminelle aktører har lykkes med BGP hijacking. Symantec, MasterCard og Visa er blant dem som ble rammet i 2017 da trafikken til disse sidene ble rutet gjennom en russisk-kontrollert ISP. Mye tyder på at dette var en tilsiktet handling. Google, Facebook, Apple og Microsoft er andre eksempler på store virksomheter som har fått sin trafikk rutet gjennom Russland.

Flere tiltak kan iverksettes for å øke sikkerheten rundt BGP. Blant annet kan man, ved hjelp av autentiseringsnøkler, forsikre seg om eierskap ved annonsering av IP-adresser. Dette vil bidra til å hindre uvedkommende fra å påvirke trafikken, men man er avhengig av at alle parter signerer og verifiserer annonsering av IP-adresser. Iverksettelsen av dette er påbegynt hos utstyrsleverandører, ISPer og eksterne aktører som drifter infrastruktur, men det vil være en langvarig prosess. I tillegg er flere aktører bekymret for hvordan dette vil kunne påvirke

stabiliteten i det globale ruter-nettet med hensyn til nye driftsrutiner og avhengigheter mot eksterne systemer.

2.4.2 Memcached-basert DDoS

Memcached er en tjeneste for midlertidig minnelagring av data og objekter som typisk benyttes for å øke ytelsen til dynamiske webapplikasjoner eller for å lette last på databasekall. Memcached er brukt av tusenvis av nettsteder, inkludert for eksempel Facebook, Twitter, YouTube, Github og Flickr.

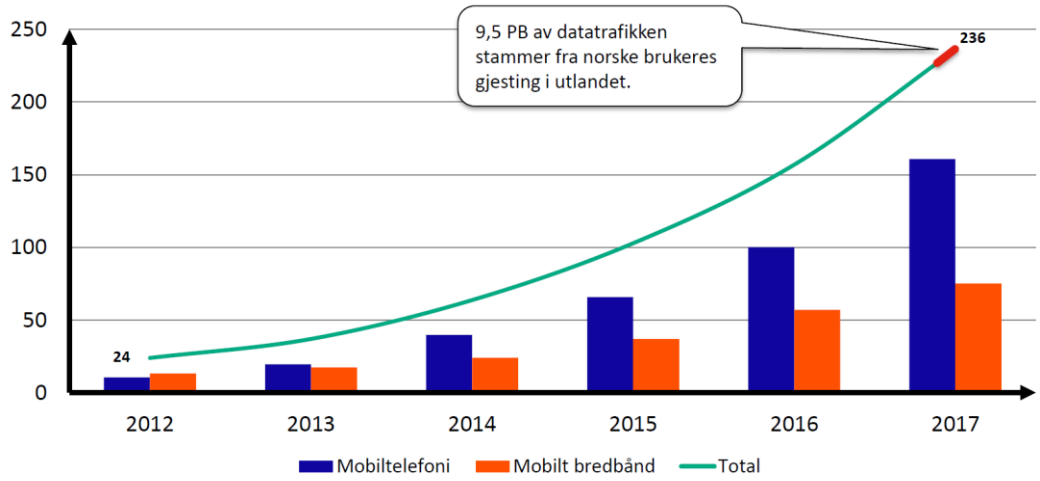
I konstruksjonen av Memcached foreligger det en sårbarhet som kan utnyttes for å utføre forsterkede DDoS-angrep, såkalt DDoS «reflective amplification»-angrep. For å utnyttes slik må Memcached samtidig være eksponert på internett. DDoS «reflective amplification»-angrep utføres ved at en angriper forfalsker sin avsenderadresse og utgir seg for å være adressen til målet man ønsker å angripe. Forespørsler med forfalsket avsenderadresse sendes til åpent tilgjengelige tjenester som DNS, NTP eller Memcached. Tjenestene vil sende svar tilbake til oppgitt avsenderadresse i stedet for angripers faktiske adresse. Forsterkningsfaktoren i angrepene er bestemt av forholdet mellom hvor mye data som sendes i en forespørsel og hvor mye data som sendes tilbake. Mengden trafikk som kommer til målet vil da gjerne overstige tilgjengelig kapasitet og kan føre til at legitim, ordinær trafikk ikke slipper gjennom.

Memcached-baserte DDoS «reflective amplification»-angrep skiller seg ut ved at forsterkningsfaktoren er flere ordenstørrelser større enn angrep som har vært observert tidligere. 28. februar 2018 ble GitHub utsatt for et stort memcached-basert DDoS-angrep. Det ble da sendt data med 1,3 terrabyte per sekund mot GitHubs servere. Forsterkningsfaktoren i dette angrepet var 1:51 000. Med andre ord ble GitHub truffet av 51 kB for hver byte angriperne sendte til Memcached-serverne. En uke senere rapporterte nettverksovervåkingstjenesten Netscout Arbor om et angrep mot en bedrift hos en amerikansk ISP som opplevde et angrep på 1.7 TB. Dette angrepet var nesten tre ganger større enn angrep man tidligere har observert. Størrelsesordenen er av en slik grad at det vil kunne påvirke all normaltrafikk hos en typisk norsk ISP. Forsterkningsfaktoren i Memcached-baserte angrep gjør denne type angrep attraktive og de vil kunne bli mer utbredt. Historisk sett har patching/lukking av sårbarheter gått sakte og det er forventet at Memcached-baserte angrep vil være en reell trussel en stund fremover.

3 Utviklingstrekk de kommende år

Den samfunnsmessige, teknologiske og markedsmessige utviklingen har stor påvirkning på hvordan sårbarhetene i ekomnett og –tjenester vil endre seg de kommende årene. Å identifisiere relevante utviklingstrekk i sektoren er derfor en viktig del av en overordnet risikovurdering.

I EkomROS 2017 fokuserte Nkom særlig på mobilnettene som sentral del av verdikjeden i stadig flere viktige samfunnsfunksjoner. Utviklingen det siste året gjør at det er ingen grunn til å underspille viktigheten av mobilnettene når vi på ny skuer noen år frem i tid.



Figur 4. Det har vært en eksponentiell økning i datatrafikk i mobilnettene siden 2012. Mobilnettene blir en stadig viktigere kommunikasjonsplattform. Trafikken er oppgitt i 1000 MB.

I tillegg ser Nkom grunn til å følge tett hvordan sikkerhet og robusthet ivaretas når norske ekomnett og –tjenester skal adoptere 5G-teknologier og håndtere en massiv økning i tingenes internett og, i sammenheng med denne utviklingen, hvordan et forsvarlig kompetansenivå skal sikres hos de norske tilbyderne.

3.1 Fremtidens nød- og beredskapstjenester i kommersielle mobilnett

Dagens Nødnett, som eies og forvaltes av Direktoratet for samfunnssikkerhet og beredskap (DSB), tilbyr kommunikasjonstjenester til nød- og beredskapsaktørene i Norge. I tillegg til taletjenester har nød- og beredskapsetatene også et økende behov for mobile bredbåndstjenester til kritisk bruk, som ikke kan tilbys gjennom dagens Nødnett. Det er derfor behov for å finne en løsning for neste generasjon nødnett som kan tilby mobile bredbåndstjenester. En ny løsning for nød- og beredskapsaktørene bør være på plass innen 2026, da statens driftskontrakt for Nødnett utløper.

I desember 2017 besluttet regjeringen at 2 x 30 MHz i 700 MHz-båndet, som i dag benyttes til digital TV-kringkasting, skal tildeles *kommersielle* aktører innen første halvdel av 2019 for bruk til mobile tjenester. Ettersom frekvensressurser i 700 MHz-båndet ville være sentrale dersom det skulle bygges et nytt *dedikert* nødnett, innebærer beslutningen at fremtidens nød- og beredskapstjenester vil realiseres i de kommersielle mobilnettene. Beslutningen ble tatt blant annet på bakgrunn av en grundig samfunnsøkonomisk analyse[2], og dette retningsvalget var støttet av fagmyndighetene både på justissiden og ekomsiden[3].

Sentrale utfordringer de neste årene vil være å finne løsninger for neste generasjon nødkommunikasjon som tilfredsstiller behovene for dekning, funksjonalitet, sikkerhet og robusthet. Dagens TETRA-baserte Nødnett og de kommersielle LTE (4G)-nettene kommer fra forskjellige «verdener», med ulik mobilteknologi, ulik infrastruktur og nett-topologi, og med ulike driftskonsepter. Det er derfor ikke hensiktsmessig å ta «blåkopi» av kravene fra dagens Nødnett, og fremsette disse for å løse fremtidens nød- og beredskapstjenester i kommersielle nett.


Frykter flere nye strømbrudd

Agder Energi ber fredag abonnentene forberede seg nye strømbrudd. I innlandet har det i løpet av et døgn falt opptil en halv meter tung nysnø.

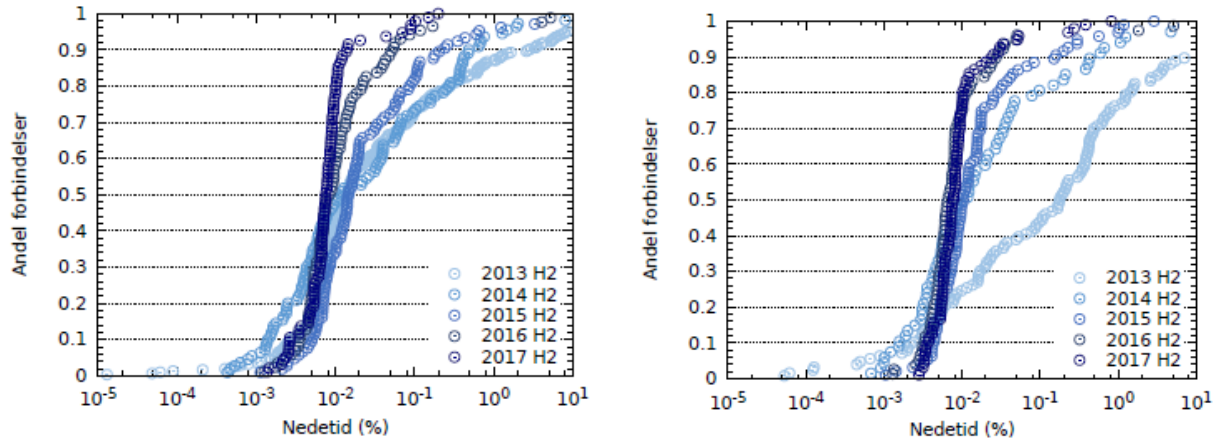
Figur 5. Nye langvarige strømbrudd på Agder vinteren 2018 som følge av snøvær. Utfallene rammet både Nødnett og de kommersielle mobilnettene (utklipp: fvn.no).

Det kan argumenteres for at robusthetsnivået i de kommersielle mobilnettene er lavere enn i dagens Nødnett. Reservestrømkapasiteten og de doble transmisjonslinjene til alle basestasjoner i Nødnett, finner man ikke i samme grad i de kommersielle mobilnettene i dag. Men det å uten videre for eksempel utøke reservestrømkapasiteten i de kommersielle mobilnettene til samme nivå som dagens Nødnett (basert på batterier og aggregater på basestasjoner) vil ha både praktiske utfordringer og innebære svært høye kostnader, som staten langt på vei i tilfelle er forventet å dekke. For det første er det en langt høyere tetthet av basestasjonslokasjoner i de kommersielle nettene. For det andre er mange av dem plassert på husvegger og -tak som ikke uten videre egner seg for store batteripakker og aggregater. Det vil utvilsomt være nødvendig med en risikobasert forsterking av reservestrømkapasiteten i de kommersielle nettene. Samtidig vil man også komme til et nivå hvor det vil være mer kost-/nyttesvarende å rette statlige investeringer direkte mot kraftsektoren for å sikre strømforsyningssikkerheten.

