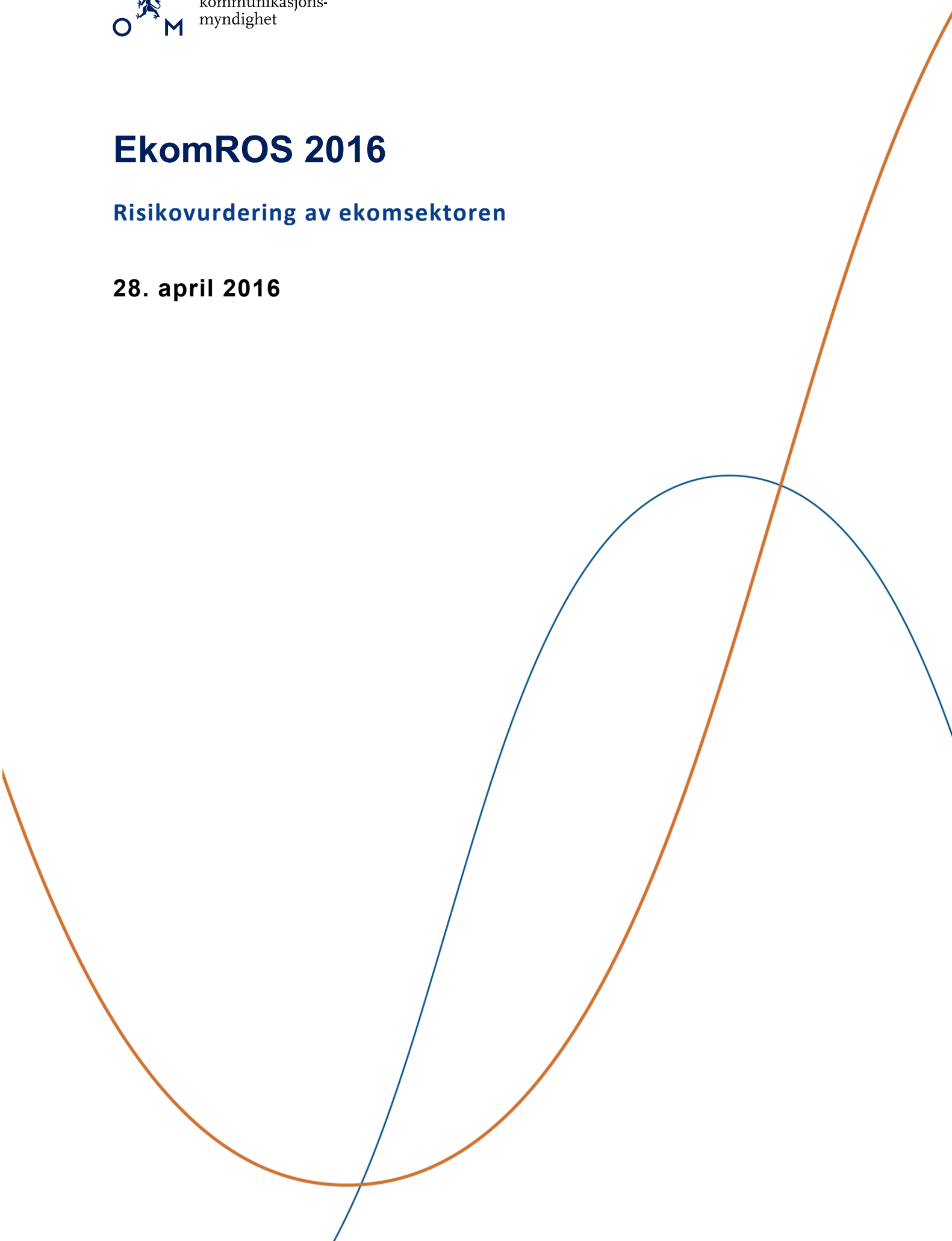
Nasjonal kommunikasjons-myndighet

EkomROS 2016

Risikovurdering av ekomsektoren

28. april 2016



Forord

Samfunnet er helt avhengig av elektronisk kommunikasjon (ekom). I utredninger om samfunnssikkerhet de senere årene har ekom fått stor oppmerksomhet. Lysne-utvalget uttaler i sin rapport «Digital sårbarhet – sikkert samfunn» (NOU 2015:13) at *[d]e verdiene og funksjonene som ekomnett og -tjenester leverer, er en helt sentral forutsetning for at andre samfunnsfunksjoner skal kunne levere det de skal. Samtidig er det en stadig økende forventning i samfunnet om at ekom som innsatsfaktor er stabil og tilgjengelig. 100 prosent oppetid tas mer eller mindre for gitt, og det er meget lav aksept for brudd.*

Når verdien av et system er høy, er det viktig å kartlegge risikofaktorer og sårbarheter som kan true systemet. Dette er første gang Nasjonal kommunikasjonsmyndighet (Nkom) legger fram en overordnet risiko- og sårbarhetsvurdering (ROS) av ekomsektoren. I tråd med oppdraget fra Samferdselsdepartementet, vil Nkom nå gjennomføre årlige ROS-vurderinger. Slik blir arbeidet for å sikre nett og tjenester og for å unngå at sårbarheter og risiko forblir ukjent eller feilvurdert, enda bedre systematisert. ROS-arbeidet legger premisser for Nkoms regelverksutvikling på sikkerhets- og beredskapsområdet, og for forvaltning av beredskapsmidler.

Økt bruk av elektronisk kommunikasjon, i kombinasjon med målrettet arbeid for å redusere risiko, vil bidra til fortsatt utvikling og effektivisering av hele det norske samfunnet. Samtidig som tjenestene skal være effektive og stabile, må de være trygge å bruke for alle.

Torstein Olsen
direktør, Nasjonal kommunikasjonsmyndighet

Sammendrag

I løpet av 2014 og 2015 mottok Nkom varsler om litt over 200 ulike uønskede hendelser i elektroniske kommunikasjonsnett (ekomnett). De aller fleste gjaldt utfall som førte til at tjenestene ikke virket slik de skulle. Vanlige årsaker var fiberbrudd, strømbrudd og utilsiktede feil i utstyr eller programvare. Relativt mange utfall skjedde i forbindelse med planlagt arbeid.

I perioden ble det publisert artikler i pressen om sårbarheter i mobilnettene, blant annet falske basestasjoner, sårbarheter i signaleringssystem nummer 7 (SS7) og kompromittering av SIM-kortprodusenten Gemalto. At sårbarheter gjøres kjent, øker risikoen for at de kan bli forsøkt utnyttet. Nkom mener likevel at det er positivt at disse sakene kommer frem i offentligheten, slik at både de berørte virksomhetene og myndighetene kan adressere problemene.

I tillegg til erfaring fra hendelser og kunnskap om avdekte sårbarheter, er det også viktig å vurdere endringer i risikobildet som følge av teknologiske, organisatoriske og samfunnsmessige utviklingstrekk. Hovedsakelig fører denne utviklingen til fremskritt gjennom både rimeligere og tryggere elektroniske kommunikasjonstjenester for brukerne. Men samtidig som gamle trusler og sårbarheter reduseres, introduseres nye. Felles IP-basert infrastruktur, virtualiseringsteknologi, utkontraktering og internasjonalisering er utviklingstrekk som Nkom mener det er viktig å følge med på. Samtidig vil stadig flere kritiske samfunnsfunksjoner bæres av elektroniske kommunikasjonsnett og -tjenester. Et eksempel på dette er at Forsvarets kommunikasjonsbehov i økende grad vil måtte dekkes av sivil infrastruktur.

Nkom har i EkomROS 2016 foretatt risikoanalyser innenfor tre områder:

- Nasjonal sambandsinfrastruktur og sentralisert tjenesteproduksjon
- Kompleks og omfattende utstyrsportefølje
- Utkontraktering og internasjonalisering

Den høyest identifiserte risikoen er knyttet til potensielle uønskede hendelser i landsdekkende transportnett (hovedsakelig Telenors), utløst av utilsiktede logiske feil eller av tilsiktede handlinger som involverer etterretning eller utpressing. Det er naturlig nok høy usikkerhet knyttet til disse analysene, men relevansen for tilsiktede handlinger understøttes tydelig i sikkerhetsmyndighetens trusselvurderinger. Disse omtaler blant annet en uforutsigbar sikkerhetspolitisk situasjon og stadig mer målrettede og avanserte etterretningsoperasjoner.

Det er noe lavere risiko knyttet til uønskede fysiske hendelser, som fiberbrudd og strømbrudd. Slike hendelser får uten tvil betydelige konsekvenser, noe de mange ekstremværsituasjonene de siste årene har vist. Samtidig har økt krisehåndteringsevne hos både myndighetene, ekomtilbyderne og andre eiere av kritisk infrastruktur bidratt til å redusere risikoen.

Analysen identifiserer en rekke tiltak for å redusere risikoen for de potensielle uønskede hendelsene. Enkelte av tiltakene har bred effekt. Det vil si at tiltakene har risikoreduserende effekt på mange av de analyserte hendelsene, inkludert de det er knyttet høyest risiko til. Disse er:

- Utveksling av trusselbilde mellom sikkerhetsmyndighetene og aktørene i ekomsektoren, og mellom NorCERT og hendelseshåndteringsmiljøene i sektoren.
- Håndtering av logiske sårbarheter og skadevare i nett og komponenter, som autorisasjon og tilgangskontroll, logging og sporing.
- Økt operative krisehåndteringsevne hos tilbydere og myndigheter gjennom proaktiv beredskap, anskaffelse av beredskapsutstyr og utvikling av samhandlingsløsninger.

Videre viser analysen at tilbyderne i større grad bør gjennomføre systematiske og dokumenterte risikovurderinger som identifiserer risikoreduserende tiltak, rettet mot følgende risikoområder:

- Planlagt arbeid i nett
- Teknologiske og organisatoriske endringer
- Avhengighet til underleverandører

Erfaring viser at mange uønskede hendelser utløses i forbindelse med planlagt arbeid i nett. Videreutvikling av prosesser og rutiner for å redusere risiko vil derfor være viktig. Når det gjelder teknologiske og organisatoriske endringer og avhengighet av underleverandører, vil mer målrettede vurderinger av tilknyttede sårbarheter være viktig for å sette i verk proaktive risikoreduserende tiltak.

Som sikringstiltak mot potensielle uønskede hendelser som rammer fysiske infrastruktur, har analysen pekt på særskilt to tiltak som vil ha risikoreduserende effekt:

- Økt redundans i regionalnett
- Vanskeliggjøre fremmede staters kartlegging og etterretning mot fysisk infrastruktur

Med bakgrunn i de potensielle uønskede hendelsene som er analysert vurderer Nkom at tiltak for å øke diversitet og redundans særlig bør rettes mot regionalnettene (mellom transportnett og aksessnett). Nkom vurderer også at det er for lett å kartlegge den nasjonale kritiske ekominfrastrukturen, noe som i en eskalert sikkerhetspolitisk situasjon vil kunne utnyttes til for eksempel å utføre sabotasje.

Innholdsfortegnelse

1 Innledning

Tilbydere av elektronisk kommunikasjon (ekom) er pålagt å utarbeide beredskapsplaner og tiltak for å opprettholde forsvarlig sikkerhet i sine nett. Som bakgrunn for slike planer og tiltak skal det gjøres risiko- og sårbarhetsvurderinger.

Tilbydernes ROS-vurderinger tar utgangspunkt i egen virksomhet og eget nett, og gir ikke et samlet risikobilde av ekomsektoren. Nkom har derfor behov for å gjennomføre overordnede vurderinger av risiko og sårbarheter for til sammen å danne et bilde av situasjonen i sektoren.

Nkom mottar gjennom året mange varsler om hendelser i ekomnettene. Når det er behov for nærmere redegjørelse om årsakene, innhenter vi mer utførlige rapporter. Videre innhenter vi data om de største tilbydernes nett- og tjenestetopologi. Denne faktainformasjonen utgjør sammen med analyse av utviklingstrender og egenutviklede scenarioer grunnlaget for vår ROS-vurdering.

Nkoms ROS-vurdering består i å identifisere potensielle uønskede hendelser, og vurdere sårbarheter og risiko. På denne bakgrunn identifiseres mulige tiltak for å redusere *uakseptabel* risiko. Selv etter at risikoreduserende tiltak er gjennomført, vil det alltid være en restrisiko som samfunnet må leve med. Det er et mål at denne er så lav som mulig, men like viktig er det at restrisikoen er erkjent og forstått.

I kapittel 2 omtales hendelser og sårbarheter fra de siste to årene, mens vi i kapittel 3 ser framover og drøfter betydningen av relevante utviklingstrekk. Risikoanalyse av et utvalg av potensielle uønskede hendelser er gjennomført, og hovedtrekkene i disse gjengis i kapittel 4. I kapittel 5 oppsummeres funn og foreslåtte tiltak.

2 Erfaringer fra 2014 og 2015

2.1 Uønskede hendelser

I 2014 og 2015 ble Nkom varslet om litt over 200 ulike hendelser. Det var stor variasjon, både i varighet og omfang av det som skjedde. Vanlige årsaker til utfall var fiberbrudd, strømbrudd og utilsiktede feil i utstyr eller programvare. Relativt mange utfall skjer i forbindelse med planlagt arbeid. Vi har valgt ut noen ulike hendelser og omtaler disse nærmere.

2.1.1 Storbrannen i Lærdal og brannene på Flatanger og Frøya

Sent lørdag 18. januar 2014 brøt det ut brann i Lærdal, som på grunn av sterk vind spredde seg raskt og fikk et stort omfang. Telenors sentral, som rommet knutepunktutstyr i nettene, var blant de som brant helt ned. Telenor og Telia[1] var tidlig ute med å etablere kriseteam og entreprenørene ble satt i beredskap meget raskt. Likevel gjorde omfanget av brannen og den store varmeutviklingen at det var vanskelig å få startet feilretting mens brannen pågikk.

Telenor hadde utfall på 22 basestasjoner i området, og totalt utfall av fasttelefoni- og bredbåndstjenester på grunn av brannen i sentralen. Telia og Tele2 hadde utfall på hhv. 16 og én basestasjon i Lærdalsområdet.

Tilbyderne gjennomførte flere tiltak for å reetablere mobildekning i området. God midlertidig dekning av ekomtjenester var på plass i Lærdal etter mindre enn to døgn. I reetableringen ble det blant annet benyttet beredskapsutstyr fra regionale lagre som Nkom har bidratt med finansiering til, gjennom statlige tilskuddsmidler. Erfaringer fra denne hendelsen viser at oppsettet med regionale beredskapslagre hos tilbydere er en effektiv løsning for sikring mot langvarige utfall av ekomtjenester.

