Nasjonal kommunikasjons-myndighet

Risiko- og sårbarhetsanalyse for ekomsektoren

Nasjonal kommunikasjonsmyndighet

1. Oktober 2024

Sammendrag

Digitaliseringen av samfunnet er i stadig utvikling og Norge er et av verdens mest digitaliserte land. For at vi skal møte fremtidens utfordringer må vi ta i bruk de mulighetene som ligger i teknologien, og vi må gjøre det på en forsvarlig måte. For at digitaliseringen av samfunnet skal lykkes er vi avhengig av en sikker og robust digital grunnmur. Samfunnet er sterkt avhengig av den digitale grunnmuren og den er bærer av flere grunnleggende nasjonale funksjoner. En stadig raskere digitaliseringstakt og den sikkerhetspolitiske utviklingen øker gapet mellom dagens sikkerhetsnivå og samfunnets behov for sikre og robuste nett.

Norge har et av verdens mest robuste og sikre ekomnett og -tjenester. Det er generelt lite utfall, men ekomnettene blir utsatt for stadige nye farer og trusler. Nasjonal kommunikasjonsmyndighet (Nkom) ser en betydelig endring i risiko- og trusselbildet for ekomtilbydere og datasenteroperatører de siste årene på grunn av den sikkerhetspolitiske situasjonen. Det er krig i Europa, og vi må gå fra å ha god sikkerhet i fred, til å ha sikkerhet som kan stå imot krise og krig. Nkom opplever en stor variasjon mellom ekomtilbyderne på hvor forberedt de er på kriser i det øvre spennet.

Virksomheter må også ta inn over seg det nye risikobilde og vurdere ulike scenarioer når de skal vurdere hvor robuste ekomtjenester de skal ha. Særlig samfunnskritiske virksomheter må ha oversikt egne verdier og hvilken avhengighet de har til ekomtjenester og sikre at de har tilstrekkelig motstandskraft og redundans. Det er her særlig viktig at det offentlige går foran og stiller krav til sikkerhet og robusthet når offentlige virksomheter skal anskaffe ekomnett- og tjenester.

Risiko- og sårbarhetsanalysen 2024 for ekomsektoren setter fokus på flere områder hvor det bør vurderes å iverksette tiltak. Det er avdekket utfordringer knyttet til personellsikkerhet i sektoren i en tid hvor innsidetrusselen er økende. Sikkerhetsmyndighetene har uttalt at det må forventes å være innsidere i norske virksomheter, og Nkom anser ekomtilbydere og datasenteroperatører som sannsynlige mål. Innsidere er også en virkningsfull fremgangsmåte for å kunne plante skadevare, dele sårbarheter og sensitiv informasjon med uvedkommende. Et destruktivt cyberangrep med bistand av en innsider hos en av de nasjonale tilbyderne vil medføre betydelige skade samtidig som det kan være utfordrende å sikre seg mot.

Sikkerhetspolitiske omveltninger i verden vil kunne påvirke leveranser av kritiske komponent og tilgangen til personell. Det er også sterk avhengighet til enkelte lokasjoner, produsenter og land som gjør at en sårbarhet hos en leverandør kan bli delt av hele sektoren. NATO medlemskapene til Sverige og Finland vil være med på å legge til rette for et bedre nordisk samarbeid både for infrastruktur og kompetanse.

Det har vært flere hendelser i Europa knyttet til undersjøisk infrastruktur herunder sjøfiberkabler. Nkom anser sjøfiberkabler som utsatt for en rekke farer og trusler samtidig som det er regulatorisk utfordrende når infrastrukturen befinner seg i internasjonalt farvann. Statistisk sett er tråling og ankring den største trusselen mot sjøfiberkabler. Det kan videre være utfordrende å avgjøre om skader er som følge av en ondsinnet handling eller et uhell.

Norske sikkerhetstjenester fremhever at risikonivået for sabotasje har økt. Det er de siste årene vært flere tilfeller av sabotasje mot samfunnskritisk infrastruktur i Europa. Det er i 2024 observert sabotasje mot fiberinfrastruktur i Norge.

Selv om det er et stort fokus på den sikkerhetspolitiske situasjonen vil ekomsektoren fortsatt ha betydelig utfordringer og hendelser som kan relateres til mer vedvarende problemstillinger. En gjenganger som historisk har forårsaket flere større utfall i Norge er planlagt endringsarbeid i kjernenett og transportnettene. Dette så vi eksempel på under pinseaften i år hvor alle tre

mobilnettene hadde landsdekkende forstyrrelser i rundt 30 min. Nkom og tilbyderne har stort fokus på dette, men kompliserte nettverksstrukturer og uforutsette feil gjør det vanskelig å hindre at feilene likevel skjer. Forstyrrelser som hindrer mottak av GNSS (satellittbaserte navigasjonssystemer) har økt de senere årene. Forstyrrelsene er blitt et globalt problem ettersom GNSS-systemer i dag benyttes overalt i samfunnet. GNSS-mottakere er en innvevd teknologi i dagens mobiltelefoner, IoT enheter, styringssystemer for industrien, finans, maritim trafikk, vei og lufttrafikk. I tillegg til posisjonering, er GNSS systemer også viktig for korrekt angivelse av tid, som er sentralt i mange elektroniske systemer. Nær grensen til Russland oppleves forstyrrelser av GNSS daglig, noe som særlig rammer luftfartsnæringen.

Været skal bli villere, våtere og det blir vanskeligere å forutse hvor ekstremvær treffer. Langsiktig planlegging av infrastrukturen med fokus på klimaendringene er nødvendig både fra tilbydere og offentlige myndigheter.

For å holde følge med den stadig raskere utviklingen på digitaliseringsfeltet, og den nye sikkerhetspolitiske situasjonen, er det nødvendig at det planlegges langsiktig for utviklingen av den digitale infrastrukturen. Nasjonale sikkerhetsbehov og den økende forventingen hos befolkningen og næringslivet om tilgjengelighet, konfidensialitet, integritet og autentisitet i elektronisk kommunikasjon medfører nye behov som må tas høyde for. Det krever systematisk og planmessig arbeid over flere år for å bygge og sikre den digitale grunnmuren mot det nye trusselbildet og for ikke å ligge i etterkant av utviklingen.

Nkom mener derfor at det er nødvendig med en langtidsplan for den digitale grunnmuren som involverer offentlig-privat samarbeid mellom myndighetene, ekomtilbydere og datasenteroperatører. Planen må inkludere hvordan den digitale grunnmuren er forberedt på krise og krig, hvordan datasentre, transmisjonsnett og mobilnett skal få økt robusthet, sikres bedre og sikre tilstrekkelig nasjonal teknisk kompetanse.

Den graderte utgaven av risiko- og sårbarhetsanalysen har et utvalg av relevante scenarioer.

Innholdsfortegnelse

1. Bakgrunn og tilnærming

Formålet med denne risiko- og sårbarhetsanalysen er å beskrive trussel- og risikobildet knyttet til uønskede hendelser i sektoren for elektronisk kommunikasjon (ekom). Målgruppen for analysen er Digitaliserings- og forvaltningsdepartementet (DFD), andre departementer, myndigheter, kommuner, datasenteroperatører og virksomheter som er avhengig av ekom. Videre er målet å gi ekomtilbydere innspill til eget ROS arbeid og vurdering av tiltak for å sikre egen virksomhet. Denne EkomROS er basert på Nkom sin graderte utgave fra våren 2024.

1.2 Aktører i ekomsektoren

Digitaliserings- og forvaltningsdepartementet

DFD har det øverste ansvaret for utformingen av politikk og forvaltning innen ekomsektoren. Gjennom ekomloven med tilhørende forskrifter, instrukser, årlige tildelingsbrev og supplerende tildelingsbrev gir departementet føringer og rapporteringskrav til underliggende direktorat.[1]

Nasjonal kommunikasjonsmyndighet

Nkom er utøvende tilsyns- og forvaltningsmyndighet i ekomsektoren, og er administrativt underlagt DFD. Direktoratet innehar spesielt ansvar for sikkerhet og beredskap i ekomnettene mht. ulike former for påkjenninger fra ekstremvær til cyberangrep. Nkom har egen vaktordning med 24/7 beredskapsvakt for monitorering og rapportering av hendelser både i det fysiske og logiske domenet.[2] Nkom's EkomCERT er sektorens responsmiljø og er en operativ enhet med kontaktflater nasjonalt og internasjonalt. Nkom deltar også i sentrale beredskapsforumer med sin koordineringsfunksjon innad i egen sektor og mot andre sektorer.[3]

Ekomtilbydere

En tilbyder er etter ekomlovens § 1-5 definert som «*enhver fysisk eller juridisk person som tilbyr andre tilgang til elektroniske kommunikasjonsnett eller -tjeneste*». Ekomtilbyderne er jf. ekomlovens §2-10 ansvarlige for å tilby brukerne elektroniske kommunikasjonsnett og -tjenester med forsvarlig sikkerhet i fred, krise og krig. Herunder skal nødvendig beredskap opprettholdes og viktige samfunnsfunksjoner prioriteres etter behov. Tilbyder skal også formidle viktige meldinger fra statsmyndigheten.

