Nasjonal kommunikasjons-myndighet

EkomROS 2017

Risikovurdering av ekomsektoren

7. juni 2017

Forord

Nkom publiserte i fjor vår for første gang en overordnet risikovurdering av ekomsektoren, EkomROS 2016. I årets EkomROS bygger vi videre på risikobildet som vi tegnet da, men samtidig justerer vi oss inn i henhold til erfaringene vi har fra det siste året.

Å forutse hvilke risikoer vi vil møte de nærmeste årene er en krevende oppgave i en bransje som utvikler seg raskt. Likevel mener vi at arbeidet med årlige overordnede risikovurderinger bidrar til å peke ut hvilke hovedretninger myndighetene og virksomhetene i sektoren må rette sin oppmerksomhet mot i sikkerhets- og beredskapsarbeidet.

En viktig forutsetning for en riktig vurdering av risiko innenfor vår sektor, er å forstå hvilken rolle elektronisk kommunikasjon spiller i samfunnet. Å *forstå samfunnets behov* anser vi som så essensielt at det nå inngår som et av Nkoms tre hovedmål i inneværende strategiperiode.

Et illustrerende eksempel har vi fra evalueringen av et uvær i Agder i november i fjor, med sterk vind og snøfall som medførte lengre strømbrudd og ekomutfall, og hvor rådmannen i Vegårshei uttalte følgende i et notat:

> «*Vår erfaring etter denne hendelsen er blant annet at bortfall av mobilnettet kan ha større konsekvenser for kommunens mulighet til å levere nødvendige tjenester til innbyggerne enn det bortfall av strøm isolert har. En rekke av de løsningene som er grunnlaget for trygghet for brukere og pasienter er avhengig av mobildekning i dag, og etter hvert som vi lykkes i arbeidet med å digitalisere tjenester og ta i bruk ny trygghetsteknologi vil konsekvensene bli enda mye større.*»

Samtidig som vi skal legge til rette for næringsutvikling og innovasjon slik at kommuner som Vegårshei skal kunne forbedre og effektivisere sin drift med nye digitale tjenester, må vi også sørge for at disse tjenestene blir trygge å bruke i en hver samfunnstilstand.

Torstein Olsen
direktør, Nasjonal kommunikasjonsmyndighet

Sammendrag

I løpet av 2016 og så langt i 2017 har Nkom mottatt varsler om litt under 150 uønskede hendelser i elektroniske kommunikasjonsnett (ekomnett). Omfanget av hendelser som varsles til Nkom er sammenlignbart med årene før, og de vanligste årsakene er fortsatt fiberbrudd, strømbrudd og utilsiktede feil i utstyr eller programvare.

I perioden har det vært værpåkjenninger som i tre av tilfellene har blitt klassifisert som ekstremvær. Konsekvensene for ekom har vært moderate, men særlig uværet på Sørlandet i november 2016, hvor det sammen med sterk vind uventet kom store mengder våt snø på kort tid, illustrerte kommunenes sårbarhet overfor langvarige strømbrudd med påfølgende mobilutfall.

Hendelsene som har hatt størst kundekonsekvens har vært hendelser hvor det har oppstått feil i programvare eller konfigurasjon. Det er slike logiske feil som har størst potensiale til å ramme mange brukere av ekomtjenester samtidig. Ute i verden har vi også sett eksempler på cyberangrep som har rammet ekominfrastruktur og ekomtilbydere. DDoS-angrep som utnytter IoT-utstyr og løsepengevirus er trusler vi må forvente at også kan ramme ekomsektoren i Norge i årene som kommer.

Nkom har i 2016 og 2017 jobbet med flere proaktive sårbarhetsreduserende aktiviteter. Blant annet har Nkom, sammen med de nordiske søsterorganisasjonene, arbeidet videre med oppfølging av de fellesnordiske anbefalingene for sikkerhet i signaleringssystem nr. 7 (SS7). Videre har det nordiske kollegiet vurdert sikkerheten i signaleringsprotokollen DIAMETER, som erstatter SS7 i 4G, samt sikkerheten i tale over LTE (VoLTE).

I tillegg til erfaringer fra hendelser og kunnskap om avdekte sårbarheter, er det også viktig å vurdere endringene i risikobildet som følge av teknologiske, organisatoriske og samfunnsmessige utviklingstrekk. Hovedsakelig fører denne utviklingen til fremskritt gjennom både rimeligere og tryggere ekomtjenester for brukerne. Men samtidig som gamle trusler og sårbarheter reduseres, introduseres også nye.

De neste årene forventes betydelige endringer i sektoren. Utviklingen innenfor nettverksvirtualisering og automatisering fortsetter, langt på veg drevet frem av kravene som 5G er ment å innfri. 5G vil også innebære et paradigmeskifte innenfor mobiløkosystemet, der vi vil se nye aktørkonstellasjoner, og hvor de store internasjonale internettselskapene ventelig styrker sin posisjon og rolle i sektoren. Parallelt med dette vil særlig mobilnettene bære stadig flere og større samfunnsverdier. Blant annet vil nød- og beredskapsbrukere etter all sannsynlighet realisere sine datatjenester helt eller delvis i de kommersielle mobilnettene.

I risikovurderingen av ekomsektoren legger Nkom det generelle risikobildet i samfunnet til grunn, og ser dette opp mot sårbarhetene i dagens ekomnett og -tjenester, og de potensielle nye sårbarhetene som følger av de kontinuerlige samfunnsmessige, teknologiske og markedsmessige endringene som skjer i sektoren. Formålet med dette er å kunne identifisere viktige risikoområder som sektoren sannsynligvis vil møte de nærmeste årene, og som både ekommyndigheten og bransjeaktørene bør være oppmerksomme på. I EkomROS 2017 har Nkom fokusert på følgende risikoområder:

- Økt internasjonalisering i bransjen svekker den nasjonale kontrollen på kritisk tjenesteproduksjon. Sett i sammenheng med økt avhengighet til disse tjenestene, og et uforutsigbart sikkerhetspolitisk bilde, utgjør dette en økende risiko.

- Tilgang til informasjon om brukere, trafikkdata og innhold har høy verdi i hybrid krigføring. Sammenholdt med stadig mer komplekse verdikjeder, vil risikoen for integritets- og konfidensialitetsbrudd i ekomnett- og tjenester øke.

- Den forventede massive økningen i IoT vil skape mange nye utfordringer i nettene i årene som kommer. Stor vekst av billig utstyr av dårlig kvalitet, samt tilgang til og effekt av jammeutstyr, vil øke risikoen for forstyrrelser i kritisk trådløs kommunikasjon.

- Kombinasjonen av store arealer og lav befolkningstetthet og sterke værpåkjenninger gjør ekominfrastrukturen sårbar i nordområdene. Risikoen påvirkes i tillegg av nordområdenes betydning for både næringsutvikling, sikkerhet og beredskap.

Nkom vurderer at det er en høy risiko forbundet med en forringelse av nasjonal kontroll med kritisk tjenesteproduksjon, gjennom en gradvis økende avhengighet til funksjoner i utlandet de kommende årene. Dette krever at myndighetene må ha en aktiv rolle og finne en god balanse mellom å tilrettelegge for innovasjon, samtidig som nødvendig nasjonal kontroll med nett og tjenester ivaretas for å sikre forsvarlig sikkerhet i fred, krise og krig.

Nkom vurderer også at risikoen er høy for uønskede hendelser knyttet til infrastrukturen i nordområdene. Risikoen påvirkes både av at det er høyere sannsynlighet for langvarige brudd enn ellers i landet, og av den potensielle konsekvensen av tilsiktede handlinger mot infrastrukturen i dette området i en krise- eller konfliktsituasjon.

Risiko knyttet til integritet- og konfidensialitetsbrudd, og forstyrrelser i kritisk trådløs kommunikasjon må også håndteres. Her har imidlertid myndighetene stor drahjelp fra bransjen, som har egeninteresse i å få bukt med problemene, for å ivareta brukernes tillit.

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 dermed ikke et overordnet sektorperspektiv. Nkom har derfor behov for å gjennomføre overordnede vurderinger av risiko og sårbarhet for å danne et helhetlig risikobilde av sektoren.

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

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 fra året som har gått, mens vi i kapittel 3 ser fremover og drøfter betydningen av relevante utviklingstrekk i sektoren. Sammen med det generelle risikobildet i samfunnet, danner dette grunnlag for å identifisere viktige risikoområder. I kapittel 4 utforsker vi potensielle uønskede hendelser (scenarioer) innenfor de identifiserte risikoområdene. Den samlede risikovurderingen oppsummeres i kapittel 5.

2 Erfaringer fra 2016 og første halvår 2017

2.1 Uønskede hendelser

Tilbyderne er forpliktet til å varsle Nkom om hendelser som vesentlig kan redusere eller har redusert tilgjengeligheten til ekomtjenester. I 2016 og så langt i 2017 har Nkom mottatt varsel om i underkant av 150 hendelser. De innrapporterte hendelsene varierte i varighet og omfang, men vanlige årsaker var fiberbrudd, strømbrudd og utilsiktede feil i utstyr eller programvare. Både omfang og feilårsaker er sammenlignbare med årene før, og viser at de generelle utfordringene knyttet til vær, strømutfall, graveskader og feil i forbindelse med endringer, fortsatt er aktuelle.

Ved større hendelser innhenter Nkom hendelsesrapport fra ekomtilbyderne. I siste periode har Nkom innhentet rapport for totalt 12 hendelser som har blitt vurdert nærmere opp mot ekomlovens krav til sikkerhet og beredskap. Ved ett tilfelle ble tilbyder ilagt overtredelsesgebyr for mangelfulle rutiner for testing i etterkant av utført endrings- og vedlikeholdsarbeid i nettet. Ut over dette medførte ikke hendelsene sanksjoner fra Nkoms side.

2.1.1 Fiberbrudd og sjøkabler

Enkelthendelser setter fokuset på spesifikke sårbarheter. Bruddet på fiberkabelen utenfor kysten av Varangerhalvøya i januar 2017 medførte at 3500 innbyggere i to kommuner var uten nett og telefon i to døgn. Bruddet forårsaket også at maritim nødsamband var nede langs store deler av Finnmarkskysten. Hendelsen bidro til oppmerksomhet på lokalsamfunn som er avhengige av sjøkabler for at ekomtjenester skal fungere.

Et sjøkabelbrudd i Bindal i starten av februar 2017 medførte at deler av kommunen var uten ekom i mer enn fem døgn. Kritikken i etterkant av hendelsene har vært at sjøkabelberedskapen er for dårlig og at feilretting på sjøkabler ofte tar lang tid.

Mobilnettene benytter mange steder felles transmisjonsløsning og der hvor de gjør det, vil et fiberbrudd kunne ramme alle disse mobilnettene. Dette skjedde i februar 2016, hvor en fiberfeil mellom Aurskog og Blaker førte til utfall i 19 timer for Telenors og Telias mobilkunder i kommunene Fet, Nes, Aurskog-Høland og Rømskog. I tillegg var bredbånds- og fasttelefonkunder rammet av samme feil.

2.1.2 Ekstremvær

I perioden har det vært tre ekstremvær, Tor (januar 2016), Urd (desember 2016) og Vidar (januar 2017). Tor og Urd ble klassifisert som ekstremvær på grunn av vindstyrken mens høy vannstand (springflo) var hovedingrediensen i Vidar. Typisk for konsekvensen av ekstremvær

er skade på infrastruktur for strøm og ekom. Reservestrømkapasiteten for ekom er ofte begrenset, slik at langvarige strømutfall fører til ytterligere utfall av ekom.