Brannene på Flatanger og Frøya noe senere samme måned, resulterte ikke i ekomutfall av betydning. Tilbyderne var likevel proaktive med kriseberedskap, og var klare med reservemateriell i tilfelle det skulle bli større utfall.

2.1.2 Strømutfall i Ålesund

Natt til 6. mars 2014 mottok Telenor alarmer fra Ålesund sentral, knyttet til forstyrrelser i strømnettet. I situasjonen ble ikke alarmer tolket korrekt, med den følge at utstyret på sentralen ble stående uten strømtilførsel. Utfallet førte til store konsekvenser for Telenor og Telia. Broadnet, Norkring og TDC ble også berørt av hendelsen. På grunn av utfall av mobil- og fasttelefon var det problemer med å få kontakt med entreprenørene. Kortleseren i døren på sentralen virket heller ikke uten strøm.

[1] 1. mars 2016 byttet TeliaSonera Norge AS navn til Telia Norge AS (Telia). Samtidig ble merkevarenavnet NetCom erstattet med Telia.

Telenor hadde utfall på 162 basestasjoner for mobiltelefoni. I tillegg ble 7000 bredbåndskunder og 5000 fasttelefonikunder rammet i Ålesund-området. Som følge av feilen hadde også Telia utfall på alle basestasjoner i Møre og Romsdal, i tillegg til store områder i Sogn og Fjordane og Hordaland. Broadnet hadde utfall på 1400 kundesamband. Ti timer etter første alarm meldte Telenor at feilen var rettet og tjenestene ble satt i drift forløpende, mens Telia meldte at de hadde normaldrift først etter ytterligere seks timer.

I henhold til klassifiseringsforskriften, som trådte i kraft i januar 2013, skal nettilbydere klassifisere alle anlegg ut fra hvor viktig eget utstyr i anleggene er for offentlige ekomtjenester. Sentralt i forskriften er bestemmelsen som krever at nettilbyder skal gjennomføre en helhetlig ROS-vurdering for sine anlegg, og sørge for at disse er forsvarlig sikret i samsvar med denne vurderingen. Fristen for å implementere sikringstiltakene var 1. juli 2014. I lys av dette, fant Nkom det kritikkverdig at det på tidspunktet for utfallet ikke forelå oppdaterte ROS-vurderinger verken hos Telenor eller Telia. En slik ROS-gjennomgang ville etter Nkoms vurdering vært sentral for å avdekke risikoen ved en slik hendelse som skjedde i Ålesund.

I løpet av toårsperioden har det vært meldt om ytterligere fire liknende hendelser, men hvor konsekvensene har vært mer begrenset. Felles for hendelsene er at reservestrøm ikke har koblet inn som forutsatt når strømmen har gått. Nkom vil følge opp kraftfeilene ved tilsyn i løpet av 2016.

2.1.3 Ekstremvær

I 2014 og 2015 ble Norge rammet av ni ekstremvær. I fem av disse var det vindstyrken som førte til at de ble klassifisert som ekstremvær, i de øvrige fire var det i første rekke nedbørsmengdene som var ekstreme. Under Jorunn, Kyrre, Lena og Mons var utfallene relativt ubetydelige, og tilbyderne var proaktive og dokumenterte god oversikt over status i nettene. Disse uværene traff Vestlandet og Nord-Norge.

Ekstremværet Nina traff Vestlandet og Sørlandskysten i januar 2015, og denne gang ble utfallene større. Rundt 150 basestasjoner ble satt ut av drift, og over 1000 bredbåndkunder og 250 fasttelefonikunder mistet forbindelse. Stormen Ole rammet Nordland og Troms i februar 2015. Høsten 2015 rammet tre tilfeller av ekstreme nedbørsmengder i tur og orden: Petra, Roar og Synne. Under Synne falt strømmen ut flere steder i Rogaland og Agder. I tillegg var oversvømmelsene så store at det ble nødvendig å koble ut strøm kontrollert enkelte steder. Strømbrudd førte til utfall i fast- og mobilnett lokalt og redusert redundans i landsnettet.

I desember 2015 ble Longyearbyen på Svalbard rammet av et snøskred som tok to menneskeliv. Ulykken forårsaket ingen feil i ekomnettene. Situasjonen ble likevel fulgt tett siden ekom var svært viktig under redningsarbeidet etter skredet, hvor det ble arbeidet intens for å sikre liv og verdier.

2.1.4 Problemer for trygghetsalarmer

4.og 5. april 2014 opplevde brukere av GSM-baserte trygghetsalarmer at disse ikke fungerte. Alarmene kom ikke gjennom til mottakene. Det er Telenor som leverer telefonitjenesten til alarmene, og det var i forbindelse med implementeringen av en ny programvare at det oppsto en konfigurasjonsfeil hos Telenor. Utfallet hadde liten og kun lokal konsekvens i starten, men økte i omfang etter hvert. Feilen hadde en varighet på 30 timer.

For trygghetsalarmer er det gjerne én leverandør av telefoniløsningen (her Telenor), mens selve trygghetsalarmen leveres av andre. Det kan komplisere feilsøking og -retting i slike situasjoner, og gjorde det også her.

2.1.5 Utfall av Svalbardforbindelse

2. juni 2014 oppsto en feil på strømforsyningen i forbindelse med en planlagt oppgradering av et fibersystem. Hendelsen førte blant annet til brudd i kommunikasjonen mellom fastlandet og Svalbard. Konsekvensen var til at nesten all ekom til Svalbard falt ut i 4,5 timer, med unntak av satellittkommunikasjon. Det var også et 30 minutters utfall i Harstad og Sortland. Feilen ble midlertidig rettet samme dag, og dagen etter ble forbindelsen reetablert med redundans.

2.1.6 DDOS-angrep

8. juli 2014 ble Nkom varslet av Telia om et mulig DDOS-angrep mot deres portaler. Angrepet kom i to bølger og var trolig en del av et større angrep mot finanssektoren og andre store virksomheter.

Konsekvensene av angrepet for ekomsektoren var relativt små. Telia fikk noen problemer med BankID på mobil og MMS-tjenesten. Både Telia og Telenor ble dessuten rammet slik at nettportaler ble utilgjengelige under angrepene.

2.1.7 Landsdekkende utfall 9. september og 30. oktober 2014 for Telenor

9. september ble Telenors mobilnett rammet av et landsdekkende utfall, og dette varte i omtrent én time. Telenor opplyste at rundt 50 prosent av anropene ikke kom igjennom, og det var i tillegg problemer med SMS og datatrafikk.

30. oktober fikk Telenor et nytt landsdekkende utfall i mobilnettet. Denne gangen var omfanget større og gjaldt alle mobiltjenester. Ca. tre millioner brukere (altså samtlige mobilkunder) ble berørt, også kunder med kritiske samfunnsfunksjoner. Feilen oppsto i forbindelse med arbeid på Telenors kundedatabase for mobil. Hovedfeilen ble rettet etter 2,5 timer, men det oppsto en følgefeil som rammet cirka 500 000 kunder fordelt over hele landet. Denne feilen ble rettet en time etter at hovedfeilen ble rettet.

Nkom anså at Telenors risikovurdering forut for arbeidet i databasen hadde betydelige svakheter og at det forelå uaktsom overtredelse av ekomloven § 2-10 første ledd og fattet vedtak om overtredelsesgebyr på ni millioner kroner.

2.1.8 Flom på Vestlandet førte til sjøkabelbrudd

I forbindelse med flommen på Vestlandet 29. okober 2014, ble det brudd i to sjøkabler, i Leikanger og Hopland. Bruddene ble lokalisert og et sjøkabelskip ble sendt ut dagen etter. Sjøkabelbruddene ble rettet 7. november, etter nedetid på hele ti døgn.

2.1.9 Signaleringsstormer i Phoneros mobilnett 30. januar og 30. mars 2015

En feil i Phoneros nett 30. januar utløste en signaleringsstorm som nettet ikke klarte å håndtere. Dermed ble all mobiltrafikk i Phoneros nett rammet inntil de etter ca. 3,5 timer hadde greid å normalisere situasjonen. Funksjonalitet for bedre å kontrollere tilløp til signaleringsstormer ble innført 11. februar.

Tiltaket viste seg likevel å ikke være tilstrekkelig, for den 30. mars utløste en annen feil en ny, men mindre omfattende signaleringsstorm. Datatjenester var ute i 45 minutter, mens for tale og SMS var det nedsatt kapasitet og ikke totalt utfall.

Både ved utfallet 30. oktober 2014 i Telenors nett og 30. januar 2015 i Phoneros nett ble mobilnettene rammet på en måte som gjorde at heller ikke abonnenter med prioritetsabonnement kunne ringe. Slike abonnenter er definert til å ha særlig viktige samfunnsfunksjoner i kriser, og utfall i dette systemet er derfor særlig uheldig. Politiet var i begge disse tilfellene særlig rammet. Etaten er kunde av Phonero på mobiltelefoni, og Phonero er igjen bruker av Telenors nett. Politiets prioriterte brukere opplevde dermed to alvorlige utfall på kort tid.

2.1.10 Hendelser i forbindelse med planlagt arbeid

Mange hendelser i perioden inntraff under planlagt arbeid i nettene, som blant annet Telenors landsdekkende mobilutfall 30. oktober 2014. Andre fikk begrensede konsekvenser og er ikke omtalt særskilt. Disse eksemplene er alle fra 2015:

- Ved en anledning rammet det bredbåndskunder som hadde tatt i bruk IPv6, ved en annen ble DNS navnetjener utilgjengelig i en halv times tid.
- På Jæren mistet 50 000 bredbåndskunder tilgang til Internett og IP-telefoni i tre kvarter i forbindelse med migrering til ny plattform.
- Programvareoppdatering utført i servicevindu utløste feil i utstyr, noe som fikk konsekvens for basestasjoner i Akershus og Buskerud.

2.2 Logiske sårbarheter i mobilnettene

2.2.1 Lekkasje/manipulering av mobilnummer

Mandag 24. november 2014 hadde Computerworld en reportasje om lekkasje av mobilnummer. Redaksjonen hevdet at Telenor og Telia hadde sikkerhetshull i sine nett i Sverige og Danmark. Som en arv fra løsninger som ellers ikke lenger er i bruk (WAP), benyttes mobilnummeret som identifikator ved besøk på innholdsleverandørers sider.

Hensikten er å kunne fakturere abonnenten for innholdstjenester over mobilregningen på en enkel måte.

Løsningen har flere sikkerhetsmessige svakheter. De to største er knyttet til kravet om samtykke og faren for manipulasjon. Mobilnummer er omfattet av taushetsplikten etter ekomloven § 2-9, og eventuell deling av dette med andre enn ens tilbyder må være basert på samtykke fra abonnenten. Det påstås ikke i reportasjen at tilbydere med vitende og vilje videresender til nettsider som abonnenten ikke har gitt samtykke til, men det skisseres en framgangsmåte hvor en fra mobiltelefonen manipulerer adressen som mobilnummer videreformidles til.

Nkom kontaktet de tre største tilbyderne, som kunne bekrefte at den omtalte sårbarheten også var til stede i de norske nettene. Selv om den konkrete sårbarheten ble lukket, står den som et eksempel på et mer generelt problem, nemlig muligheten for å manipulere adresser.

2.2.2 Falske basestasjoner

I desember 2014 hadde Aftenposten en serie reportasjer om påståtte falske basestasjoner i Oslo. Det som omtales som falske basestasjoner kan spenne fra passivt utstyr som fanger opp mobiltelefonens identitet (IMSI), til mer avansert utstyr som er i stand til å dekryptere og avlytte kommunikasjon i sann tid.

Uavhengig av hva som var realiteten i disse påståtte tilfellene, tok Nkom konsekvensen av at falske basestasjoner er en reell trussel. Kostnaden knyttet til anskaffelse er blitt lav, og flere kan derfor skaffe og bruke utstyr i negativ hensikt. Sammen med norske mobiloperatører utredet Nkom mulighetene for å avdekke falske basestasjoner, og hva som gjøres og kan gjøres for å beskytte seg mot slike. De største svakhetene er i dag knyttet til 2G-nettene, og det er begrenset i hvor stor grad disse svakhetene kan bøtes på.

Nkom har fått tildelt midler til å investere i utstyr som skal avdekke bruk av falske basestasjoner. Det har også blitt etablert forbedrede rutiner for varsling mellom Politiet, Nasjonal sikkerhetsmyndighet (NSM), Nkom og tilbyderne ved bruk av, eller mistanke om bruk av falske basestasjoner.

2.2.3 Signaleringssystem nummer 7

Signaleringssystem nummer 7 (SS7) er en protokoll for kommunikasjon mellom offentlige ekomnett. Protokollen ble utviklet på 70-tallet og det har lenge vært kjent at den har hatt svakheter. Under Chaos Communication Congress' årlige konferanse i Berlin i desember 2014, ble det imidlertid demonstrert for offentligheten hvordan sårbarheter i SS7 kunne utnyttes til sporing, manipulering og avlytting. Det er særlig i mobilnettene at sårbarhetene er påvist. Mens 3G-nettene er relativt sikre mot falske basestasjoner, ble det i konferansen dokumentert at også disse er sårbare via SS7.

I etterkant har Nkom, sammen med øvrige nordiske regulatører, gitt konkrete anbefalinger til operatørene for å redusere disse sårbarhetene. Hovedsvakheten i SS7 – mangelen på autentisering av kommuniserende parter – kan ikke fullt ut kompenseres for med disse anbefalte tiltakene. Hvis én med ondsinnede hensikter får tilgang til SS7-nettet, kan han derfor gjøre betydelig skade. Både alene og i kombinasjon med falske basestasjoner, representerer SS7 en vesentlig sårbarhet.

2.2.4 Gemalto-saken

19. februar 2015 skrev nettstedet The Intercept om påståtte kompromitteringer av den nederlandske SIM-kortprodusenten Gemaltos nettverk. Amerikansk og engelsk etterretning skal ha fått tilgang til nøkkelmateriale som har vært lagret på SIM-kort. Med denne informasjonen skal man potensielt ha hatt mulighet til å dekryptere kommunikasjonen mens disse SIM-kortene har vært i bruk.

Sikkerheten i mobilnettene er i stor grad knyttet til funksjonaliteten i SIM-kortene. Denne hendelsen rokket dermed ved noe av grunnmuren for sikkerhet i mobilnettene. Nkom fulgte opp hendelsen overfor de norske tilbyderne, og studerte hele kjeden fra produksjon, transport, personalisering og til oppdatering av SIM-kort. Det ble ikke avdekt sårbarheter i måten dette har blitt håndtert hos de norske tilbyderne, som har krevd videre oppfølging av Nkom.