2. Elektroniske kommunikasjonsnetts generelle oppbygning

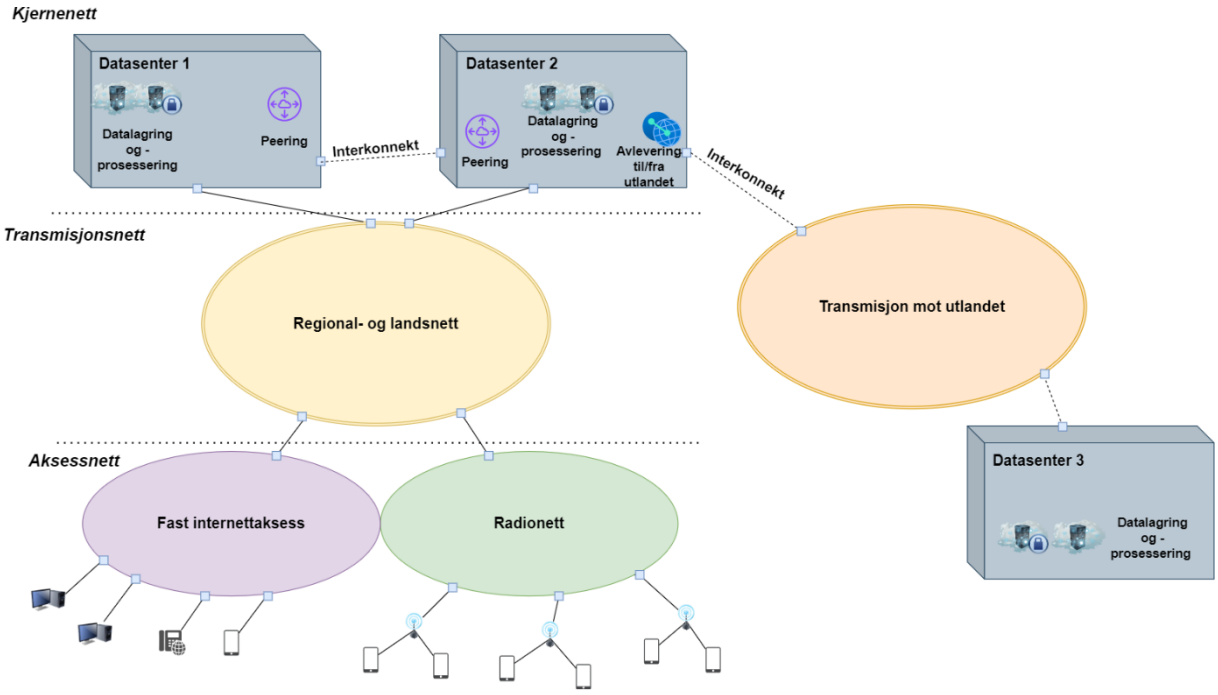
Elektroniske kommunikasjonsnett (ekomnett) er system for formidling av informasjon som muliggjør overføring av lyd, tekst, bilder eller andre data ved hjelp av elektromagnetiske signaler. Med elektronisk kommunikasjonstjeneste menes en tjeneste som helt eller i det vesentlige omfatter formidling av signaler i elektronisk kommunikasjonsnett og som normalt ytes mot vederlag.[4]

Høykapasitets fiberkabler er den vanligste teknikken brukt for å frakte de elektromagnetiske signalene over lengre avstander. Fastnett, mobilnett og andre typer ekomnett er ofte avhengig av den samme underliggende («backbone») infrastrukturen. I en del tilfeller brukes også radiolinjer for å overføre elektromagnetiske signaler, eksempelvis der det er vanskelig eller lite kostnadseffektivt å legge fiberkabler.

---

[1] *Om Kommunal- og distriktsdepartementet - regjeringen.no*
[2] *Kva gjer Nkom - Nkom*
[3] *NOU 2023: 17 - regjeringen.no*
[4] *Lov om elektronisk kommunikasjon (ekomloven) § 1-5, punkt. 3*

Ekomnett er sammensatt av flere tjenestelag som omfatter både fysiske og logiske elementer. Sammen muliggjør lagene tjenesteleveranse til sluttbruker.[5]



Figur 1: Forenklet nettverksstruktur for elektronisk kommunikasjon – Kjernenett, transportnett og aksessnett (basestasjoner)

Ekomnettenes struktur er kompleks, og det vil være variasjon i nettstrukturen i mobil- og fastnettene til ekomtilbyderne, samt i underliggende transmisjonsnett.

I figur 1 vises en forenklet fremstilling av nettverksstrukturen i ekomnett. I det aktuelle tilfellet er både fast internettaksess og radionett realisert på samme underliggende transmisjonsnett (regional- og landsnett). Transmisjonsnettene består som hovedregel av høykapasitets fiberkabler.

> **Kjernenettet –**betegnes som de mest sentrale deler av ekomnettene – som er nødvendig for logisk tjenesteproduksjon og styring av nettene.
> **Transmisjonsnett** er "motorveien" i ekomnettene som frakter ekomtrafikk over lengre avstander og består av fiberkabler. Transportnettene består av landsnett, regionnett og lokalnett, og er det som kobler kjernenettene til aksessnettene (radionett og fast internettaksess)
> **Aksessnettet** er punktet der brukerne tilslutter seg ekomnettene og får levert tjenester.

Ekomtjenester kan kjøpes og omsettes både på det fysiske og de logiske nettverkslagene. For å realisere transportnett kjøpes og selges tjenester som blant annet mørk fiber, optisk kapasitet/bølgelengde, og/eller IP-VPN. På mørk fiber setter kjøper på lyssettingsutstyr selv, mens ved optisk kapasitet settes lyssettingsutstyr på av selger. Dersom kjøper kun ønsker et logisk adskilt nett med tilhørende forbindelser, for eksempel et bedriftsnett, kan SD-WAN og IP-VPN[6] kjøpes som tjenester fra en ekomtilbyder.

---

[5] *For mer om dette henvises det til referansemodellen OSI.*
[6] *Henholdsvis Software-Defined Wide Area Network og Internet Protocol-Virtual Private Network.*

3. Den sikkerhetspolitiske situasjon

Den sikkerhetspolitiske situasjonen har endret seg betydelig de siste to årene og påvirker også ekomsektoren.

Figur 2. De hemmelige tjenesters ugraderte vurderinger

3.1 Etterretningstrusselen

Etterretningstjenesten skriver i sin åpne sikkerhetsvurdering, Fokus 2024, at Russland er en mindre forutsigbar nabo grunnet reduksjonen i diplomatiske møtepunkter mellom Russland og Vesten etter krigen i Ukraina. Tilgang til informasjon om vestlige og norske forhold avhenger mer av russiske etterretnings- og sikkerhetstjenester enn før. Etterretningsaktiviteten skjer både i det fysiske og digitale rom. Ifølge Etterretningstjenesten søker russiske aktører aktivt etter informasjon vedrørende norsk politikk, energi, nordområdene, alliert aktivitet og forsvar.

Videre skriver Etterretningstjenesten at kinesisk etterretningsaktivitet mot Vesten i hovedsak foregår i cyberdomenet for innhenting av informasjon. Interesseområder er politisk etterretning og industrispionasje. Kinesisk lovgivning forplikter kinesiske virksomheter og enkeltpersoner om å bistå Kinas etterretnings- og sikkerhetstjeneste.

Nasjonal sikkerhetsmyndighet (NSM) skriver i sin åpne trusselvurdering *Risiko 2024* at droner kan benyttes til både etterretning, sabotasje og terrorvirksomhet. Krigen i Ukraina har belyst hvordan kommersielt tilgjengelige droner kan brukes til etterretning og at de med enkelhet kan modifiseres til å bli angrepsdroner.