[2] «Anvendelse av 700 MHz-båndet – samfunnsøkonomisk analyse», Nexia Management Consulting, Menon Economics, februar 2017

[3] «Neste generasjon nødnett i kommersielle nett – fremgangsmåte for videre arbeid», Notat utarbeidet i fellesskap av DSB og Nkom

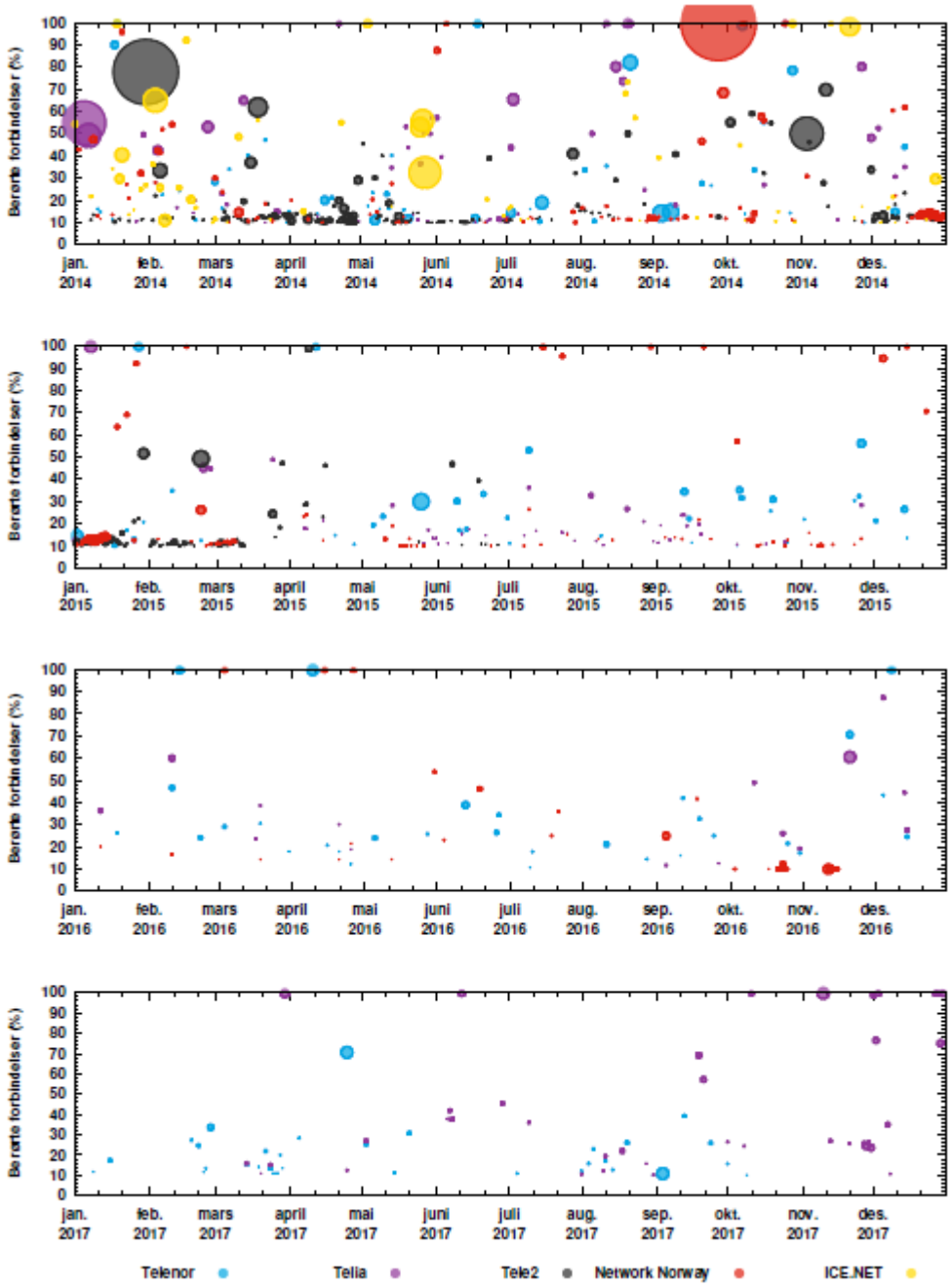
En klar fordel med å implementere løsninger for nød- og beredskapsbrukere i de kommersielle mobilnettene, er at de kan ta del i den generelle teknologi-, nett- og tjenesteutviklingen. Av den samlede omsetningen av ekomtjenester i 2017 på 34,4 milliarder kroner, gikk over 9,7 milliarder kroner tilbake til investeringer i sektoren. Dette er 28 % av sluttbrukeromsetningen. Av disse gikk ca. 4,6 milliarder til utbygging av fibernett mens ca. 2,4 milliarder gikk til mobilnettene. Over tid utgjør disse reinvesteringene til videreutvikling av nett og tjenester en vesentlig sikkerhets- og robusthetsgevinst. Det er vanskelig å se for seg at et dedikert, statlig finansiert nett ville være i stand til å opprettholde en tilsvarende endringstakt som de kommersielle nettene.



Figur 6. Ved hjelp av målenoder har forskningsinstitusjonen Simula målt en stadig økning i stabiliteten i mobilnettene siden 2013. Telenor mobil til venstre og Telia til høyre. Hvert målepunkts nedetid er representert ved en sirkel, og kurven representerer dermed fordelingen av nedetid på målepunktene. En stadig brattere kurve viser økt stabilitet totalt sett. Kilde: «Norske mobilnett 2017», Simula.

Prosessen fremover er imidlertid langt fra fri for utfordringer. Dette har man blant annet erfart i Storbritannia, hvor man nå er midt i utrullingen av *Emergency Services Network (ESN)*, som skal leveres over det kommersielle mobilnettet til operatøren EE. Prosjektet har den siste tiden vært preget av både kostnadsoverskridelser og forsinkelser.

DSB og Nkom mener imidlertid at nød- og beredskapsbrukerens behov kan bli ivaretatt gjennom en kombinasjon av å bruke regulatoriske virkemidler og kommersielle anskaffelser. DSBs spørring i markedet, en såkalt RFI-prosess (Request for information) som ble gjennomført i begynnelsen av 2018, viser også at de kommersielle mobiloperatørene har en egeninteresse i å tilby nød- og beredskapstjenester. Nkom skal det neste halvannet år bistå DSB i konseptvalgutredningene som skal lede frem til en hensiktsmessig modell for fremtidens nød- og beredskapstjenester i kommersielle mobilnett.

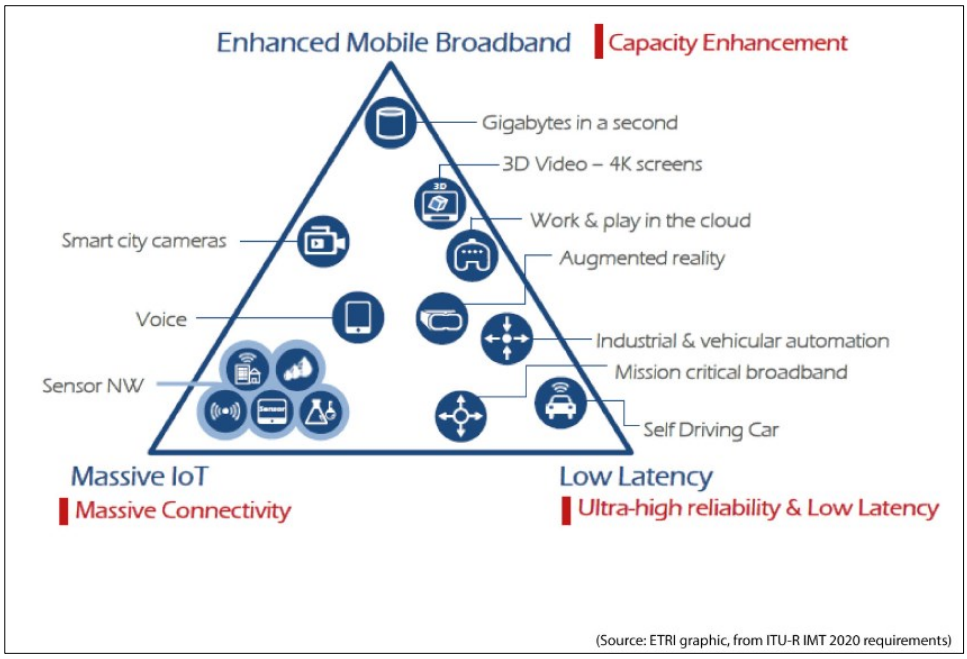


Figur 7. Hendelser med stort pakketap 2014-2017 målt fra Simulas målenoder. Sirkelens diameter representerer alvorlighetsgraden til hendelsen og kan forstås som det totale volumet av trafikk som gikk tapt. Det har vært en positiv utvikling de siste år med færre hendelser med store pakketap. Kilde: «Norske mobilnett 2017», Simula.

Arbeidet med tilrettelegging for nød- og beredskapsbrukere i kommersielle nett vil legge viktige premisser for utviklingen av sikre og robuste mobilnett i fremtiden. Dette vil komme alle mobilbrukerne i det norske samfunnet til gode.

3.2 Nye muligheter og utfordringer med 5G og IoT

Begrepene 5G, IoT og kunstig intelligens kommer frem i stadig flere sammenhenger. Overordnet handler 5G om å kunne møte tre ulike kravkategorier; høye båndbredder for video og kunstig/utvidet virkelighet, massiv maskin-til-maskin-kommunikasjon med lavt batteriforbruk for IoT, og lav responstid og høy sikkerhet for kritiske applikasjoner som for eksempel selvkjørende biler.



Figur 8. Ett og samme 5G-nett skal kunne tilfredsstille svært ulike krav innenfor tre brukerkategorier. (Kilde: ITU).

Overgangen til denne «nye virkeligheten» vil ikke skje over natten, men EU har satt mål om at 5G skal være introdusert i løpet av 2020. Standardiseringen er godt i gang i standardiseringsorganer som 3GPP, ETSI og ITU, og industrien ved utstyrsleverandører og nettoperatører har kjørt operative tester og planlegger pilotløsninger. For eksempel vil Telenor etter planen gjennomføre 5G-piloter i Kongsberg allerede i 2018. Dette skjer i samarbeid blant teknologimiljøet på Kongsberg, og Kongsberg sykehus.

Senest i mai 2018 signerte også de nordiske statsministrene en intensjonsavtale om at Norden skal bli den første og beste sammenkoblede 5G-regionen i verden. Avtalen spesifiserer at det skal tilrettelegges for testfasiliteter, frekvenssamarbeid og dekningsutbygging, og at det skal fokuseres på områdene transport, nødkommunikasjon, industriautomatisering, energi, miljø og land- og havbruk. Statsministrene ber om at intensjonsavtalen følges opp av de nordiske ministrene ansvarlig for digitalisering. En støtteerklæring til avtalen ble også gitt av de store nordiske leverandørene Nokia og Ericsson, og operatørene Telenor, Telia, TDC, Tele2 og Vodafone.