2.3 Sammenfattende om hendelser og avdekkede sårbarheter

2.3.1 Sårbare lokale knutepunkt

Brannen i Lærdal rammet et lokalsamfull brutalt, og i dette tilfellet brant også bygget som rommet knutepunktutstyr i ekomnettene for store områder helt ned. Selv om ekomnettene bygges ut med stadig større grad av redundans, er det lokalt og regionalt fortsatt mange enkeltknutepunkter som kan forårsake betydelige ekomutfall når de feiler. Dette var tilfellet med sentralen i Lærdal som brant ned til grunnen. I nyhetssendingene umiddelbart etter hendelsen, var reetableringen av ekomtjenester noe av det som ble tettest omtalt og diskutert. Det illustrerer at under ekstremvær og store ulykker blir samfunnets, virksomheter og enkeltpersoners avhengighet av ekom svært tydelig.

2.3.2 Sentrale funksjoner må sikres godt

Det er heldigvis relativt sjelden at vi opplever at et mobilnett er helt nede. Noen sentrale funksjoner er nødvendige for i det hele tatt å kunne avvikle trafikk. Disse funksjonene er derfor sikret på mange måter. Like fullt opplevde vi i perioden flere utfall som rammet hele landet. Noen av disse hendelsene viste at mobilnett fortsatt kan ha problemer med å håndtere signaleringsstormer, og at sentrale funksjoner kan feile selv om det er bygget inn betydelig fysisk redundans.

2.3.3 Hjelpeteknisk utstyr

Vi opplevde flere utfall i perioden som viser sårbarhet for svikt i hjelpeteknisk utstyr. Ved flere anledninger koblet ikke reservestrøm inn når den primære kraftforsyningen forsvant. Ved strømutfall generes ofte mange alarmer og i ett av tilfellene var noe av problemet å tolke et sammensatt alarmbilde.

Moderne ekomutstyr blir stadig mer kompakt og varmeutviklingen pr volumenhet blir høyt. Utstyret er ofte avhengig av kjøleanlegg og bortfall av kjøling kan være svært tidskritisk. Nkom er kjent med et tilfelle av kjølesvikt i en datahall i 2015, selv om hendelsen ikke er omtalt særskilt. Ofte er det direkte ansvaret for hjelpeteknisk utstyr plassert hos andre enn de som drifter ekomutstyret i de samme anleggene. Dette stiller krav til klare avtaler og rutiner.

2.3.4 Planlagt arbeid

Mange hendelser i perioden har fellestrekket at de ble forårsaket av planlagt arbeid i nettene. Det er Nkoms vurdering at de som har utført arbeidet ikke alltid har hatt nødvendig oversikt til å vurdere de potensielle konsekvensene av arbeidet. Eksemplene som er nevnt illustrerer at det fortsatt er et betydelig potensiale i å forbedre rutiner for planlagte endringer.

2.3.5 Logiske feil

Mange utfall skyldes programvarefeil. I noen tilfeller oppstår feilene ved oppgraderinger eller konfigurasjonsendringer, andre ganger kan feilene ligge latent over tid og utløses av endringer andre steder i nettet. Ved programvarefeil i sentrale komponenter i nettene, blir konsekvensene noen ganger landsomfattende.

Flere alvorlige logiske sårbarheter har blitt kjent i perioden. SS7 og GSM er systemer som har hatt lang levetid i ekomnettene, mens forutsetningene de bygger på med hensyn til sikkerhet har endret seg.

3 Utviklingstrekk de kommende år

Å identifisere relevante utviklingstrekk er en viktig del av risikoanalysen. Den teknologiske, organisatoriske og samfunnsmessige utviklingen påvirker hvilke risikoområder innenfor ekomsektoren som vi mener det er relevant å studere nærmere.

Nkom har gjennomført to prosesser i 2014 og 2015 hvor fremtidige utviklingstrekk i sektoren har vært et viktig tema. Den ene var prosjektet «Teknisk-regulatorisk utvikling» (TRU). Prosjektet hadde som formål å se på markeds-, tjeneste- og nettutviklingen de kommende årene, for bedre å sette Nkom i stand til å tilpasse rollen som utøvende tilsynsorgan, ressursforvalter og fagmyndighet. Den andre prosessen var Nkoms arbeid med innspill til Samferdselsdepartementet om Ekomplanen, som inngår som del av Meld. St. 27 (2015-2016) *Digital agenda for Norge*.

I november 2015 la Lysne-utvalget fram NOU 2015:13 *Digital sårbarhet – sikkert samfunn*. Denne gir en utførlig status på digitale sårbarheter og digitale sikkerhetsutfordringer på tvers av ulike samfunnssektorer.

I EkomROS 2016 har vi valgt å avgrense trendbildet til tre hovedtrekk i utviklingen innenfor sektoren som vil mener vil ha betydning for sikkerhet og beredskap de neste årene:

1) Den teknologiske utviklingen fra «fysiske» til «logiske» nettverk
2) Den organisatoriske utviklingen knyttet til utkontraktering og internasjonalisering
3) Samfunnets og Totalforsvarets økende avhengighet til ekom

3.1 Fra fysiske til logiske nettverk

All ekom er avhengig av en tilgjengelig og fungerende fysisk infrastruktur bestående av rutere, svitsjer, fiberkabler, basestasjoner mm., i tillegg til nødvendig hjelpeteknikk som strømforsyning og kjøling. Produksjon av ekomtjenester som fasttelefoni, mobiltelefoni og ulike datatjenester besto tidligere av spesialiserte produkter av maskin- og programvare på separate infrastrukturer. Nå blir funksjonalitet i ekomnett i økende grad realisert på felles IP-basert infrastruktur og gjennom konfigurerbar programvare på standardiserte komponenter.

3.1.1 Felles IP-basert sambandsinfrastruktur

Ekomtilbyderne benytter i dag IP-nett i produksjonen av de fleste av sine ekomtjenester. IP-infrastrukturen er således i ferd med å bli en felles plattform. Tilbyderne har gjerne egne aksessnett (mot sluttbrukerne) samt kontroll med produksjonen av egne tjenester, men for å binde aksessnett og tjenesteproduksjon sammen, er de avhengig av den felles sambandsinfrastrukturen. De ulike tilbyderne av ekomtjenester benytter i stor utstrekning både Telenors sambandslinjer og selskapets IP-infrastruktur.

Telenors IP-nett vil de nærmeste årene bære alle Telenors egne faste og mobile telefoni- og bredbåndstjenester, i tillegg til å være det nasjonale transportnettet for mange andre tilbydere. IP-infrastruktur generelt, og Telenors IP-nett spesielt, er og vil fortsette å være svært viktig for produksjon av ekomtjenester på nasjonalt nivå.

Dette innebærer at både de styrker og de sårbarheter som denne infrastrukturen har, er felles for mange tilbydere: høy sikkerhet vil komme flere til gode, samtidig som konsekvensen ved feil blir tilsvarende større.

3.1.2 Network function virtualisation (NFV) og software defined networks (SDN)

Network function virtualisation (NFV) går ut på å trekke ut de samme fordelene som virtualisering og skybaserte løsninger har gjort i den «tradisjonelle» IT-verdenen, gjennom å realisere nettverksfunksjoner som virtuelle funksjoner på standard servere. *Software defined networks* (SDN) kan forstås som en nettarkitektur hvor kontroll- og dataplan er adskilt. Det vil si at mens nettelementene som formidler dataene fra sender til mottaker i nettet er distribuert, kan sentraliserte kontrollfunksjoner styre disse via egne kontrollprotokoller. Dette er ikke noe nytt i ekom, men splittingen mellom kontroll- og dataplan har relevans for NFV, ved at den legger til rette for virtualisering.

For ekomnett og -tjenester vil dette kunne innebære at prisene på maskinvare går ned, ettersom man i større grad kan benytte standard IT-utstyr. Dette bidrar også til at flere og nye aktører kan komme på banen og utfordre de tradisjonelle leverandørene. Virtualisering medfører at utvikling og utrulling av nye tjenester på markedet vil gå raskere, og at tilbydere lettere kan skalere sine systemer etter bruker- og trafikkmasse. Dynamisk skalering gir også potensiale for redusert strømforbruk.

Selv om ekom langt på vei har smeltet sammen med IT, er det fortsatt et stykke frem før fullverdige NFV-løsninger antas å være implementert i norske ekomnett. Imidlertid har nettverksleverandørene løsninger på plass og på verdensbasis har enkelte tilbydere av ekomnett satt i gang konsepttesting.

European Telecommunications Standards Institute (ETSI) har de siste tre årene arbeidet iherdig for å legge grunnlaget for standardisering og realisering av NFV i ekomsektoren. Herunder er også fordeler og utfordringer knyttet til sikkerhet utredet. Et viktig hovedtrekk er at ekomnett og -tjenester som i større og større grad benytter IP-basert teknologi og virtualisering vil møte de samme sikkerhetsutfordringene som ved IT-systemer generelt og skybaserte løsninger spesielt. Det vil dukke opp utfordringer knyttet til personvern, til *utilsiktede* feil i programvaredesign, implementasjon eller konfigurasjon, og til *tilsiktede* handlinger som hacking, tjenestenektangrep og cyberspionasje. Sentralisering av tjenesteproduksjon kan dessuten føre til økt skadepotensiale, ved at feil kan ramme flere kritiske nettverksfunksjoner og flere tjenestetilbydere samtidig.

På en annen side kan utviklingen også bidra til å øke sikkerheten på enkelte områder. For eksempel bør økt diversitet, muligheten for dynamisk konfigurering og virtualisering utnyttes til å utvikle systemer som raskt kan gjenopprette sikker funksjon etter å ha vært utsatt for påkjenninger (*resiliens*).

3.2 Utkontraktering og internasjonalisering

I likhet med andre bransjer, blir stadig flere tjenester utkontraktert også innenfor ekomsektoren. Med utkontraktering menes her at en tilbyder benytter eksterne leverandører, enten i Norge eller utenlands, for å levere en vare eller tjeneste, i stedet for å produsere denne selv. I tillegg har vi sett en økende konsolidering av virksomheter på tvers av de nordiske landene. Dette innebærer at enkelte ekomtjenester som tilbys i Norge blir produsert i andre land.

3.2.1 Utbygging, drift og vedlikehold av nettutstyr

I ekomsektoren er utkontrakteringen av leveranser innen installasjon, drift og vedlikehold økende. Tilbydere har i mange år satt bort nettutbygging, installasjon, drift og vedlikehold av tilbyders nettutstyr til eksterne entreprenører, som Relacom, Eltel Sønnico, Rejlers og andre. Utkontraktering av entreprenørtjenester er kosteffektivt i en normalsituasjon. Samtidig kan dette medføre utfordringer i håndteringen av mer ekstreme situasjoner, for eksempel dersom de samme entreprenørressursene blir presset fra flere av ekomtilbyderne (og andre kunder) på samme tid.

3.2.2 Datasentre

Nkoms erfaring fra tilsyn og befaringer er at det er stor variasjon i beskaffenheten på de fysiske byggene som tilbydernes tjenesteproduksjonsutstyr er innplassert i. Plasseringen har gjerne vært betinget av det som historisk har vært sentrale transmisjonsknutepunkter, men hvor bygningene ikke har blitt oppgradert i takt med moderniseringen av infrastruktur og teknologi. Dette har gitt seg utslag i at en del kritisk nettutstyr i dag er plassert i bygg preget av suboptimale løsninger hva gjelder arealbruk, strøm og kjøling, fysisk sikring og adgangskontroll.

Det er også stor variasjon i hvordan byggene, hjelpeteknikken og den fysiske sikkerheten forvaltes. Ved enkelte kritiske lokasjoner er det fortsatt tilbyderne som selv har kontroll med disse forholdene. Ved andre lokasjoner leier tilbyder kun et avgrenset areal hos en huseier eller hos en annen tilbyder (telelosji) for å innplassere og tilknytte nettutstyret. De nødvendige tjenestene tilknyttet det fysiske bygget og hjelpeteknikken inngår da i leieavtalene.

De siste årene har Nkom sett at tilbydere i forbindelse med oppgradering og modernisering av nettene sine velger å innplassere utstyret hos profesjonelle «IT-housing»-leverandører eller

datasentre. Dette er bygg som tilbyr innplassering av nettutstyr i anlegg med definerte nivåer på fysisk sikkerhet og tilgang til hjelpeteknisk utstyr som strømforsyning og kjøling, og som tilbyr tjenestenivåavtaler med garanterte oppetidskrav. Dette er på mange måter et utviklingstrekk som bedrer sikkerheten i ekomnettene. Kombinert med virtualisering (ref. 3.1.2) vil en ved serverfeil kunne oppnå at funksjoner raskt kan overtas av en annen server i datasenteret. Dersom man utplasserer utstyr i eksterne datasentre kun ut fra en kostnadsvurdering, og uten samtidig å utnytte mulighetene denne utviklingen åpner for økt sikkerhet, vil disse sentrene imidlertid kunne representere enkeltpunkter i infrastrukturen som kan medføre store tjenestekonsekvenser hvis de feiler.

3.2.3 IT- og nettverksdrift og managed services

Behovet for reduserte kostnader, spesialisert kompetanse og fleksibilitet gjør at flere og flere funksjoner innenfor IT- og nettverksdrift settes ut til tredjeparter, særlig i lavkostland.

En annen trend er «managed services», der leverandører i tillegg til å selge og installere selve nettutstyret eller programvaren, også står for den daglige nettverksdriften. Direktoratet for nødkommunikasjon har valgt å kjøpe driftstjenestene for Nødnett av Motorola Solutions også etter at disse har fullført utbyggingsoppdraget. I Myanmar har Telenor inngått avtale med Ericsson om drift av store deler av sitt mobilnett i landet, mens TDC i Danmark har inngått avtale med Huawei om drift av TDCs mobilnett. Tilsvarende må man forvente at også operatører av norske offentlige nett vil finne det formålstjenlig å kjøpe driftstjenester av sine utstyrsleverandører.

Tjenesteutsettingen kan ha mange fordeler, både bedriftsøkonomisk og med hensyn til sikkerhet gjennom leverandørens spesialiserte kompetanse og kapasitet. Samtidig innebærer dette en ytterligere fragmentering av tilbyders ansvar og oppgaver. Dette utfordrer dermed både sikkerheten i nett og kommunikasjons- og personvern på nye måter.