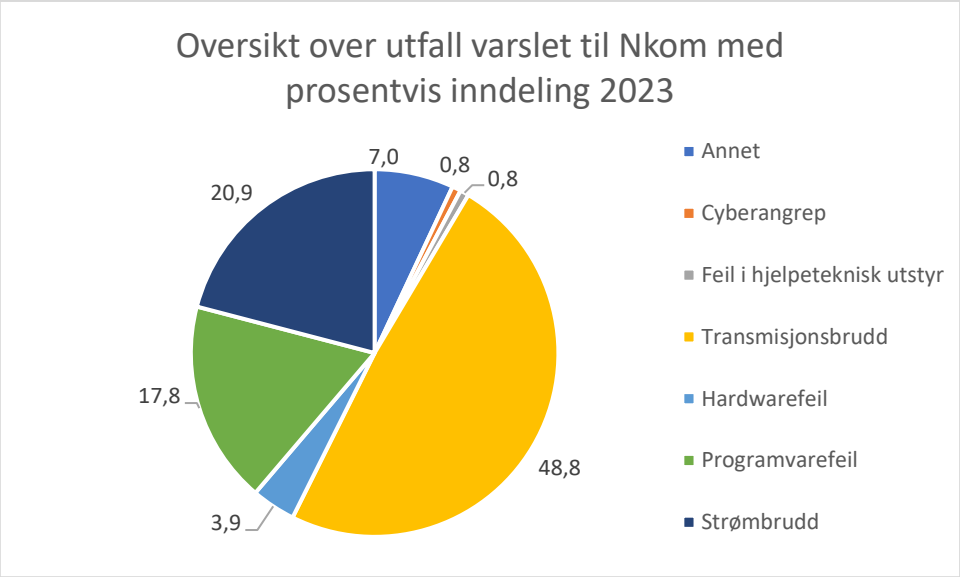
Kartlegging av ekominfrastruktur vil trolig være sentralt for å få tilgang til eller påføre skade på infrastrukturen ettersom ekom er en samfunnskritisk infrastruktur og tjeneste. Ekom understøtter i tillegg andre samfunnskritiske tjenester. Ekomsektoren vil derfor være et mulig mål for kartlegging og etterretningsoperasjoner fra andre nasjoners sikkerhetstjenester.

4. Kjente farer, trusler og sårbarheter i ekomsektoren

Gjennom regionale analyser, varslinger til Nkom, oppfølging av hendelser og gjennomførte tilsyn har Nkom god oversikt over kjente farer, trusler og sårbarheter innen ekomsektoren

4.1 Overordnet risikobilde og utviklingstrekk

Naturhendelser, er sammen med graving, to av de hyppigste årsakene til utfall av ekomtjenester på fastlandet i Norge. Skader i forbindelse med storm, kraftig nedbør og skred er relativt ofte grunnen til utfall av ekom. Andre årsaker til utfall kan være feil i forbindelse med planlagt arbeid i ekomnettene, kantslått, brann, utstyrsfeil og programvarefeil. Av innrapporterte hendelser til Nkom de siste årene er transmisjonsbrudd og tap av strømforsyning noen av de vanligste feilårsakene. De innrapporterte hendelsene omfatter kun større hendelser som er rapportert til Nkom. Oversikten inkluderer dermed ikke samtlige utfall i sektoren, og representerer derfor kun et overordnet bilde av utfall av ekomtjenester.

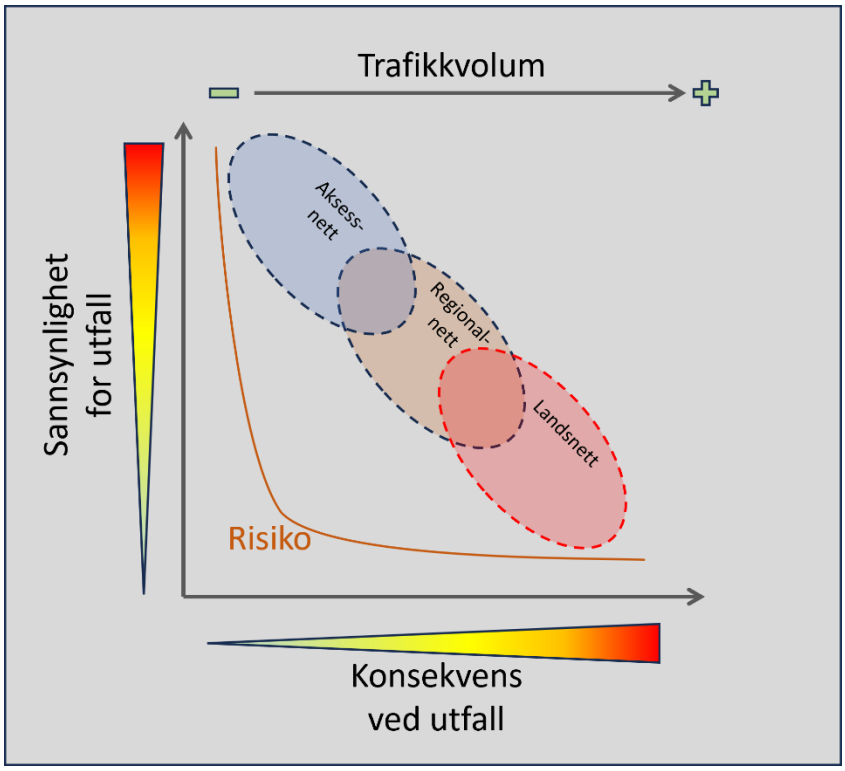


Figur 3: Fordeling av årsak til utfall som ekomtilbydere har varslet om til Nkom i 2023

Figur 2 viser at den viktigste årsaken til utfall av ekom er transmisjonsbrudd. Transmisjonsbrudd og strømbrudd står for ca. to tredjedeler av utfallene i tilbydernes ekomnett. Konsekvensene av transmisjonsbrudd og bortfall av strøm varierer, men de fleste utfall av ekomtjenester får gjerne kun lokale eller regionale konsekvenser.

Programvarefeil står for noen av de mer omfattende utfallene. Dette er feil som ikke har geografisk begrensning og kan være landsdekkende. De mest alvorlige programvarefeilene som Nkom har registrert er knyttet til planlagt arbeid i nettene. Mindre lokale utfall av f. eks. enkelt mobilbasestasjoner på grunn av strømbrudd er vanlig og rapporteres normalt ikke til Nkom.

I figuren under gis en grafisk illustrasjon av risikoen for utfall i de ulike delene av ekomnettene, her vist ved sannsynlighet for, og konsekvensen av, de ulike uønskede hendelser i ekomnettene. Figuren illustrerer også hvordan trafikkvolumet øker fra aksessnettene og inn mot transportnettene. I tråd med dette er konsekvensene ofte større ved utfall i regional- og landsnett (transportnett) enn ved utfall i aksessnett. Til gjengjeld er sannsynligheten lavere for utfall i transportnettene, grunnet høyere robusthet, som blant annet skyldes annerledes nettverkstopologi og flere risikoreduserende tiltak.



Figur 4: Risiko for utfall i ulike ekomnett

4.2 Fysisk sabotasje

Etterretningstjenesten skriver i sin åpne trusselvurdering *Fokus 2024* at det forutsettes at Russland har kartlagt norsk olje- og gassinfrastruktur over flere år. Russland har en betydelig kapasitet til å true norsk og vestlig kritisk undervannsinfrastruktur. Videre fremheves sjøfiberkabler og infrastruktur tilknyttet europeiske havner som et område Russland har kartlagt og vist vilje og evne til å ramme i en konfliktsituasjon. I større havner blir logistikk og ekom sammensmeltet, og det kan gjøre forsyningskjeden mer utsatt dersom disse skulle bli rammet.

Flere sjøfiberkabler har blitt skadet som følge av menneskelig aktivitet de siste årene. Eksempelvis ble Svalbardfiberen sannsynligvis utsatt for skader gjennom tråling.[7] Houthiene senket et skip utenfor kysten av Yemen, hvor skipets anker trolig ødela tre sjøfiberkabler da det sank i Rødehavet.[8] Frakteskipet New New Polar Bear seilte med skipsankeret ute og ødela både en gassrørledning[9] og sjøfiberkabel syd for Finland. Konsekvensen av skadene som oppstår er i stor grad den samme om handlingen er tilsiktet eller ei; trafikken må rutes om på andre veier og feilretting iverksettes. Det kan være utfordrende ved hendelser i internasjonalt farvann, eller når sivile aktører er involvert, å avdekke om det har vært en tilsiktet handling.

Eksemplene på hendelser beskrevet over er ikke nødvendigvis tilsiktede handlinger fra en stat, men viser at infrastruktur på havbunnen er sårbar for menneskelig aktivitet. Ca. to tredjedeler av sjøkabelbrudd i verden skjer grunnet menneskelig aktivitet som fiske og ankring.[10]

[7] *NRK Troms og Finnmark 2024-05-26*
[8] *CBS News 2024-03-06*
[9] *Reuters 2023-10-24*
[10] *ICPC mars 2021*

Norge har sjøkabelforbindelser til flere land. Dette er Sverige, Danmark, Storbritannia, Irland og USA. Fra fastlandet er det også forbindelser til olje og gassproduksjonen på norsk sokkel samt at det er sjøkabler som forbinder fastlandet til Svalbard. Disse kablene er sentrale for kommunikasjon og utveksling av informasjon for myndigheter og private virksomheter. Rettetiden på sjøfiberkabler er lang sammenlignet med kabler på land på grunn av forhold som logistikk, værforhold, dybder og lite tilgjengelig rettekapasitet.

NATO allierte uttrykker bekymring over Russlands hybride virkemiddelbruk og at den truer alliert sikkerhet.[11] NATO tekker frem de baltiske landene, Tsjekkia, Polen og Storbritannia, og viser til sabotasje, vold, cyber, elektronisk interferens, desinformasjon og andre virkemidler.