Ekstremværet Tor traff Norge med voldsom kraft 29. januar 2016. På tross av at det ble satt ny vindrekord utenfor Møre og Romsdal ble konsekvensene for ekom mindre enn forventet. Nkom avsluttet sin beredskap etter tre dager. Konsekvensen var da kun sporadiske utfall fordelt utover området ekstremværet hadde rammet. Urd rammet Vestlandskysten 26. desember 2016. Urd var mindre kraftig enn Tor og konsekvensene var også mindre.

Med ødeleggelsene etter ekstremværet Dagmar fortsatt friskt i minne var forventningen at den kraftige vinden i ekstremværene Tor og Urd ville forårsake store ekomutfall som følge av strøm- og fiberbrudd. Konsekvensene ble langt mindre enn forventet ved begge ekstremværene. En av årsakene til dette kan være at infrastrukturen i de mest værutsatte områdene er gjort mer robust enn tidligere. Dette gjelder blant annet reservestrømkapasitet, fysisk og logisk redundans samt fysisk sikring av infrastruktur. Nkom opplever også at tilbyderne har blitt flinkere til å øke beredskapen i forkant av ekstremvær, med det resultat at rettetiden for de enkelte utfallene reduseres. Det var heller ikke større strømutfall under ekstremværene, noe som tyder på en tilsvarende positiv utvikling for kraftsektoren.

Sterk vind og tung, våt snø natt til søndag 6. november 2016 i Aust-Agder, Vest-Agder, Telemark og Vestfold, førte til omfattende trefall med påfølgende skade på kraftlinjer og enkelte fiberkabler. Ekstremvær varsles vanligvis i god tid og beredskapen kan heves før utfallene inntreffer. Det var ikke mulig i dette tilfellet. Den spesielle værsituasjonen kom uventet og var utfordrende for tilbyderne. Mer enn 9000 husstander var uten strøm de første timene. Strømutfall og spredte fiberbrudd medførte utfall i alle de tre mobilnettene. Også ved denne hendelsen viste felles transmisjon for flere mobiltilbydere seg som en sårbarhet. Samtidig med uværet fikk Telenor et dobbeltbrudd i landsnettet. Det tok fire dager før situasjonen var normalisert.

Konsekvensene av snøværet ble størst et stykke inn i landet, som kjennetegnes med lavere befolkningstetthet og dårlig fremkommelighet for retting av feil på kraftsambandet.

2.1.3 Logiske feil

Natt til 2. februar 2016 oppstod en ustabilitet i hele Telenors mobilnett i forbindelse med et planlagt arbeid som avsluttet en periode med pilottest. En parameter ble konfigurert feil under dette arbeidet. Feilen ble oppdaget da man så at trafikkvolumet i nettet utover morgenen ikke var som normalt, og Telenor opplyste at opp mot 25 % av kundene kunne oppleve problemer med datatrafikk denne morgenen.

19. februar 2016 sviktet sentrale komponenter i Telenors mobilnett på grunn av innkommende signalering (SS7) som viste seg å komme fra et utenlandsk sikkerhetsselskap. Signaleringen

trigget en programvarefeil i kjernenettet til Telenor. Hendelsen var en påminnelse om at programvare kan inneholde feil som ikke blir avdekket i test, men først viser seg etter lengre tid i ordinær produksjon. Det hadde forut for det aktuelle tidspunktet vært oppmerksomhet på sårbarheter i SS7. Selv om det viste seg at utfallet ikke skyldtes noen slik sårbarhet eller forsøk på å utnytte slike, ga hendelsen læring i hvordan hendelser knyttet til signalering mellom operatører og over landegrenser må håndteres.

Telias mobilnett i Norge har funksjoner i sitt kjernenett lokalisert i Sverige. 15. juni 2016 forårsaket en feilkonfigurert ruter i Sverige at norske mobilkunder ble rammet. Telia oppgir at over 63 000 abonnenter fikk problemer med å få tilgang til mobilnettet. Feilen oppstod i forbindelse med planlagt arbeid, varte i en time, og ble rettet ved at arbeidet ble stoppet og reversert.

På formiddagen 29. august 2016 meldte Telia til Telenor at deres kunder hadde problemer med å nå abonnenter hos Telenor. Videre undersøkelse avdekket at også intern trafikk i Telenors nett var berørt. Antall samtidige anrop og samtalevarighet i nettet gikk ned og feilrate for anropsoppsett gikk opp. Feilen viste seg ikke å være konsekvent og det var tilfeldig om et anrop ble berørt. Årsaken til feilen viste seg å være en konfigurasjonsendring i forbindelse med planlagt arbeid i nettet. 30 % av taletrafikken i Telenors mobilnett ble berørt av problemet i en tretimers periode.

28. november 2016 ble ICE rammet av et strømbrudd i en av sine kjernenettlokasjoner. I følge ICE oppstod det en feil da redundante noder i kjernenettet skulle ta over trafikken, såkalt failover. Strømmen var borte i en halv time, men feilen som oppstod forårsaket ustabilitet i tjenesteproduksjonen for tale og meldingstjenester i ti timer.

Utilsiktede logiske feil i kjernenettet og transportnettet er den type feil som potensielt har de største konsekvensene for brukere og tilbydere av tjenester som er avhengige av ekom. Mens ekstremvær stort sett rammer enkeltområder kan logiske feil slå ut eller redusere tjenestekvalitet i hele landet. Planlagt arbeid er fortsatt den hyppigste utløsende årsaken til logiske feil. Nkom har overfor tilbyderne påpekt viktigheten av rutiner og etterlevelse av disse, i forbindelse med planlagte endringer i nett. Risiko- og sårbarhetsanalyser er grunnlaget for god beredskap også for den logiske sikkerheten.

2.1.4 Ondsinnet programvare

Mirai er navnet på en skadevarefamilie som kobler sammen IoT-utstyr til et botnet. I august 2016 ble koden oppdaget og i oktober ble kildekoden til skadevaren sluppet på Internett. På senhøsten 2016 forårsaket Mirai at den amerikanske DNS-leverandøren[1] Dyn ble tatt ned ved hjelp av et tjenestenektangrep (DDoS), og dette medførte at mange tjenester var utilgjengelige

[1] Leverandør av tjeneste som omsetter domenenavn til IP-adresser, en kritisk tjeneste for Internett.

i en lang periode. Med økningen av IoT-utstyr som forventes de kommende årene må man også forvente at denne type DDoS-angrep vil øke i omfang.

I mai 2017 ble over 230.000 datamaskiner i 150 land rammet av løsepengeviruset WannaCry. Viruset er en kryptoorm som angrep sårbare datasystemer. De mest kjente ofrene var Britiske National Health Service (NHS), teleoperatøren Telefónica, Tyske jernbaner og FedEx.
En av årsakene til at WannaCry fikk stor oppmerksomhet er at sårbarhetene som benyttes tidligere er benyttet i programvare utviklet av/for den amerikanske etterretningsorganisasjonen NSA. Dette ga hendelsen også en politisk dimensjon. Wannacry rammet også noen norske virksomheter, men ingen i ekomsektoren. Nkoms nyopprettede EkomCERT arbeidet under hendelsen i nær dialog med NorCERT, og bidrog med informasjonsdeling og formidling av skadeforebyggende og skadereduserende tiltak til virksomhetene i ekomsektoren.

2.2 Avdekte sårbarheter

Markedet i ekomsektoren er i stadig endring og der gamle sårbarheter fjernes, vil ofte nye sårbarheter introduseres. Nkom har det siste året hatt flere proaktive aktiviteter rettet mot å identifisere og håndtere viktige sårbarheter.

2.2.1 Sikkerhet mellom mobilnett

SS7 består av et sett av protokoller som brukes for å styre tjenester i både faste og mobile nett. SS7 ble designet for å operere i et tillitsbasert miljø der samarbeidende tjenestetilbydere kunne stole på at meldingene som ble sendt utelukkende hadde legitime formål. Slik som ekomsektoren har endret seg, har nå et stort antall aktører tilgang til SS7-grensesnitt og kan sende signaleringsmeldinger til andre tjenestetilbydere. Skadepotensialet ved urettmessig utnyttelse av SS7 er størst i mobilnettene og det er særlig på grensesnittet mellom operatører det er viktig med forbedret kontroll.

I siste generasjon mobilnett er SS7 i stor utstrekning erstattet av et nyere sett med protokoller, DIAMETER. Nkom har derfor sammen med de andre nordiske ekommyndighetene valgt å kartlegge i hvilken grad operatører adresserer sikkerhet i DIAMETER. Det synes vanskelig å finne løsninger som gir fullgod sikring av meldingsutvekslingen. Meldingsutveksling skjer mellom operatører i hele verden og selv om en operatør sikrer kommunikasjonen til sine nærmest tilgrensende partnere, vil en ikke være sikret fullt ut uten at alle innfører tilsvarende tiltak. Nkom har likevel tro på at kommunikasjonen langt på veg kan sikres med avbøtende tiltak.

2.2.2 Taletjenester

Tale i 4G eller Voice over LTE (VoLTE), er en taletjeneste som nå er tilgjengelig for mange norske mobilabonnenter. Noen av fordelene ved VoLTE er raskere oppkoblingstid, uavhengighet til 3G/2G-dekning for å kunne ringe og motta samtaler, redusert batteribruk og

HD talekvalitet. VoLTE er gjerne utvidet med mulighet for tale over lokalt bredbåndsnett, Wifi-tale. Det har vært demonstrert sikkerhetsproblemer ved uheldige tekniske implementeringer av tale over LTE og Wifi.

Nkom er videre kjent med at det i Norge og noen av våre naboland har vært rapportert om tjenestenektangrep for telefoni (TDoS). TDoS har blitt et økende problem med økende forekomst av Voice over IP (VoIP). Mens manipulering på gamle telefonisystemer krevde spesialkunnskap, er tale over IP på en helt annen måte sårbar for manipulering på grunn av at IP-protokollen er så utbredt og kjent. TDoS ses ofte i kombinasjon med manipulering av avsenderadresse i VoIP. Nkom deltok i siste år i en felles nordisk undersøkelse av status for sikkerheten i disse nyere taletjenestene.

Samtidig som disse teknologiene åpner for rimelige og fleksible tjenester, viser erfaring at det er viktig at det legges vekt på sikkerhet når operatørene gjør sine implementasjonsvalg.

2.2.3 Avhengighet til satellittbasert tid (PNT-strategi)

Posisjonsbestemmelse, navigasjon og tidsbestemmelse (PNT) spiller en stadig større rolle i dagens samfunn. I tillegg til bruk i navigasjon innen luft- og sjøfart, er nøyaktig tidsangivelse viktig blant annet innenfor finans, elektrisitetsdistribusjon og ikke minst innenfor elektronisk kommunikasjon. Regjeringen har besluttet å utarbeide en nasjonal og tverrsektoriell strategi for PNT hvor hensikten er å øke bevisstheten rundt bruk av PNT i egne sektorer, samt for å forsøke å identifisere tverrsektorielle gevinster der slike finnes. Arbeidet ledes av Norsk Romsenter.

For produksjon av elektroniske kommunikasjonstjenester er nøyaktig bestemmelse av tid og takt (frekvens) viktig. Absolutt tid brukes til tidsstempel for eksempel i logger, mens takten benyttes for å synkronisere radiofrekvenser og datastrømmer i og mellom nettverk. I de elektroniske kommunikasjonsnettene benyttes i stor grad GNSS[2] direkte eller indirekte som kilde til nøyaktig tid, frekvens og takt. Tid, frekvens og takt implementeres ulikt i de forskjellige elektroniske kommunikasjonsnettene, og således vil også konsekvensene ved bortfall av eller feil på satellittbasert tid/takt kunne variere ut fra ulikheter i nett og teknologi.