3.2.4 Konsolidering av selskaper og tjenesteproduksjon på tvers av landegrensene

Internasjonalisering og konsolidering av ekomsektoren har medført at ekomnett og tjenestetilbud etableres og drives på tvers av landegrensene. For eksempel har de tidligere telemonopolistene Telenor, Telia og TDC alle virksomhet i flere land og leverer ekomtjenester på tvers av landegrenser. Dette er også tilfelle for mange nye ekomtilbydere. Utviklingen kan potensielt gi gevinster når det gjelder tilgang til kompetanse og sikkerhet rundt selve installasjonene, men medfører også utfordringer med hensyn til jurisdiksjon i de ulike landene, kommunikasjonsvern og tilgang i forbindelse med tilsyn. Internasjonaliseringen medfører også en svekkelse av nasjonal autonomi, det vil si evnen til å kunne utføre drift og vedlikehold av tjenestetilbudet med personell og tekniske løsninger som er lokalisert på nasjonalt territorium.

3.3 Samfunnsavhengighet og Totalforsvaret

Det er 30 år siden Seip-utvalget la frem rapporten «Datateknikk og samfunnets sårbarhet». Allerede da ble avhengigheten mellom informasjonsteknologi og kommunikasjonsteknologi ansett som så stor at sårbarhetsanalyse av samfunnets økende datamaskinavhengighet ikke kunne utføres uten å inkludere fagområdet elektronisk kommunikasjon.

Neste år er det 20 år siden Forsvarets forskningsinstitutt (FFI) gav ut den første rapporten i prosjektserien «Beskyttelse av samfunnet (BAS)». Rapporten var starten på FFIs forskningsserie på samfunnssikkerhet og fremholdt at svært mange funksjoner i det norske samfunnet var avhengig av ekom for å virke.

Det er 10 år siden Infrastrukturutvalget la frem sin rapport «Når sikkerheten er viktigst» hvor blant annet behovet for å se nærmere på gjensidige avhengigheter i kritisk infrastruktur ble påpekt. Nødvendigheten av etablering av lovhjemler for å sikre reserveløsninger for produksjon av ekomtjenester, er også omtalt i utvalgets rapport.

Avhengighetene har altså vært kjent i en årrekke, men de har blitt sterkere og involverer stadig flere sektorer. Lysne-utvalget har påpekt at avhengigheten vår av IKT i samfunnsmessige, næringsmessige og private sammenhenger er stor og økende.

I løpet av de siste årene har den sikkerhetspolitiske situasjonen i Europa og våre nærområder endret seg. Endringene har vist at det er et behov for økt beredskap, kortere reaksjonstid og styrket operativ evne. Samtidig har den gjensidige avhengigheten mellom Forsvaret og det sivile samfunnet økt, noe som igjen har aktualisert totalforsvarskonseptet. Totalforsvaret er fellesbetegnelsen på det militære forsvaret og den sivile beredskapen som skal sørge for at samfunnets samlede ressurser anvendes på en best mulig måte ved krisehåndtering i hele konfliktspekteret fra fred til krig.

Fremtidens kommunikasjonsbehov i Forsvaret vil i økende grad måtte dekkes ved bruk av sivilt og kommersielt tilgjengelig teknologi og infrastruktur. Dette for å møte behovet for lett og brukervennlig utstyr med høy datakapasitet i felt, samt til forbedring av samhandling med andre lands innsatsstyrker. Nye sensorer, våpensystemer og droner er eksempler på drivere av datakapasitetsbehov. Bruk av kommersiell tilgjengelig teknologi og infrastruktur vil bidra til å redusere kostnadene. Forsvaret kan også på sikt bli en egen virtuell mobiloperatør (MVNO - Mobile Virtual Network Operator) med nasjonal gjesting hos alle tre mobilnetteierne i Norge, og således tilpasse sivilt utviklet teknologi til militære anvendelser.

Går vi tilbake til den kalde krigens dager, da Seip-utvalget la frem sin rapport, ser vi at fokuset var å sikre produksjon av ekomtjenester selv i en ekstremsituasjon som væpnet konflikt. Med det moderniserte totalforsvarskonseptet vil dette være aktuelt som aldri før.

Trusselen fra ikke-statlige aktører utfordrer det tradisjonelle konfliktspekteret. Det gjør også den økte aktiviteten innenfor det digitale domene, hvor reaksjonstiden er svært kort. Gitt samfunnets avhengighet av ekom, er det i dag vanskelig å se for seg en væpnet konflikt som ikke ledsages av krigføring også i det digitale domenet.

4 Risikoanalyse

Et kjent sitat av den amerikanske forsvarsministeren Donald Rumsfeld i 2002 lyder:

> *«Reports that say that something hasn't happened are always interesting to me, because as we know, there are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns – the ones we don't know we don't know.»*

Selv om dette omhandlet masseødeleggelsesvåpen i Irak, har innholdet en generell overføringsverdi til risikostyring. Hvordan skal man forberede seg på å håndtere utfordringer som man kan forvente vil oppstå i framtiden? Og hva med framtidige utfordringer som man ikke forventer? I risikoanalyser av tenkte framtidige hendelser mangler det ofte et empirisk erfaringsmateriale. Dette er særskilt gjeldende for komplekse ekomsystemer. Et eksempel er Telenors omfattende mobilutfall i juni 2011 som introduserte et nytt begrep; *signaleringsstorm*. Denne signaleringsstormen var et resultat av at «alle» mobiltelefonene tilknyttet Telenors mobilnett forsøkte å registrere seg i nettet samtidig, etter at en sentral server måtte restartes etter en feilretting. Mobilnettet klarte ikke å prosessere all denne samtidige signaleringstrafikken og gikk derfor ned. Det ville ha vært krevende å analysere seg fram til en slik årsaks- og konsekvenskjede på forhånd, selv om det er lett i ettertid.

Risikostyring inngår som en integrert del av virksomheten til de fleste ekomaktører, enten dette gjelder forretningsmessig risiko eller risiko knyttet til sikkerhet og beredskap. Dette er med å danne grunnlag for de valg og prioriteringer som den enkelte aktør gjør. Samtidig er det viktig at ekommyndigheten har en overordnet oversikt over risiko i sektoren med utgangspunkt i regelverket som ekommyndigheten forvalter. Gitt samfunnets gjennomgripende avhengighet av ekom, vil uønskede hendelser som rammer ekomsektoren raskt kunne påvirke kritiske samfunnsverdier som liv og helse, personvern, økonomi, samfunnsstabilitet og i ytterste konsekvens nasjonal styringsevne og kontroll.

Risiko må vurderes i sammenheng med de utviklingstrekk som vi ser i bransjen. Dette vil bidra til å utvikle og forvalte regelverket slik at det balanserer hensynene til å ivareta samfunnssikkerhet på den ene siden, og det å stimulere til næringsutvikling, innovasjon og rimelige tjenester på den andre siden.

Nkoms risikovurdering gjøres i to steg. Det første steget er en *risikoanalyse*. En standard metode for dette er å identifisere farer og potensielle uønskede hendelser og deretter analysere risikoen knyttet til disse hendelsene. For utilsiktede hendelser (naturhendelser, feil, uhell, ulykker) beregnes risiko ofte som et produkt av sannsynligheten for at en uønsket

hendelse skal skje og konsekvensen av hendelsen (NS 5814:2008). For tilsiktede hendelser (kriminalitet, sabotasje, terror, mv.) er risiko gjerne uttrykt som forholdet mellom trusselen mot en gitt verdi og denne verdiens sårbarhet overfor trusselen (NS 5832:2014). I Nkoms risikovurderinger brukes begge disse metodene.

Risikovurderingens andre del er å identifisere skadeforebyggende eller skadereduserende tiltak som kan fjerne eller redusere den identifiserte risikoen. At hendelser vil oppstå som man ikke har tatt høyde for i risikovurderingene er imidlertid uunngåelig. Risikovurderingen vil derfor ha størst effekt dersom det identifiseres tiltak som har avhjelpende effekt ikke bare på det utvalg av uønskede hendelsene som inngår i risikoanalysen, men også på andre relaterte uønskede (og uforutsette) hendelser.

De konkrete analysene er gjennomført av et tverrfaglig team av interne ressurser hos Nkom og med bakgrunn i eksternt og internt kildemateriale. Eksterne kilder er blant annet de årlige trussel- og risikovurderingene fra E-tjenesten, PST og NSM, samt andre utredninger fra for eksempel FFI, Direktoratet for samfunnssikkerhet og beredskap (DSB) og Det europeiske byrå for nett- og informasjonssikkerhet (ENISA).

Interne kilder er egne utredninger, kartlegginger og tilsyn de siste årene, informasjon gjennom samarbeid med de øvrige nordiske ekommyndighetene, samt informasjon mottatt fra virksomhetene i sektoren. Våren 2015 gjennomførte Nkom møter med Telenor, Broadnet, Telia, Altibox og TDC der tjeneste- og nettverksarkitektur, redundans, robusthet, sårbarhet og utviklingsstrategier var sentrale tema. Informasjonen som ble innhentet og analysert i den forbindelse utgjør en sentral del av kunnskapsgrunnlaget.

Konklusjonene er basert på Nkoms egne vurderinger. Som alltid i analyser, er vurderinger 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. Selve analysedokumentasjonen inneholder teknisk informasjon og konkrete sårbarhetsvurderinger som er unntatt offentlighet. I denne rapporten er analysene av de enkelte hendelsene derfor bare omtalt på overordnet nivå.

I teksten omtales risikoen knyttet til en potensiell uønsket hendelse som *lav/moderat*, *moderat* eller *moderat/høy*, basert på Nkoms vurderinger av sannsynlighet for, og konsekvens av, hendelsen. I konsekvensvurderingen er det tatt hensyn til om hendelsen svekker kommunikasjonsvernet (konfidensialitet/integritet) eller ekomtjenesters tilgjengelighet. Videre tas det hensyn til geografiske omfang, varighet og hvilke ekomtjenester som påvirkes, om hendelsen påvirker 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.

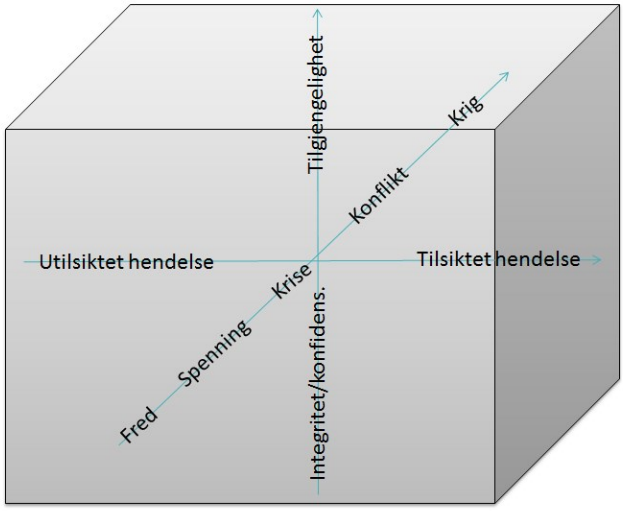
4.1 Risikoområder

For 2016 har Nkom analysert av et utvalg av potensielle uønskede hendelser innenfor følgende risikoområder:

- Nasjonal sambandsinfrastruktur og sentralisert tjenesteproduksjon
- Kompleks og omfattende utstyrsporteføljе
- Utkontraktering og internasjonalisering

Disse risikoområdene springer ut fra tidligere erfaringer fra hendelser omtalt i kapittel 2, utviklingstrekkene som omtales i kapittel 3, og Nkoms vurderinger av sårbarhets- og trusselbildet som baseres på de interne og eksterne kildene omtalt over. De samme risikoområdene trekkes også fram av Lysne-utvalget.

For å identifisere mulige uønskede hendelser innenfor disse risikoområdene har Nkom definert et mulighetsrom som spenner ut de sikkerhetskrav som ekomregelverket stiller til tilbyderne. Dette mulighetsrommet er et hjelpemiddel for å identifisere et så vidt spekter som mulig av uønskede farer og hendelser.



Figur 1. Mulighetsrom for uønskede hendelser

Den ene aksen representerer *hendelsestype*. Dette kan være utilsiktede hendelser som ekstremvær, ras, tekniske feil og menneskelige feil, eller tilsiktede handlinger som avlytting, sporing, sabotasje, terror og så videre.

Den andre aksen representerer *type sikkerhetsbrudd*: om hendelsen rammer konfidensialitet, integritet eller tilgjengelighet.

Den tredje aksen representerer *bakteppet for hendelsen*; om hendelsen oppstår under normale, fredelige omstendigheter eller som følge av en eskalert situasjon som for eksempel ekstremvær, terrorsituasjon, sikkerhetspolitisk krise eller – i ytterste konsekvens – strategisk overfall og militært angrep. Bakgrunnen for å ta med dette i mulighetsrommet er tilbydernes plikt etter ekomloven § 2-10 til å tilby tjenester med «forsvarlig sikkerhet for brukerne i fred, krise og krig».

De følgende underkapitlene oppsummerer potensielle uønskede hendelsene som har blitt analysert innenfor de tre utvalgte risikoområdene. Disse representerer utilsiktede og tilsiktede hendelser som omfatter konfidensialitets-, integritets- eller tilgjengelighetsbrudd. Til hver hendelse er det knyttet et bakteppe, som blant annet angir om hendelsene skjer i «fredstid» eller som følge av en eskalert situasjon.

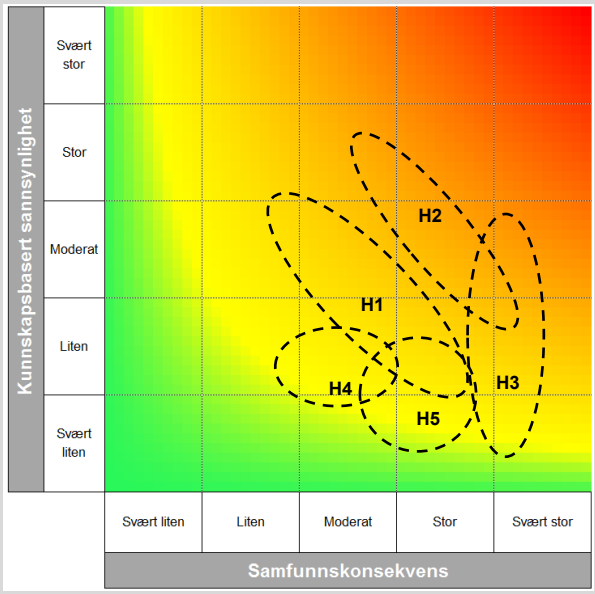
I analysen har Nkom valgt ut potensielle uønskede hendelser som enten vil kunne ha negative konsekvenser for flere tilbydere samtidig og dermed større samfunnskonsekvens, eller som på annen måte vil ha prinsipiell eller strategisk betydning. Utvalget er dermed ment å være utfyllende for de uønskede hendelser som naturlig vil inngå i ROS-analysene til den enkelte tilbyder, selv om det i noen tilfeller vil være overlapp.