Implementering av 5G vil kreve ny design både i mobilkjernenettet og i radionettet. I mobilkjernenettet krever 5G endringer både i den den logiske og fysiske arkitekturen. I 4G og eldre generasjoner mobilnett benyttes telekomspesifikke signaleringsprotokoller som SS7 og DIAMETER og særskilte grensesnitt mellom de ulike nettfunksjonene i mobilkjernenettet; det vil si funksjonene som «under panseret» styrer autentisering av brukerne, mobilitet, sammenkobling av samtaler, trafikkstyring, kontroll med databruk osv. De siste årene har det vært påvist sårbarheter i disse protokollene og grensesnittene. Sårbarhetene har potensiale til å kunne utnyttes til både sporing, manipulering og avlytting, noe Nkom har omtalt både i EkomROS 2016 og 2017. Samtidig kreves det helt spesialisert kompetanse for å kunne utnytte disse sårbarhetene.

I 5G skjer en utvikling mot å erstatte disse protokollene og grensesnittene med standardiserte løsninger som vi kjenner fra IT- og internettdomenet. Blant annet vil nettfunksjonene i kjernenettet kommunisere via standard klient-tjener-protokoller som HTTP. Arkitekturen fører til at alle funksjoner i mobilkjernenettet i prinsippet kan nå alle andre, og protokollene er «allment» kjente. En konsekvens av dette kan også være at mobilkjernenettene vil ha mange av de samme iboende sårbarhetene som man finner ellers i internettdomenet, og som dermed kan unyttes av bredere omfang av angrepsmetoder og trusselaktører. Det vil derfor være svært viktig å implementere gode sikkerhetsløsninger for blant annet autentisering og autorisasjon i 5G.


Telia fortsetter forberedelsen av nettet for 5G: inngår avtale med Eidsiva bredbånd

Pressemelding • nov 16, 2017 07:00 CET

Share

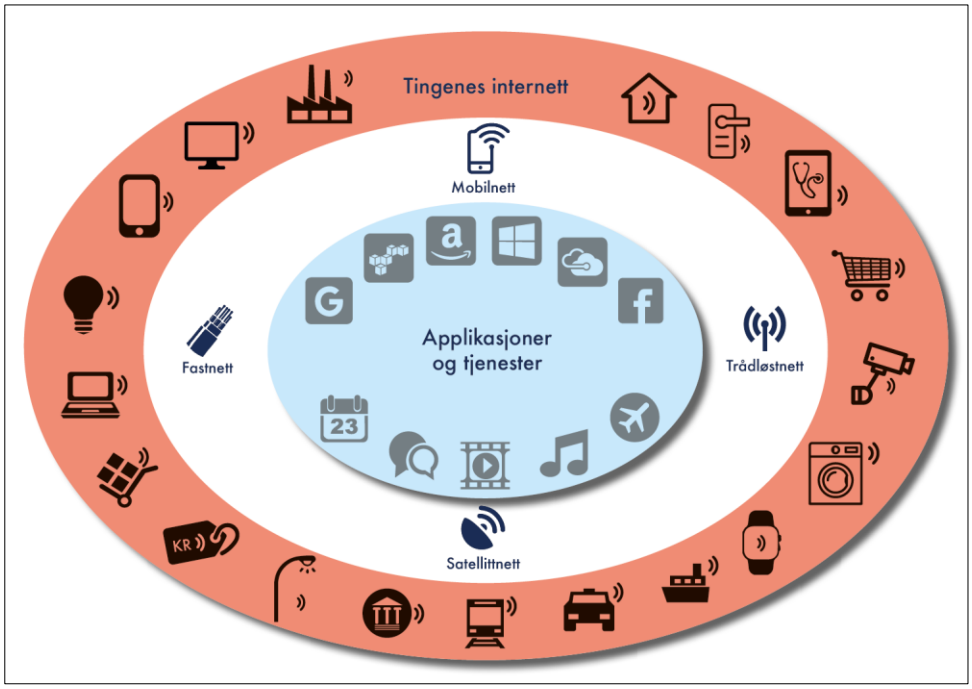
Telia har inngått en fiberavtale med Eidsiva bredbånd som omfatter fiberleveranser i Hedmark, Oppland og øvre Romerike for å styrke nettkvalitet og kapasitet samt øke robustheten i Telias mobilnett i innlandet på vei mot 5G.

Figur 9. Telia reduserer avhengigheten til Telenors nett og tar større kontroll på fiberinfrastrukturen i mobilnettet, gjennom avtaler med regionale fiberleverandører. (Kilde: Pressemelding Telia).

Når det gjelder den fysiske arkitekturen, vil de strenge kravene til forsinkelse i mobilnettene forutsette at mange kjernenettfunksjoner ikke lenger kan være sentralisert, men må distribueres og flyttes nærmere brukeren, til regionale og lokale «datasentre». Det forutsettes også at det bygges en rask og effektiv transmisjons-infrastruktur, det vil si fiberforbindelsene mellom basestasjonene, de distribuerte datasentrene og det sentrale mobilkjernenettet. For eksempel har Telia startet et arbeid for å tilrettelegge eget mobilnett for 5G gjennom å ta kontroll på større deler av transmisjonsinfrastrukturen. Dette skjer gjennom fiberavtaler med regionale fiberaktører og innebærer en frigjøring fra Telenors nett. Dette grepet bidrar dermed også positivt med tanke på å redusere

avhengigheten av Telenors nett, noe som ble problematisert i Lysneutvalgets rapport og Nkoms ROBIN-rapport[4].

Samtidig som 5G gradvis vil innføres, må teknologien i mange år også virke sammen med eldre generasjoner, som 4G. Snur man på bildet, ser man også allerede i dag funksjonalitet i 4G-nettene som er i ferd med å tilpasse seg 5G-brukerbehovene. Et eksempel er Telias og Telenors utrulling av ny radioteknologi, som NB-IoT og LTE-M[5], som legger til rette for massiv IoT. Dette er teknologi som bygger på 4G-nettet vi kjenner, men som er tilpasset for IoT-



Figur 10. Oversikt over hovedkomponenter i et IoT-økosystem. Viser «tingene», aksess-teknologien og tjenesteplattformene.

kommunikasjon gjennom å redusere båndbredden og signaleringen og forenkle radioprotokollene. Dette øker dekningsutbredelsen i nettet, samtidig som det legger til rette for betydelig redusert strømforbruk og kompleksitet i IoT-enhetene, sett i forhold til smarttelefonene. I følge Nkoms ekomstatistikk var det ved utgangen av 2017 ca. 1,6 millioner aktive SIM-kort for maskin-til-maskin-kommunikasjon, en økning på nærmere 350 000 fra 2016. Mange er fortsatt basert på 2G, og begrenset til IoT-enheter som kan være tilkoblet ekstern strømforsyning. Med tilretteleggingen for strømgjerrige og billige IoT-enheter, som skjer gjennom for eksempel NB-IoT-dekningen, forventes enhetsveksten å øke kraftig. Telenor anslår at de innen 2020 har minst like mange ting koblet til mobilnettet som det er mennesker i Norge, og både Telia og Telenor vil innen få år ha landsdekkende dekning med de nye teknologiene.

[4] "Digital sårbarhet – sikkerhet samfunn" (NOU 2015:13) og "Robuste og sikre nasjonale transportnett – målbilder og sårbarhetsreduserende tiltak", Nkom, 2017
[5] NB-IoT: Narrowband IoT, LTE-M: LTE for Machines

IoT-veksten vil selvsagt også komme på andre aksessteknologier enn mobilnettet. Avhengig av bruksområde, utvikles IoT-løsninger som tilknyttes både trådløse (Wifi, Bluetooth, Zigbee, RFID, NFC osv.) og trådbundne (fastnett) aksesser. En bekymring er at mye av IoT-utstyret som vil komme på markedet kan ha dårlig innebygd sikkerhet, noe som kan utnyttes for eksempel til å gjennomføre tjenestenektangrep i nettene de er tilkoblet.

De fremtidige 5G-nettene, og deres samvirke med 4G, vil medføre svært komplekse drifts- og forvaltningsprosesser. Kompleksiteten vil forutsette at flere oppgaver tidligere utført manuelt må helt eller delvis automatiseres. Her forventes det at kunstig intelligens gradvis vil overta tidligere manuelle oppgaver. Enkelt fortalt innebærer kunstig intelligens programvareteknikker som er inspirert av måten mennesker lærer og handler. Således er programvaren designet for å lære av omgivelsene og tilpasse handlinger etter forholdene istedenfor å være statisk programmert til å utføre en bestemt oppgave. Innenfor elektronisk kommunikasjon vil kunstig intelligens kunne utnyttes til å automatisere stadig flere oppgaver innen kundebehandling, provisjonering, nettverkskonfigurasjon, feildiagnostisering, osv.

På den ene siden vil økt bruk av kunstig intelligens kunne bidra til færre feilsituasjoner. For eksempel kjenner Nkom til flere eksempler de siste årene hvor driftspersonell i operasjonssentrene ikke har evnet å oppdage enkelte alvorlige feilsituasjoner tidlig, fordi alarmbildet har vært for komplekst og man ikke har evnet å tolke sammenhengene. På den annen side vil kunstig intelligens innføre nok et lag med kompleksitet, noe som i seg selv medfører økt sårbarhet.

3.3 Tilstrekkelig kompetanse i egen organisasjon?

Bildet av utviklingen innenfor sektoren som tegnes over, fører til at tilbydere av elektronisk kommunikasjon i stadig større grad blir avhengig av utstyrsleverandører og andre underleverandører innenfor alt fra design, utrulling, drift og forvaltning av sine nett og -tjenester. Dels er dette en naturlig følge av den spesialiserte kompetansen som behøves for de ulike og stadig mer komplekse løsningene som utgjør bestanddelene i elektroniske kommunikasjonsnett og -tjenester. Dels er det begrunnet i behovet for kostnadseffektivisering. Bruk av underleverandører er i dag ofte helt avgjørende for tilbydere av elektronisk kommunikasjon for å utvikle nye produkter og forretningsområder og for å være konkurransedyktige i markedet.

Dette innebærer imidlertid også at den samlede kritiske kompetansen som er nødvendig for å opprettholde nett og tjenesters tilgjengelighet, integritet og konfidensialitet fragmenteres og flyttes nedover og utover i ulike underleverandørkjeder. Hos de mindre ekomaktørene er avhengigheten til underleverandørenes kompetanse gjerne fullstendig, i den forstand at både

design, utrulling og drift ivaretas av disse, gjennom «managed services». For de større norske ekomaktørene er det i større grad system- og driftskompetanse i egen organisasjon, i alle fall på de kritiske deler av nett og tjenester, men hvor man likevel har avhengighet til underleverandørenes kompetanse for andre- og tredjelinjesupport. Men også store ekomtilbydere benytter managed services. I Norge er det Motorola som leverer nettverksutstyr og som drifter Nødnett. Tilsvarende er det Huawei som leverer og drifter TDCs mobilnett i Danmark.

Valg av driftsløsning beror på både forretningsmessige og sikkerhetsmessige hensyn, og i mange tilfeller kan utstrakt bruk av underleverandører til både design, utvikling og drift være hensiktsmessig hvis utført riktig.[6] Utfordringene oppstår imidlertid når avstanden i leverandørkjedene blir for stor mellom de som sitter med utførerkompetansen og de som har ansvaret for kontrakten med brukerne, dvs. nett- og tjenestetilbyderne. Jo lengre og mer kompleks leverandørkjeden er, jo mer krevende blir det for tilbyderen å opprettholde forsvarlig kontroll med sikkerheten i nett og tjenester.