I EkomROS 2016 vurderte Nkom hvilke konsekvenser bortfall av GPS kunne ha for elektroniske kommunikasjonsnett og -tjenester og dernest hvordan dette ville bidra til negativ samfunnskonsekvens. Vurderingen var da at et bortfall av satellittbaserte systemer som gir tid/takt ikke vil ha umiddelbare konsekvenser for elektroniske kommunikasjonstjenester, men at det ved lang varighet, typisk rundt 30 dager, vil kunne skape økende grad av degradering av kritiske tjenester.

[2] Global Navigation Satellite System, en samlebetegnelse for satellittbaserte navigasjonssystemer som GPS, Galileo, Glonass mv.

Nkom vil likevel påpeke at det eksisterer øvrige risikoer og sårbarheter som det bør rettes fokus mot. Et eksempel er indirekte påvirkning gjennom komplekse verdikjeder. I drift og vedlikehold av nett og tjenesteproduksjon er det sterke avhengigheter til for eksempel elforsyning, IT- og støttesystemer og vare- og persontransport, som igjen er avhengig av satellittbaserte tjenester. Bortfall av satellittbaserte tjenester vil således indirekte kunne påvirke elektronisk kommunikasjon. Nkom anser derfor at den nasjonale, tverrsektorielle PNT-strategien vil være et viktig virkemiddel for å adressere denne type sårbarheter.

2.2.4 Slukking av FM-nettet

Etter at utbyggingen av DAB hadde oppfylt de kravene til dekning som Stortinget hadde satt[3], startet slukkingen av FM-nettet i januar 2017 og skal være gjennomført i desember. Nkoms rolle har vært å måle og beregne at dekningen er minst så god som forutsatt. Det har vært lagt til grunn at sammenlikningene skulle gjøres for stereosignaler.

FM-nettet har hatt flere viktige funksjoner i beredskapssammenheng. For det første er NRK P1 primærkanalen for meldinger til befolkningen ved kriser. Derfor er det viktig at DAB-nettet har like god rekkevidde som FM. Sivilforsvaret har benyttet FM-nettet som bærer av utløsersignaler for tyfonsirenene for nasjonal befolkningsvarsling. Denne bærerfunksjonen er nå overtatt av Nødnett.

Slukkingen av FM-nettet har vært møtt med mye skepsis og til dels også aktiv motstand. Ett argument har vært at FM i monokvalitet kunne nå lenger ut enn DAB og at dette kan bety at en noen steder får marginalt dårligere dekning enn før. Det har på den andre siden vært argumentert med at dekningen i vegtuneller er vesentlig bedre bygd ut for DAB og at utstyr bygd på ny teknologi er langt mer driftssikkert enn gammelt utstyr. Matingen av senderne er også mer robust mot enkeltutfall enn før, idet alle sendere mates individuelt og svikt i én sender ikke forplanter seg til flere i samme kjede.

Ca. 5 % av befolkningen dekkes av DAB-sendere som mates via satellitt. Den 18. januar 2017 førte to fiberfeil til at disse var uten mating i noen timer. Løsningen for satellittmating av DAB ble styrket som en følge av hendelsen.

2.3 Veiledning og tilsyn - utkontraktering

I 2016 og frem til mai 2017 har Nkom gjennomført tre stedlige tilsyn, hos henholdsvis Telenor, Broadnet og Telia, med fokus på sikkerhet og beredskap. Et funn som har gått igjen er mangler og svakheter ved gjennomføring av ROS-analyser og utarbeidelse av

[3] NRKs radiotilbud må ha digital dekning tilsvarende dagens P1-dekning i FM-nettet, altså 99,5 % befolkningsdekning

beredskapsplaner. Ved noen tilfeller er det også avdekket manglende involvering fra ledelsen når det kommer til risikostyring og beredskap. Nkom er særlig bekymret for disse manglende når de kommer i forbindelse med utkontraktering av tjenester.

Etter å ha sett en økning i utkontraktering av tjenester de siste år, har Nkom tidligere gitt veiledning til tilbydere om hvilke begrensninger som følger av regelverket. Veiledningen gitt av Nkom rettes både mot konfidensialitets- og taushetsplikt, krav til sikkerhet, bruksbegrensning, objektsikkerhet og risikovurderinger.

I desember 2016 ble Direktoratet for nødkommunikasjon (DNK) varslet om at deres transmisjonsleverandør Broadnets indiske underleverandør Tech Mahindra hadde fått tilgang til transmisjonsnoder som inngikk i leveransen til Nødnett. I februar 2017 slo NRK saken opp, og den fikk bred oppmerksomhet, ettersom dette av flere var ansett som et brudd på sikkerhetslovens bestemmelser.

Som oppfølging av hendelsen, gjennomførte Nkom i februar og mars 2017 tilsyn med Broadnet og Tech Mahindra. Tilsynet hos Broadnet er ikke avsluttet, men hendelsen illustrerer viktigheten av barrierer, deteksjon, verifikasjon og reaksjon også i den logiske dimensjonen av sikkerhet.

3 Utviklingstrekk de kommende årene

Den samfunnsmessige, teknologiske og markedsmessige utviklingen har stor påvirkning på hvordan ekomnett og -tjenesters sårbarheter vil endre seg de kommende årene. Å identifisere relevante utviklingstrekk i sektoren er derfor en viktig del av en overordnet risikovurdering. Fremover ser Nkom grunn til å ha særskilt fokus på mobilnettenes rolle, utviklingen mot 5G, og endringer i aktørbildet i sektoren.

3.1 Mobilnettene bærer samfunnet på sine skuldre

Svært mye av utviklingen innenfor digitalisering i alle samfunnssektorer, baserer seg enten fullt ut på, eller inkluderer, mobilnett og mobilkommunikasjon. Digitalt sårbarhetsutvalg (NOU 2015:13) beskriver tilstanden på denne måten:

> *De siste tiårene har digitaliseringen ført til gjennomgripende samfunnsmessige endringer. Den har effektivisert arbeidshverdagen for de fleste av oss, slik at det samme arbeidet nå kan utføres av langt færre hender. Den har forandret måten vi styrer prosesser på, slik at komplekse operasjoner og infrastrukturer nå kan kontrolleres fra ett eller noen få sentrale steder. Den har gitt befolkningen en lang rekke nye tjenester, som kontantløs handel og finansielle tjenester på mobil, elektronisk samhandling med det offentlige og sanntids trafikkinformasjon som lar oss finne den mest hensiktsmessige reiseveien mellom to steder. Videre har den revolusjonert måten vi kommuniserer på, ved at mobiltelefoner, sosiale medier og samarbeidsstøtteverktøy er blitt dagligdags.*

Bortfall av mobildekningen, eller brudd på konfidensialiteten eller integriteten i mobilkommunikasjonen får derfor allerede i dag betydelige samfunnskonsekvenser. Alle tegn tyder også på at denne utviklingen vil fortsette i økende fart de kommende årene. Mobilnettene og -tjenestene blir utnyttet for stadig nye bruksområder, noe som gjør at Nkom har alle grunner til å tro at konsekvensene ved bortfall og sikkerhetsbrudd bare vil øke i tiden fremover.

I tillegg til den økende bruken av mobiltelefonplattformen for nye tjenester, som for eksempel mobilbetaling, så forventes det de kommende årene også en formidabel økning i antallet maskiner og sensorer (IoT) som skal kobles til blant annet mobilnettene for maskin-til-maskin-kommunikasjon. Ved utgangen av 2016 var det i Norge registrert nærmere 1,24 millioner SIM-kort for maskin-til-maskin-kommunikasjon. Dette var en økning på over 200 000 fra året 2015. Til sammenligning var økningen fra 2014 til 2015 i overkant av 100 000 SIM-kort. Vi regner med at vi fortsatt bare er i startgropa. En bekymring er at mye av IoT-utstyret som vil komme på markedet kan ha dårlig sikkerhet, noe som også kan utnyttes for eksempel til å gjennomføre tjenestenektangrep i nettene de er tilkoblet.

Ut over den dagligdagse bruken av mobiltjenester, vil også mobilnettene få en stadig viktigere rolle for totalforsvaret i Norge og for landets evne til å håndtere krisesituasjoner, konflikter og krig. I dag, og frem til 2026, har nødetatene anledning til å dekke talekommunikasjonsbehov gjennom sitt dedikerte mobilnett, Nødnett. Dette nettet har imidlertid ikke kapasitet til å håndtere fremtidens datatjenester. Fremtidens datatjenester for nødetatene vil derfor etter all sannsynlighet måtte realiseres i de kommersielle mobilnettene. Også den nye langtidsplanen for Forsvaret[4] går langt i å legge opp til økt bruk av, og avhengighet til sivil teknologi i Forsvaret:

> *Forsvarets infrastruktur vil i større grad enn i dag fremstå som en integrert del av samfunnets øvrige IKT-infrastruktur. Nødvendig robusthet vil i størst mulig grad oppnås ved at samfunnets eksisterende infrastruktur forbedres og suppleres med tilgjengelig militær og sivil teknologi.*

Den økte bruken av sivile og kommersielle ekomnett og -tjenester også for kritiske samfunnsfunksjoner henger sammen med at man ikke er i stand til å utvikle proprietære og dedikerte kommunikasjonssystemer som kan holde følge med innovasjonstakten, kapasitetsøkningen og tjenesteutviklingen som skjer i de kommersielle mobilnettene. For eksempel har man i Storbritannia valgt å basere det nye nødnettet på den kommersielle mobiloperatøren EEs LTE-nett. De norske myndighetene er derfor opptatt av å tilrettelegge for at de kommersielle mobilnettene, i størst mulig grad skal kunne bære fremtidige tjenester for nød- og beredskapsbrukere, og har også dette som uttalt mål i Digital agenda for Norge[5]. I nært samarbeid med Direktoratet for samfunnssikkerhet og beredskap (DSB) og Forsvaret har Nkom jobbet med tilsvarende problemstillinger i forbindelse med forberedelsene til tildeling av 700 MHz-båndet, som regjeringen har bestemt skal benyttes til mobile tjenester.

En konsekvens av dette er at sikkerheten og robustheten i mobilnettene og i underliggende ekominfrastruktur, stadig må videreutvikles for å kunne håndtere hendelser i den øvre delen av krisespekteret, som naturkatastrofer, sikkerhetspolitiske kriser og konflikt. Dette underbygges blant annet av Nkoms rapporter til Samferdselsdepartementet om robuste og sikre transportnett[6], forslag til krav om nasjonal autonomi[7], og at det i Nasjonal transportplan[8] er foreslått satt av 80 millioner kroner i første planperiode til et pilotprogram for styrking av den nasjonale transportnettinfrastrukturen.

[4] Prop. 151 S (2015-2016) Kampkraft og bærekraft
[5] Meld. St. 27 (2015-2016) Digital agenda for Norge
[6] «Robuste og sikre transportnett», Nkom, april 2017
[7] «Nasjonal autonomi i norske elektroniske kommunikasjonsnett», Nkom, mars 2017.
[8] Meld. St. 33 (2016-2017) Nasjonal transportplan 2018-2029

3.2 Veien mot 5G, virtualisering og automatisering

Neste generasjons mobilnett – 5G – har vært omtalt i flere år, men i løpet av bare det siste året har utviklingen av 5G-økosystemet skutt fart. EU-kommisjonen la i slutten av 2016 frem en handlingsplan med mål om å introdusere 5G-nett fra 2018 frem til kommersiell introduksjon i EU senest mot slutten av 2020. De nordisk-baltiske myndighetene arbeider nå også om en felles handlingsplan for 5G for Norden og Baltikum. Standardiseringsorganer, utstyrsleverandører og operatører utvikler spesifikasjoner og standarder, og utvikler og tester løsninger som skal tilfredsstille de uttalte brukerkravene. I Norge arrangerte Telenor i mars 2017 et pressetreff med en første live test av 5G i Norge, i samarbeid med Huawei.