4.2 Nasjonal sambandsinfrastruktur og sentralisering av tjenesteproduksjon

Den nasjonale sambandsinfrastrukturen har blitt trukket fram i Lysne-utvalgets rapport som en komponent som inngår i nær sagt alle digitale verdikjeder. Både Telenor, Broadnet og Altibox har landsdekkende (og i stor grad uavhengige) nasjonale transportnett, men konsekvensene er utvilsomt størst ved bortfall av Telenors transportnett. Det er derfor viktig at denne avhengigheten gjenspeiles i risikovurderingene.

Sentralisering og konsolidering av tjenesteproduksjonen påvirker risikobildet i samme retning. Selv om dette ofte fører til mer robuste løsninger som reduserer sannsynligheten for feil, vil samtidig enkeltfeil ha et tilsvarende større skadepotensiale. Telenors landsdekkende mobilutfall i oktober 2014, som følge av en mindre feilretting i abonnentsdatabasen, er et eksempel på dette.

I Nkoms risikoanalyse er det tatt utgangspunkt i fem potensielle uønskede hendelser som kan ramme nasjonale sambandsinfrastruktur og sentraliserte løsninger. Risikobildet er oppsummert i Figur 2, og beskrives nærmere i de følgende underkapitlene.



H1: Multippel transmisjonsfeil i transportnett
Det er redusert redundans i landsdekkende transportnett på grunn av planlagt arbeid. Samtidig oppstår et dobbelt fiberbrudd pga. to sammenfallende uavhengige hendelser.

H2: Konfigureringsfeil i landsdekkende IP-nett
En større oppdatering i konfigurasjonssystemet til landsdekkende IP-nett utløser en latent programvarefeil.

H3: Utpressing av nøkkelressurs
Under en sikkerhetspolitisk konflikt blir en nøkkelressurs utpresset til å slette konfigurasjonsfiler i transportnett.

H4. Fiberbrudd i Finnmark og Svalbard
Under en anstrengt sikkerhetspolitisk situasjon i Norge, oppstår brudd i sjøkabelen til Svalbard samtidig med brudd på fibernettet i Finnmark.

H5: Samtidig strømsvikt på kritiske anlegg i Oslo
Ekstremvær i indre Oslofjord fører til stedvis kortere og lengre strømbrudd og generell ustabilitet i strømforsyningen i Oslo i en 2-3 dagers periode.

Figur 2. Risikoanalyser – nasjonal sambandsinfrastruktur og sentralisering av tjenesteproduksjon. Usikkerhet representeres ved størrelsen på det stiplede arealet.

4.2.1 Multippel transmisjonsfeil i transportnettet (H1)

Det oppstår ofte kabelbrudd i transportnettene. Imidlertid er det betydelig redundans i nettene, og bruddene blir vanligvis rettet i løpet av forholdsvis kort tid. Flere brudd som sammenfaller i tid er mindre sannsynlig, men vi har likevel sett flere eksempler på dette de siste årene. Denne potensielle hendelsen innebærer tre samtidige bortfall i Telenors transportnett og dermed betydelig påvirkning på samfunnsfunksjoner, men over forholdsvis kort tid. Fiberbrudd er relativt enkle å påvise, og rettes normalt i løpet av kort tid. Risikoen er skalerbar i den forstand at sannsynligheten for ett fiberbrudd er større enn for to eller tre samtidige, mens konsekvensen er begrenset for ett brudd men større for to og tre samtidige. Ved tre samtidige fiberbrudd, vil konsekvensen reduseres gradvis etter hvert som de enkelte fiberbruddene rettes. Samlet anser Nkom risikoen for multiple fiberbrudd i transportnettet som *moderat*.

4.2.2 Konfigureringsfeil i landsdekkende IP-nett (H2)

Feil i programvare og konfigurering er årsak til mange feil i ekomnettene. Denne potensielle hendelsen tar utgangspunkt i en programvarefeil, som fører til alvorlig feilkonfigurasjon i Telenors landsdekkende IP-nett. Dette vil ramme mange andre tilbyderes kritiske ekomtjenester. Analysen er beheftet med usikkerhet, men Nkom mener det er relevant å problematisere forholdet mellom kompleksiteten i disse systemene og systemenes kritikalitet.

Nettopp på grunn av kompleksiteten vil også feilrettingstiden potensielt være betydelig lengre enn ved fysiske brudd. Nkom anser den samlede risikoen for å være *moderat* til *høy*.

4.2.3 Utpressing av nøkkelressurs (H3)

Mens de to foregående potensielle hendelsene gjelder utilsiktede feil, beskriver denne en tilsiktet, ondsinnet handling. I alle tekniske organisasjoner vil man være avhengig av nøkkelressurser som må ha vide tilganger, fullmakter og rettigheter til kritiske systemer. Det er samtidig kjent at trusselaktører i dag systematisk kartlegger kritisk personell i organisasjoner av interesse. Den utstrakte bruken av sosiale medier, som vever sammen både private og profesjonelle opplysninger, gjør denne jobben enklere. Med bakgrunn i gjeldende trusselbilde vurderer Nkom at en trusselaktør vil ha *kapasitet* til å utføre en utpressingshandling mot en slik ressurs. Selv om det per i dag ikke foreligger en kjent *intensjon*, vil effekten av å gjøre en slik handling imidlertid ha så stor effekt, at man i en sikkerhetspolitisk eskalert situasjon må kunne forvente at en slik handling vil bli forsøkt. Det er stor usikkerhet knyttet til sannsynligheten for at dette kan skje, men samlet anser Nkom risikoen for å være *moderat* til *høy*.

4.2.4 Kommunikasjonsbrudd i Finnmark og mot Svalbard (H4)

Fiberforbindelsen mellom Svalbard og fastlandet er en sentral del av Norges infrastruktur i nordområdene. I tillegg til å være kritisk for at ekomtjenestene til innbyggerne på Svalbard skal fungere, har fiberforbindelsen også betydelig forretningsmessig og strategisk betydning. På fastlandet har utbyggingen av fiberringen til Ishavslink i Finnmark ført til både økt kapasitet og robusthet. Den potensielle hendelsen som er analysert tar utgangspunkt i et rettet angrep mot disse infrastrukturene samtidig. Ut fra gjeldende trusselbilde vil det være trusselaktører med både kapasitet og intensjon til å *kartlegge* disse infrastrukturene. For eksempel er det kjent fra media at amerikanerne er bekymret over at russiske skip driver operasjoner nær de transatlantiske fiberkablene, på steder der rettearbeid vil være vanskelig. En villet bruddskade på kabelen vil ha betydelig symboleffekt, noe som kan gjøre dette til et svært relevant scenario i en eskalert sikkerhetspolitisk situasjon. Nkom vurderer den samlede risikoen som *moderat*. Symboleffekten vil imidlertid være høy.

4.2.5 Multippel strømsvikt på kritiske anlegg i Oslo (H5)

Siden ekstremværet Dagmar i 2011, har tilbyderne etter hvert opparbeidet god beredskap for å håndtere ulike ekstremværsituasjoner. Øvelser og reelle hendelser har også vist at de ulike beredskapsaktørene, inkludert lokal kriseledelse, er blitt flinkere til å samhandle og treffe tiltak for å redusere konsekvensen av for eksempel bortfall av strøm og ekom. Erfaringsgrunnlaget er hovedsakelig fra områder som oftest blir berørt av ekstremvær, slik som Vestlandet og Nord-Norge. Vi har imidlertid mindre erfaring med konsekvenser for strøm og ekom dersom det sentrale østlandsområdet skulle bli rammet av et kraftig ekstremvær, slik hendelsen i vår analyse legger opp til. Sentrale nettelementer for tjenesteproduksjon er i utgangspunktet godt beskyttet både gjennom fysiske sikkerhetstiltak, redundans og reservestrømkapasitet. Nkom har de siste årene likevel erfart flere tilfeller av svikt både på reservestrømforsyning (aggregat) og på redundans-funksjoner. Blant annet har vi erfart at også rettemannskapenes tilgang til

anlegg vanskeliggjøres ved at strømbruddet rammer det elektroniske adgangskontrollsystemet. Samlet anses risikoen som *moderat*, men vurderingen er beheftet med betydelig usikkerhet.

4.2.6 Risikoreduserende tiltak – nasjonal sambandsinfrastruktur

Nkom mener at et virkningsfullt tiltak for å redusere risiko ved fysiske brudd i ekomnettene, er å øke redundansen gjennom kontinuerlig å bygge ut alternative framføringsveier. Dette gjelder både i transportnettene, men også i regionalnettene og ytterst ut mot kundene – i aksessnettene – hvor det i dag er mye mindre redundans enn lenger inn i nettene. Dette vil ikke nødvendigvis redusere omfanget av brudd – kanskje tvert imot ettersom det blir rullet ut mer nett - men konsekvensen av bruddene vil bli mindre og mer lokale. Et parallelt tiltak er å utnytte den eksisterende infrastrukturen bedre ved å tilrettelegge samtrafikkpunkter, og at de ulike eierne av transportnett inngår bytteavtaler (*swapping*). Dette vil bidra til å gjenopprette tjenester raskere når nettene utsettes for ekstraordinær påkjenning (resiliens).

Disse tiltakene vil ikke avhjelpe sårbarheter knyttet til utilsiktede logiske feil, som for eksempel konfigureringsfeilen omtalt i H2. Men også her anser Nkom at resiliens er et viktig stikkord for å redusere risiko. Vi må erkjenne at det i komplekse systemer alltid vil foreligge feil og svakheter i programvare og konfigurasjon, og at også mennesker gjør feil. Resiliens må da sikres ved å ha gjennomført forsvarlige risikovurderinger på forhånd og ha etablert feilhåndteringsprosesser som bidrar til å gjenopprette normaltilstand i løpet av kort tid.

I H3 og H4 er informasjonsinnsamling et sentralt tema. Man må anta at det foregår etterretning i form av kartlegging og sammenstilling av informasjon om både menneskelige og tekniske ressurser og infrastruktur i ekomsektoren. Dette er en utfordring som sikkerhetsmiljøene hos myndighetene og i virksomhetene gjerne er oppmerksomme på, men som øvrige tekniske miljøer, markedsmiljøer eller ledelse ikke nødvendigvis er like bevisste på. Ved å sammenstille informasjon som er offentlig tilgjengelig, med informasjon som er hentet fra etterretningskilder «på innsiden», kan en trusselaktør danne seg et ganske detaljert bilde av den samlede norske ekominfrastrukturen. Et risikoreduserende tiltak er at ekomtilbyderne i arbeidet med *security awareness* i egen organisasjon intensiverer innsatsen for å øke bevisstheten rundt trusselen fra fremmede staters etterretning.

Nkom har, i samarbeid med E-tjenesten, PST og NSM etablert et forum for å utveksle trusselbildet på gradert nivå. Et risikoreduserende tiltak er derfor å videreføre og videreutvikle dette forumet, samt å etablere gode arenaer for informasjonsdeling mellom NorCERT, de ulike sektor-CSIRT-ene (inkludert NkomCSIRT) og ekomtilbyderne.

H5 omhandler strømsvikt på kritiske ekomanlegg. Disse anleggene har normalt alternativ strømforsyning (dieselaggregat). Når kritiske anlegg går ned på grunn av strømsvikt skyldes dette derfor feil på reservestrømforsyningen, noe som kan være forårsaket av manglende

vedlikehold og oppfølging. Krav til både dimensjonering og vedlikehold er beskrevet i regelverket. Et sannsynlighetsreduserende tiltak kan være å trappe opp tilsynsaktiviteten, for å gi tilbyderne tilstrekkelige insentiver til å følge opp rutiner for vedlikehold og testing av reservestrømsystemene. Dette gjelder ikke minst der tilbyder har innplassert utstyret i datasenter/telelosji hvor tredjepart står for drift og vedlikehold av reservestrømsystemene. Da må tilbyder gjennom avtale forsikre seg om at disse forholdene blir ivaretatt og fulgt opp.

I tabellen nedenfor oppsummeres de risikoreduserende tiltakene knyttet til nasjonal sambandsinfrastruktur og sentralisering av tjenesteproduksjon.

	Tiltak	Beskrivelse
T1	**Redundans og swapping**	*Øke redundans i transportnett og regionalnett. Tilrettelegge for sammenkopling av nett og inngå bytteavtaler (swapping) for beredskapsformål.*
T2	**Risikovurdering og tiltak - planlagt arbeid i nett**	*Videreutvikle prosesser og rutiner for risikovurdering ved planlagt arbeid i nett med tilhørende skadeforebyggende og skadereduserende tiltak.*
T3	**Utveksling av trusselbilde**	*Videreføre og videreutvikle sikkerhetsforum med Nkom, tilbyderne og de hemmelige tjenestene, og etablere arenaer for informasjonsutveksling mellom NorCERT, sektor-CSIRT-ene (inkludert Nkom-CSIRT) og ekomtilbyderne.*
T4	**Awareness – etterretning**	*Vanskeliggjøre fremmede staters etterretning, både fra åpne og lukkede kilder gjennom økt awareness i tilbydernes organisasjoner.*
T5	**Vedlikehold av reservestrøm**	*Forbedre rutiner for test og vedlikehold av reservestrømsystemer, ev. avtaler i de tilfeller hvor tredjepart utfører dette.*

Tabell 1. Risikoreduserende tiltak - nasjonal sambandsinfrastruktur og sentralisering av tjenesteproduksjon.