Nkom mottar jevnlig rapportering om hærverk og innbrudd i ekominfrastruktur. I hovedsak er det knyttet til hærverk og innbrudd i mindre viktige lokasjoner hvor motiv fremstår uklart. I 2024 er det observert sabotasje mot kabler i ulike deler av landet som f. eks, jammetest 2024, fiberkabel til Evenes flyplass og til et steinbrudd i Rogaland.

Under OL i Paris i 2024 opplevde franske ekomtilbydere at fiberkabler ble kuttet i en tilsynelatende koordinert sabotasjeaksjon. Det franske togselskapet SNCF ble også rammet av driftsforstyrrelse som følge av sabotasjeaksjoner. Aksjonene ble ansett som et angrep på de olympiske leker.[12] Tyskland har også opplevd kutting av kabler i jernbanenettet.[13] Disse aksjonene viser at det finnes grupperinger som bruker ødeleggelse av fiberinfrastruktur som virkemiddel. Det er noe både norske og internasjonale ekomtilbydere bør inkludere i sine risiko- og sårbarhetsanalyser.

4.3 Personellsikkerhet og innsidetrusler

Siden fullskalainvasjonen av Ukraina i 2022 er flere europeiske borgere blitt pågrepet og tiltalt for etterretningsaktivitet på vegne av russiske etterretningstjenester. Noen av dem hadde utført aktiviteter på grunn av press mot dem og deres familie, men for de fleste involverte var økonomiske insentiver som var motivet. Personer med familiær eller annen nær tilknytning til Russland, vil være særlig sårbare for rekrutteringsforsøk.

Politiets sikkerhetstjeneste (PST) skriver at kinesiske etterretningstjenester rekrutterer norske borgere for å få tilgang til sensitiv og gradert informasjon. Dette skal ofte være personer som har tilknytning til Kina i form av studier, arbeid, venner eller familie.[14] NSM skriver i *Risiko 2024* at det er avdekket flere innsidere i europeiske land med høy sikkerhetsklarering og tilgang til svært sensitiv informasjon. Det vil ifølge NSM være naivt å tro at det ikke finnes innsidere i betrodde stillinger også i Norge. Tilbyderne i ekomsektoren er bevisste på den potensielle innsidetrusselen, og samtidig erkjenner at det er en trussel som er krevende å sikre seg mot.

Funn fra Nkoms tilsynsarbeid de siste årene viser at det er rom for forbedringer hos flere tilbydere på personellsikkerhet. Det er observert mangelfull tilgangs- og adgangsstyring, fellesbrukere i sentrale systemer, manglende sporing av aktivitet i programmer og manglende sikkerhetsrevisjoner av tilgangslister og logger.

Ekomsektoren har også avhengigheter til utenlandsk personell med teknisk kompetanse. Dette kan være utfordrende ved feilretting på lokasjoner og systemer som krever sikkerhetsklarering eller adgangsklarering. Erfaringer viser at det tar lang tid å klarere utenlandsk personell og dette skaper

---

[11] NATO pressemelding 2. mai 2024
12 Oppdatering nr. 4-2024 – Varsling av hendelser til myndigheter. Ugradert situasjonsrapport fra Nkom.
13 telenors_sikkerhetsrapport-compressed.pdf
[14] PST, Nasjonal trusselvurdering 2024

utfordringer for tilbydere ved implementering av ny teknologi, oppgraderinger og infrastruktur. Ekomsektoren er i stor grad avhengig av utenlandske leverandører og ansatte for å levere sine tjenester og lange klareringsprosesser representerer en betydelig sikkerhetsutfordring.

4.4 Verdi- og leverandørkjeder

Flere hendelser de siste årene har vist at verdi- og leverandørkjeder er utsatt for endringer og påvirkning utenfor norsk kontroll, dette være seg pandemi, konflikt, krig og sanksjoner. Logiske og fysiske tjenester og infrastruktur tjenesteutsettes i økende grad, som kan påvirke risikobildet og graden av kontroll tilbyderne har over nett og tjenester.

4.4.1 Kompleksitet i verdikjeder og eierskapsstrukturer

Covid-19 pandemien og grunnstøtingen av fraktskipet fra Evergreen i Suezkanalen i 2021 illustrerer hvor sårbart samfunnet har blitt for forstyrrelser i logistikk og leveranser. Sanksjonene mot Russland har belyst utfordringene ved å ha store avhengigheter til leverandører i land som Norge ikke har sikkerhetssamarbeid med. Selv om ekomnett og –tjenester har klart seg godt ved disse hendelsene, viser det også hvor sårbart samfunnet er overfor forstyrrelser i forsyningssikkerhet. Sårbarheter i forsynings- og verdikjeder fremheves også som en utfordring i Totalberedskapskommisjonens rapport.[15]

Næringslivet er blitt en viktigere del av både totalforsvaret og beredskapsapparatet da infrastruktur, varer og tjenester ofte er i privat eierskap. Elektronisk kommunikasjon er intet unntak. Strategiske oppkjøp av virksomheter fra land som Norge ikke har sikkerhetspolitisk samarbeid med, kan være en metode for å innhente informasjon. Etterretningstjenesten skriver blant annet om kinesiske oppkjøp og investeringer i vestlig mikrobrikketeknologi og datasentre, dette for å bøte på Kinas utfordringer i teknologirivaliseringen med Vesten.[16]

Høy grad av spesialisering, koblet med et stort kapitalbehov, inklusive valg av proprietære løsninger kan føre til at det er forholdsvis få leverandører av kritiske systemer, tjenester og utstyr som understøtter drift og tjenesteproduksjon. Sabotasje og/eller andre virkemidler mot verdi- og leverandørkjeder kan true tilbudet av programvare og fastvare. Et mulig risikomoment er også logiske sårbarheter og/eller feil i programvare som kan påvirke flere tilbydere i sektoren.

4.4.2 Tilgang til teknisk kompetanse

Tilgang til personell med riktig kompetanse er en kritisk innsatsfaktor for ekomsektoren. Utviklingstrekk i samfunnet tyder på at det innen få år vil være mangel på kompetent arbeidskraft på tekniske fagområder. Det blir rapportert om tilsvarende utfordringer internasjonalt.

Ekomtilbyderne opplyser at det tas grep for å rekruttere kompetent personell. Eksempel på dette er rekruttering av studenter fra universitet til deltidsjobber, og å tilby ansettelse ved endt utdannelse. Per i dag er ekomsektoren avhengig av tilgang til utenlandsk personell for å dekke behovet for nødvendig teknisk kompetanse. Flere tilbydere informerer om utfordringer tilknyttet ansettelse og å beholde kvalifisert personell innen tekniske fagområder. Under Covid-19 var det også utfordringer knyttet til forflytting av personell med teknisk kompetanse over landegrenser, som følge av nedstengte grenseoverganger.

Ekomtilbydere og datasenteroperatører understøtter direkte og indirekte flere grunnleggende nasjonale funksjoner, og flere virksomheter er og kan bli underlagt sikkerhetsloven. I visse tilfeller må

[15] *NOU 2023:17 «Nå er det alvor – Rustet for en usikker fremtid».*
[16] *Fokus 2024*

personell med kritisk kompetanse hentes fra utlandet, og det kan som beskrevet tidligere oppstå utfordringer med sikkerhetsklarering av personellet.

4.4.3 Tilgang til komponenter og reservedeler

Den teknologiske utviklingen går raskt og utstyr fornyes stadig. Det kan i enkelte tilfeller når eldre utstyr benyttes være utfordrende å få tak i eldre reservedeler dersom tilbyderne ikke har dette på eget lager. Enkelte tilbydere har inngått samarbeid med andre aktører som benytter seg av utstyr tilsvarende det virksomhetene selv benytter. Slike ordninger medvirker til å avhjelpe på tilgjengeligheten på reservedeler.

Leveransen av komponenter for elektronisk utstyr, som halvledere, vurderes som utsatt. Taiwan står for produksjon av omkring 60% av verdens halvledere, og en svært stor andel av de aller mest avanserte halvlederne.[17] Ifølge World Economic Forum er Taiwan ett av områdene sammen med Midtøsten og Ukraina hvor det pågår eller er potensiale for konflikter som kan påvirke leverandørkjeder.[18] Just in time - prinsippet utfordres når det forekommer hendelser i de globale verdi- og leveransekjedene.

Sterk avhengighet til en eller få leverandører av viktige komponenter kan øke sårbarheten for forstyrrelser i verdi- og leveransekjeder. Den geopolitiske situasjonen i for eksempel Øst-Europa, Sør-Øst-Asia og Midtøsten kan få konsekvenser for tilgang til reservedeler og samtidig betraktelig øke leveringstider. Det er derfor viktig å sørge for et riktig nivå av reservedeler, og planlegge tilstrekkelig langt frem i tid for å opprettholde forsvarlig sikkerhet og fungerende tjenester. Der det lar seg gjøre kan sentrale og desentraliserte reservedelslager og avtaler om prioritet med underleverandører være hensiktsmessig for å redusere leveringstiden og eksterne sårbarheter i enkelte deler av verdikjeden.