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. For å få til dette vil nettverksvirtualisering være en nøkkelteknologi. Virtualiseringen skal legge til rette for at ett og samme fysiske mobilnett kan deles inn i flere logiske nett med forskjellige egenskaper tilpasset ulike tjenestetyper (omtalt som *network slicing*). For eksempel krever videostrømming til en mobiltelefon stor båndbredde i motsetning til sensoren i oppdrettsanlegget, som bare skal sende små datamengder av og til, og ellers gå i dvalemodus for å spare batteri. Autonome kjøretøy må på sin side ha garantert tilgang og svært lav responstid i kommunikasjonen i nettet. Slik kan også brukergrupper med særskilte behov, som for eksempel nød- og beredskapsbrukere, få egen *network slice* med tilpassede funksjoner og egenskaper.

Virtualiseringen innebærer at maskinvaren i større grad blir generisk, mens de ulike funksjonene blir definert i programvare. Dette tilrettelegger også for at nettverksfunksjoner og tjenesteproduksjon etter hvert kan flyttes til «skyen». Det vil si at utførelsen av funksjonene kan frikobles fra en bestemt maskinvare i en bestemt lokasjon. Mens felles kontrollfunksjoner kan utføres fra sentraliserte datasentre, må innhold og brukerdata flyttes og prosesseres så nærme brukerne som mulig for å redusere responstiden. Den faktiske prosesseringen av de sentraliserte kontrollfunksjoner og sentrale databaser forventes plassert i eksterne datasentre, fremfor proprietære teleanlegg. Tilrettelegging for datasenterindustrien i Norge vil derfor bidra til å legge til rette for at disse funksjonene kan utføres i Norge[9].

Implementering av 5G vil kreve ny design både i mobilkjernenettet og på radioaksessen. Samtidig som 5G gradvis innføres, må teknologien i mange år virke sammen med eldre generasjoner som 4G. Dette vil innebære svært komplekse programvaresystemer og vil kreve avansert konfigurasjon. Blant annet på grunn av den økte kompleksiteten forventes det også at konfigurasjonen i større og større grad vil automatiseres. Automatiseringen bidrar videre til å

[9] «Kartlegging og vurdering av infrastruktur som kan nyttiggjøres av datasentre», Nkom, desember 2016

effektivisere bestillingsprosesser, provisjonering av nye kunder, trafikkstyring mm. Automatiseringen vil dermed bidra til større dynamikk og muligheten til raskere endringer, og til lavere kostnader. I sum forventer Nkom at programvarekompleksiteten i mobilnettene vil øke betraktelig i fremtiden. Sårbarhetene knyttet til programvare, til konfigurasjon, endringer og endringshåndtering vil derfor bli viktige å håndtere.

3.3 Markeds- og aktørbilde i endring – nye konstellasjoner

De raske teknologiske endringene som skjer i sektoren medfører endringer i aktørbildet i ekomsektoren. De tradisjonelle ekomtilbyderne opererer i et marked hvor de utfordres av nye typer aktører. For eksempel har mobiltilbyderne over mange år vært utfordret av de store Internett-aktørene som tilbyr «gratis» tale- og meldingstjenester over-the-top (OTT), som iMessage, Skype, Messenger, WhatsApp osv. Dette har gjort at tilbyderne har måttet endre prisstrukturer, og i dag har de fleste mobilabonnementer fastprisstruktur med en gitt datamengde, uten særskilt taksering av tale og SMS.

Hvordan markeds- og aktørbildet vil se ut de neste årene er svært vanskelig å forutse. Nkom forventer at markeds- og aktørbildet vil være preget av disruptive endringer. Det vil si at det vil dukke opp nyskapinger innen teknologi og tjenester som «forstyrrer» det eksisterende markedet ved å gjøre eksisterende forretningsmodeller irrelevante. Gode eksempler på disruptiv teknologi er iPhone, iPad og Tesla. Markedslederen Nokia klarte ikke å svare på utfordringen fra Apple og Google og falt på under to år til en tiendeplass av verdens produsenter av smartmobiler. Tesla kom fra «ingenting» og ble på ett år markedsleder for luksusbiler i Norge.

Det pågår en omfattende posisjonering og alliansebygging i nær sagt alle virksomheter for å være forberedt på endringene som 5G og IoT vil innebære. Et av mange eksempler er Ericsson og Microsoft som i en pressemelding 17. mai annonserte at de blant annet vil samarbeide om «Simplifying the launch of mobile network-based IoT services for enterprises». I Norge ser man at Telenor og Telia kappes om å promotere sine løsninger for IoT gjennom å bygge allianser med samarbeidspartnere.

Aktører som Google og Apple har et solid grep om smartmobilmarkedet med sine økosystemer og mobiltelefoner (Android/Pixel og iOS/iPhone). Analyseselskapet Gartners tall for smarttelefonsalget i fjerde kvartal 2016 viser at Android og iOS har henholdsvis 82 % og 18 % markedsandel på verdensbasis. Sammen med Microsoft, som fortsatt er størst i desktopmarkedet, kan de store aktørene tilby produkter og tjenester basert på sin allerede dominerende posisjon i markedet. De innehar også finansielle muskler til å kjøpe opp nyskapninger og konkurrenter for å befeste sin posisjon i markedet.

Konkurransen fra OTT-tjenester gjør at fremtiden for tradisjonell tale og video i mobilnettene er usikker. 5G kan bli en plattform hvor store aktører kan sy sammen logiske nett på tvers av landegrenser og ekomtilbydere. Google sitt Project Fi er et eksempel på en tjeneste som blant annet tilbyr et logisk nett på tvers av ulike mobil- og bredbåndsnett.

Teknologi- og markedsendringene og globaliseringen i form av oppkjøp/sammenslåing av aktører, gjør at ekomtilbyderne er avhengige av å posisjonere seg i de nye verdikjedene for ikke å ende opp som rene transmisjonstilbydere.

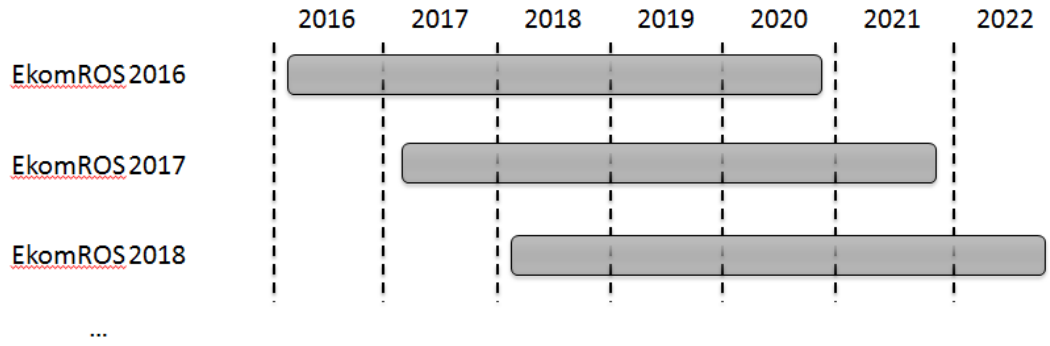
Den innovasjonskraften som pågår vil skape nye tjenester som i neste omgang vil bidra til effektivisering innenfor alle samfunnssektorer. Men dette forutsetter samtidig at disse tjenestene til en hver tid, og i en hver samfunnstilstand, må være tilgjengelige og at integritet, konfidensialitet og personvern ivaretas.

4 Risikovurdering

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 både utilsiktede og tilsiktede uønskede hendelser i hele krisespekteret, og samtidig alle aspekter av sikkerhet: tilgjengelighet, integritet og konfidensialitet.

Nkom har i vurderingen lagt til grunn det generelle risikobildet i samfunnet, og sett dette opp mot sårbarhetene i dagens ekomnett og -tjenester, og de potensielle nye sårbarhetene som følger av de kontinuerlige samfunnsmessige, teknologiske og markedsmessige endringene som skjer i sektoren. Nettopp på grunn av denne raske utviklingen, har Nkom sett på potensielle uønskede hendelser (scenarioer) i en antatt virkelighet innenfor de neste fem årene. Fremskrivingen baserer seg på det generelle trendbildet. Formålet med dette er å kunne identifisere viktige risikoområder som sektoren sannsynligvis vil møte de nærmeste årene, og som både ekommyndigheten og bransjeaktørene bør være oppmerksomme på.

Risikovurderingene som presenteres for 2017 ugyldiggjør ikke vurderingene fra 2016. Årets vurdering er heller dels en utfylling og dels en justering av fjorårets. Sammenhengen mellom dem illustreres i Figur 1.



Figur 1. De årlige vurderingene av fremtidig risiko kompletterer hverandre

Som alltid er risikovurderinger beheftet med større eller mindre grad av usikkerhet på bakgrunn av erfaringsmateriale og kunnskapsgrunnlag. Angivelse av usikkerhet inngår derfor som en viktig del av vurderingene. I teksten omtales risikoen knyttet til en potensiell uønsket hendelse som *lav/moderat*, *moderat* eller *moderat/høy*, basert på Nkoms vurderinger av den kunnskapsbaserte sannsynligheten for, og konsekvens av, hendelsen.[10] I konsekvensvurderingen er det tatt hensyn til om hendelsen svekker kommunikasjonsvernet (konfidensialitet/integritet) eller ekomtjenesters tilgjengelighet. Videre tas det hensyn til geografisk omfang, varighet og hvilke ekomtjenester som påvirkes, om hendelsen påvirker

[10] Metodegrunnlag er NS 5814 (Krav til risikovurderinger) og NS 5832 (Krav til sikringsrisikoanalyse)

dagliglivet gjennom uro/påkjenninger, om den påvirker liv og helse, eller om den kan svekke sentrale institusjoners funksjons- eller styringsevne. For tilsiktede hendelser tar konsekvensvurderingen også hensyn til om handlingen er rettet mot tilfeldige mål eller er målrettet, og om handlingen er økonomisk, politisk, sikkerhetspolitisk eller militært motivert.

4.1 Det generelle risikobildet

Ekomsektoren består av aktører med et vidt virksomhetsområde; fra fysisk infrastruktur i sjø, land og i verdensrommet, til formidling og produksjon av elektroniske kommunikasjonstjenester og innholdstjenester. Sektoren påvirkes derfor svært ofte direkte av risikoene som samfunnet for øvrig møter, enten det er utilsiktede hendelser som ekstremvær, tekniske eller menneskelige feil, eller det er tilsiktede ondsinnede handlinger. Digitaliseringen innenfor alle samfunnsområder gjør også at hendelser som rokker ved den underliggende ekominfrastrukturen, raskt får alvorlige samfunnskonsekvenser.