Nkom har ved flere tilfeller sett at sikkerhetskravene i ekomloven og sikkerhetsloven har satt begrensninger for utkontrakteringsprosesser som ellers, av kommersielle grunner, ville ha blitt gjennomført. Enten ved å ikke bli gjennomført i det hele tatt, eller ved å bli gjennomført på en annen måte enn først tenkt, for eksempel i en mer begrenset grad. Felles for prosessene har vært at tilbyder har måttet finne løsninger for å beholde forsvarlig kontroll og dermed kompetanse i egen organisasjon, for slik å kunne tilfredsstille sikkerhetskravene. Likevel er det utfordrende for myndighetene å utarbeide regulering som balanserer mellom det å tilrettelegge for utvikling, innovasjon og konkurranse, samtidig som man skal sikre tilstrekkelig kompetanse i egen organisasjon for å ivareta sikkerheten.

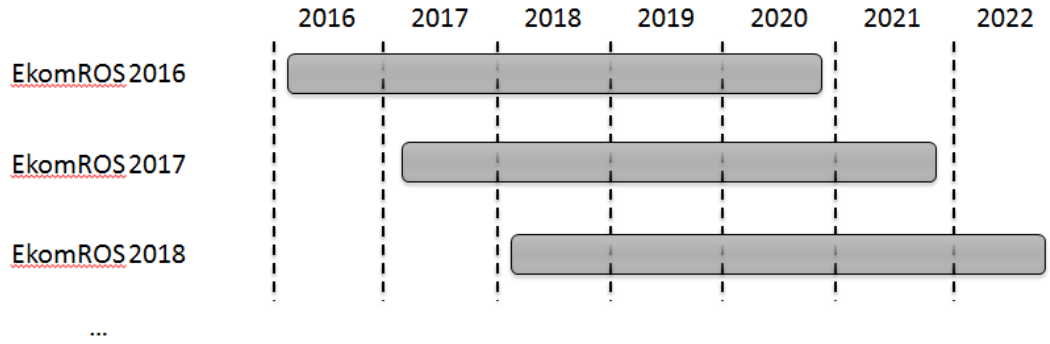
Den nye sikkerhetsloven, som skal tre i kraft 1. januar 2019 vil de neste årene legge viktige føringer for hvordan tilbyderne skal sikre kompetanse i egen organisasjon. I 2018 foregår det også et arbeid med å utarbeide tre forskrifter med utfyllende bestemmelser til den nye sikkerhetsloven. Forsvarsdepartementet leder forskriftsarbeidet, og Nkom deltar som sektor- og tilsynsmyndighet innenfor ekom.

Den nye sikkerhetsloven legger opp til at flere aktører enn i dag innen ekomsektoren blir underlagt dette regelverksregimet. Kravene i loven og forskriftene blir også funksjonelt utformet, noe som innebærer en fleksibilitet for virksomhetene som skal etterleve disse. Denne fleksibiliteten er helt nødvendig for å ta høyde for dynamikken i den teknologiske utviklingen og i trusselbildet. Samtidig vil det kreve høy grad av kompetanse i virksomhetene, når de funksjonelle kravene skal omsettes til de rette sikringstiltakene for å oppnå et forsvarlig sikkerhetsnivå.

[6] «Sikkerhetsfaglige anbefalinger ved tjenesteutsetting». NSM, 2018.

4 Risikovurdering

Dette er det tredje året Nkom publiserer en risikovurdering av ekomsektoren, og det er viktig å presisere at vurderingen ikke er uttømmende eller gjør tidligere års vurderinger ugyldige. Hver rapport tar for seg noen utvalgte risikoområder. Rapportene utfyller hverandre slik at de over noen år til sammen fanger opp de vesentligste sikkerhetsutfordringene i sektoren.



Figur 11. De årlige vurderingene av fremtidig risiko kompletterer hverandre.

Ekomloven stiller krav til at tilbyderne skal tilby ekomnett og -tjenester med forsvarlig sikkerhet for brukerne i fred, krise og krig. I den overordnede risikovurderingen ser derfor Nkom på uønskede hendelser i hele krisespekteret, både utilsiktede og tilsiktede, og samtidig alle aspekter av sikkerhet: tilgjengelighet, integritet og konfidensialitet.

I en komplett risikovurdering av et mer avgrenser objekt, vil det være naturlig å identifisere konkrete tiltak for å motvirke kjente trusler. EkomROS legger først og fremst vekt på å skape oppmerksomhet om aktuelle risikoområder. Konkrete tiltak som må iverksettes hos tilbyderne, må følges opp i de de enkelte aktørers handlingsplaner. For Nkom vil ekomROS 2018, som de foregående rapportene, inngå i Nkoms grunnlag for prioritering av egne tiltak.

Risikovurderinger er alltid beheftet med usikkerhet. Når det gjelder risiko knyttet til teknologier som ennå ikke er fullt ut implementert, har vi lite eller ingen erfaring å bygge på. En kan heller ikke angi sannsynlighet for villede hendelser på samme måte som for mer kjente naturhendelser og tekniske feil. I vurderingen av konsekvens, inngår om hendelsen svekker konfidensialitet/integritet eller tilgjengelighet av en tjeneste, geografisk omfang, tjenesteomfang og påvirkning på samfunnet. For tilsiktede handlinger tar en også hensyn til om handlingen er målrettet og om den har økonomisk, politisk eller sikkerhetspolitisk/militært motiv.

4.1 Det generelle trusselbildet

Etterretningstjenesten (E-tjenesten), Politiets sikkerhetstjeneste (PST) og Nasjonal sikkerhetsmyndighet (NSM) utgir årlige trussel- og risikovurderinger innenfor sine myndighetsområder. I tillegg gir DSB jevnlig ut analyser av utvalgte krisescenarioer.

Elektronisk kommunikasjon berøres i stor grad i disse vurderingene, da de kan være et mål så vel som et middel for ondsinnede handlinger. Ekom er i kraft av å være en kritisk infrastruktur et mulig mål for sabotasje, samtidig som den utnyttes til etterretning, påvirkning og sabotasje rettet mot andre sektorer i samfunnet.

E-tjenesten har oppmerksomheten rettet mot ytre trusler mot Norge. Deres åpne vurdering av aktuelle sikkerhetsutfordringer, *Fokus 2018*, beskriver blant annet trusler i det digitale rom. Rapporten deler truslene i tre kategorier: påvirkning, etterretning og sabotasje. *Fokus 2018* peker på at russiske sikkerhets- og etterretningstjenester bruker sosiale og tradisjonelle medier aktivt for å påvirke. Feilinformasjon og propaganda blir spredd gjennom blant annet videoer, nyhetssaker og blogginnlegg. Robotiserte spammekampanjer på Twitter og bruk av kaprede eller falske profiler på blant annet Facebook i regi av såkalte «trollfabrikker» er andre eksempler. I forkant av valgene i Frankrike og Tyskland har de registrert en klar vinkling i dekningen av valgkampen i russiskkontrollerte medier. Hensikten synes å være å påvirke politiske valg eller beslutningsprosesser gjennom å skape forvirring, splid og mistillit til etablerte alternativer.

I flere år har det vært drevet etterretningsoperasjoner mot norske myndigheter og virksomheter. Først og fremst har aktiviteten vært rettet mot tradisjonelle politiske og militære mål, som utenrikstjenesten og Forsvaret. Nettverksangrepet mot Helse Sør-Øst i januar 2018 viser etter E-tjenestens vurdering, at etterretningsaktivitet mot Norge ikke er begrenset til tradisjonelle politiske og militære mål.

Det digitale rom gir statlige aktører en rekke nye muligheter til å sabotere både sivile og militære mål i andre stater. Sivile mål kan være systemer som er av kritisk betydning i moderne, industrialiserte samfunn, som styrings- og administrasjonssystemer for kraft, elektronisk kommunikasjon, transport og finansielle tjenester. E-tjenesten skriver at russisk interesse over tid for energiselskaper og industrielle styringssystemer, kan tyde på ambisjoner om å kunne sabotere kraftinfrastruktur. Erfaringer fra Ukraina i 2016 tilsier at Russland har evne til å påføre kritisk infrastruktur stor skade ved å ta kontroll over IT-systemer for styring. I stedet for å ta ut skadepotensialet, kan det synes som målet har vært å tilegne seg erfaring og kunnskap for fremtidige sabotasjeaksjoner i en eventuell militær konflikt.

PST tar i sin trusselvurdering for 2018 primært for seg forhold i Norge som kan påvirke norsk sikkerhet og skade nasjonale interesser. Relevant for sektoren elektronisk kommunikasjon er hva de oppsummerer om etterretning: «Rekruttering av kilder og agenter, kartlegging av virksomheter og kritisk infrastruktur samt nettverksoperasjoner, vil utgjøre de mest alvorlige utfordringene knyttet til fremmede staters etterretningsvirksomhet i 2018*».* Blant kritiske infrastrukturer som er interessante for kartlegging nevnes kommunikasjonslinjer og energiforsyning. For 2018 forventer PST at enkeltpersoner blir forsøkt rekruttert som kilder og agenter, og at norske virksomheter blir utsatt for kartlegging og nettverksangrep. I tillegg vil beslutningsprosesser bli forsøkt påvirket og undergravet, og norske virksomheter bli utsatt for forsøk på ulovlig anskaffelse av kunnskap og teknologi.

Nettverksoperasjoner består i å kartlegge svakheter i kommunikasjonsnett og utnytte disse. Den mest vanlige måten å innføre skadevare på, er fortsatt målrettede e-poster. Skadevaren kan bestå i en bakdør for seinere tilgang og skjulte kommunikasjonskanaler. PST skriver at «i de aller fleste datanettverksoperasjonene vi har sett, er inntrengerne interessert i å hente ut informasjon fra virksomheten. Internasjonalt har vi imidlertid også sett eksempler på at noen trusselaktører har evne og vilje til både å manipulere informasjon og sabotere digitale systemer*.»*

NSM gir årlig ut rapporten *Helhetlig IKT-risikobilde* og en mer overordnet rapport om sikkerhetstilstanden. Den siste av disse, *Risiko 2018*, peker på at tjenesteutsetting og komplekse verdikjeder som delvis er utenfor norske myndigheters kontroll bidrar til å øke den totale digitale angrepsflaten. Rapporten viser til hendelser fra det siste året som illustrerer sårbarheter knyttet til teknologiutviklingen.

En av de største og mest alvorlige cyberhendelsene i 2017, som i utlandet fikk konsekvenser for kritiske samfunnsfunksjoner, var ormen som spredte krypteringsviruset WannaCry. Ormen utnyttet en sårbarhet i Windows. Etterslep på sikkerhetsoppdateringer hos virksomheter førte til at angrepet fikk store konsekvenser. I september 2017 ble det svenske Trafikverket (tilsvarende Bane NOR i Norge) og flere andre virksomheter tilknyttet svensk jernbane utsatt for tjenestenektangrep mot noen av sine web-baserte tjenester. Blant disse tjenestene var systemene for overvåking og dirigering av tog. Dette skapte varierende grad av forsinkelser i en og en halv dag. Det ble aldri klart hvem som utførte disse angrepene.