4.4.4 Verdikonsentrasjon

Samfunnskritiske funksjoner og virksomheter har en økende avhengighet til kommersielle datasentre. Dette gjelder også tilbyderne i ekomsektoren, som er til stede både i kommersielle datasentre og i samlokaliserte anlegg. Det oppstår dermed en verdikonsentrasjon på enkelte samlokaliserte anlegg. Det er samtidig en utfordring at man som ekomtilbyder ikke nødvendigvis vet hvem som har telelosji i samme lokale, eller hvilket personell som får tilgang til rommet. Slik verdikonsentrasjon behøver ikke være et problem, men det kan være en sårbarhet som det bør tas høyde for i vurderingen av hvordan utstyr skal innplasseres og sikres.

Flere ekomanlegg og datasentre er lokalisert i nærheten av hverandre. Datasentrene er viktige både for utveksling og transport av trafikk på tvers av ekomnett[19] og sektorer, samt for avlevering av trafikk til og fra utlandet. Datasentrene er også viktige for produksjon av skytjenester og kritisk samfunnstjenester.

Flere ekomtilbydere er avhengig av de samme utenlandske leverandørene av kritiske utstyr og programvare som benyttes i kjernenettet. Begrenset diversitet representerer en generell sårbarhet for sektoren og flere tilbydere vil dele de samme sårbarhetene.

---

[17] *The Economist (2023), Taiwan's dominance of the chip industry makes it more important.*

[18] *World Economic Forum (2024), The Global Risks Report 2024.*

[19] *Gjelder både privat samtrafikk, som er direkte utveksling av ekomtrafikk mellom to ekomnett, og offentlig samtrafikk, der ekomtrafikken går via et offentlig tilslutningspunkt.*

4.5 Naturhendelser

Naturhendelser er en kjent fare for ekom og det antas at forekomsten av ekstremvær vil øke i takt med klimaendringene. I dette delkapittelet settes det fokus på ekstremvær, brann og romvær.

4.5.1 Ekstremvær

Ekstremvær vil i stadig større grad føre til utfall av ekom i årene som kommer. Ifølge meteorologisk institutt kan vi forvente økende temperaturer og nedbør i hele landet gjennom hele året, og vi må være forberedt på flere episoder med kraftig styrtregn og sterk vind. Ekstremvær vil også kunne treffe områder som vi fra tidligere ikke er kjent med at har opplevd slik type uvær. Slike eksempler omfatter blant annet uværet i Innlandet i november 2021 og ekstremværet Hans i august 2023.

Regionale analyser av Trøndelag og Nordland påpeker sårbarheter i den digitale infrastrukturen og hvordan viktige deler av infrastrukturen går gjennom et begrenset geografisk område. Denne sårbarheten synliggjorde seg under ekstremværet Ingunn da det ble et dobbeltbrudd på to føringsveier nord for Bodø. Det medførte for eksempel at to av tre føringsveier for Helsenett var nede i Nord-Norge.[20]

På grunn av økende temperaturer vil det oftere komme perioder med kraftig nedbør, og det er korttidsnedbøren som øker mest. Intense nedbørsmengder og tung snø på kort tid skaper de største problemene, som for eksempel flom, overvann og oversvømmelser i byer. Dette vil også føre til skader på ekominfrastruktur.[21]

Ekominfrastruktur er sårbar for alle typer skred. Skred kan skade både nedgravde fiberkabler, fiberkabler som er trukket i luftspenn, og ødelegge basestasjoner og noderom lokalisert i rasområdet. I tillegg til å utgjøre en fare mot ekominfrastruktur, vil skred også utgjøre en fare mot personer og virksomheter som befinner seg i skredområdet. Dette kan medføre utfordringer i forbindelse med rettearbeid i skredsoner.

I august 2023 var det store nedbørsmengder i Innlandet og Viken i forbindelse med uværet Hans. Uværet traff et område av landet som historisk sett har hatt lavere forekomst av store nedbørsmengder enn andre deler av landet. Uværet førte til store oversvømmelser og ras på flere steder. Hallingdal ble hardt rammet, hvor Ål og Nesbyen til tider var isolert på grunn av vannmasser og skred, og det forekom lokale ekomutfall. Rettemannskaper hadde store utfordringer med å komme frem grunnet stengte veier.

Sterke vindkast kan føre til både strøm- og fiberbrudd. Langvarige strømbrudd kan føre til ekomutfall på de lokasjonene som ikke har tilstrekkelig reservestrømkapasitet. De vanligste årsakene til langvarige strømbrudd er trefall over strømlinjer og at strømmaster velter i uvær. Fiberstrekk som er spunnet rundt høyspentlinjer er utsatt på lik linje som strømlinjer.

4.5.2 Brann

Skogbrann og brann i sentraler og anlegg kan forårsake ekomutfall, men slike tilfeller forekommer relativt sjeldent. Skogbranner i Norge har historisk sett vært relativt små. Skogbrannfaren er likevel stor i varmere perioder, og flere europeiske land har opplevd svært store skogbranner de siste årene, blant annet Sverige sommeren 2018. Norge opplevde også flere skogbranner dette året. Brann i sentraler og anlegg i ekominfrastrukturen kan forekomme, men dette er svært sjeldent og ekomtilbyderne er pålagt en rekke krav til brannsikring. I storbrannen i Lærdal i 2018 brant imidlertid en av Telenors sentraler, som var et knutepunkt for mobil, fasttelefon og bredbånd og videre kommunikasjon til andre basestasjoner i området. Omfanget på brannen og varmeutviklingen skapte

[20] *https://status.nhn.no/incidents/nzww2ky8rg5l*
[21] *Meteorologisk institutt https://www.met.no/vaer-og-klima/det-blir-vatere*

forsinkelser med rettearbeidet. Det tok i underkant av to dager å opprette midlertidig dekning i området ved hjelp av flyttbare basestasjoner og aggregat.

4.5.3 Romvær

Romvær er en betegnelse på ekstreme forhold i verdensrommet som kan forårsake store skader på kommunikasjonssystemer som går i bane rundt jorden. Det kan blant annet føre til store elektromagnetiske forstyrrelser i atmosfæren. Solstormer kan slå ut kommunikasjonssystemer på jorden, påvirke satellittsystemer og kraftnett. Solstorm-aktiviteten går statistisk sett i en syklus på en periode på ca. elleve år. På toppen av denne syklusen forekommer solstormer i gjennomsnitt hyppigere og sterkere, men store enkelthendelser har forekommet i perioder med lav aktivitet. Nytt maksimumsnivå er estimert å være juli 2025.[22] I 1989 traff en solstorm jorden og lammet blant annet krafttilførselen i Quebec i Canada.

4.6 Planlagt arbeid i nettet

Programvare og utstyr oppgraderes, oppdateres eller byttes ut med jevne mellomrom. Tidvis oppstår det feil i forbindelse med planlagt arbeid som resulterer i redusert tjenestetilgjengelighet til kundene.

Felles for programvareoppgraderinger og -endringer i kjernenett til mobilnett og fastnett er at konsekvenspotensialet ved feilkonfigurering og feiltilstander ofte er stort. Gjensidige avhengigheter og tett kobling mellom noder og delsystemer medfører at feil fort kan propagere til større deler av ekomnettene. Risiko kan eksempelvis være knyttet til databaser som speiles på flere noder i mobilnett, samt konfigurering av ruting som sørger for at IP-trafikk adresseres til og termineres på riktig destinasjon.

EUs cybersikkerhetsbyrås (ENISAs) årsrapport fra 2022[23] viser at feilslåtte oppgraderinger/endringer i programvare i forbindelse med planlagt arbeid har vært den viktigste årsaken til store og langvarige utfall i ekomnettene i medlemslandene. Disse hendelsene, som utgjorde 12 % av hendelsene i 2022, sto for 8634 millioner tapte brukertimer i EU/EØS. Nkom registrerer samme tendens i Norge: de største utfallene forårsakes ofte av feilslåtte oppgraderinger eller endringer i programvare og fastvare i kjernenettene.

4.7 Satellitt

Det er en økende bruk og avhengighet til satellittbaserte systemer, og systemene integreres stadig tettere med bakkebaserte kommunikasjonssystemer. Vi omtaler her farer, trusler og sårbarheter innen satellittbasert kommunikasjon og forstyrrelser av GNSS.

4.7.1 Satellittbasert kommunikasjon

European Space Policy Institute (ESPI) viser i sin rapport[24] at ved Russland fullskalainvasjon av Ukraina, gjennomførte Russland et cyberangrep mot Viasats KA-SAT satellitt nettverk som blant annet ble brukt av den ukrainske hæren. Først ble det utført DDoS angrep mot internettmodemer lokalisert i Ukraina som ble brukt av den ukrainske regjeringen, hæren og sikkerhetstjenester. Dette hindret modemene å fungere normalt. Deretter utnyttet angriperne seg av en miskonfigurert VPN som gjorde det mulig for angriper å få fjernaksess til styringssegmentet til Viasats KA-SAT nettverk.