Naturhendelser og klimarelaterte endringer som medfører økende grad av ekstremvær påvirker ekomsektoren i stor grad, og da spesielt hendelser knyttet til strømbrudd og fiberbrudd. DSB gjennomførte i 2016 en rekke risikoanalyser av ulike scenarioer. Et av dem var «regnflom i by», hvor konsekvenser for blant annet ekomsektoren er beskrevet. Konsekvensene som ble beskrevet i scenariet til DSB er typiske for hvilke hendelser som potensielt kan oppstå ved ekstremværhendelser - store mengder vann på avveie kan forårsake fiberbrudd (jordskred og utvasking), graving under oppryddingsarbeid kan føre til nye fiberbrudd, stengte veier som følge av flom eller skred kan hindre feilretting på fiberkabler, strømtilførsel og andre skader.

I Etterretningstjenestens rapport «Fokus 2017», fremheves terrortrusselen fra militante islamister, trusler i det digitale rommet og geopolitiske motsetninger mellom Russland og Vesten. Etterretningstjenesten viser til at terrortrusselen fra militante islamister generelt har blitt mer alvorlig og kompleks og at antall terrorangrep i Europa øker, hvorav de fleste kan knyttes til ISIL. Trusler i det digitale rommet mot politiske, militære og økonomiske mål i Norge beskrives som økende, hvor etterretningstjenesten beskriver en forventning av omfattende etterretningsoperasjoner mot Norge i året som kommer. I denne sammenheng trekkes Russlands omfattende digitale operasjoner for å påvirke valgkampen i USA frem som eksempel, hvor man i så måte ikke kan se bort fra at fremmede makter også kan forsøke å påvirke valget i Norge og andre steder i Europa.

I etterkant av konfliktene i Ukraina og Syria, ser Etterretningstjenesten en markant økning i de geopolitiske motsetningene mellom Russland og Vesten. Russland beskrives som sikkerhetspolitisk selvsikkert og militært styrket, samtidig som også å ha økt vilje til å bruke makt for å hevde sine interesser. Blant annet vises det til at russiske styresmakter i økende

grad fokuserer på sikkerhetspolitiske aspekt i Arktis-politikken og behovet for å styrke den nasjonale kontrollen i en region der den sivile aktiviteten trappes opp på ny.

I PSTs trusselvurdering for 2017 vises det til at Norge og norske interesser i løpet av 2017 vil utsettes for fremmed etterretningsvirksomhet som kan ha stort skadepotensiale. Videre viser PST til at etterretningsaktiviteter vil rettes mot mål innenfor forsvars- og beredskapssektor samt mot politiske beslutningsprosesser og kritisk infrastruktur. Systemer innenfor kraftsektoren og elektroniske kommunikasjonstjenester trekkes frem som spesielt etterretningsutsatt kritisk infrastruktur. PST viser også i sin rapport til at det vil bli gjennomført avanserte datanettverksoperasjoner mot norske myndigheter, IKT-tjenestetilbydere, teknologimiljøer og mot aktører med ansvar for kritisk infrastruktur.

NSM har i sin rapport «Risiko 2017 - Risiko og sårbarheter i en ny tid» beskrevet at en økning i alvorlige cyberangrep, kompromittering av nettverk i mindre virksomheter, bruk av cyberangrep og stjålet informasjon til påvirkning og et stort volum økonomisk motiverte hendelser er trender som vil fortsette i tiden fremover. NSM har videre i sin rapport fokusert på hvordan økt digitalisering kan bidra til å gjøre kritiske samfunnsfunksjoner sårbare, blant annet ved at lange og uoversiktlige verdikjeder skapes som følge av at mange virksomheter knyttes sammen i produksjon av varer og tjenester, som ofte inkluderer tjenester i andre land. NSM vurderer i sin rapport at virksomheter har god evne til å utvikle og ta i bruk nye løsninger, men at virksomhetene ikke har tilsvarende evne til å ivareta sikkerheten, slik at utviklingen kan gjøres på en kontrollert og sikker måte.

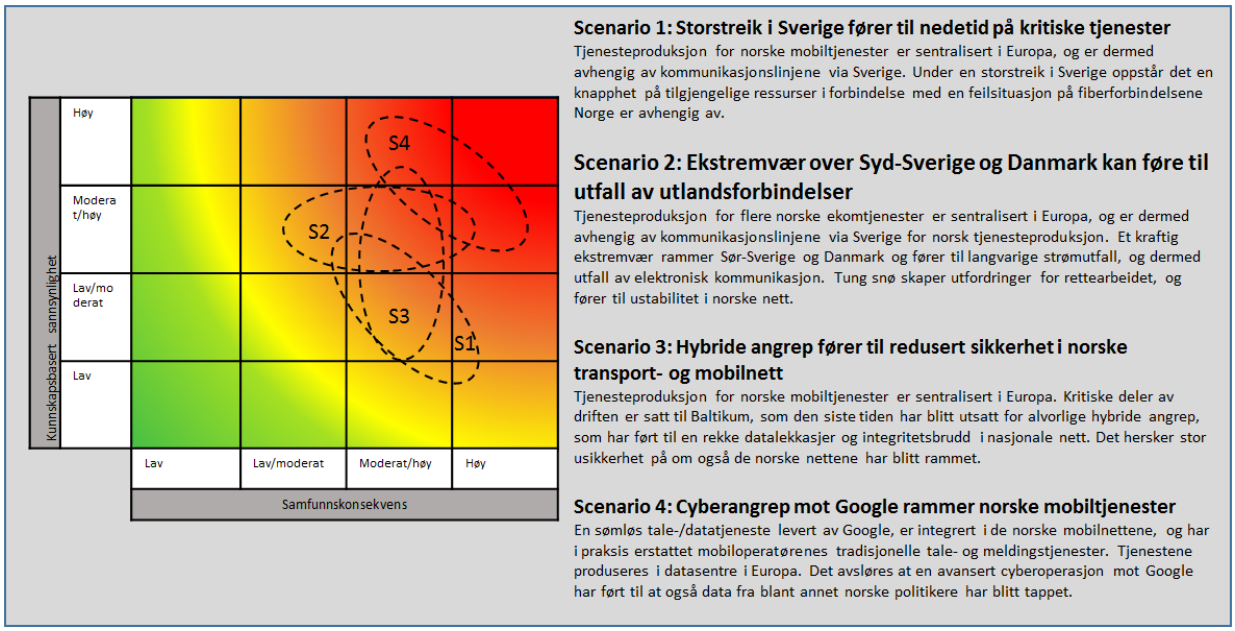
Både PST, E-tjenesten og NSM beskriver en økning i såkalte «hybride trusler», der et av virkemidlene som beskrives er fordekt påvirkning av politiske prosesser. PST ser at etterretningstjenester spiller en rolle i planleggingen og utførelsen av påvirkningsoperasjoner ved å plante falske dokumenter, støtte nettrollaktivitet og bidra til falske nyhetsoppslag i andre land. Ved en tilspisset sikkerhetspolitisk situasjon forventer PST at Norge vil bli utsatt for et spekter av virkemidler, inkludert etterretningstjenesters involvering i påvirkningskampanjer og spredning av desinformasjon.

4.2 Minsket nasjonal kontroll på kritisk tjenesteproduksjon

I EkomROS 2016 pekte Nkom på trender som går i retning av både økende sentralisering av tjenesteproduksjon og økende internasjonalisering. Det er ingenting som tilsier endringer i denne trenden. Utviklingen innenfor virtualisering og endringene i aktørbildet som omtalt i kapittel 0 vil langt på veg bidra i samme retning. Kan vi da forvente at om noen år frem i tid så er for eksempel all tjenesteproduksjon av norske mobiltjenester sentralisert et sted utenfor Norge? På den ene siden er det mange argumenter for at dette kan være driftsmessig rasjonelt, særlig for tilbydere som opererer i flere land. På en annen side så vil kravene til økt

responstid på tjenestene føre til et behov for prosessering så nærme brukeren som mulig. Programvaredefinerte og virtualiserte nettverk gjør at det vil være fullt mulig å oppnå begge deler. Samtidig forventer også Nkom at for enkelte tjenester så vil kunder med svært høye krav til oppetid og sikkerhet, komme til å kreve både at kritiske deler av tjenestene produseres i Norge, og at kritiske data lagres i Norge.

Nkom har vurdert potensielle risikoscenarioer som tar utgangspunkt i en fremtidig situasjon hvor større deler av produksjon og drift av norske ekomtjenester foregår i utlandet. Disse er oppsummert i Figur 2, og risikobildet omtales i de følgende underkapitlene.



Figur 2. Risikovurdering av scenarioer knyttet til nasjonal kontroll på kritisk tjenesteproduksjon.

4.2.1 Nær all trafikk mot utlandet rutes i fiberforbindelser via Sverige (S1, S2)

Det er flere sårbarheter knyttet til utsetting av tjenester og tjenesteproduksjon til utlandet. I forhold til tilgjengelighet til tjenestene skaper dette en økt avhengighet til fiberforbindelsene mot utlandet. Nær all trafikk mot utlandet føres i dag i et begrenset antall fiberforbindelser fra Oslo-området og via Sverige. Hoveddelen av trafikken som går ut av Sverige blir i neste omgang i stor grad rutet i fiberforbindelser mellom Malmø og København. Ensidigheten i trafikkrutingen fra Norge mot utlandet via Sverige og deretter Danmark, kan være utfordrende med tanke på hendelser som kan oppstå i disse landene.

Et klima i endring kan gi flere og mer alvorlige naturhendelser, både i Norge, i våre naboland, men også i regioner som det typisk skjer tjenesteutsetting til, som India, Baltikum og andre land i Øst-Europa. I Meld. St. 10 (2016-2017) «Risiko i et trygt samfunn», poengteres det at globalt kan alvorlige klimaendringer bidra til vann- og matmangel, hyppigere sykdomsutbrudd, politisk uro og kriminalitet.

I Norden er det hovedsakelig de direkte følgene av ekstremvær, flom og skred som har potensiale til å påvirke tilbudet av elektroniske kommunikasjonstjenester i Norge. Dette kan for eksempel være ekstremvær i Sverige som fører til utfall på tjenesteproduksjonsutstyr, eller brudd på norske sambandslinjer mot utlandet. Ved alvorlige naturhendelser ellers i verden kan det også være indirekte følger for norske ekomtjenester. Et eksempel er politisk uro, som kan påvirke evnen til å levere produksjon av eller driftstjenester til norske ekomtjenester med forsvarlig sikkerhet.

Foruten naturhendelser kan det også oppstå andre uønskede og utilsiktede hendelser i Sverige og Danmark som norske myndigheter har liten mulighet til å påvirke utfallet av. Dette kan være nasjonale forhold som politisk uro, streik eller andre interne forhold, som utilsiktet kan påvirke produksjonen av norske ekomtjenester, drift- og overvåkningstjenester i norske nett, eller på annen måte kan utgjøre en trussel mot sikkerheten i de norske nettene.

Scenarioene S1 og S2 tar utgangspunkt i hendelser som skaper ressursknapphet i forbindelse med feilsituasjoner i Sverige og Danmark. Samlet anser Nkom risikoen for å være *moderat*/*høy*.

4.2.2 Direkte påvirkning av sikkerhetstruende hendelser i utlandet (S3, S4)

Det sikkerhetspolitiske landskapet har de siste årene gjennomgått omfattende endringer. Utfordringene er mer komplekse enn tidligere, og en ser i økende grad at terrorisme, organisert kriminalitet og utfordringer i det digitale rom får konsekvenser for global stabilitet, sikkerhet og utvikling.

En ser også at et bredt register av konvensjonelle og ukonvensjonelle virkemidler kombineres for å nå strategiske mål, slik at skillelinjene mellom fred, konflikt og krig blir utvisket, jf. blant annet Russlands framferd i Ukraina. Slik hybrid krigføring inkluderer bruk av umerkede regulære styrker, kriminelle nettverk, kontraktører, informasjonsoperasjoner, spesialstyrker, cyberangrep og økonomiske virkemidler. Bruk av ukonvensjonelle strategier, metoder, taktikker og handlemåter gjør det vanskelig å identifisere hvilken stat som står bak.