Forsvarets forskningsinstitutt (FFI) beskrev i 2017 viktige trender og sikkerhetsutfordringer i fremtidens ekom-tjenester på oppdrag fra NSM. En av trendene er virtualisering av nettverksfunksjoner. Denne frikobler funksjoner fra maskinvare med en bestemt fysisk plassering. Potensielt kan store deler av norsk ekominfrastruktur drives fra helt andre steder i verden, men den samme teknologien kan gjøre det mulig å flytte driften hjem ved behov. En annen trend er at 5G mobilteknologi skal møte ekstreme krav til henholdsvis datahastigheter,

forsinkelse og sikkerhet og samtidig kunne håndtere et stort antall enheter som sporadisk kommuniserer med nettet (IoT). Med 5G vil det skje en utvikling fra spesialprotokoller og -grensesnitt mot standard webteknologi i kjernen. En tredje trend er bruk av kunstig intelligens for å håndtere økende kompleksitet i nettene og oppnå mer autonome ekomsystemer. FFI ser på denne siste utviklingen som uunngåelig, men ikke uproblematisk. Systemer vil ikke lenger være fullt ut verifiserbare og det vil ligge stor makt i å ha denne nye type kompetansen og det vil være en risiko for at Norge ikke vil ha nok kompetanse på feltet.

DSB har i flere år utgitt risikoanalyser av en rekke alvorlige scenarioer som kan ramme det norske samfunnet. Analysene er presentert i samlerapporter kalt *Nasjonalt risikobilde*, mens de i de seinere årene har publisert delrapporter for enkeltanalyser kalt *Krisescenarioer*. I desember 2016 publiserte DSB rapporten *Samfunnets kritiske funksjoner*. Elektroniske kommunikasjonsnett og –tjenester regnes der som en av syv samfunnsfunksjoner som utgjør ulike typer forsyninger og infrastrukturbaserte tjenester. Felles for de funksjonene som inngår i denne kategorien, er at de i tillegg til å tjene befolkningen direkte, er innsatsfaktorer for virksomheter som igjen er ansvarlig for andre kritiske funksjoner i samfunnet.

I *Befolkningsundersøkelse om risikopersepsjon og beredskap i Norge – 2018* spurte DSB et representativt utvalg i befolkingen om deres bekymring for at ulike hendelser kan inntreffe i Norge de neste 5 år. Hendelsene omfatter ulike naturhendelser, store ulykker, langvarig knapphet på viktige varer og tjenester og villede angrep. «Cyberangrep på styringssystemer» er den hendelsen som man er mest bekymret for i undersøkelsen. At dette er en type hendelse hvor potensiell konsekvens er mer utslagsgivende enn sannsynlighet for risikovurderingen, viser det faktum at bare 3% svarer at de har vært direkte berørt av denne trusselen de siste ti årene. Det siste fremgår av DSBs befolkningsundersøkelse i 2017 og 2013.

4.2 Risikoområder

Når vi har indentifisert risikoområder, har de generelle utviklingstrekkene som vi har omtalt i kapittel 3 veid tungt. Kapittel 3 fanger opp internasjonale trender som ekomsektoren i Norge vil bli berørt av, men som vi ikke har erfart ennå. I tillegg har vi tatt hensyn til erfaringer fra hendelser de siste år og trusselvurderingene fra norske sikkerhetsmyndigheter. Denne ROS-vurderingen har en horisont på fem år. Vi omtaler likevel enkelte teknologiutviklinger som først vil ha effekt utenfor denne horisonten, men som sektoren må ta hensyn til i femårsperioden. Eksempelvis regner en ikke med at fremtidens nødnett vil være realisert i kommersielle mobilnett før i 2026, men viktige valg med betydning for risiko må gjøres langt tidligere. Det samme vil gjelde på andre områder. Vi har dette året valgt å fokusere på satellittnavigasjonssystemer, totalforsvaret, neste generasjon nødnett og tingenes internett.

4.3 Økt avhengighet til satellittnavigasjonstjenester

Målene for norsk romvirksomhet er fastsatt i Meld. St. 32 (2012-2013) *Mellom himmel og jord: Norsk romvirksomhet for næring og nytte*. Hovedmålet for den norske satsingen på romvirksomhet er at virksomheten skal være et verktøy for norske interesser. Det er satt fire delmål for satsingen:

- Lønnsomme bedrifter, vekst og sysselsetting
- Dekning av viktige samfunns- og brukerbehov
- Bedre utnyttelse av internasjonalt samarbeid om romvirksomhet
- God nasjonal forvaltning av norsk romvirksomhet

Meldingen fastsetter videre at Norsk Romsenter skal være statens strategiske, samordnende og utøvende organ for å sikre en effektiv utnyttelse av verdensrommet til beste for det norske samfunnet. Det skal arbeides for at offentlige investeringer i romvirksomhet forvaltes kostnadseffektivt og fører til størst mulig samfunnsnytte. Satsingen skal bidra til økt konkurranseevne og verdiskapning i norsk næringsliv. Videre skal det arbeides for at romvirksomhet bidrar til å realisere regjeringens mål for andre politikkområder, slik som nordområdene, klima- og miljøpolitikk, samfunnssikkerhet, transport og forskning.

Infrastruktur i verdensrommet er viktig for flere funksjoner som ivaretar sikkerhet og beredskap i samfunnet. Satellittkommunikasjon kan spille en viktig rolle for å sikre liv og helse og gjenopprette infrastruktur når deler av bakkebaserte systemer er satt ut av spill, for eksempel ved naturhendelser. I denne rapporten, er det imidlertid den rombaserte infrastrukturens betydning for posisjonsbestemmelse, navigasjon og tidsbestemmelse (PNT) vi ser på. Siden samfunnet i økende grad er avhengig av systemer for PNT og eldre bakkebaserte systemer har blitt bygd ned eller blir mindre brukt, har de rombaserte systemene blitt viktigere. Det bakkebaserte navigasjonssystemet Loran-C ble vedtatt nedlagt i 2015 og er nå avviklet. Det finnes fortsatt i noen grad alternative systemer til hjelp for navigasjon og presis klokke, men nøyaktighet, responstid og kapasitet kan være dårligere. Dessuten kan kompetansen på bruk av alternative systemer forvitre etter hvert som rombaserte systemer har vist seg pålitelige over lang tid.

Global Navigation Satellite System (GNSS) er fellesbetegnelsen på satellittbaserte systemer for navigasjon, posisjonering og nøyaktig tid med global dekning. To systemer har vært etablert i mange år, amerikanske GPS og det russiske GLONASS, mens europeiske GALILEO og kinesiske BeiDou fortsatt er under oppbygging.

Norsk Romsenter og Nkom har fått utført en kartlegging av samfunnets behov for kontinuitet av GNSS-tjenester og evne til å detektere og fjerne forstyrrelser. Kartleggingen viser at bruken av GNSS er omfattende. Det er forventet at innen 2019 vil det være 7 mrd. GNSS-enheter i

bruk. Den store veksten skyldes i stor grad at de finnes i personlig utstyr som smarttelefoner og klokker. Videre viser kartleggingen at samfunnet blir stadig mer avhengig av GNSS-tjenester i takt med økt digitalisering og automatisering. Eksempler er optimal flyt i flytrafikken, flåtestyring for transportselskaper og tidsstempling av finanstransaksjoner. Endelig går det frem at mange av funksjonene som benytter GNSS representerer store samfunnsmessige verdier. De økonomiske gevinstene av GNSS i UK er estimert til £ 6,7 mrd. per år. Hvis en forutsetter samme gevinst per innbygger i Norge, vil tallet hos oss bli NOK 5,4 mrd. per år.

Signalene som benyttes i GNSS kommer fra satellitter ca 20.000 km over jordoverflaten og er meget svake når de kommer frem og er derfor sårbare for forstyrrelser. Det er i hovedsak to måter å forstyrre signalene på, som kalles jamming og spoofing. Jamming innebærer at noen sender støysignaler i det aktuelle frekvensområdet i den hensikt å ødelegge for mottak av de ekte signalene. Enkle utgaver av jammere forekommer i transportsektoren, f.eks. om sjåfører skulle ønske å unngå at arbeids- eller oppdragsiver kan spore kjøretøyets posisjon til enhver tid. En har også sett eksempler på at vinnerviljen hos enkelte Pokémon-entusiaster har drevet dem til å anskaffe seg utstyr for å lage falske GPS-signaler. Med kraftigere og dyrere utstyr kan kriminelle så vel som myndigheter gjøre satellittbasert sporing umulig i større områder.

Signalene kan, i tillegg til å bli blokkert av støy, bli manipulert slik at de gir mottakeren feilaktig informasjon om posisjon og tid. I dette tilfellet narres (ref. spoofing) mottakeren til å oppfatte de falske signalene som ekte. Både informasjon om normale signaler, satellittbaner og billig programmerbart utstyr er lett tilgjengelig på internett, så det er ingen stor barriere for den som har viljen. Det er imidlertid relativt overkommelig å oppdage slik manipulering med mottiltak. Dersom slike mottiltak ikke er tatt i bruk, kan manipulering av tidsinformasjon kunne ha store økonomiske konsekvenser for finanstransaksjoner som er basert på nanosekunders nøyaktighet. Andre områder som er avhengig av nøyaktig klokke er elektronisk kommunikasjon og strømnett. Innenfor transport vil manipulering av posisjonsdata kunne føre til både ulykker og økonomisk tap.

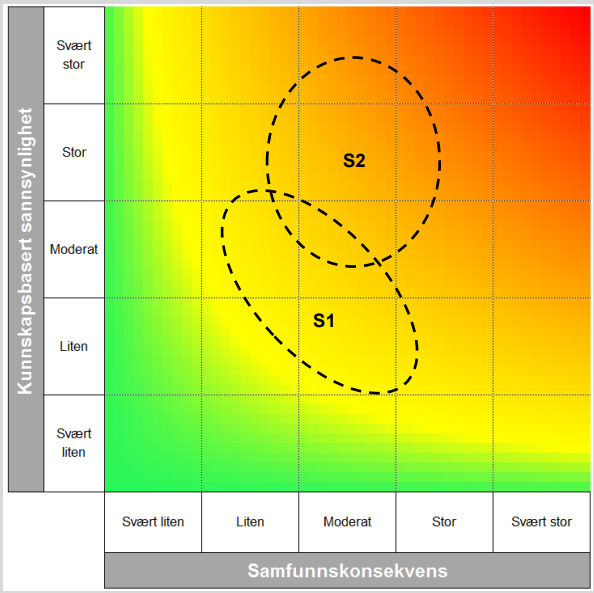
Elektronisk kommunikasjon var tidligere svært avhengig av nøyaktig takt og frekvens for sine synkrone transmisjonssystemer. Moderne transmisjonsnett er i mindre grad avhengig av dette og en har dessuten bakkebaserte atomklokker som holder takt med tilstrekkelig presisjon i en måneds tid. Vi har fortsatt brukere med samfunnskritisk funksjon som bruker synkrone transmisjonssystemer, og disse er mer sårbare for svikt i taktreferanse.