---

[22] *National Oceanic and Atmospheric Administration – www.weather.gov/news/201509-solar-cycle*
[23] *Telecom Security Incidents 2022 – Annual Report*
[24] *ESPI Report 84 - The war in Ukraine from a space cybersecurity perspective*

Videre penetrerte angriperne seg dypere inn i nettverket og oppsøkte et spesifikt segment som brukes til å styre og operere nettverket. Gjennom dette kunne angriperne nå få kontroll over styringssegmentet og iverksette kommandoer som lastet opp wiper skadevare på brukeres modemer. Skadevaren slettet harddisker på KA-SATs internetmodemer og koblet dem dermed ut fra KA-SAT nettverket. Tusenvis av brukere i Ukraina ble rammet. Flere titusener av andre satellitt bredbåndstjenester ble også rammet, blant annet K2-systemet for 5800 vindturbiner i Tyskland og 2000 abonnenter i Norge. Eksempelet viser at det er mulig å gjennomføre storstilte logiske angrep mot satellittbaserte kommunikasjonssystemer.

Satellittbaserte kommunikasjonssystemer har flere sårbarheter og mulige angrepsflater. Dette inkluderer klassiske cyberangrep som man finner i tradisjonelle IT-systemer, gjerne målrettet mot bruker og kontrollsegmenter. Det er også mulig med angrep som fokuserer på satellitter i rommet.

Totalberedskapskommisjonens nylige rapport[25] peker på konsekvenser ved bortfall av satellittbaserte tjenester:

«Bortfall av satellittbaserte tjenester vil føre til konsekvenser for en rekke kritiske samfunnsfunksjoner. Dette gjelder for eksempel Forsvaret, nødetatene, den offentlig organiserte redningstjenesten, meteorologiske tjenester, finanssektoren, kraftsektoren og transportnæringen.»

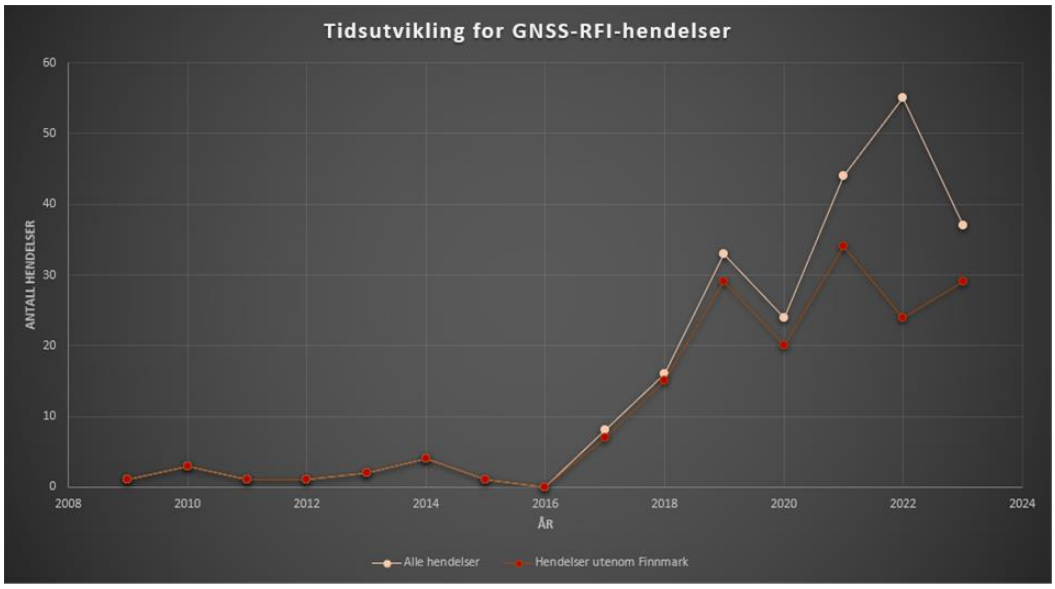
4.7.2 GNSS

Forstyrrelser som hindrer mottak av Global Navigation Satellite System (GNSS – satellittbaserte navigasjonssystemer) har økt de senere årene. Både tilsiktet og utilsiktet forstyrrelser kan få de samme konsekvensene. GNSS-satellitt-signaler er svake signaler, og dermed mer utsatt for både utilsiktete og tilsiktede forstyrrelser, sammenlignet med andre bakkebaserte radiokommunikasjonssystemer.

Forstyrrelsene er blitt et globalt problem ettersom GNSS-systemer i dag benyttes overalt i samfunnet. GNSS-mottakere er en innvevd teknologi i dagens mobiltelefoner, IoT enheter, styringssystemer for industrien, finans, maritim trafikk, vei og lufttrafikk. I tillegg til posisjonsbestemmelse er GNSS-systemer også viktig for korrekt angivelse av tid, som er sentralt i mange elektroniske systemer. I 2021 antok en at det var omtrent 6.5 milliarder GNSS mottakere i bruk. Frem mot 2031 er det estimert å vokse til 10.6 milliarder GNSS-mottakere[26].

Figuren under viser at det har vært en betydelig økning i antall RFI[27] hendelser knyttet til GNSS som er innrapporter til Nkom. Den samme tendensen kan også sees i Eurocontroll sin oversikt over GNSS forstyrrelser.

[25] *NOU 2023: 17 – Nå er det alvor. Rustet for en usikker fremtid*
[26] *https://www.euspa.europa.eu/sites/default/files/uploads/euspa_market_report_2022.pdf*
[27] *RFI – Radiofrekvensinterferens*



Figur 5: GNSS hendelser innrapportert til Nkom.

Utilsiktet interferens er i all hovedsak knyttet til elektronikkprodukter som har en form for feiltilstand som resulterer i at de utstråler energi i frekvensbåndene der GNSS-systemene GPS, Galileo, GLONASS og BeiDou opererer. Klassiske eksempler er selvsvingfenomener fra mottakerne selv, LED-lyspærer og SMPS- strømforsyninger. Nkom har eksempelvis avdekket et ettermontert ryggekamera på bil som forstyrret GNSS.

Tilsiktet interferens har ved flere anledninger påvirket signaler i norsk luftrom. Eksempler som kan nevnes er russisk militær aktivitet ved Øst-Finnmark og små GNSS-jammere i lastebiler som forstyrrer navigasjonssystemer.

Figur 6: Enkel jammer for kjøretøy

I tillegg til den jammingen som man etter hvert har blitt kjent med, så har også GNSS-spoofing blitt et framtredende problem det siste året. Dette er narreangrep som har til hensikt å lure GNSS-mottakerne til å regne ut feil posisjon og/eller tid. Som Luftfartstilsynet skriver på sine nettsider[28], så har rapporter om spoofing økt enormt det siste året.

Blokkering av GNSS-signaler kan påføre store komplikasjoner avhengig av hva det brukes til og hvor avhengig systemet er av disse signalene. Konsekvensen er at GNSS ikke kan brukes, slik at det vil være umulig å bruke posisjonsdata til GPS og tidssynkronisering ved bruk av GNSS.

Jammetest 2024

Som et av tiltakene for å arbeide med å forsterke robustheten i systemer og teknologi som bruker GNSS, har Nkom vært med på å arrangere en testarena for GNSS-RFI. Denne kalles for Jammetest[29] og samler industri, forskningsmiljøer og myndigheter fra hele verden (i 2024 var det godt over 200 deltagere fra 20 land). Her testes kjente og ukjente GNSS-sårbarheter slik at sikkerhetshull som avdekkes kan lukkes. Verdifulle innsikter er:

[28] *https://luftfartstilsynet.no/om-oss/nyheter/nyheter-2024/gps-spoofing--en-okende-sikkerhetsutfordring/*
[29] *https://jammertest.no/*

- Av enheter som kan motta signaler fra flere GNSS-systemer[30] er det mange som bruker GPS for kontroll av de tre andre. Det er dermed mulig å lure multi-GNSS-systemer gjennom angrep på kun GPS.
- Det er på større systemer med kombinasjoner av ulike sensorer og teknologier vanskelig å forutse hvordan forstyrrelser vil påvirke systemet. Resultatet vil man først vite når systemet er testet.
- Overganger mellom å ikke være forstyrret til å bli forstyrret medfører noen ganger større feil enn forstyrrelser over lengre tid.
- Narreangrep mot tid kan forårsak feil på utstyr selv etter at angrepet er slutt. Det vil være behov for å tilbakestille til fabrikkinnstillinger, sikkerhetssertifikater må oppdateres og lisenser må fornyes.

Med den økende trusselen fra tilsiktet GNSS-spoofing, spesielt fra aktører med avanserte kapasiteter som Russland, kan det være kritisk at Norge og Nkom intensiverer innsatsen for å beskytte og styrke robustheten i GNSS-systemer for å sikre nasjonal sikkerhet og operasjonell pålitelighet.

4.8 Svindel

Svindel ved bruk av ekom har blitt et samfunnsproblem. Det totale svindeltapet hadde en økning på 51 prosent fra 2022 til 924 millioner kroner 2023. Den største økningen skjer ved svindel fokusert på kontooverføringer. Ved mange av svindeltilfellene blir spoofede telefonnummer [31]og/eller SMS med svindel-lenke brukt i kommunikasjon med offeret.