Økt grad av tjenesteproduksjon og tjenesteutsetting til utlandet gjør at norske ekomnett og -tjenester i større grad påvirkes direkte av det sikkerhetspolitiske bildet i utlandet. Dette kan være i form av at norske ekomnett og -tjenester rammes av hendelser i utlandet som ikke er direkte rettet mot norske interesser. Men internasjonaliseringen skaper også flere angrepsflater som kan benyttes for målrettet å ramme norske ekomnett og -tjenester. Her må risikoen vurderes ut fra at Norge, i det internasjonale sikkerhetspolitiske landskapet, på mange områder spiller en viktig rolle med vår suverenitetshevdelse og vårt engasjement i nordområdene, vårt naboskap til Russland og medlemskap i NATO, og som olje-, gass- og elektrisitetseksportør.

I scenario S3 blir norske nett og -tjenester «tilfeldig» rammet av sikkerhetstruende hendelse i utlandet, men hvor det vil herske betydelig usikkerhet om hendelsen påvirker sikkerheten i norske ekomnett og -tjenester. Den samlede risikoen vurderes å være *moderat*/*høy*.

Scenario S4 tar utgangspunkt i nye konstellasjoner der tilbyderne og utstyrsleverandørene går i samarbeid med de store internasjonale Internett-aktørene for å utvikle nye tjenester, og at dette skaper nye angrepsflater som utnyttes for målrettet avlytting av brukere. Den stadig økende kompleksiteten i disse verdikjedene gjør at Nkom vurderer den samlede risikoen ved et slikt scenario til å være *moderat/høy*.

4.2.3 Samlet vurdering og tiltak

Kjennetegnene for de fire scenarioene som er vurdert i tilknytning til økt internasjonalisering er en relativt høy risiko. Dels er risikoen forbundet med *hvor* tjenesteproduksjon og drift blir utført, dels er risikoen forbundet med *hvordan*. Nkom har det siste året utført tre utredninger som berører disse risikoene. I rapporten «*Kartlegging og vurdering av infrastruktur som kan nyttiggjøres av datasentre*»[11] vurderes tiltak som bidrar til å tilrettelegge for datasenterindustri i Norge. Noen av tiltakene går ut på å etablere trafikk mot utlandet via alternative forbindelser utenom Sverige. Dersom det skapes generelt større diversitet på trafikkrutingen fra norske ekomnett mot utlandet, vil dette også bidra til å redusere sårbarhetene forbundet med den ensidige rutingen via Sverige. Dersom det skapes en betydelig datasenterindustri i Norge, vil dette i neste omgang kunne legge til rette for at tjenesteproduksjon og lagring av data kan skje i Norge. Dette vil kunne bidra til å redusere sårbarheten knyttet til norske nett og tjenesters påvirkning av sikkerhetspolitiske hendelser i utlandet. Andre mulige tiltak for å redusere sårbarheter og risiko knyttet til internasjonaliseringen fremkommer av de tidligere omtalte Nkom-rapportene om robuste og sikre transportnett, og forslag til krav om nasjonal autonomi.

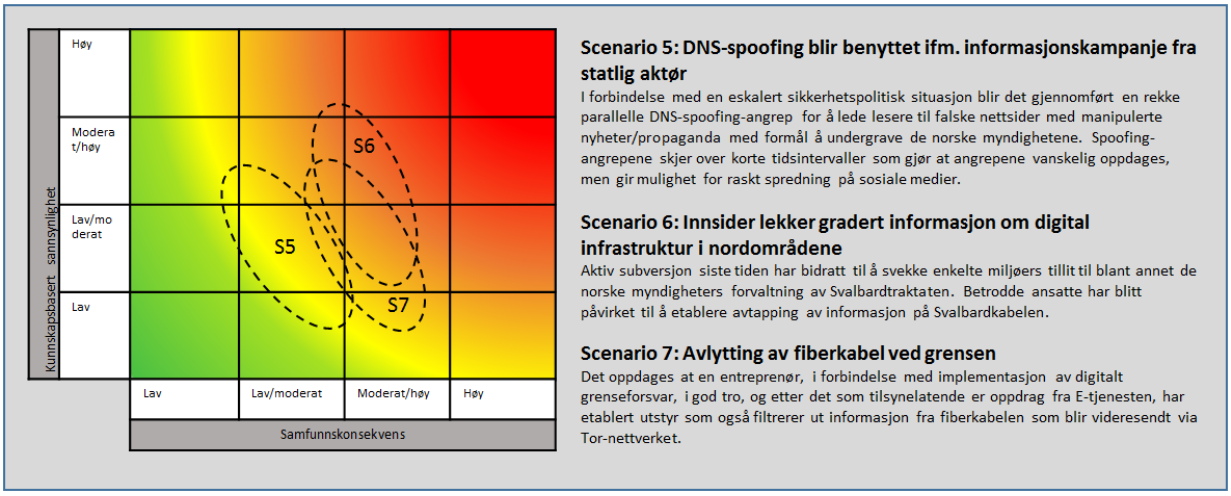
Når det gjelder risikoen knyttet til *hvordan* tjenestene vil produseres i fremtiden, og av hvilke aktører, er det lite hensiktsmessig å ha en sikkerhetsregulering som legger for store hindringer for tjenesteutvikling og innovasjon. Et viktig spørsmål er likevel i hvor stor grad en som tilbyr norske ekomnett og -tjenester skal ha mulighet til å overlate kontrollen av nasjonal kritisk tjenesteproduksjon til underleverandører/samarbeidspartnere utenfor landets grenser.

4.3 Hybride trusler – økt fare for integritets- og konfidensialitetsbrudd

Trusler mot elektronisk kommunikasjon kan inngå i scenarioer sammen med helt andre typer trusler. De seinere årene har man i konflikten mellom Russland og Ukraina sett eksempler på at angrep på ekominfrastruktur har vært en del av et større militært og storpolitisk maktspill. Cyberdomenet har blitt et viktig nytt domene for krigføring. Også fra aktører uten stor militær kapasitet eller territoriale ambisjoner, men med antatt ønske om å skape ustabilitet og spre

[11] «Kartlegging og vurdering av infrastruktur som kan nyttiggjøres av datasentre», Nkom, desember 2016

frykt og desinformasjon, ser vi eksempler på at ekom utnyttes. I de fleste tilfeller vil en angriper se seg tjent med at ekomnett og -tjenester forblir tilgjengelig. Det er derfor integritet og konfidensialitet som først og fremst er under press i scenarioene vi har valgt til å illustrere for hybride trusler (Figur 3).



Figur 3. Risikovurdering av scenarioer knyttet til integritets- og konfidensialitetsbrudd

4.3.1 Ekomnett og -tjenester som verktøy for subversjon (S5)

Det er ikke noe nytt at parter i konflikter søker å påvirke informasjonen som når ut til befolkningen eller til beslutningstakere. I større grad enn før forholder vi oss til informasjon som vi henter direkte fra digitale media. Manipulering av disse kildene kan ha sterk og umiddelbar effekt. DNS er en viktig støtteinfrastruktur på Internett som sørger for at en bruker ledes til riktig nettsted uten å kjenne til den IP-adressen som nettet internt benytter. Ved å manipulere på de tabellene som sørger for å oversette mellom domenenavn og IP-adresse, kan man oppnå å lede brukere til steder med «alternativ» informasjon. I scenario S5 velger en angriper avgrensede og målrettede manipuleringer av utvalgte nyhetssider fremfor en massiv kompromittering av DNS som raskt ville blitt oppdaget. Slik manipulering av f.eks. spesifikke nyhetssider, kombinert med rask utbredelse av informasjon på sosiale medier, vil kunne bidra til å undergrave norske myndigheter.

Nkom anser at det finnes relevante fysiske og logiske sikringstiltak mot sårbarheten, blant annet DNSSEC. Nkom anser videre at konsekvensen av en kompromittering mest sannsynlig vil ha relativt kort varighet. Samlet risiko anslås derfor til *lav/moderat*.

4.3.2 Innsidertrusselen – påvirkning av ansatte i organisasjonen (S6)

Bakteppet for dette scenarioet er at informasjonskampanjer og aktiv subversjon over noen år har bidratt til å svekke tilliten til norske myndigheter, blant annet til Norges aktive suverenitetshevdelse på Svalbard og i nordområdene. Oljeressurser i nord og generell økt strategisk betydning av nordområdene har gjort ansatte i norske bedrifter mer utsatt for press fra andre lands myndigheter. I denne situasjonen har teknologer med tilgang til gradert

informasjon om digital infrastruktur, lekket informasjon om systemer som de mener strider med Svalbardtraktaten, til Russland.

Et slikt scenario vil kunne ha betydning for norsk evne til å ivareta nasjonale interesser i nordområdene og svekke kommunikasjonsvernet i området i måneder. Konsekvensene med hensyn til svekket kommunikasjonsvern vil være små målt i antall berørte kunder, og alvoret vil først og fremst være knyttet til økt politisk spenning og uforutsigbarhet.

Et alternativt scenario mot samme bakteppe, kunne være direkte knyttet til det kontroversielle ved Norges oljeaktivitet i nord i en tid med store klima- og miljøutfordringer. Med bakgrunn i ekte miljøengasjement eller under skinn av slikt engasjement, men av rent opportunistiske grunner, kunne ulike aktører presse sympatiserende eller misfornøyde ansatte for informasjon som kunne brukes til å skade Norges omdømme og påvirke politiske prosesser.

Innsidertrusselen er vanskelig å sikre seg mot og Nkom bedømmer den samlede risikoen til *moderat*.

4.3.3 Ukrypterte data i fiberkabler (S7)

Kommunikasjonen over fiberkabler er i liten utstrekning kryptert. I scenario S7 utnyttes dette ved at en trusselaktør får installert avlyttingsutstyr på en av fiberforbindelsene mot utlandet. Denne type angrep forutsetter fysisk tilgang til fiberkabelen. Det er relativt enkelt å lokalisere og få tilgang til fiberkabler i den norske ekominfrastrukturen. Det å filtrere ut spesifikt innhold, kan derimot være ressurskrevende. En ethernettforbindelse over fiber inn til en bedrift, kan trolig avlyttes med beskjedne ressurser, men en høykapasitets DWDM-forbindelse mot utlandet, anser vi vil kreve avansert og kostbart utstyr for å avlytte. Nkom antar at det vil være statlige eller andre svært kompetente og ressurssterke aktører som kan stå bak denne type trussel. Samlet anser Nkom risikoen å være *moderat*.

4.3.4 Samlet vurdering og tiltak

De tre scenarioene med hybride trusler representerer henholdsvis manipulering av informasjon, lekkasje av informasjon om ekominfrastruktur og avlytting av innhold i kommunikasjon. Scenario S7 viser at moderne kommunikasjonsløsninger er sårbar for tapping av usikret informasjon i veldig stor skala hvis en har tilgang til avansert utstyr. I de tilfellene vi kjenner fra media, hvor ekom inngår i hybride trusler, ser en også manipulering av informasjon. I begge tilfeller vil kryptografisk beskyttelse være aktuelt mottiltak. Men også kontroll med planlagt arbeid i nett, og fysisk tilgangskontroll vil være viktige barrierer. Scenario S6 skiller seg fra de to andre ved at her spiller den menneskelige faktor størst rolle. En kan treffe tiltak for å øke sannsynligheten for å oppdage kilden til lekkasjer, men om de det gjelder er tilstrekkelig dedikerte, er det vanskelig å forhindre kompromittering av informasjon.