Det synes å variere i hvor stor grad de høye kravene til synkronisering i 5G vil bli løst uavhengig av GNSS-signaler. Norske operatører oppgir å kunne benytte synkronisering via fiberinfrastrukturen. Men for aktører uten egen fiber kan GNSS være en aktuell kilde for

synkronisering i 5G. I en britisk rapport[7] fra januar 2018 beskrives avhengigheter til satellittbasert tid og posisjon for ulike sektorer, blant disse ekom. I mobilnettene er det stigende krav til presisjon for tid. Forfatterne av rapporten ser en viss fare for at produsenter vil basere seg på GNSS-basert tid selv om GNSS vil kunne ha problemer med å levere med tilstrekkelig nøyaktighet og stabilitet.

Et viktig tiltak for å redusere sårbarheten for bortfall eller manipulering av GNSS-signaler må være å sikre alternative jordbundne løsninger for nøyaktig posisjon og tid. For ekom er dette i stor grad tilfellet, men ekom kan ikke betraktes som en isolert infrastruktur. I drift og vedlikehold av nett og tjenesteproduksjon er det sterke avhengigheter til for eksempel kraftforsyning, IT- og støttesystemer og vare- og persontransport, som igjen har avhengigheter til satellittbaserte tjenester. Ettersom bortfall av satellittbaserte tjenester også vil kunne påvirke slike systemer og funksjoner, vil dette indirekte kunne påvirke elektronisk kommunikasjon. Nkom anser derfor at de sammensatte og sektorovergripende verdikjedene som digitalt sårbarhetsutvalg pekte på i 2015, kan bety at også elektronisk kommunikasjon er mer sårbar for utfall i rombasert PNT-infrastruktur enn en isolert sektoranalyse avdekker.

Nkom har sett på to scenarioer knyttet til samfunnets økte avhengighet til GNSS.



Scenario 1: Populært mobilspill utløser omfattende spoofing-aktivitet
Erfaringer fra Pokémon GO viste at noen spillere genererte falske GPS-signaler for å oppnå fordeler. Det kommer et nytt mobilspill kalt «Ghost Hunter» som er betydelig mer avansert enn Pokémon GO og som blir enormt populært både blant barn og voksne. Det følger stor prestisje med å nå det høyeste nivået. Det har vært en utvikling hvor det etableres et marked på Internett for billig og lett tilgjengelig utstyr for å generere falske GPS-signaler. Prestisjen som følger med de høyere nivåene av «Ghost Hunter» fører til at titusenvis av spillere sender ut falske GPS-signaler for å nå de høyeste nivåene. Den massive spoofing-aktiviteten gjør at GPS mange steder blir upålitelig.

Scenario 2: Brudd i tilgang til satellittdata i en spent situasjon
Romsikkerhet er et sektorovergripende politikkfelt som krever samordning mellom en rekke offentlige aktører. Landbasert elektroniske kommunikasjonsinfrastruktur og tjenester inngår også i verdikjeden i romvirksomheten. Tilgang til satellittdata via en av de norske jordstasjonene blir svært viktig i forbindelse med en nasjonal sikkerhetshendelse. Samtidig, og uavhengig, oppstår et dobbelt fiberbrudd i transportnettet som gjør at en mister tilgangen til satellittdataene i en kritisk fase. Tilbyder har ikke forutsetninger for å forstå hvilke konsekvenser de tilfeldige bruddene får, og fordi feilen berører mange offentlige myndigheters ansvarsområde på ulike måter, tar det tid før man ser årsakssammenhenger og skadeforebyggende tiltak blir iverksatt.

Figur 12. Risikoanalyse for scenarier knyttet til økt avhengighet til GNSS-tjenester.

[7] *"Satellite-derived Time and Position. A Study of Critical Dependencies", Government Office for Science (UK) (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/676675/satellite-derived-time-and-position-blackett-review.pdf)*

4.3.1 Scenario 1: Populært mobilspill utløser omfattende spoofing-aktivitet

Scenario 1 beskriver en mulig kilde til spoofing av posisjon, nemlig mobilbasert spillaktivitet som går fra å være uskyldig avkobling til å bli alvor. Da kan det i tillegg til høye premier, utilsiktet også ligge sikkerhetsrisikoer i potten. Hvis det blir mange kilder til feilaktige posisjonsdata, kan disse potensielt forstyrre for eksempel trafikk og navigering.

Det er Nkoms vurdering at dette scenarioet kan gi forstyrrelser i alle deler av landet og at det kan ta måneder å få bukt med problemet. Vi anser at scenarioet kan skape påkjenninger i dagliglivet og i verste fall påvirke liv og helse, slik også Nkom har erfart i frekvenskontrollene omtalt i kapittel 2. De enkeltstående spoofing-aktivitetene har nødvendigvis begrenset geografisk rekkevidde, men scenarioet legger opp til at omfanget øker raskt på grunn av populariteten til enkelte spill. Rettede informasjonskampanjer og kontrollvirksomhet fra Nkoms og øvrige myndigheters side vil kunne slå ned på omfanget etter en viss tid. Den samlede risikoen anses å være *moderat til liten*.

4.3.2 Scenario 2: Brudd i tilgang på satellittdata i en spent situasjon

Romvirksomhet er et sektorovergripende politikkfelt. Det legges derfor vekt på samordning mellom Norsk Romsenter og et tosifret antall andre offentlige aktører som har roller på dette feltet. Nkom er en av disse aktørene. I ett scenario 2 har vi valgt å synliggjøre utfordringen ved at så mange aktører har delansvar innenfor norsk romvirksomhet gjennom en verdikjede som er sektorovergripende. I en spent sikkerhetspolitisk situasjon hvor tilgang til satellittdata er av stor sikkerhetsmessig betydning, skjer et dobbelt fiberbrudd i tilknytning til en av de norske jordstasjonene, som fører til at en mister denne tilgangen over en periode. At hendelsen oppstår under en anspent situasjon bidrar i tillegg til usikkerhet om hendelsen er tilsiktet eller en ren tilfeldighet.

Dette scenarioet vil berøre mange ulike aktører og offentlige myndigheters ansvarsområde, og det er en risiko for at manglende oversikt over avhengigheter og ansvar kan forsinke gjenopprettingen. Nkom vurderer at de mange aktørene og det fragmenterte myndighetsansvaret i dette tilfellet bidrar til å øke risikoen. Samtidig er problemstillingen med fragmentert ansvar innenfor romvirksomhet nå godt belyst. Blant annet med bakgrunn i Meld. St. 10 (2016-2017) *Risiko i et trygt samfunn* og Meld. St. 38 (2016-2017) *IKT-sikkerhet*, jobber nå Romsikkerhetsutvalget nettopp med denne problemstillingen. Nkom har bidratt med innspill i dette arbeidet. Vår samlede vurdering av risiko for det angitte scenarioet er *moderat til stor*.

4.4 Ekomsektorens betydning for totalforsvaret

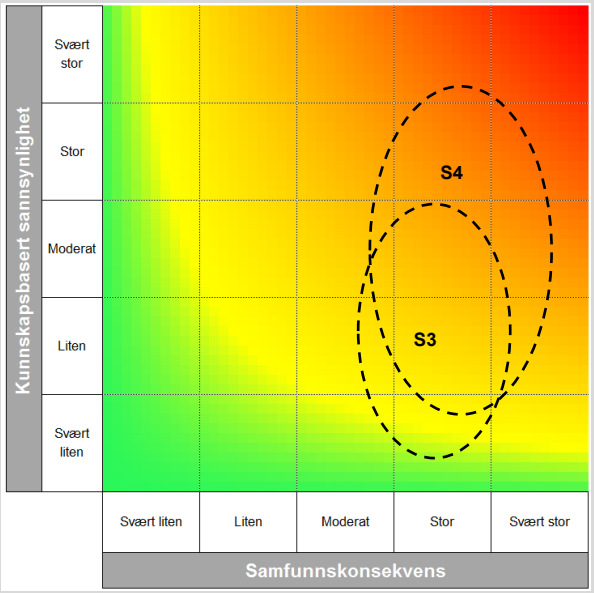
Høsten 2016 vedtok regjeringen gjennomføring av «Program for videreutvikling av totalforsvaret og øke motstandsdyktigheten i samfunnskritiske funksjoner» (Totalforsvarsprogrammet). Totalforsvarskonseptet omfatter gjensidig støtte og samarbeid

mellom det sivile og militære samfunn, hvor det etter den kalde krigens slutt har blitt rettet mye oppmerksomhet mot Forsvarets muligheter til å bistå den sivile siden i eventuelle krisesituasjoner.

Som følge av endringer i det sikkerhetspolitiske bildet, vises det også nå til et behov for å fornye og styrke sivile myndigheters og det sivile samfunnets støtte til Forsvaret. NATO understreker i dokumentet *Compendium of Baseline Requirement, Resilience Guidelines, Initial Evaluation Criteria and Initial Best Practices* at sivil beredskap, krisehåndtering og robuste samfunnskritiske funksjoner er en forutsetning for det enkelte lands, og dermed også alliansens, samlede beredskap og forsvar. NATO har her formulert forventninger og ambisjonsmål til medlemslandenes sivile beredskap for syv kritiske funksjoner: I alle kriser skal landene sørge for å kunne opprettholde en fungerende nasjonal kriseledelse, håndtere mange skadde og forflytning av mennesker, sikre mat-, vann- og energiforsyning og sikre kommunikasjons- og transportsystemer. Oppfølgingen av NATOs ambisjonsmål er tatt inn som prosjekter i totalforsvarsprogrammet, hvor den enkelte sektor må vurdere i hvilken grad Norge er sikret på disse områdene.

Nkom har på oppdrag fra SD vurdert NATOs ambisjonsmål nr. 6, motstandsdyktig sivilt kommunikasjonssystem, opp mot allerede etablerte systemer, responsmiljøer og utredninger på feltet. Nkoms konklusjon etter denne vurderingen var at det foreligger en rekke tiltak som bidrar til å oppfylle NATOs «grunnkrav» innenfor sivile kommunikasjonssystem. Samtidig viser en del av disse tiltakene til Nkoms ansvarliggjøring av tilbydere av ekomtjenester og deres oppfyllelse av blant annet ekomloven § 2-10 første ledd som sier at: «Tilbyder skal tilby elektronisk kommunikasjonsnett og -tjeneste med forsvarlig sikkerhet for brukerne i fred, krise og krig. Tilbyder skal opprettholde nødvendig beredskap, og viktige samfunnsaktører skal prioriteres ved behov [..]». En del av tiltakene viser derfor til Nkoms gjennomføring av tilsyn som overordnet tiltak innenfor spesifikke områder hvor NATO i sin beskrivelse stiller mer spesifikke krav. I hovedsak stilles det store krav til tilbydernes oppfyllelse av begrepet «forsvarlig sikkerhet» for at NATOs krav om et motstandsdyktig sivilt kommunikasjonssystem skal oppfylles.

Nkom har definert to scenarioer knyttet til totalforsvaret. Scenarioene er valgt ut fra trusler som er skissert i sikkerhetsmyndighetenes trusselvurderinger. Begge har en anspent sikkerhetspolitisk situasjon som bakteppe.



Scenario 3: Hybrid hendelse med manipulering av befolkningsvarsling

Ved en anspent situasjon i forhold til en fremmed makt, så greier noen å bryte seg inn i system for mobilbasert befolkningsvarsling. Det går ut en befolkningsvarsling til mobilene i Oslo om å evakuere byen. Det oppstår forvirring og kaos som det tar mange timer å løse opp i, og det falske varselet er avkreftet av norske myndigheter.