De siste årene er det anmeldt årlig over 20 000 bedragerier til politiet, og mørketallene antas å være store. Svindel har både økonomiske og psykologiske konsekvenser for fornærmede, i tillegg til at svindeltrykket kan utfordre tilliten til ekomtjenester.

Telenor Norge har meldt til Nkom at de blokkerte eller sensurerte 17,6 millioner svindelanrop i 2023. I tillegg blokkerte Telenor Linx 13,8 millioner anrop mot Norge. Telia meldte våren 2024 at de på to måneder hadde blokkert 20 millioner anrop fra utlandet.

Nkom etablerte i 2023 i partnerskap med Økokrim nasjonal ekspertgruppe mot ekomsvindel. Her deltar foruten Nkom og Økokrim, mobilnetteiere, Nasjonal referansedatabase og observatører fra NSM, FinansNorge, Næringslivets sikkerhetsråd og DigDir. Nkom har også vært sentral i etableringen av Global Informal Regulatory Antifraud Forum – GIRAF, som et ledd i det globale initiativet «Restore Trust».[32]

4.9 Cyberdomenet

Cyberdomenet er et område hvor trusselaktører kan kartlegge og gjennomføre angrep mot ekom nett og tjenester. Nkom har valgt å behandle dette som et eget risikoområde selv om det kan være en del av sikkerhetspolitiske hendelser, svindel, kriminalitet og hendelser mot satellittsystemer.

4.9.1 Politisk og teknologisk utvikling

Det foregår endringsprosesser i det globale politiske landskapet som har betydning for cyberdomenet. Kina har innført en etterretningslov som pålegger enkeltpersoner og virksomheter å

---

30 Det finnes fire forskjellige GNSS systemer i verden: GPS, Galileo, GLONASS og BeiDou

31 Spoofing er en teknikk for å kamuflere identiteten bak et f. eks. et legitimt eller trygt telefonnummer eller IP-adresse

32 Restore Trust in International Telecommunications – i3Forum

dele informasjon med kinesiske myndigheter. Slike lovendringer kan gi det kinesiske forsvaret og etterretningsapparatet mer handlingsrom til å utnytte nye angrepsflater, og dessuten øke andre staters sårbarhet for cyberangrep.

I cyberdomenet er det krevende å holde oversikt over trusselbildet, ettersom cyberangrep gjerne er udiskriminerende og ikke behøver være rettet mot et konkret selskap, sektor eller en stat. Digitaliseringen i samfunnet og utviklingen av nye generasjoner av arkitekturer og tjenester i ekomsektoren har muliggjort nye tjenester og gitt et løft i tjenestekvalitet. Samtidig har det ført med seg nye angrepsflater og sårbarheter, og angrep som tidligere bare har rammet andre sektorer rammer nå også ekomsektoren.

For at ekomtjenester skal fungere må grunnleggende funksjoner og systemer som understøtter ekomnettene være i drift. Disse er naturlige mål for cyberangrep, fordi bortfall av funksjonene kan føre til store problemer med tjenesteleveranse. Enkelte systemer og funksjoner er mer eksponert enn andre, blant annet systemer med direkte eksponering mot det åpne internettet, og systemer og nettverk som har manglende segmentering. Sårbarheter som utnyttes i cyberangrep finnes ofte i utstyrs og systemers firmware og software. Kontinuerlig oppdatering av firmware- og softwareversjoner er derfor et viktig risikoreduserende tiltak i cyberdomenet.

4.9.2 Trusselbilde og trender

Cyberangrep kan både være politisk og økonomisk motivert. Statlige aktører forsøker ofte å skjule sin sikkerhetstruende virksomhet i cyberdomenet ved hjelp av ulike virkemidler.[33] Dette medfører at det er vanskelig å attribuere angrep, og virksomheter og myndigheter må gå etter TTP-indikatorer[34] for å si noe om hvem som kan stå bak angrepene.

Tjenestenektangrep (DDoS) er en mye anvendt angrepstype, og utføres ofte når motivet er politisk innflytelse eller påvirkningskampanjer. Disse angrepene er forholdsvis enkle å gjennomføre sammenlignet med mer komplekse angrep der trusselaktører trenger seg inn i informasjonssystemer. Ved politisk motiverte tjenestenektangrep er symbolverdien vel så viktig som de faktiske konsekvensene. For eksempel kan en fremmed stat demonstrere at den har evne og kapasitet til å forårsake forstyrrelser i ekom- og IT-tjenester, uten å følge opp med mer alvorlige angrep.

Internasjonalt har det vokst frem et marked for kjøp og salg av verktøy som brukes i cyberangrep, dette kan være informasjon om nulldagssårbarheter, innloggingsinformasjon til ulike systemer og andre sårbarheter. Forskjellige typer cyberangrep, inkludert tjenestenektangrep, er nå tilgjengelig som tjenester i lukkede forum. Terskelen senkes dermed for hvem som kan utføre angrep og kompetansen som kreves. Cyberangrep tilbudt som en tjeneste kan også gjøre det vanskeligere å attribuere angrep til konkrete aktører.[35]

Ukraina-konflikten har ført til en oppblomstring i tilgangen til verktøy innen Hacktivist-nettverk. Verktøyene benyttes i logiske angrep og deling av verktøyene medfører at trusselaktører får en større ressurs- og kunnskapsbase å ta av. Det har imidlertid skjedd en skjerping av hva som tilgjengeliggjøres av slike verktøy.[36]

Bruk av kunstig intelligens kan også øke angriperes kapabiliteter, blant annet ved at man kan ramme flere mål med tilsvarende ressurser som tidligere. Et eksempel på dette kan være svært sofistikerte spearphishing-operasjoner som kan sendes ut i stort omfang. Slike masseutsendelser har hittil vært forbeholdt phishing-kampanjer som er relativt enkle å gjennomskue og dermed har hatt lav

---

[33] For eksempel ved å bruke «hactivister» eller andre ikke-statlige aktører som dekke for angrepene.
[34] Taktikk, teknikk og prosedyre, der de ulike formene knyttes til forskjellige trusselaktører.
35 Farlig trend: Hackere selger tilgang til enorme mengder stjålne, sensitive data via nettskytjenester | Digi.no
36 Ukraine war sparks revival of hacktivism (ft.com)

suksessrate. Masseutsendelser av spearphishing-kampanjer ved hjelp av kunstig intelligens kan derimot øke omfanget og treffsikkerheten betydelig. Brukerdata ervervet gjennom kommersiell digital sporing kan være et viktig kildegrunnlag for utvikling av svært troverdige og sofistikerte spearphishing-operasjoner.

4.9.3 Cybertrusler og ulike typer angrep mot ekomsektoren

Destruktive angrep innebærer at en trusselaktør trenger seg inn i systemer og infiserer dem med skadevare eller virus. Skadevare og virus kan ha ulike egenskaper, og kan innføres i systemer på ulike måter. Misbruk av VPN-løsninger av utro ansatte eller salg av innloggingsinformasjon til administrasjonssystemer er eksempler på hvordan uautorisert tilgang kan oppnås.

Skadevare fører typisk til at viktig konfigurasjon endres eller slettes i systemer, mens løsepengevirus fryser og låser inn systemer for å forhindre legitim tilgang. Effekten av disse to angrepsformene kan dermed være nokså lik, ettersom det vil kunne oppstå store forstyrrelser i tjenesteleveransen. Resultatet av destruktive angrep er dermed at grunnleggende funksjoner som er nødvendige for å holde tjenesteproduksjon i gang faller bort.

Til forskjell fra tjenestenektangrep som utføres fra «utsiden», gjennomføres destruktive angrep ofte av trusselaktører som har trengt seg inn i informasjonssystemer. Angrepene krever derfor større kapabiliteter og kompetanse enn tjenestenektangrep. Destruktive angrep kan også utføres gjennom kompromittering av brukerkontoer som har legitim tilgang, dette er observert ved flere tilfeller av løsepengevirus de siste årene. Dersom kompromitterte brukerkontoer attpåtil har utvidede administratorrettigheter og tilganger innenfor systemer, øker skadepotensialet. Ved mangel på sikkerhetstiltak som nettverkssegmentering og tilgangsstyring, øker risikoen for alvorlige angrep, med betydelige konsekvenser.

Tidlig i krigen i Ukraina ble det rapportert om tilfeller av BGP-kapring. Det vil si at trafikk som egentlig skal til en sluttbruker, rutes om og sendes til en ondsinnet aktør. Det har blitt innført tiltak som vanskeliggjør BGP-kapring etter hendelsene i 2022. Gode sikkerhetstiltak og oversikt over potensielle angrepsveier vil kunne gjøre at slike hendelser enten stoppes før de skjer eller stoppes etter kort tid.