Det gjøres utvilsomt mye mer enn før for å sikre konfidensialiteten og integriteten av kommunikasjonen, men sett opp mot det økte omfanget og den økte betydningen ekom har, kan tiltakene bli utilstrekkelige. Gjennom etableringen av de ulike sektorresponsmiljøene – EkomCERT for ekomsektoren sin del – adresseres hybride trusler og intendert kompromittering av konfidensialitet og integritet mer kraftfullt enn før fra myndighetenes side. Det vil øke muligheten for å detektere kompromittering, men det viktigste mottiltaket for å forhindre kompromittering vil likevel være kryptografisk beskyttelse.

4.4 Forstyrrelser i kritisk trådløs kommunikasjon

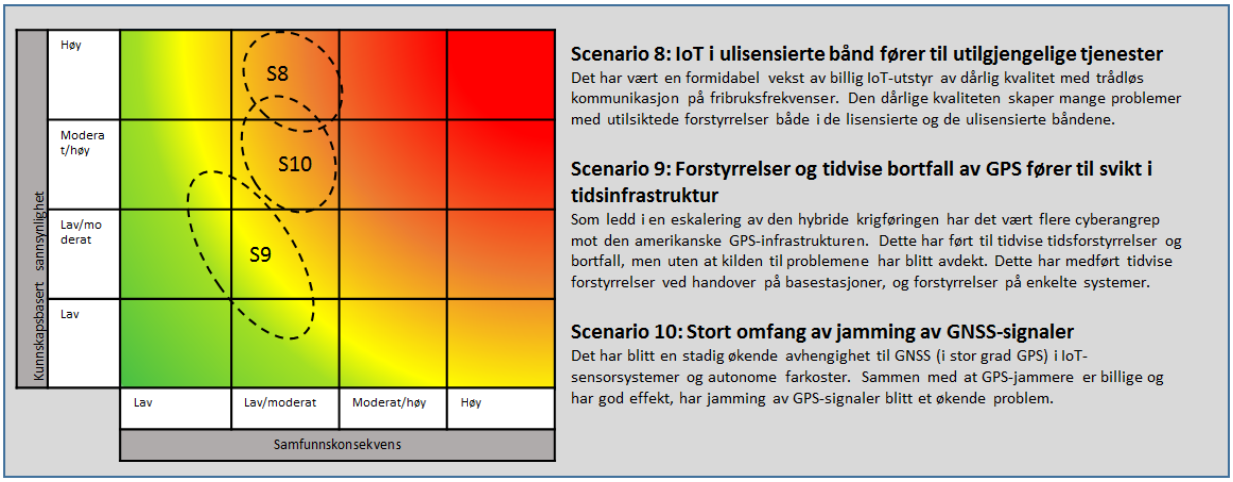
Det forventes en formidabel vekst i antall enheter som kommuniserer på fribruksfrekvenser[12]. At det blir «trangere om plassen» i radiospektrumet gjør at interferens og stråling utover frekvensområdet som er satt av for utstyret kan få en samfunnsmessig større konsekvens. Det vil være utfordrende å finne effektive tiltak for å holde tritt med denne utviklingen.

Svært mange elektroniske enheter, inkludert mobiltelefoner, inneholder GNSS-mottakere. GPS kom på begynnelsen 1990-tallet og er i dag det mest utbredte. Det russiske GLONASS kom i 2011 og det europeiske alternativet GALILEO gikk på lufta i desember 2016. Bruksområdene for GNSS-signaler er navigasjon og tidsangivelse. I mobilnettene benyttes GPS til tidsangivelse for blant annet basestasjoner. Felles for de tre GNSS systemene er at de benytter veldig svake nyttesignaler og er derfor svært sårbare for interferens. Tilgang på utstyr for jamming av GNSS-signaler er enkel gjennom internett, og prisen er lav. En rimelig jammer kan slå ut GNSS-signaler i en omkrets på flere hundre meter.

Forstyrrelser i kritisk trådløs kommunikasjon kan skyldes både tilsiktede og utilsiktede handlinger. Selv om omsetning, besittelse og bruk av jammere i Norge er forbudt, viser målinger at jammere er i bruk.

Nkom har vurdert potensielle risikoscenarioer som tar utgangspunkt i en fremtidig situasjon hvor vi har massiv IoT og hvor det i stort omfang benyttes GNSS-tjenester. Disse er oppsummert i Figur 4, og risikobildet omtales i de følgende underkapitlene.

[12] Frekvenser som ikke krever individuell frekvenstillatelse fra Nkom, og som ikke har krav på beskyttelse mot annen lovlig bruk av frekvenser.



Figur 4. Risikovurdering av scenarioer knyttet til forstyrrelser i trådløs kommunikasjon

4.4.1 Massiv IoT – økning i interferensproblemer (H8)

WiFi- og Bluetooth-kommunikasjon er blant de mest kjente applikasjonene som opererer på fribruksfrekvenser. Et problem som mange har stiftet bekjentskap med er interferens. I et nabolag med et stort antall trådløse rutere kan man oppleve dårlig kapasitet på luftgrensesnittet hvis ruterne ikke er konfigurert til å benytte kanaler som ikke overlapper.

Veksten i markedet for billig IoT-utstyr, spesielt innen smarthjemteknologi, vil gjøre det trangt om plassen i de ulisensierte båndene. Dessverre er mye av utstyret som selges av dårlig kvalitet. Resultatet er at problemene med interferens vil øke. Det registreres også en økende tendens til at dårlig kvalitet og feil på utstyr resulterer i stråling utover frekvensbåndene og sendestyrken som utstyret er produsert for. Et eksempel er droner hvor sendestyrken økes over lovlige verdier for å kunne fly dronen i stor avstand fra dronepiloten.

Det har lenge vært et problem med ulovlig innførsel av trådløst utstyr fra land hvor frekvensområdene for trådløs kommunikasjon er annerledes enn i Norge. En gjenganger har vært innførsel av DECT-telefoner som benytter frekvenser som i Norge brukes av de offentlige mobilnettene.

De ulisensierte frekvensbåndene blir i stor grad benyttet til formål som enkeltvis ikke regnes som samfunnskritisk. Konsekvensen av enkelthendelser er derfor lav, men den den høye sannsynligheten for at slike hendelser oppstår gjør likevel at den samlede samfunnskonsekvensen i scenario S8 er *moderat*. Det som veier tyngst er det økonomiske aspektet ved å avdekke og nøytralisere utstyr som skaper problemer. Nkom forventer at denne kostnaden vil øke i tiden fremover.

4.4.2 Forstyrrelser av satellittsignaler (S9, S10)

Jammere er utstyr som reguleres av internasjonal overenskomst, blant annet EMC-direktivet, som Norge har sluttet seg til gjennom EØS-avtalen. Jammere oppfyller ikke de grunnleggende kravene i direktivet og er dermed ikke lov til å besitte, omsette eller ta i bruk[13]. I særskilte tilfeller kan Nkom gi tillatelse til bruk av jammere i overenstemmelse med konsesjonshaver for det berørte frekvensområdet.

Jamming av GNSS-signaler er en type angrep som har stor effekt, grunnet den lave signalstyrken i slike signaler, og som er relativt enkelt å skjule. I en krigssituasjon er jamming et effektivt våpen for å lamme kommunikasjons- og navigasjonssystemer. I krigen i Ukraina ble det brukt jamming på en måte som ble en vekker for hvor stort skadepotensiale dette virkemidlet kan ha. En annen form for angrep er å manipulere GNSS-signaler. En trusselaktør kan benytte avansert utstyr som sender ut falske GPS-signaler som gir feil tidsangivelse i utstyr og som medfører feilnavigasjon.

Scenario S9 tar utgangspunkt i en sikkerhetspolitisk situasjon hvor hybride angrep er tatt i bruk. Samfunnet forventer at GNSS er stabilt og mange systemer mangler redundante løsninger for å håndtere utfall av GNSS. Ekomnettene er forholdsvis robuste overfor bortfall eller feil i satellittbaserte tidssignaler, men lengre bortfall kan likevel forårsake ustabiliteter i nett. Risikoen vurderes som *lav/moderat*.

Økende bruk og avhengighet av GNSS i IoT sensorsystemer og autonome farkoster medfører at den geografiske tettheten til slikt utstyr øker. Scenario S10 gjenspeiler en forventning om at dette også vil øke tettheten av jammeutstyr. Den samlede risikoen anses som *moderat*.

4.4.3 Samlet vurdering og tiltak

Så langt er det ikke registrert kritiske GNSS-relaterte hendelser. Dette bidrar nok også til at kunnskapen om samfunnets sårbarhet frem til nå har vært relativt lav, og at mange funksjoner og systemer har tatt i bruk GNSS ukritisk uten å vurdere konsekvenser av utfall, forstyrrelser eller manipulasjon av disse signalene.

Nkom deltar i prosjektet *Interferens Deteksjon og Mottiltak (IDM)* sammen med blant annet Norsk Romsenter og FFI. Prosjektet skal kartlegge hvilke sårbarheter utfall av GNSS mottakere kan ha for brukere med kritiske behov og høye krav til tilgjengeligheten av GNSS-data. Man ønsker også å redusere usikkerheten rundt sårbarhetene i kritisk infrastruktur som benytter GNSS ved å etablere en nasjonal IDM-plan.

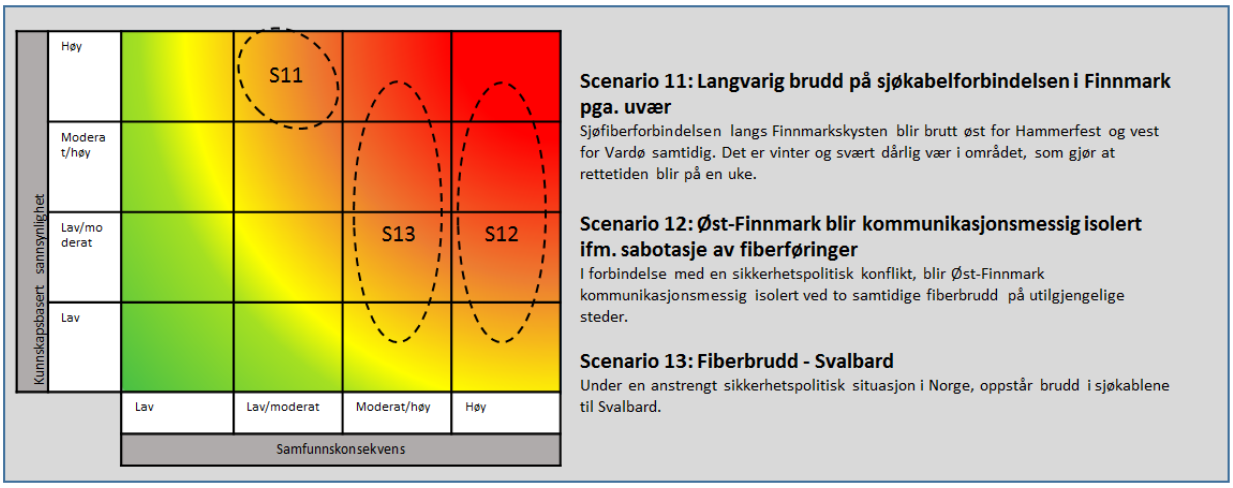
[13] For Politiet, Forsvaret, Nasjonal sikkerhetsmyndighet og Kriminalomsorgen gjelder egne regler, jf. ekomloven §§ 6-2a og 8-1 annet ledd.