Scenario 4: Cyberangrep som medfører anmodning om nedstenging av trafikk

I en politisk anspent situasjon med et annet land, kommer det alvorlige cyberangrep rettet mot norske statlige institusjoner. Angrepene er av et slikt omfang at eksisterende beskyttelsesløsninger er utilstrekkelige, og tiltakene for nedstenging av trafikk er lite treffsikre. Det norske statsapparatet blir sterkt berørt. Angrepet avtar etter en tid.

Figur 13. Risikoanalyse for scenarier knyttet til ekomsektorens betydning for totalforsvaret.

4.4.1 Scenario 3: Hybrid hendelse med manipulering av befolkningsvarsling

Scenario 3 er en hybrid hendelse hvor manipulering av informasjon for befolkningsvarsling benyttes for å spre kaos og utrygghet. Nkom kjenner eksempler hvor det har blitt sendt ut mobilbasert befolkningsvarsling i områder ved feiltakelse. Selv i disse situasjonene kan skadepotensialet være betydelig ved at det kan skape frykt og farlige situasjoner. Dersom slike systemer blir utnyttet målrettet med ondsinnede hensikter, vil skadepotensialet være desto høyere. Jamfør trenden med økt programvarekompleksitet og lange leverandørkjeder omtalt i kapittel 3, kan man ikke utelukke at det vil være mulig å skaffe seg urettmessig tilgang til slike systemer. I tillegg vil det å utnytte slike systemer ha stort skadepotensiale. Nkom anser at det finnes tiltak som reduserer sannsynligheten for scenarioet, men konsekvensen vil være stor. For denne trusselen, er det ytterligere sannsynlighetsreduserende tiltak som vil være mest effektive mottiltak. Muligheten for å utløse slik varsling må være strengt beskyttet av fysiske og logiske tilgangskontroller. Den samlede risiko vurderes som *moderat til stor*.

4.4.2 Scenario 4: Cyberangrep som medfører anmodning om nedstenging av trafikk

Vi har sett eksempler på ulike former for cyberangrep i konfliktområder. I scenario 4 har vi tatt utgangspunkt i et svært omfattende cyberangrep som tilsynelatende har sitt utspring i et bestemt land og som kan betraktes som et målrettet angrep for å påvirke den nasjonale styringsevnen.

I scenarioer som dette, hvor dette skjer i forbindelse med en anspent sikkerhetspolitisk situasjon, vil man forutsette at det nasjonale beredskapsplanverket iverksettes. Planverket er overordnet, og øvelser har vist at det kan være utfordrende å omsette overordnede (og

kanskje tverrsektorielle) tiltak til effektive og treffsikre tiltak hos den enkelte tilbyder av elektronisk kommunikasjonsnett og -tjenester. Utfordringene handler ofte om at nett og tjenesters oppbygging er kompleks og sammensatt, og at det kan finnes en rekke ikke-avdekte avhengigheter som er vanskelige å oppdage på forhånd. Dette kan medføre at tiltakene får uventede og uønskede bieffekter. For eksempel vil omfattende nedstenging av trafikk for å motvirke massive angrep potensielt kunne få følger for egen kommunikasjonsevne. I slike scenarier må man også forvente at et sett med hybride virkemidler benyttes for å utfordre den nasjonale styringsevnen. De som tilsynelatende står bak et angrep er ikke nødvendigvis de som faktisk står bak angrepet. Påvirkningsoperasjoner vil bidra til å skape forvirring og usikkerhet.

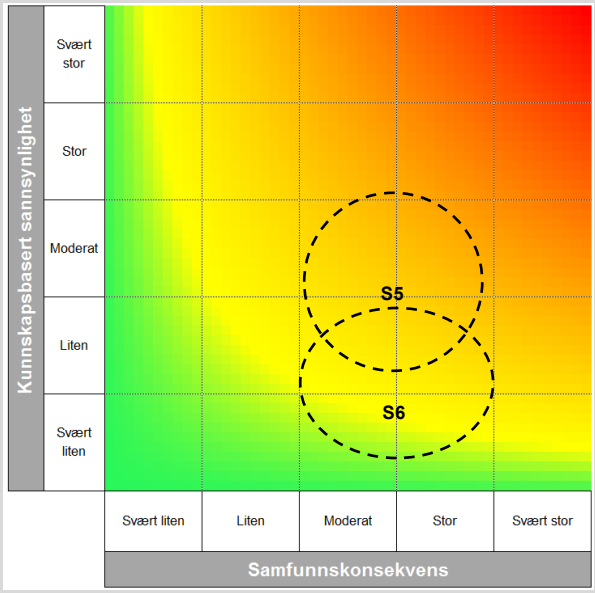
Tilsiktede, ondsinnede handlinger lar seg ikke lett plassere langs sannsynlighetsaksen, men vi kjenner til at denne type handlinger skjer. Vi mener at konsekvensen potensielt er stor. Et tilleggsmoment i dette scenarioet er at muligheten for effektiv nedstenging av trafikk er øvd på overordnet nivå, men hvor treffsikkerhet og potensielle bieffekter av tiltakene i mindre grad er verifisert. Dette vil være et viktig tema for Nkom i høstens NATO-øvelse. Samlet vurderer Nkom risikoen som *moderat til stor*.

4.5 Nødnett i kommersielle nett

Ved å realisere neste generasjon nødnett i kommersielle nett vil en få tilgang til gode, mobile bredbåndstjenester som savnes i dagens Nødnett. Det fremtidige nødnettet vil profitere på det høye drivet bak utviklingen av kommersielle nett og tjenester. Regjeringens beslutning om 700 Mhz-frekvensene i desember 2017 innebærer videre at nettet skal realiseres ikke bare på samme *teknologi* som de kommersielle nettene, men *i* de kommersielle radionettene. Det gjenstår likevel mange valg med hensyn til løsning som kan ha betydning for risiko.

Dagens Nødnett stiller høye krav til robusthet og dekning. Et vesentlig spørsmål har vært om det vil la seg gjøre å oppfylle de høye kravene som denne brukergruppen har, i kommersielle nett. Valget med å realisere neste generasjon nødnett i kommersielle nett forutsetter medvirkning fra offentlige myndigheter i form av regulering og bevilgninger. Samtidig er det et mål å opprettholde og stimulere en fortsatt konkurranse i de kommersielle nettene. Det vil derfor være viktig å finne virkemidler fra myndighetenes side som er effektive med hensyn på å oppfylle kravene og rettferdige med hensyn på konkurranse. For samfunnet er det et mål at tiltak fra myndighetene i størst mulig grad hever standarden i nettene på en slik måte at det kommer alle brukere til gode.

Nkom har definert to scenarioer som belyser sentrale utfordringer knyttet til å benytte kommersielle nett for nød- og beredskapskommunikasjon.



Scenario 5: Ekstremvær med store utfall i strøm og sambandslinjer
Neste generasjon nødnett er realisert i de kommersielle nettene og det gamle Tetranettet skal snart fases ut. Vinterstormen Storeslem blir av tilsvarende omfang og geografisk område som Dagmar. Dette medfører brudd i transmisjonslinjer i tillegg til langvarige strømbrudd i de berørte områdene.

Scenario 6: Brudd på kommunikasjonsvern som følge av programvaresårbarhet i mobilkjernenettet
Utilsiktet programvarefeil i mobilkjernenettet fører til brudd på kommunikasjonsvernet i et av de kommersielt mobilnettene i forbindelse med innføring av funksjonalitet som skal tilbys bedriftsmarkedet. NGN er separert fra det kommersielle kjernenettet men benytter samme leverandør, som dermed åpner for de samme logiske sårbarhetene.

Figur 14. Risikoanalyse for scenarier knyttet til nødnett i kommersielle nett.

4.5.1 Scenario 5: Ekstremvær med store utfall i strøm og sambandslinjer

Ekstremværet Dagmar i 2011 førte til store påkjenninger på ekomnettene. I scenario 5 ser vi på hvordan et neste generasjon nødnett i de kommersielle nettene vil rammes av et nytt ekstremvær av lignende omfang. En full overgang til nytt nett ligger utenfor vår 5 års horisont for EkomROS, men en kan tenke seg at dataløsninger i mellomtiden gradvis blir etablert etter mal for neste generasjon nødnett, mens tale fortsatt skjer i det Tetra-baserte nettet. Vi tror konsekvensene ved en ny hendelse av et slikt omfang fortsatt kan bli relativt høye. Sannsynlighet for denne type ekstremvær kan vi gjøre lite med, og den er økende. Det er dermed konsekvensreduserende tiltak som reservestrøm og redundant transmisjon som en må videreføre og intensivere.

En hel rekke tiltak har blitt gjennomført etter Dagmar, noe som gjør at ekomnettene i dag er mye bedre rustet enn de var i 2011. Det forutsettes imidlertid at robustifiseringsarbeidet og satsingen på beredskapstiltak i de kommersielle nettene også fortsetter de kommende årene, slik at man over tid vil nå tilsvarende nivå som, og passere, dagens Tetra-nett. Dette er også samferdselsmyndighetene forpliktet til å følge opp gjennom regjeringsbeslutningen om 700 MHz-tildelingen. Dette vil likevel ta tid, og i en overgangsperiode vil man kanskje måtte akseptere en noe forhøyet risiko. Samlet anser Nkom risikoen knyttet til dette bestemte scenarioet som *moderat*.

4.5.2 Scenario 6: Brudd på kommunikasjonsvern som følge av programvaresårbarhet i mobilkjernenettet

Det innebærer en viss risiko for samfunnet å basere neste generasjon nødnett på samme teknologi, samme operatører og i stor grad samme leverandører som de kommersielle mobilnettene. Scenario 6 innebærer en logisk feil i programvare fra en leverandør. Selv om en har høy grad av redundans, godt sikret strømforsyning og separate nettelementer i kjernen vil en logisk feil fra én leverandør potensielt kunne ramme både de ordinære brukerne og nød- og beredskapsbrukerne. Informasjon om hvor nødnettbrukere befinner seg vil være sensitivt. Vi vurderer konsekvensen til å være stor, ettersom scenarioet også innebærer brudd på kommunikasjonsvernet til nød- og beredskapsbrukere. Skadepotensialet ville være enda større dersom Forsvaret også tar i bruk kommersielle nett for sine kommunikasjonsbehov. Samlet anser Nkom risikoen knyttet til scenarioet som *moderat til liten.*

4.6 Økt omfang av IoT

Få utviklingstrender har et så høyt potensiale for å endre vår måte å leve og arbeide på som Internet of Things, IoT. Teknologien åpner for store muligheter for å gjøre det enklere og tryggere å leve i en kompleks verden. Mulighetene spenner fra hjelp til de som trenger tilrettelegging i hjemmet, via trafikkstyring i store byer til beslutningsstøtte i arbeidet med globale klimautfordringer.