En gruppering som støtter Russlands krigføring i Ukraina fremsatte sommeren 2024 trusler mot og gjennomførte tjenestenektangrep mot Nkom og flere norske ekomtilbydere. Truslene og angrepene var begrunnet med at regjeringen ville overføre seks F16 jagerfly til Ukraina og at norske myndigheter var russofobiske. Dette viser at Norges bidrag til forsvaret av Ukraina også gjør ekomsektoren til et mulig mål for angrep.

4.9.4 Skytjenester

Hurtig digitaliseringstakt i det norske samfunnet og ekomsektoren har ført til økt bruk av skybaserte tjenester. Stadig flere systemer baserer seg helt eller delvis på skybasert infrastruktur og tjenester levert av internasjonale skytjenesteleverandører. Infrastrukturen gir muligheter for raskt opp-/nedskalering av prosesserings- og lagringskapasitet, og er viktig for å understøtte digitaliseringen i samfunnet.

Tjenesteutsetting av datalagring og -prosessering kan medføre at skyleverandører, underleverandører og andre kunders risiko og sårbarheter også blir en del av ekomtilbyders risikobilde. Skytjenester realiseres ofte gjennom en lang leverandørkjede og lagvis oppbygning der blant annet styrings- og administrasjonssystemer ikke behøver være plassert i Norge. Sikkerhetsovervåking, herunder kontroll med hvem som har tilgang til og rettigheter innenfor systemene, kan være utfordrende dersom systemene driftes og administreres utenfor Norge.

5 De største utfordringene

Når Nkom skal vurdere hva som er de største sikkerhetsmessige utfordringene er det vanskelig å unngå bakteppet som den sikkerhetspolitiske situasjonen gir. Det er krig i Europa, spenninger i Sør-Kina havet og økende væpnet konflikt i Midt-Østen. En stadig raskere digitaliseringstakt og den sikkerhetspolitiske utviklingen øker gapet mellom dagens sikkerhetsnivå og samfunnets behov for sikre og robuste nett.

Det er særlig disse syv områdene som Nkom ønsker å fokusere på som sikkerhetsmessige utfordringer i årets EkomRos:

- Avhengigheter og konsentrasjon i verdi- og leverandørkjeder
- Cyberangrep
- Ekstremvær
- Feil forbindelse med planlagt arbeid
- Personellsikkerhet og innsidetrusselen
- Sabotasje
- Sjøfiberkabler

Avhengigheter og konsentrasjon i verdi- og leverandørkjeder

Nkom ser alvorlig på muligheten for at tilgangen til kritisk utstyr og utenlandsk arbeidskraft kan bli vesentlig redusert på grunn av forverring av den sikkerhetspolitiske situasjonen i verden. Handel og produksjon av strategisk ressurser blir i økende grad brukt som pressmiddel i rivaliseringen mellom stater. Det tar lang tid å sikkerhetsklarere utenlandsk arbeidskraft og det representerer en betydelig sikkerhetsutfordring for norske ekomtilbydere underlagt sikkerhetsloven.

Flere norske ekomtilbydere benytter de samme leverandørene for sentralt utstyr og programvare. Sårbarheter i dette utstyret og programvaren vil dermed deles av store deler av sektoren. En ondsinnet aktør som har informasjon om skjulte sårbarheter i det aktuelle utstyret eller programvaren kan dermed volde stor skade hos flere virksomheter samtidig.

Feil forbindelse med planlagt arbeid

Over flere år har Nkom observert at utfallene med størst konsekvens ofte skyldes feil i forbindelse med planlagt arbeid. Programvarefeil har ofte et stort konsekvenspotensial, spesielt hvis de forekommer i sentrale styrings- og tjenesteproduksjonssystemer. som kunder i hele landet er avhengig av for å få levert tjenester. Nkom gjennomfører hvert år flere tilsyn med tilbydere etter feil i forbindelse med planlagt arbeid, og funn fra tilsynene tilsier at manglende risikovurderinger i forbindelse med planlagt arbeid er noe som går igjen. Nkom er bekymret for manglende risikovurderinger i forkant og underveis i planlagt arbeid vil medføre større ekomutfall en hva som er nødvendig i Norge.

Sjøfiberkabler

Det å angripe undervannskommunikasjonslinjer i krig har blitt gjennomført siden 1898.[37] Sjøfiberkabler representerer «low-cost, high-impact» mål i en militær operasjon da det å ta ut kommunikasjonslinjer kan betydelig svekke den som blir angrepet. Fraværet av flere redundante føringsveier for visse områder gjør at områdene mer utsatte grunnet manglende føringsveier. I Norge

[37] *Den Spansk-Amerikanske krig – USA kuttet sjøkabler mellom Spania, Cuba og Filippinene.*

er særlig Svalbard utsatt på grunn avhengighet til svalbardfiberen, utfordrende rettemuligheter og manglende alternativer.

Uønskede hendelser knyttet til sjøfiberkabler vil også skje fremover slik vi har sett de siste årene. Basert på tilgjengelig statistikk er sannsynligheten størst for at utilsiktede handlinger vil skje. Nkom er bekymret for at tilsiktede handlinger mot infrastrukturen kan skjules som uhell slik at attribusjon mot en spesifikk aktør blir vanskelig.

Ekstremvær

I årene som kommer vil ekstremvær føre til utfall av ekomnett og tjenester. Ekstremværet Hans (2023) er et eksempel hvor store nedbørsmengder og skred medførte fiberbrudd og utfall av ekom i flere områder. I uke 5 2024 ble Møre og Romsdal, Trøndelag, Nordland, Troms og Finnmark truffet av flere stormer og spesielt ekstremværet Ingunn førte til utfall av ekom. Hovedårsaken til utfall av ekom var tap av ekstern strømforsyning og fiberbrudd. Områder som tidligere ikke har vært rammet av ekstremvær i større grad vil i fremtiden kunne oppleve mer av dette.

Cyberangrep

Cyberangrep er en kontinuerlig trussel mot ekomnett og -tjenester. Angrepene kommer i mange varianter, og de alvorligste variantene kan få store konsekvenser for leveransen av ekomtjenester, som for eksempel observert i Ukraina. Vanskeligheter med å attribuere handlinger og manglende sanksjonsmuligheter kan senke terskelen for å gjennomføre angrep i cyberdomenet.

Trusselbildet i cyberdomenet påvirkes i stor grad av geopolitisk og teknologisk utvikling, og teknologiske nyvinninger kan både føre med seg nye sårbarheter og bidra til økt sikkerhet i løsninger. Bruk av skybasert infrastruktur og tjenester er eksempler på dette, og fordrer god oversikt over sikkerheten i løsningene og bevissthet rundt hva man har kontroll over. Herunder hvor servere og viktige delsystemer som understøtter drift og administrasjon er plassert, hvem som har fysisk og logisk tilgang, og hvordan uønskede hendelser håndteres. I mange tilfeller kan økt tjenesteutsetting også bety at man gir fra seg kontroll over deler av verdikjeden.

Fremmede stater og trusselaktører kan ha kjennskap til bakdører og sikkerhetshull i viktig programvare og fastvare som kan bli utnyttet på strategiske tidspunkt. Innsidere kan også lette gjennomføringen av logiske angrep, for eksempel ved at påloggingsinformasjon til viktige systemer blir kompromittert, eller ved at logiske sårbarheter blir gjort kjent for trusselaktører.

Nkom er særlig bekymret for destruktive cyberangrep mot sentrale styringssystemer som vil sette tilbydernes nett ut av funksjon. Dette skjedde med Kievstar i slutten av 2023 hvor det ble gjennomført et cyberangrep som medførte tap av ekomtjenester for mer enn 24 millioner abonnenter i over en uke. Det fikk også konsekvens for flyalarmer og finanssektoren i Ukraina. I Norge er angrepene på Hydro og Østre Toten kommune mest kjente eksemplene på cyberangrep som har medført alvorlige konsekvenser for virksomhetens drift.

Personellsikkerhet og innsidetrusselen

Personellsikkerhet og innsidetrusselen er blitt en stadig mer aktuell problemstilling i takt med hvordan den sikkerhetspolitiske situasjonen har utviklet seg de senere årene. De hemmelige tjenestene påpeker at når digital sikkerhet forbedres vil innsidere bli en attraktiv inngangsport til sensitiv informasjon samt viktige anlegg og skjermingsverdig infrastruktur. NSM skriver i sin rapport Risiko 2024 at i løpet av 2022 og 2023 ble det avslørt flere innsidere i vestlige land.[38] Nkom har, som nevnt i kapittel 3, også erfart på tilsyn at det er mangler ved personellsikkerheten som kan gi handlingsrom for innsidere. Innsidere er vanskelig å sikre seg mot da de kan være både bevisste og

38 Risiko 2024.pdf (nsm.no)

ubevisste. Videre er sektoren avhengig av mye utenlandsk personell som det tar lang tid å få sikkerhetsklarert. Nkom mener at bruk av innsidere hos ekomtilbydere og datasenter utgjør en risiko med tanke på kartlegging og eventuell gjennomføring av sabotasje- eller cyberangrep.