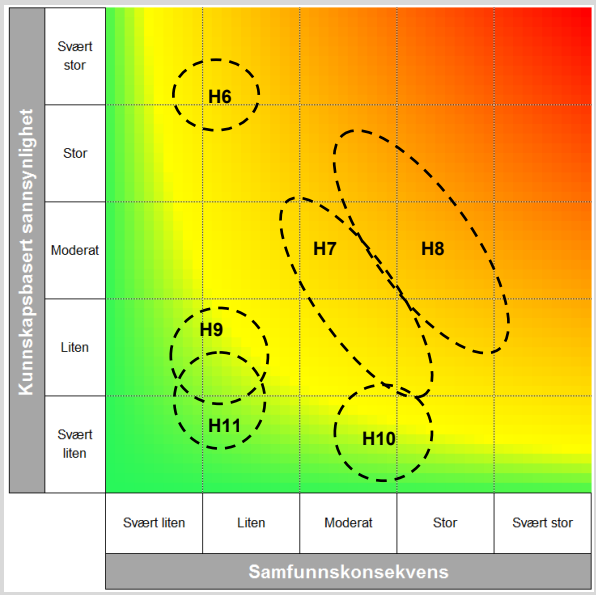
4.3 Kompleks verdikjede og omfattende utstyrsportefølje

Ekomnett er sammensatt av en omfattende portefølje av maskin- og programvare fra ulike leverandører for alt fra fysisk infrastruktur, tjenesteproduksjon, nettverksadministrasjon, brukeradministrasjon og overvåkning, til diverse tekniske støttefunksjoner. Systemene som ligger til grunn for å styre og konfigurere de ulike elementene og sørge for at disse samhandler, er svært komplekse.

På toppen av denne verdikjeden legges atter andre systemer som skal underbygge ulike tjenester for sluttbrukerne, det være seg *over-the-top*-tjenester[2], finansielle tjenester eller transport- og logistikktjenester. Mange av disse tjenestene forutsetter at det kan utføres tillitsbaserte transaksjoner over nett, som for eksempel banktjenester. Disse er igjen avhengig av infrastruktur og systemer for elektroniske sertifikater og digitale signaturer.

[2] Audio-/video-/meldingstjenester som tradisjonelt har blitt levert av ekomtilbyder, men som leveres over Internett av tredjepart (Skype, iMessage osv.).

Det vil være umulig å verifisere at det ikke foreligger alvorlige logiske sårbarheter i de mange leddene i disse verdikjedene. I risikoanalysen har Nkom sett på seks potensielle uønskede hendelser innenfor dette risikoområdet (Figur 3).



H6: Signaleringsstorm i landsdekkende mobilnett
Konfigurering i forbindelse med oppgradering utløser en feil som medfører uventet høy signaleringstrafikk

H7. Sikkerhetshull i VoLTE-løsningen
En sårbarhet i VoLTE-løsningen utnyttes til sporing og avlytting. Sårbarheten utnyttes mot myndighetspersoner.

H8: Utpressingsforsøk mot ISP
Indentert (myndighetsinnlagt) SW-sårbarhet i sentralt nettverksutstyr blir oppdaget av hackergruppe og utnyttet i utpressingsforsøk mot ISP med trusler om å ta ned ruterne.

H9: DNS-angrep
Flere ISPer får klager fra kunder at brukernavn og passord har blitt misbrukt, pga.oppdaget uautoristert handel på nett. Det er domenenavnetjenerne (DNS) som står i ISP-enes eget nett som er angrepet.

H10: Sertifikatutsteder er kompromittert
En angriper får tilgang til rotserver og kan utstede falske elektroniske sertifikater. Dette påvirker tilgang på offentlige og private tjenester og transaksjoner over Internett.

H11. Bortfall av GPS
En kraftig solstorm rammer de globale navigasjons-satellittene og fører til bortfall av GPS i flere dager.

Figur 3. Risikoanalyser – kompleks verdikjede og omfattende utstyrsportefølje. Usikkerhet representeres ved størrelsen på det stiplede arealet.

4.3.1 Signaleringsstorm i landsdekkende mobilnett (H6)

Problemet med signaleringsstorm oppstår som følge av at mange mobiltelefoner på samme tid må signalere med mobilnettet. Dette skjer vanligvis når telefonene skal reetablere kontakt med nettet etter en primær feilsituasjon, eller etter planlagt arbeid i sentrale komponenter i mobilnettet. I etterkant av signaleringsstormen i Telenors nett i juni 2011 har det vært oppmerksomhet rundt problemstillingen både hos tilbyderne og utstyrsleverandørene. Det har blitt implementert ulike mekanismer som skal forhindre at høy signaleringstrafikk skal forårsake blokkeringer i mobilnettet, men likevel opplevde en mobiltilbyder senest i 2015 landsdekkende utfall på grunn av signaleringsstorm. Nkom anser at tilsvarende hendelser fortsatt vil kunne oppstå i fremtiden. Man skal heller ikke se bort fra muligheten for at store mengder signaleringstrafikk kan genereres av skadevare på mobiltelefoner, etter tilsvarende mønster som tradisjonelle DDOS-angrep. Imidlertid har tilbyderne etter hvert opparbeidet bedre kompetanse og innsikt til å håndtere slike hendelser, noe som gjør at feilsituasjoner rettes

raskere. Den samlede risikoen for signaleringsstorm i landsdekkende mobilnett anses derfor å være *moderat*.

4.3.2 Sikkerhetshull i VoLTE-løsningen (H7)

Siden 4G ble innført i Norge i 2009, har teknologien utelukkende vært benyttet for mobile datatjenester. Når en mobilbruker i 4G-nettet skal sette opp en samtale, har samtaleoppsettet automatisk blitt flyttet over til 2G eller 3G. I løpet av 2016 vil imidlertid flere mobiltilbydere introdusere tale over 4G (VoLTE). Dette teknologiskiftet innebærer at nytt utstyr og ny programvare blir implementert i mobilnettene. Dette vil brukerne oppleve gjennom blant annet raskere oppkoblingstid på samtaler, bedre lydkvalitet og mindre batteriforbruk. Samtidig forventer Nkom at dette også vil medføre at nye logiske sårbarheter blir introdusert og forsøkt utnyttet av ulike trusselaktører. Den potensielle hendelsen Nkom har analysert er én av mange mulige innfallsvinkler, som tar utgangspunkt i en sofistikert trusselaktør som har både kapasitet og intensjon til å foreta avlytting/sporing. Den samlede vurderingen er at risikoen for at sikkerhetshull i VoLTE-løsningen blir funnet og utnyttet er *moderat*, men også beheftet med betydelig usikkerhet.

4.3.3 Utpressingsforsøk mot ISP (H8)

Vi har de siste årene sett flere eksempler på skadevare som har som hensikt å ramme kritisk infrastruktur eller samfunnsfunksjoner, og hvor det virker åpenbart at det ligger sikkerhetspolitisk eller militære motivasjon bak. Stuxnet[3] er et slikt eksempel. Trusselen for denne type skadevare er langt mindre spesifikk enn den som i Nkoms analyse omhandler avlytting/sporing (H7), men er likevel reell.

Hendelse H8 i analysen beskriver et tilsiktet angrep mot en tilbyder gjennom å utnytte en oppdaget skadevare som har blitt plantet i en sentral nettverkskomponent. I dette scenarioet er skadevaren oppdaget av en sofistikert hackergruppe og utnyttet til utpressing og digital sabotasje, hovedsakelig for å skape oppmerksomhet. Konsekvensen av handlingen vil likevel kunne være den samme som om det lå en sikkerhetspolitisk motivasjon bak. Dette illustrerer en uforutsigbarhet som gjør at man ikke kan se bort fra at avansert skadevare også kan utnyttes i «fredstid». Samlet anses risikoen som *moderat* til *høy*, men med et betydelig usikkerhetsspenn.

4.3.4 Angrep på DNS (H9)

Domain Name System (DNS) er internettjenesten som kobler domenenavn sammen med IP-adressen til en tjener på Internett og også gir en enklere tekstlig representasjon i adresseringen av systemer. DNS-tjenesten er bygget opp av et hierarkisk nettverk av navnetjenermaskiner, spredd i topologisk og geografisk forstand. For at systemet skal fungere, er det viktig at alle navnetjenerne har korrekt registreringsinformasjon. Et mulig angrep på

[3] Stuxnet, oppdaget i 2010, var en avansert dataorm spesielt utviklet for å angripe SCADA-kontrollsystem, og som skal ha blitt satt inn mot det iranske atomprogrammet.

DNS er ved hjelp av *DNS-spoofing*, hvor kobling mellom domene eller maskinnavn mot IP-adresser er forfalsket og uriktig. Ved slike angrep kan internettbrukere lures til å aksessere ondsinnede forfalskede nettjenester. Svindel, phishing og nedlastning av skadevare er eksempler på hvordan dette kan utnyttes dersom systemet er kompromittert.

I analysen av denne potensielle hendelsen har Nkom tatt utgangspunkt i at flere norske ISP-er har blitt utsatt for DNS-spoofing slik at brukere blir utsatt for skadevareangrep. Hendelsen oppdages ved uautorisert handel på nett ved at angriperne har fått til gang til kundenes brukernavn og passord. Den samlede risikoen vurderes som *lav* til *moderat*, men vil kunne oppleves svært belastende for de som blir berørt. Det er knyttet liten usikkerhet til hendelsen.

4.3.5 Kompromittering av elektroniske sertifikat (H10)

Public Key Infrastructure (PKI) er et system for å opprette, lagre og distribuere elektroniske sertifikater og sikrer knytning mellom et sertifikat og bestemte entiteter eller ressurser. Elektroniske sertifikat og PKI benyttes i dag for å muliggjøre kryptering og autentisering i en rekke tjenester på Internett. PKI benyttes særlig for sikring av websider og som grunnlag for elektronisk signatur. Infrastrukturen er hierarkisk bygget opp hvor en sentral server (*certificate authority rootserver*) benyttes for sikker fremstilling av sertifikater brukt til ulike tjenester.

Nkom har analysert en potensiell hendelse hvor en sentral sertifikatutsteder er blitt kompromittert via en programvaresårbarhet i certificate authority rootserver. Et slikt angrep vil kunne gi kontroll over sertifikat brukt ved utstedelse av sertifikater, tilbaketrekkingslister eller lignende. Integritet til tjenester, transaksjoner og trafikk vil ikke lengre kunne opprettholdes, når en utsteder av sertifikater er kompromittert. Avhengig av bruksområde, kan dette påvirke sikker tilgang til offentlige og private tjenester og transaksjoner. Denne typen angrep krever stor teknisk kompetanse og intensjonen er som regel å angripe andre tjenester enn sertifikatutstederens tjenester. Sertifikatet blir brukt som verktøy for å gjennomføre angrep. Som regel er serverplattformer komplekse og vil alltid inneha et element av usikkerhet knyttet til tilstedeværelse av sikkerhetshull som lar seg utnytte. Sannsynlighet for angrep anses likevel lav, og samlet anses risikoen som *lav* til *moderat*.

4.3.6 Bortfall av GPS (H11)

Det har de siste årene vært rettet fokus på kritiske samfunnsfunksjoners avhengighet av satellittbaserte tjenester, og særlig avhengigheten av det amerikanske Global Positioning System (GPS). Dette har senest blitt belyst av Lysne-utvalget, som stiller opp hvordan ulike kritiske samfunnsfunksjoner er avhengig av posisjon, navigasjon, tid og kommunikasjon fra satellittbaserte tjenester.

Utfall av satellittbaserte tjenester vil uten tvil skape store utfordringer i samfunnet. Risikoanalysen av H11 er imidlertid avgrenset til hvordan et bortfall av GPS vil påvirke

ekomnett, og dernest hvordan dette bidrar til negativ samfunnskonsekvens. I ekomnettene benyttes GPS hovedsakelig til klokkesynkronisering. De større netteierne har imidlertid egne nettklokker for synkronisering som er uavhengig av GPS i lengre perioder (flere uker). En annen utfordring kan oppstå dersom GPS-klokken «driver» litt, slik at nettklokken blir justert feil uten at dette i første omgang oppdages. Nettverksteknologien som er mest avhengig av klokkesynkronisering (SDH) blir stadig mindre utbredt. Nkom har vurdert at den samlede risikoen ved bortfall av GPS for ekomnett er *lav* til *moderat.*

I tilfellet hvor GPS rammes på grunn av en solstorm, vil solstormen i seg selv kunne ramme kommunikasjonssatellittene og i tillegg skape forstyrrelser på HF-samband. Det er også en viss risiko for at svært kraftige solstormer kan ramme strømnettet, som igjen kan føre til utfall av ekomtjenester. Dette perspektivet inngår imidlertid ikke i denne analysen.

4.3.7 Risikoreduserende tiltak – kompleks og omfattende utstyrsportefølje

Mobiltilbyderne har de siste årene etablert tiltak i nettet for å redusere problemer som følge av høy signaleringstrafikk (H6). Et slikt tiltak er *throttling*, en funksjon i nettet som kontrollerer at det ikke slippes gjennom mer signaleringstrafikk enn det som de sentrale nettelementene klarer å håndtere. Dette, sammen med det tidligere nevnte tiltaket om å styrke prosessene for planlagt arbeid og feilhåndtering (T2), vil bidra til å redusere risikoen for signaleringsstormer.

I moderniseringsprosjekter og ved innføring av ny teknologi, som for eksempel ved innføring av VoLTE (H7), foreligger det i forkant risikovurderinger og omfattende testing. For å sikre stabil drift gjennom overgangsperioden overvåkes også situasjonen nøye for å verifisere at alt fungerer, og at eventuelle feil som oppstår blir oppdaget og rettet raskt. Nkoms erfaring så langt er at slike teknologiskifter i all hovedsak gjennomføres på en god måte og uten negative konsekvenser for sluttbrukerne. Innføring av ny teknologi medfører også ikke bare forbedret funksjonalitet, men også økt sikkerhet. For eksempel utnytter falske basestasjoner, som fikk stor oppmerksomhet i 2015, sårbarheter som finnes i 2G, men ikke i 3G og 4G. Men selv om ny teknologi fjerner kjente sårbarheter, innføres nye typer sårbarheter. Nkom er mindre sikker på at alle tilbyderne er like bevisste på å adressere disse på en systematisk måte. Et risikoreduserende tiltak vil være at tilbyder gjennomfører egne risikovurderinger, hvor de fokuserer på de *nye potensielle sårbarhetene* som kommer som resultat av teknologiskiftene. Tilsvarende risikovurderinger vil være viktige ved organisatoriske endringer, som for eksempel utkontraktering, jf. kap. 4.4.

De siste årene har vi sett tilstrekkelig antall eksempler på logiske sårbarheter i nettverkskomponenter, til å måtte forvente at slike også kan ligge latent i programvare i norske ekomnett (jf. H8). Det finnes dessverre ingen tiltak som kan garantere at programvare er fri for sårbarheter eller skadevare. Tilbyderne bør derfor forutsette at sårbarheter eller skadevare allerede finnes eller kan innføres i nettene, og på bakgrunn av en risikovurdering etablere nødvendige risikoreduserende tiltak. Dette kan være tiltak knyttet til autorisasjon og

tilgangskontroll, logging og sporing av all tilgang til og endring i systemene, og rutiner for logginspeksjon. Tiltakene vil ikke nødvendigvis hindre at skadevare utnyttes, men vil kunne bidra til å redusere konsekvensene. Et viktig underlag for å vurdere riktig omfang av sikkerhetstiltakene vil være det tidligere nevnte tiltak som omhandler utveksling av trusselbilde mellom myndighetene og tilbyderne (T3).