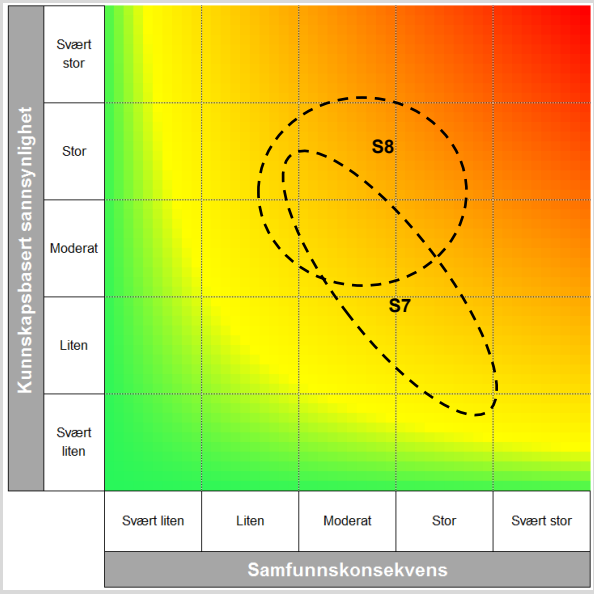
IoT fører også med seg trusler mot sikkerhet. En kan forenklet si at i en første fase av IoT har den dominerende mekanismen bestått i en passiv innsamling av data fra mange kilder for videre analyse. I en slik setting er *personvernet* en viktig pådriver for sikkerhet. Fremover ser en for seg større grad av lukkede, autonome systemer hvor tingene ikke lenger bare samler data, men også aktiveres via styresignaler den andre veien. Et hyppig brukt eksempel er selvkjørende biler. Da blir sikkerhet i betydningen *trygghet* særlig viktig. Oxford Online Dictionary bruker denne eksempelsetningen i definisjonen av Internet of Things: «If one thing can prevent the Internet of Things from transforming the way we live and work, it will be a breakdown in security.» Vi tror utsagnet treffer godt i denne sammenhengen.

I et internett som til nå i hovedsak har knyttet *datamaskiner* sammen, har sikkerhet etter hvert blitt svært viktig for de enhetene som inngår. Enhetene har tilgang til betydelig regnekraft og stabil strøm, de oppdateres jevnlig og har en begrenset levetid. De aller fleste av tingene som inngår i IoT er utviklet for et spesifikt primærformål som ikke er sikkerhet. Mange av dem er optimalisert for å klare seg uten tilsyn og uten ekstern strømkilde. Funksjonalitet må strippes til det aller mest nødvendige for å tjene sin primærhensikt. Kompetanse på sikkerhet har kanskje heller ikke vært tilgjengelig og det er derfor en fare for at sikkerhet er dårlig ivaretatt i designfasen.

Erfaring viser at teknologi som er bundet opp i mange nok enheter er kostbart og tungvint å avvikle. Eksempler på det kan være GSM, IPv4 og signaleringssystemet SS7. Alle disse teknologiene har blitt etterfulgt av bedre og sikrere teknologier, men høye kostnader ved utskifting og ønske om bakoverkompatibilitet fører til at disse teknologiene har fått et langt liv. Levetiden for utstyret med hvor disse teknologiene inngår, kan være lenger enn «holdbarheten» av de sikkerhetsløsningene de ble utstyrt med ved lansering. I IoT-enhetenes levetid vil sikkerhetsløsninger høyst sannsynlig bli kompromittert og hvis løsningene ikke blir oppdatert, enten det er fordi det er teknisk umulig, for dyrt eller praktisk uoverkommelig, er resultatet at vi må leve med en potensiell sårbarhet i lang tid.

Med IoT forventer man at et svimlende stort antall enheter vil kommunisere via Internett. Mange av disse enhetene skal ha en lav kost og sikkerhet vil bli prioritert lavt i forhold til funksjoner som er nødvendige for primærformålet med enheten. Sårbarheter kan være dårlig fysisk sikring, svak logisk tilgangsstyring, manglende konfigurerbarhet og manglende mulighet for sikkerhets-oppdateringer. Hvis sikkerheten ikke blir godt nok ivaretatt i IoT over tid, vil mange scenarioer være mulig, avhengig av hvilke sårbarheter som utnyttes. Ulike sårbarheter kan representere en fare for lekkasje av sensitive data fra dårlig sikrede enheter, avlytting av kommunikasjon på lufta, manipulering av meldinger, utnyttelse for DDoS, osv.

I denne analysen trekker vi frem to scenarioer.



Scenario 7: DDoS fra IoT-enheter mot ekominfrastruktur
Av det enorme antallet av IoT-enhetene vil en høy andel være i de private husholdningene og derfor gjenstand for tilfeldig og helst svak sikkerhetsoppgradering. Det fører til at disse er en attraktiv plattform for effektive DDoS-angrep. Noen utnytter denne muligheten og retter angrepet mot ekom-infrastruktur for å ramme tilgjengeligheten til tjenester. Siden enhetene som benyttes i angrepet er spredt både i egne og andres nett innenlands, blir det komplisert å stenge av for den uønskede trafikken.

Scenario 8: Feilsituasjon som kunstig intelligens ikke klarer å håndtere
For å håndtere høy kompleksitet i 5G, tas kunstig intelligens i økende grad i bruk. Det medfører blant annet at kunstig intelligens er nødvendig for å tolke sammensatte feilsituasjoner. På et tidspunkt oppstår det en spesiell tilstand i nettene, pga. endret trafikkmønster fra IoT-enheter. Dette er en anomali, som det automatiserte drifts-/managementssystemet feiltolker. Pga. kompleksiteten blir det vanskelig å finne årsakssammenhengen og normalisere tilstanden igjen.

Figur 15. Risikoanalyse for scenarier knyttet til økt omfang av IoT.

4.6.1 Scenario 7: DDos fra IoT-enheter mot ekominfrastruktur

Scenario 7 innebærer et DDoS mot ekominfrastruktur fra IoT-enheter. Selv om de hver for seg representerer en liten kapasitet, vil det ventelig enorme antallet med enheter gjøre at potensialet for effektive botnetbaserte DDoS-angrep være stort. Hvis slike angrep rettes mot sentrale nettelementer i selve ekominfrastrukturen, vil det kunne få store konsekvenser. Det store antallet modem og rutere som terminerer bredbåndslinjer i hjemmene har vært pekt på som mulige plattformer for denne type angrep tidligere. Med IoT i stor skala, vil en ha en enda mye større potensiell base for DDoS mot ekominfrastruktur.

Nkom vurderer både sannsynligheten for og konsekvensen av at et slikt scenario skal inntreffe er veldig skalerbar, og avhengig av hvilke nettelementer og tjenester som rammes. De potensielle sikkerhetsutfordringene med IoT vil sannsynligvis materialisere seg gradvis i takt med omfanget. Vi forventer derfor at nettilbyderne også gradvis vil utvikle tilpassede mottiltak for å håndtere trusselen. Samlet anser Nkom risikoen for *moderat*.

4.6.2 Scenario 8: Feilsituasjon som kunstig intelligens ikke klarer å håndtere

Under dette risikoområdet har vi valgt å trekke inn elementer også fra andre tilknyttede teknologier som 5G og kunstig intelligens. 5G skal legge til rette for et stort mangfold av anvendelser, hvorav IoT er ett område, og for å håndtere den høye kompleksiteten i 5G-nettene vil en måtte ta i bruk kunstig intelligens. Vi kan anta at de aller fleste situasjoner som oppstår i nettene, vil kunstig intelligens håndtere på en adekvat måte. Hvis derimot en helt ny og uventet kombinasjon av hendelser oppstår, en anomali, er det en mulighet for at kunstig intelligens reagerer på en måte som fører nettet ut i en ukjent tilstand som det tar tid å analysere og komme ut av. En kan trekke en parallell til tilfellene av signaleringsstormer som Telenor opplevde i mobilnettet i 2011. En hadde ikke fullt ut forutsett konsekvensene av veksten i smarttelefoner og endrede bruksmønstre og havnet i et tilstand i nettet som en ikke hadde forutsetninger for å kjenne igjen. En massiv vekst i IoT for et mangfold av formål, er en utvikling som kan ha potensiale til å romme også helt uforutsette endringer i trafikkmønstre som kan skape tilsvarende utfordringer.

Scenario 8 er derfor knyttet til kompleksitet og kunstig intelligens. Evnen til å håndtere slike situasjoner handler i stor grad om kompetanse og helhetlig systemforståelse av egne nett og –tjenester. Som omtalt i kapittel 3 er dette med nødvendig kompetanse i egen organisasjon en utfordring som vil øke i årene som kommer. Slike scenarioer har større usikkerhet, men vi anser risikoen for en slik situasjon i løpet av de neste 5 årene som *moderat til stor*.

4.7 Samlet oversikt over risiko

Tabellen under viser en samlet oversikt over de fremtidige risikoscenarioer som har blitt vurdert innenfor hvert av risikoområdene over. Det er viktig å understreke at denne oversikten

alene ikke gir et fullstendig risikobilde, men heller et utsnitt. Risikoområdene må også sees i sammenheng med risikobildene presentert i de foregående EkomROS-rapportene.

ID	Scenario	Risiko	Usikkerhet
S2	Brudd i tilgang på satellittdata i en spent situasjon	Moderat/stor	Moderat
S4	Cyberangrep som medfører anmodning om nedstenging av trafikk	Moderat/stor	Stor
S8	Feilsituasjon som kunstig intelligens ikke klarer å håndtere	Moderat/stor	Moderat
S3	Hybrid hendelse med manipulering av befolkningsvarsling	Moderat	Stor
S5	Ekstremvær med store utfall i strøm og sambandslinjer	Moderat	Liten
S7	DDos fra IoT-enheter mot ekominfrastruktur	Moderat	Moderat
S1	Populært mobilspill utløser omfattende spoofing-aktivitet	Moderat/liten	Moderat
S6	Brudd på kommunikasjonsvern som følge av programvaresårbarhet i mobilkjernenettet	Moderat/liten	Liten

Tabell 2. Samlet oversikt over risiko og usikkerhet for hvert av scenarioene sortert etter risikokategori (scenarioene innenfor hver av risikokategoriene er sortert etter nummer og ikke etter risiko).Risiko er her en samlet vurdering av både de forventede samfunnsmessige konsekvensene og sannsynligheten for at scenarioet vil inntreffe.

Ut fra vurderingen av disse risikoområdene ser Nkom det som viktig å understøtte arbeidet med romsikkerhet som blant annet koordineres i romsikkerhetsutvalget, deriblant avklaringene om ansvar og roller i i de delene av romvirksomhetens verdikjeder som angår ekomsektoren. I samarbeid med, og med finansiering fra Norsk Romsenter, ble det i juni også lyst ut en toårig prosjektstilling hos Nkom som blant annet skal jobbe med målemetoder og avvikshåndtering i tilknytning til satellittnavigasjonstjenester.

Når det gjelder risikoer knyttet til den øvre delen av krisespekteret, som krise, konflikt og krig, vil Nkom vise til høstens NATO-øvelse, Trident Juncture. Foruten å øve samhandling på myndighetsnivå, blir det viktig å erfare hvordan overordnede planverk og tiltak for totalforsvaret kan omsettes til treffsikre tiltak i ekomsektoren.

Den stadig økende kompleksiteten i ekomnettene og innføring av kunstig intelligens for å håndtere kompleksiteten, vil også kreve et høyt nivå av systemkompetanse og sikkerhetsforståelse hos ekomtilbyderne. Dette for å kunne tilby brukerne tjenester med forsvarlig sikkerhet både i normalsituasjoner og i ekstraordinære situasjoner.

Scenarioene som beskriver ekstraordinære hendelser forbundet med neste generasjon nødnett i kommersielle nett vurderer vi til moderat risiko. Det er imidlertid viktig å understreke at dette forutsetter at de viktigste sikkerhets- og robusthetsutfordringene blir utredet og påbegynt så tidlig som mulig. Den kommende konseptvalgutredningen blir viktig i så måte.