FFI og Nkom har gjennomført tester sammen for å kartlegge støy og eventuelle hendelser i GNSS-båndet. Målingene er så langt preget av en viss usikkerhet hvorvidt støy og interferens er utilsiktet eller tilsiktet. Stasjonære målinger foretatt av FFI i Oslo indikerer at det passerer kjøretøy utstyrt med GPS jammere.

4.5 Sårbar infrastruktur i nordområdene

Nordområdene er svært viktig for Norge. Området har stor strategisk betydning for Norge, og gjeldende nordområdepolitikk skal prioritere internasjonalt samarbeid, næringsliv, kunnskap, miljøvern, sikkerhet og beredskap og infrastruktur. Økende aktivitet i en region hvor det er store avstander, og som påvirkes av både klimaendringer og sikkerhetspolitiske endringer, stiller store krav til ekominfrastrukturen.

Nkom følger i årets risikovurdering opp utfordringer som ble identifisert i fjorårets vurdering, og ser på potensielle fremtidige risikoscenarioer som tar utgangspunkt i ekominfrastrukturen i nordområdene, sammenholdt med områdenes strategiske betydning. Disse er oppsummert i Figur 5, og risikobildet omtales i de følgende underkapitlene.



Figur 5. Risikovurdering av scenarioer knyttet til infrastrukturen i nordområdene

4.5.1 Utfordringer ved fiberbrudd i Finnmark (H11)

I 2009 ble ekominfrastrukturen i Finnmark betydelig styrket som følge av etableringen av fiberringstrukturen som omslutter fylket, i regi av Telenor og Ishavslink. Fiberringen har vært svært viktig for både næringslivet og for innbyggerne. Ser man imidlertid på digitaliseringen som har skjedd siden 2009 og den den videre utviklingen som ventes de nærmeste årene, så gir ikke dagens infrastruktur tilstrekkelig robusthet i Finnmark.

De siste årene har det vært flere tilfeller med brudd på sjøkabelforbindelsene i Finnmark. Store avstander og utfordrende værforhold gjør at rettetiden ofte kan ta opp til flere dager, og i noen tilfeller uker. Et aktuelt eksempel er et fiberbrudd på en sjøkabel ved Magerøya nord i

Finnmark i mars 2017. På grunn av uvær tok det over ett døgn for entreprenør å komme frem til området for å identifisere at bruddet var på sjøkabelen, slik at kabelbåt kunne rekvireres. Fartstiden fra kabelbåtens posisjon og frem til bruddstedet tok også over ett døgn, og været i området gjorde at selve rettearbeidet tok ytterligere tre døgn. Etter totalt seks døgn var forbindelsen gjenopprettet. Lang rettetid øker også sannsynligheten for at flere feil kan oppstå på fiberringen innenfor samme tidsrom. I store deler av Finnmark er et dobbeltbrudd nok til å medføre at bygder og byer blir kommunikasjonsmessig isolert, slik vi opplevde i Båtsfjord og Berlevåg så sent som i januar 2017.

Scenario S11 bygger direkte på denne type hendelse og den samlede risikoen vurderes som *moderat/høy*.

4.5.2 Ekominfrastrukturens sikkerhetspolitiske betydning i nordområdene (H12, H13)

I den åpne trusselvurderingen fra E-tjenesten for 2017 vises det til at Russland prioriterer nordområdene og Arktis høyt. Det har vært en omfattende reetablering av infrastruktur i området, det er tilført nytt og modernisert militært utstyr, og det er gjennomført stadig hyppigere og mer komplekse øvelser. Dette har medført økt russisk evne til å påvirke norsk og alliert handlefrihet i nord. I fjorårets EkomROS viser Nkom til at det er høy risiko knyttet til etterretningsvirksomhet mot infrastrukturen. Tar man utgangspunkt i at det oppstår en sikkerhetspolitisk krise som berører interesseområdene i nord, så forventes det at den innsamlede etterretningsinformasjonen vil kunne utnyttes til å utføre sabotasjehandlinger mot ekominfrastrukturen. Den begrensede konnektiviteten som finnes både mellom fastlandet og Svalbard, og i Finnmark, gjør at det ikke er svært omfattende aksjoner som må gjennomføres i en krise- eller konfliktsituasjon, før det skapes store kommunikasjonsmessige utfordringer i området.

Scenario S12 og S13 bygger begge på sabotasjeaksjoner mot infrastrukturen som gjennomføres under en sikkerhetspolitisk krise eller konflikt. Slike scenarioer vil gjerne kunne fremstå som tilfeldige og utilsiktede bruddsituasjoner, men inngå som et av flere ukonvensjonelle virkemidler i hybrid krigføring. Det høye skadepotensialet gjør at den samlede risikoen anses som *moderat/høy* for denne type scenarioer.

4.5.3 Samlet vurdering og tiltak

Nkom mener at økt sikkerhet og kapasitet i de regionale og nasjonale fibernettene i hovedsak må realiseres gjennom økt konnektivitet. Utbygging av mer fiber legger til rette for at tilbyderne kan øke redundansen og kapasiteten i egne nett. Langt på vei vil dette skje naturlig gjennom markedsdrevet utvikling, men ikke i alle tilfeller. Kanskje særlig i Finnmark, hvor avstandene er store og befolkningstettheten er liten, vil utbyggingskostnader ofte ikke kunne forsvares kommersielt. Samfunnskonsekvensen ved ekomutfall vil imidlertid være betydelig, og særlig i mindre tettsteder som er utsatt for isolasjon ved ekstremvær.

I et totalforsvarsperspektiv vil det også være viktig å legge til rette for økt konnektivitet til og i strategisk viktige områder som Svalbard og Finnmark. Som tillegg til utbygging av nye fiberforbindelser, kan man også se for seg løsninger der ulike netteiere kan utnytte hverandres infrastruktur ved brudd i egne fiberforbindelser. Det må da legges til rette for at transportnettilbydere i krise- eller beredskapssituasjoner kan samarbeide effektivt for å reetablere konnektivitet i berørte områder. Tilretteleggingen må gjøres både på det topologiske plan (strategiske samtrafikkpunkter), det tekniske plan (fiber- eller trafikkutvekslingsmekanismer) og på det administrative plan (samhandlingsavtaler mm.). Også Forsvarets transportnettinfrastruktur bør inngå i slik samhandling, for å legge til rette for Forsvarets behov for sivil støtte og motsatt.

Nkoms rapport til Samferdselsdepartementet om robuste og sikre transportnett, som omtalt i kapittel 3.1, viser til flere mulige tiltak som kan bidra til å redusere sårbarhetene i fiberinfrastrukturen i nordområdene.

5 Oppsummering

Nkom har i EkomROS 2017 fokusert på følgende risikoområder:

- Økt internasjonalisering i bransjen svekker den nasjonale kontrollen på kritisk tjenesteproduksjon. Sett i sammenheng med økt avhengighet til disse tjenestene, og et uforutsigbart sikkerhetspolitisk bilde, utgjør dette en økende risiko.

- Tilgang til informasjon om brukere, trafikkdata og innhold har høy verdi i hybrid krigføring. Sammenholdt med stadig mer komplekse verdikjeder, vil risikoen for integritets- og konfidensialitetsbrudd i ekomnett- og tjenester øke.

- Den forventede massive økningen i IoT vil skape mange nye utfordringer i nettene i årene som kommer. Stor vekst av billig utstyr av dårlig kvalitet, samt tilgang til og effekt av jammeutstyr, vil øke risikoen for forstyrrelser i kritisk trådløs kommunikasjon.

- Kombinasjonen av store arealer og lav befolkningstetthet og sterke værpåkjenninger gjør ekominfrastrukturen sårbar i nordområdene. Risikoen påvirkes i tillegg av nordområdenes betydning for både næringsutvikling, sikkerhet og beredskap.

Tabell 1 viser en samlet oversikt over fremtidige risikoscenarioer som har blitt vurdert innenfor hvert av disse risikoområdene. 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 risikobildet i EkomROS 2016.

ID	Uønsket hendelse	Risiko	Usikkerhet
S4	Cyberangrep mot utenlandsk tredjepart rammer mobiltjenester	Moderat/høy	Høy
S2	Utfall av norske ekomtjenester pga. ekstremvær i Sverige	Moderat/høy	Moderat
S3	Hybride angrep i utlandet rammer sikkerheten i norske nett	Moderat/høy	Høy
S12	Øst-Finnmark blir isolert ifm. sabotasje av fiberføringer	Moderat/høy	Høy
S13	Fiberbrudd Svalbard ifm. sikkerhetspolitisk konflikt	Moderat/høy	Høy
S11	Langvarig utfall i Finnmark på grunn av sjøkabelbrudd	Moderat	Lav
S8	IoT skaper økte forstyrrelser i kritisk trådløs kommunikasjon	Moderat	Lav
S10	Stort omfang av jamming av GNSS	Moderat	Moderat
S1	Storstreik i Sverige fører til utilgjengelige tjenester i Norge	Moderat	Høy
S6	Insider etablerer avtapping av data fra fibernett i nordområdene	Moderat	Høy
S7	Det etableres fysisk avtapping av fiberkabel ved grensen	Moderat	Høy
S5	DNS-spoofing benyttes for subversjon/opinionspåvirkning	Lav/moderat	Moderat
S9	Ustabilitet i GNSS rammer tidssynkronisering i ekomnett	Lav/moderat	Moderat

Tabell 1. Samlet oversikt over risikoscenarioer og usikkerhet sortert etter risikonivå.

Kjennetegnene for alle de fire scenarioene som er vurdert i tilknytning til økt internasjonalisering er en relativt høy risiko. Risikoen er forbundet med en forringelse av nasjonal kontroll på kritisk tjenesteproduksjon, gjennom en gradvis økende avhengighet til funksjoner i utlandet de kommende årene, sammenholdt med at komplekse verdikjeder åpner for nye typer sårbarheter. Dette krever at myndighetene må ha en aktiv rolle og finne en god balanse mellom å tilrettelegge for næringsutvikling og innovasjon, samtidig som nødvendig nasjonal kontroll på nett og tjenester ivaretas for å sikre forsvarlig sikkerhet for brukerne i hele krisespekteret.

Risikoen er også gjennomgående relativt høy for hendelser knyttet til infrastrukturen i nordområdene. Risikoen påvirkes av det er høyere sannsynlighet for langvarige brudd enn ellers i landet, som følge av at infrastrukturen er mindre utbygd samtidig som at den er utsatt for hardere værforhold. Men risikoen er også forbundet med den sikkerhetspolitiske betydningen som ekominfrastrukturen har i nordområdene.

Nkom har i 2016 og 2017 gjennomført flere utredninger med forslag til tiltak som adresserer mange av risikoene som peker seg ut som høyest i denne risikovurderingen. Utredningene om tilrettelegging for datasenterindustri i Norge, behovet for nasjonal autonomi i norske ekomnett, og målbilder og tiltak for robuste og sikre nasjonale transportnett berører alle hvordan sikkerhet og beredskap skal ivaretas i en tid hvor det skjer betydelige endringer sektoren.

Risiko knyttet til integritet- og konfidensialitetsbrudd, forstyrrelser i kritisk trådløs kommunikasjon og utfordringer knyttet til IoT vil det også være viktig å ha betydelig fokus på i årene som kommer. Her har imidlertid myndighetene også stor drahjelp fra bransjen, som har egeninteresse i å få bukt med problemene for å ivareta tjenestenes kvalitet og brukernes tillit.