I forhold til hendelse H9 er tilbydere omfattet av generelle krav til forsvarlig sikkerhet, men ingen detaljerte krav spesifikt knyttet til DNS. Det finnes Best Current Practises (BCPs) relatert til sikring av tradisjonelle DNS-tjenester som tilbydere bør følge. Videre vil utvidelser av DNS-tjenesten som DNSSEC (*DNS Security Extensions*), bedre kunne sikre DNS mot spoofing-angrep. DNSSEC er en sikkerhetsmekanisme som legges inn i domenenavnsystemet. Med DNSSEC signeres svarene på et domeneoppslag på en slik måte at det er mulig å verifisere at de kommer fra riktig kilde og ikke er endret underveis. I Nkoms arbeidsgruppe sammen med bransjen *Sikkerhet og abuse*, er aktuelle trusler og problemstillinger stadig tema, og anbefalte mottiltak diskuteres.

Hendelse H10 omhandler kompromittering av elektroniske sertifikat. Norske sertifikatutstedere reguleres gjennom esignaturloven med tilhørende forskrifter og «Kravspesifikasjon for PKI i offentlig sektor». Her stilles det krav til detaljert sertifikatpolicy, sertifikatpraksis og tilleggsdokumentasjon som skal sikre etterlevelsen av lov og reglement. Videre finnes det et rikt sett av detaljerte tekniske standarder og prosedyrer som anbefales fulgt, og som sørger for at tjenesten sikres. Forordning (EU) 910/2014 om eID og tillitstjenester utvider antall tjenester som omfattes av norsk regelverk. Parallelt med utarbeidelse av nytt regelverk foretar ETSI[4] en full gjennomgang av tekniske standarder og prosedyrer som er relevant for tjenestene. Det nye regelsettet har blant annet som mål å gi sikrere PKI tjenester.

I tabellen nedenfor oppsummeres de risikoreduserende tiltakene knyttet til komplekse verdikjeder og omfattende utstyrsportefølje.

[4] European Telecommunications Standards Institute

	Tiltak	Beskrivelse
T6	**Risikovurderinger og tiltak – teknologiske/organisatoriske endringer**	*Gjennomføre systematiske og dokumenterte risikovurderinger med fokus på nye sårbarheter som innføres i forbindelse med teknologiske eller organisatoriske endringer.*
T7	**Sikringstiltak mot logiske sårbarheter og skadevare**	*Skadeforebyggende og skadereduserende tiltak mot logiske sårbarheter og skadevare i nett og komponenter, som autorisasjon og tilgangskontroll, logging og sporing, rutiner for logginspeksjon, osv.*
T8	**DNSSEC og BCP**	*Videreføre arbeidet med innføring av DNSSEC og etterlevelse av BCP, blant annet gjennom arbeidsgruppe sikkerhet og abuse*
T9	**Implementering av forordning (EU) 910/2014**	*Implementering av forordningen og oppfølging av at kravene etterleves.*

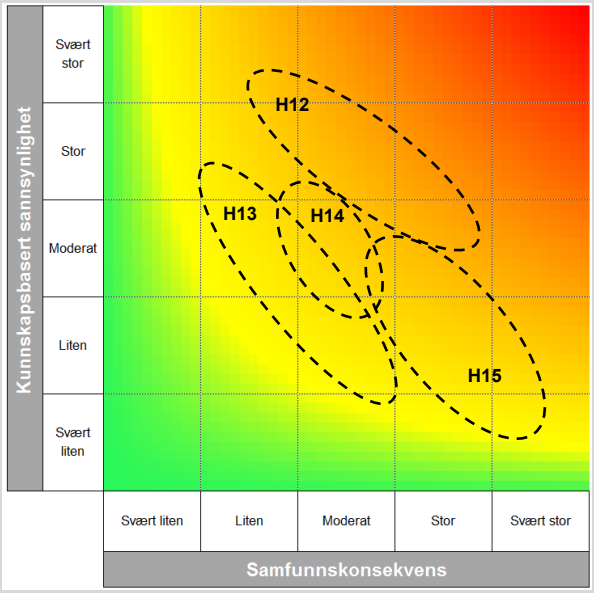
Tabell 2. Risikoreduserende tiltak – kompleks verdikjede og omfattende utstyrsportefølje

4.4 Utkontraktering og internasjonalisering

Etter at en kabelbrann på Oslo sentralstasjon 27. november 2007 førte til ca. 20 timers stans i all togtrafikk på Østlandet og bortfall av tele- og datatrafikk for et stort antall kunder i ca. 10 timer, oppsummerte DSB:

> *«Her er det en lang kjede av tjenesteytere og brukere/kjøpere som tidligere var én eier, drifter og ansvarshavende. Den organisatoriske oppsplitting som har funnet sted over tid, kombinert med at aktørene etter hvert også har fått nye markeder, kunder og oppgaver kan ha bidratt til oppstykking og utydeliggjøring av ansvar og roller. Et annet aspekt er at det med en slik utvikling følger ulike og endrede oppfatninger om hva som er kjernevirksomhet sett i et samfunnsperspektiv. Herunder kommer også manglende helhetlig vurdering av sårbarhet, risiko og konsekvenser. Dette synes å ha resultert i mangelfullt vedlikehold av teknisk utstyr og svake rutiner både ved normal drift og i feilsituasjoner. Konsekvensene vil være økt sårbarhet gjennom redusert kvalitet i oppgaveløsningen og dermed økt risiko for uforutsette hendelser.»*

Hendelsen økte bevisstheten rundt sikkerhets- og beredskapsutfordringer med utkontraktering.Utfordringene er minst like aktuelle i dag, med stadig mer komplekse aktørbilder og verdikjeder. Aktørene blir også i økende grad multinasjonale, noe som utfordrer norske myndigheters evne til kontroll og regulering. Innenfor dette risikoområdet har Nkom vurdert fire hendelser (Figur 4).



H12. Kartlegging av norsk kritisk infrastruktur
I forbindelse med en større oppgradering får en utstyrsleverandør utvidede fysiske og logiske tilganger til infrastruktur og tjenestetopologi i landsdekkende ekomnett. Opplysningene lekkes til annet lands etterretningstjeneste.

H13: Ressursproblemer - entreprenør
Påfølgende ekstremværhendelser som beveger seg over Sør-Norge, Danmark og Sverige skaper svært mange lokale og regionale utfall og tapper entreprenørene for ressurser.

H14: Ressursproblemer - leverandør
Økonomiske utfordringer hos utstyrsleverandør fører til press på kompetanse og ressurser. Norsk MVNO blir nedprioritert ifm en kompleks feilsituasjon som krever leverandørens kompetanse.

H15: Overvåkning via nett i utlandet
Svensk avis avslører massiv overvåkning av Telias mobilkunder pga. oppdaget skadevare. Rammer også norske brukere.

Figur 4. Risikoanalyser – utkontraktering og internasjonalisering. Usikkerhet representeres ved størrelsen på det stiplede arealet.

4.4.1 Kartlegging av norsk kritisk ekominfrastruktur (H12)

Tilbyderne er helt avhengig av å gi eksternt personell som utstyrs- og driftsleverandører, entreprenører og konsulenter tilganger til tilbyders objekter, systemer og informasjon. At tilganger kun gis etter tjenstlig behov er et grunnleggende prinsipp. Andre barrierer kan være ulike godkjenningsordninger. For tilgang til objekter og informasjon underlagt sikkerhetsloven, kreves det også at personellet sikkerhetsklareres og autoriseres. I mange tilfeller er tilbydere avhengig av å gi også utenlandsk personell tilganger.

Bakteppet for H12 er at utenlandsk etterretning utnytter utenlandsk personell med rettmessig tilganger hos norske tilbydere til å kartlegge norsk kritisk ekominfrastruktur. Muligheten for at utenlandske konsulentselskaper brukes som verktøy for fremmede lands etterretning, fremgår av PSTs trusselvurderinger for 2015 og 2016. Sannsynligheten for at intern informasjon kommer fremmede lands etterretning i hende, anses derfor som betydelig. Den samlede risikoen anses å være *moderat* til *høy*, og er avhengig av hvilken og hvor mye informasjon som blir lekket.

4.4.2 Ressursproblemer – entreprenør (H13)

I en rapport utarbeidet av Nexia for Post- og teletilsynet i 2012 om kost-/nyttevurdering av tiltak for styrking av norsk sambands- og IP-infrastruktur, fremgår det at

> *«ved større kriser synes aktørene ikke å være tilstrekkelig dimensjonert for å ivareta feilhåndtering. Dette gjelder både egen kapasitet og kapasitet hos partnere og leverandører (f.eks. hos entreprenørene). […] Som et eksempel ble det under feilretting av skader under stormen Dagmar innhentet forsterkninger fra entreprenørens side. Disse ressursene ble ikke utnyttet fullt ut grunnet svak koordinering med kraftselskapenes entreprenører og andre nødvendige ressurser som f.eks. treryddere.»*

H13 tar for seg et ekstremværscenario som vedvarer over lengre tid enn de ekstremværene vi normalt opplever, og som påvirker Sør-Norge, Danmark og Sør-Sverige. I nevnte rapport ble risikoen knyttet til utilstrekkelig beredskap, vurdert å være høy. Begrunnelsen var svakheter i samhandling, øving og tilrettelegging av reserveløsninger på tvers av aktører, i tillegg til ressursproblemer hos entreprenører. Nkom mener at etter ekstremværet Dagmar i romjulen 2011, har innsatsen med øvelser og økt samhandling, samt erfaring fra faktiske hendelser, bidratt til å redusere risikoen. Likevel vil det fortsatt kunne være utilstrekkelige entreprenørressurser i de mest ekstreme situasjonene. Nkom erfarer også at de siste få prosentene av feilrettingsarbeidet etter større hendelser (halen) ofte tar adskillig lengre tid å rette enn de øvrige feilene. Dette er ofte de mer krevende feilrettingsoperasjonene som samtidig berører et mindre antall brukere. Likevel kan den lange varigheten på utfallet gjøre at situasjonen blir kritisk for de brukerne det gjelder. Samlet sett vurderes risikoen å være *moderat*.

4.4.3 Ressursproblemer – leverandør (H14)

Tilbyderne er i dag helt avhengige av leverandørenes kompetanse og ressurser for å utføre oppgraderinger og endringer, og for å håndtere og analysere mange feilsituasjoner. I likhet med H13, hvor problemstillingen er mangel på entreprenørressurser, kan tilsvarende problem oppstå på utstyrsleverandørsiden. Det er svært mange faktorer som påvirker risikoen ved en slik hendelse. Utstyrsleverandørene kan vanligvis benytte seg av at de har en stor internasjonal organisasjon med betydelig kompetanse i ryggen. Ved kritiske feil på sentrale nettverkskomponenter hos de største tilbydere, vil imidlertid forlenget analysetid på bare timer kunne ha negativ samfunnsmessig konsekvens. I en kritisk og presset situasjon vil utstyrsleverandørene måtte prioritere mellom sine kunder på bakgrunn av inngåtte serviceavtaler og ellers tapspotensiale. Scenarioet i H14 er at rettetiden for en kompleks feilsituasjon hos en norsk virtuell mobiloperatør (MVNO) blir adskillig forlenget på grunn av en presset ressurssituasjon hos leverandør. Konsekvensen er langvarig utfall av MVNO-ens mobiltjenester. Sammenlignet med H13, som kan føre til lokale utfall på mange ekomtjenester samtidig, vil H14 føre til landsdekkende utfall, men på kun én tjeneste. Den samlede risikoen anses å være *moderat*.

4.4.4 Overvåkning via nett i utlandet (H15)

I dag har Telia og TDC de mest sentrale komponentene i mobilnettene plassert i utlandet, i henholdsvis Sverige og Danmark. Siden det er i disse komponentene at mobiltjenestene blir produsert (oppsett av samtaler, datasesjoner, SMS/MMS osv.) innebærer dette at signalerings- og trafikkdata, og i noen tilfeller innholdsdata, i disse mobilnettene blir prosessert og behandlet i utlandet. H15 tar for seg et scenario hvor det blir avslørt skadevare i Telias nett i Sverige. Etter hvert som nettkomponenter sentraliseres, vil effekten av å utnytte sårbarheter eller å plassere skadevare i disse komponentene bli større. Dette gjør disse nettene til attraktive mål for trusselaktørene. En slik hendelse i utlandet vil direkte ramme norske (og andre nordiske) kunders kommunikasjonsvern. Nkom vurderer den samlede risikoen som *moderat*.

4.4.5 Risikoreduserende tiltak – utkontraktering og internasjonalisering

De norske tilbyderne er i mange tilfeller helt avhengig av å gi underleverandører og deres personell, også utenlandsk, tilganger til utstyr i og informasjon om sin infrastruktur (H12). For å redusere risikoen for at disse tilgangene utnyttes av fremmede lands etterretning, gjelder for så vidt de samme prinsippene som er omtalt i kapittel 4.2.6. Også her er utveksling av trusselbilde mellom myndighetene og tilbyderne (T3), samt awareness og informasjonssikring mot etterretning (T4), viktig.

Som omtalt under H13, vil ekstreme utfallssituasjoner kunne medføre mangel på entreprenørressurser. Nkom mener at det vil være urealistisk å ha betydelig overkapasitet av entreprenørressurser i tilfelle ekstreme situasjoner. Alternative risikoreduserende tiltak vil være å vedlikeholde og forbedre den operative krisehåndteringsevnen både hos tilbydere og myndigheter, gjennom proaktiv beredskap, utvikling av samhandlingsløsninger, anskaffelse av beredskapsutstyr osv. I tillegg er tiltak for å styrke redundans og resiliens i ekomnettene (T1), som omtalt i kapittel 4.2.6, viktig.

Mens ressursproblemer hos entreprenørene gjerne påvirker aksess-delen av nettet, og særlig i områder med spredt bosetning, vil ressursproblemer hos utstyrsleverandørene (H14) potensielt ramme sentral tjenesteproduksjon. Avhengigheten av utstyrsleverandørene er stadig økende og det er derfor svært viktig at tilbyder tar høyde for dette i sine risikoanalyser og sin beredskapsplanlegging. Ekommyndighetene må på sin side vurdere om regelverket i tilstrekkelig grad er egnet til å adressere at kritisk kompetanse i stor grad er plassert hos underleverandør, og gjerne utenfor norsk jurisdiksjon. Her er det naturlig å se på reguleringen i andre sektorer, som for eksempel finanssektoren og petroleumssektoren, samt lovarbeidet som foregår på EU-nivå og nordisk nivå. Dette tiltaket må også ta hensyn til situasjoner der tilbyderne opererer på tvers av landegrensene, som illustrert i H15.

I tabellen nedenfor oppsummeres de risikoreduserende tiltakene knyttet til utkontraktering og internasjonalisering.

	Tiltak	Beskrivelse
T10	**Øke operativ krisehåndteringsevne**	*Øke operativ krisehåndteringsevne både hos tilbydere og myndigheter, gjennom proaktiv beredskap, utvikling av samhandlingsløsninger, anskaffelse av beredskapsutstyr osv.*
T11	**Risikovurderinger og tiltak – avhengighet til underleverandører**	*Gjennomføre systematiske og dokumenterte risikovurderinger med fokus på sårbarheter som følger av egen avhengighet til utstyrsleverandører og entreprenører.*
T12	**Videreutvikle regelverk – utkontraktering/ internasjonalisering**	*Videreutvikle regelverket slik at det stiller relevante sikkerhetskrav som bidrar til å redusere risiko knyttet til utkontraktering og internasjonalisering.*

Tabell 3. Risikoreduserende tiltak – utkontraktering og internasjonalisering

5 Oppsummering

EkomROS 2016 har analysert hendelser innenfor tre risikoområder:

- Nasjonal sambandsinfrastruktur og sentralisert tjenesteproduksjon
- Kompleks og omfattende utstyrsportefølje
- Utkontraktering og internasjonalisering

Den samlede oversikten under gir et bilde av risiko innenfor disse risikoområdene. Det er viktig å understreke at denne oversikten alene ikke gir et fullstendig risikobilde, men heller et utsnitt. Når de risikoreduserende tiltakene skal vurderes, må dette tas hensyn til. Kommende risikovurderinger vil måtte se på andre risikoområder og fra andre innfallsvinkler.

5.1 Samlet oversikt over risiko

I Tabell 4 vises en samlet oversikt over de analyserte hendelsene kategorisert etter risikonivå *lav/moderat*, *moderat* og *moderat/høy* med tilhørende vurdering av usikkerhet. Risikonivået er vurdert ut fra et samfunnssikkerhetsperspektiv og høyeste risiko er forbundet med hendelser som det er sannsynlig at kan oppstå og som medfører betydelige samfunnskonsekvenser i form av omfattende brudd på kommunikasjonsvernet, fare for liv og helse eller som påvirker sentrale institusjoners funksjons- eller styringsevne.

ID	Uønsket hendelse	Risiko	Usikkerhet
H2	Konfigurasjonsfeil i landsdekkende IP-nett	Moderat/høy	Høy
H3	Utpressing av nøkkelressurs – sabotasje transportnett	Moderat/høy	Høy
H8	Utpressingsforsøk mot ISP - skadevare	Moderat/høy	Høy
H12	Kartlegging av norsk kritisk infrastruktur	Moderat/høy	Høy
H1	Multippel transmisjonsfeil i transportnett	Moderat	Høy
H4	Fiberbrudd Svalbard og Finnmark	Moderat	Moderat
H5	Strømsvikt på kritiske anlegg i Oslo	Moderat	Moderat
H6	Signaleringsstorm i landsdekkende mobilnett	Moderat	Lav
H7	Sikkerhetshull i VoLTE	Moderat	Høy
H13	Ressursproblemer - entreprenør	Moderat	Høy
H14	Ressursproblemer - leverandør	Moderat	Moderat
H15	Overvåkning via nett i utlandet	Moderat	Høy
H9	DNS-angrep	Lav/moderat	Lav
H10	Kompromittering av sertifikatutsteder	Lav/moderat	Lav
H11	Bortfall av GPS	Lav/moderat	Lav

Tabell 4. Samlet oversikt over risiko og usikkerhet sortert etter risikokategori (hendelsene innenfor hver av risikokategoriene er sortert etter nummer og ikke etter risiko).

Oversikten viser at den høyeste risikoen i vår analyse er knyttet til potensielle hendelser i nettene til de store netteierne. Disse vil bli utløst enten av utilsiktede logiske feil eller gjennom

tilsiktede handlinger som involverer etterretning eller utpressing/sosial manipulering. Det er naturlig nok høy usikkerhet knyttet til disse analysene, og flere av hendelsene forutsetter en mer tilspisset sikkerhetspolitisk situasjon enn dagens. Nkom anser dem likevel for å være relevante. Dette blir understreket av det klare budskapet i sikkerhetsmyndighetenes åpne trusselvurderinger: Den sikkerhetspolitiske situasjonen er uforutsigbar, og nettverksbaserte etterretningsoperasjoner blir stadig mer målrettet og teknisk avanserte.

I kategorien moderat og lav/moderat risiko finner vi flere av de fysiske hendelsene som fiberbrudd og feil på strømforsyning. Dette er hendelser som uten tvil kan ha betydelige konsekvenser, noe særlig ekstremværet Dagmar i 2011, men også påfølgende ekstremværhendelser, har illustrert. Økt krisehåndteringsevne både hos myndighetene, ekomtilbyderne og andre eiere av kritisk infrastruktur, har imidlertid bidratt til å redusere risikoen de siste årene. Erfaringene fra ekstremværet Tor i slutten av januar 2016, underbygger dette.

5.2 Samlet oversikt over risikoreduserende tiltak

I 2015 ble det publisert flere rapporter som adresserer sårbarheter i det «digitale» samfunnet. Rapporten til Lysne-utvalget, NSMs IKT-risikobilde og sikkerhetsfaglige råd, presenterer alle forslag til menneskelige, organisatoriske og tekniske tiltak for å redusere disse sårbarhetene. Noen av disse tiltaksforslagene er knyttet til tematikk utenfor konteksten til EkomROS 2016, mens andre overlapper med de risikoreduserende tiltakene som er omtalt i denne rapporten og som er oppsummert i Tabell 5. I tabellen er det angitt hvilke hendelser tiltakene har risikoreduserende effekt på.

	Tiltak	Risikoreduserende effekt													
		H 2	H 3	H 8	H 12	H 1	H 4	H 5	H 6	H 7	H 13	H 14	H 15	H 9	H 10	H 11
T1	Redundans og swapping					X	X				X					
T2	Risikovurderinger og tiltak - planlagt arbeid i nett	X				X			X		X					
T3	Utveksling av trusselbilde		X	X	X		X			X			X	X	X	
T4	Awareness - etterretning				X		X						X			
T5	Vedlikehold av reservestrøm							X			X					
T6	Risikovurderinger og tiltak – teknologiske/ organisatoriske endringer								X	X		X				
T7	Sikringstiltak mot logiske sårbarheter og skadevare	X	X	X	X				X	X			X	X	X	
T8	DNSSEC og BCP													X		
T9	Implementering av forordning (EU) 910/2014														X	
T10	Øke operativ krisehåndteringsevne	X	X	X		X	X	X	X	X	X	X		X	X	X
T11	Risikovurderinger og tiltak – avhengighet til underleverandører										X	X	X			
T12	Videreutvikle regelverk – utkontraktering/ internasjonalisering										X	X	X			

Tabell 5. Forslag til tiltak sammen med en angivelse av hvilke hendelser tiltakene har risikoreduserende effekt på.

5.3 Konklusjon

Enkelte av tiltakene i Tabell 5 er overordnede mens andre er konkrete, noen er av organisatorisk art og andre er av teknisk art. Enkelte har risikoreduserende effekt på en spesifikk type hendelse, mens andre har risikoreduserende effekt på flere av de analyserte hendelsene. Fordi tiltakene er av forskjellig art, er det ikke nødvendigvis hensiktsmessig å sammenligne og rangere disse direkte. Nkom trekker likevel fram særlig tre hovedtrekk fra EkomROS 2016 til videre oppfølging.

5.3.1 Tiltak med bred risikoreduserende effekt

Det er særlig tre av de foreslåtte tiltakene som har risikoreduserende effekt på flere av hendelsene, inkludert de med høyest risiko. Disse er gjengitt i Tabell 6.

	Tiltak	Beskrivelse
T3	**Utveksling av trusselbilde**	*Videreføre og videreutvikle sikkerhetsforum med Nkom, tilbyderne og de hemmelige tjenestene, og etablere arenaer for informasjonsutveksling mellom NorCERT, sektor-CSIRT-ene (inkludert Nkom-CSIRT) og ekomtilbyderne.*
T7	**Sikringstiltak mot logiske sårbarheter og skadevare**	*Skadeforebyggende og skadereduserende tiltak mot logiske sårbarheter og skadevare i nett og komponenter, som autorisasjon og tilgangskontroll, logging og sporing, rutiner for logginspeksjon, osv.*
T10	**Øke operativ krisehåndteringsevne**	*Øke operativ krisehåndteringsevne både hos tilbydere og myndigheter, gjennom proaktiv beredskap, utvikling av samhandlingsløsninger, anskaffelse av beredskapsutstyr osv.*

Tabell 6. Tiltak med bred risikoreduserende effekt.

Særlig innenfor tiltak T3 og T10 har Nkom og tilbyderne allerede iverksatt flere aktiviteter, og EkomROS 2016 viser at dette arbeidet er viktig å videreføre og videreutvikle. Når det gjelder den operative krisehåndteringsevnen (T10), er erfaringene fra reelle hendelser og øvelser den siste tiden at det stadig er behov for å utvikle bedre verktøy og løsninger for krisekommunikasjon og samhandling.

Fra januar 2016 er Nkom også i gang med å bemanne opp et eget hendelseshåndteringsmiljø for det digitale domenet, Nkom-CSIRT, som langt på veg også er et svar på tiltak T3 og T10. Det vil være naturlig at hovedansvaret for å følge opp tiltak T7, sikringstiltak mot logiske sårbarheter og skadevare, ligger under Nkom-CSIRT. Oppfølgingen av tiltaket opp mot tilbyderne blir da i form av samarbeid og veiledning.

5.3.2 Gjennomføring av systematiske og dokumenterte risikovurderinger

Risikostyring inngår som en integrert del av virksomheten til de aller fleste ekomaktørene. Nkoms erfaring er likevel at det er et forbedringspotensial når det kommer til å gjennomføre systematiske og dokumenterte risikovurderinger for å oppnå forsvarlig sikkerhetsnivå. EkomROS 2016 peker på risikoområder som i sterkere grad bør adresseres i tilbydernes risikovurderinger (Tabell 7).

	Tiltak	Beskrivelse
T2	**Risikovurdering og tiltak - planlagt arbeid i nett**	*Videreutvikle prosesser og rutiner for risikovurdering ved planlagt arbeid i nett med tilhørende skadeforebyggende og skadereduserende tiltak.*
T6	**Risikovurderinger og tiltak – teknologiske/organisatoriske endringer**	*Gjennomføre systematiske og dokumenterte risikovurderinger med fokus på nye sårbarheter som innføres i forbindelse med teknologiske eller organisatoriske endringer.*
T11	**Risikovurderinger og tiltak – avhengighet til underleverandører**	*Gjennomføre systematiske og dokumenterte risikovurderinger med fokus på sårbarheter som følger av egen avhengighet til utstyrsleverandører og entreprenører.*

Tabell 7. Tiltak knyttet til gjennomføring av risikovurderinger.

Nkom vil ha særlig oppmerksomhet på disse tiltakene i det videre veilednings- og tilsynsarbeidet.

5.3.3 Sikringstiltak knyttet til den fysiske infrastrukturen

En av hovedanbefalingene i Lysne-utvalgets rapport var å redusere kritikaliteten av Telenors transportnett, ettersom den totale summen av samfunnsverdier dette nettet bærer, er uakseptabelt høy. I EkomROS 2016 har Nkom analysert flere hendelser som kan ramme denne infrastrukturen. Analysen viser at den største risikoen er knyttet til tilgjengelighetsbrudd utløst utilsiktet eller tilsiktet gjennom feilkonfigurasjon (H2, H3) eller kartlegging av denne infrastrukturen gjennom utenlandsk etterretning, som igjen kan utnyttes til å utføre sabotasje i en eskalert sikkerhetspolitisk situasjon. Dette understreker viktigheten tiltakene nevnt i kapittel 5.3.1 og 5.3.2, i tillegg til tiltak T4 (Tabell 8).

	Tiltak	Beskrivelse
T4	**Awareness – etterretning**	*Vanskeliggjøre fremmede staters etterretning, både fra åpne og lukkede kilder gjennom økt awareness i tilbydernes organisasjoner.*

Tabell 8. Tiltak T4.

Disse hendelsene vil kunne ramme nettet uavhengig av grad av fysisk redundans. Når det gjelder risiko for fysiske brudd i transportnettene har Nkom vurdert risikoen som moderat (H1, H4). Det sentrale risikoreduserende tiltaket er da økt redundans og swapping (Tabell 9).

	Tiltak	Beskrivelse
T1	**Redundans og swapping**	*Øke redundans i transportnett og regionalnett. Tilrettelegge for sammenkopling av nett og inngå bytteavtaler (swapping) for beredskapsformål.*

Tabell 9. Tiltak T1.

Her vil Nkom understreke at den fysiske redundansen i transportnettene anses som god, mens det er mindre redundans i regionalnettet og ut mot aksessnettene, særlig i de mindre tettbygde områdene av landet. Ut fra nordområdenes strategiske betydning, bør særlig den fysiske redundansen i Nord-Norge forsterkes. Gjennom programmet «Forsterket ekom», bidrar Nkom

med å bygge ut strategiske basestasjonslokasjoner i kommunene med redundant transmisjon og tre døgn reservestrøm. En positiv bieffekt av forsterkingen av transmisjon til basestasjonene er generelt økt redundans i regionalnettene. Per i dag har programmet resultert i fremføring av ny fiber over Vestfjorden i Nordland, og i Storfjorden i Møre og Romsdal. En kostnadseffektiv måte å gjennomføre tiltak T1 på er derfor å videreføre programmet «Forsterket ekom». I tillegg til dette vil Nkom gå i dialog med tilbyderne for å utrede hvordan de allerede eksisterende transportnett-infrastrukturene til blant annet Telenor, Broadnet og Altibox kan utnyttes, for eksempel gjennom bytteavtaler (swapping), for å øke resiliensen i den nasjonale ekominfrastrukturen.