



Digitaliserings- og
forvaltningsdepartementet

Handlingsplan

Nasjonal sikkerhetsplan for digital infrastruktur

Elektronisk kommunikasjon i fred, krise og krig





Innhold

1. Innledning	3
Tilspisset sikkerhetssituasjon	3
Økt avhengighet til den digitale grunnmuren	4
Forsvarets og totalforsvarets avhengighet	5
Mer ekstremvær	5
Geografiske forskjeller	7
Samarbeid om sikkerhet og beredskap mellom staten og tilbyderne	7
2. Tiltak	11
Regionale forsterkningstiltak for kritisk digital kommunikasjonsinfrastruktur	11
Regionale risiko- og sårbarhetsanalyser og tiltak	11
Regional autonomi og datasentre	12
Økt motstandsevne for mobilnettene	15
Doblet utbyggingstakt for programmet for forsterket ekom	15
Styrket beredskap til 100 tettsteder og utvalgte basestasjoner	17
Ny bransjestandard for fysisk sikkerhet for kommunikasjonskabler	18
Sikkerhet for undersjøiske kommunikasjonskabler	19
Nasjonal kontroll med kritisk digital infrastruktur	20
Satellittbasert kommunikasjon – dekning og beredskap	22
Økt robusthet for posisjonerings- og tidstjenester	23
Styrke evnen til å motstå GNSS-forstyrrelser	25
Presetid for digitale systemer og 5G posisjonering	25
Styrket nordisk samarbeid om digital sikkerhet og beredskap	26
Øvelser i ekomsektoren – gode hver for oss, best sammen	26
Styrke motstandsevnen mot digitale angrep på kritisk digital infrastruktur	28
Styrket digital egenberedskap	28
Digital egenberedskap for befolkningen	29
Digital egenberedskap for offentlige og private virksomheter	29
Pilot for styrket lokal involvering med digital beredskap	29
3. Gjennomføring av sikkerhetsplanen	32
Organisering av gjennomføringen av sikkerhetsplanen	32
Ordliste	34
Foto	36



1. Innledning

Regjeringen har store ambisjoner for digitaliseringen av Norge for å sikre velferdsstaten, løse samfunnsutfordringer og styrke norsk konkurransekraft. Samtidig står Norge overfor en ny og krevende sikkerhetspolitisk situasjon som må håndteres og stadig økende ekstremvær. Sikre og robuste mobil- og bredbåndsnett er avgjørende for å opprettholde kritiske samfunnstjenester, både under normale forhold, i kriser og i krig. Den digitale infrastrukturen må styrkes betydelig for å møte utviklingen og utfordringene som Norge står overfor, i tråd med regjeringens mål og prioriteringer slik de er beskrevet i *Nasjonal sikkerhetsstrategi* og i Meld. St. 9 (2024-2025) *Totalberedskapsmeldingen – forberedt på kriser og krig*.

Tilspisset sikkerhetssituasjon

Den sikkerhetspolitiske situasjonen har endret seg betydelig de siste årene og et stadig mer komplekst trussel- og risikobilde gjør det nødvendig å styrke innsatsen. Regjeringen har nylig lansert en nasjonal sikkerhetsstrategi. Strategien definerer hvilke nasjonale sikkerhetsinteresser som skal fremmes og forsvares, og peker på tre hovedprioriteringer som skal legges til grunn:

1. Raskt styrke forsvarsevnen
2. Gjøre samfunnet mer motstandsdyktig
3. Styrke vår økonomiske sikkerhet

Digital kommunikasjon er avgjørende for et motstandsdyktig samfunn, og understøtter også styrket forsvarsevne og økonomisk sikkerhet.

Strømbuudet i Spania og Portugal viser hvor sårbart samfunnet er ved utfall av kritisk infrastruktur, og hvor viktig det er å kjenne til verdikjeder for kritisk infrastruktur. Det viser også viktigheten av tett internasjonalt samarbeid for bistand av naboland når slike utfall skjer.



28. april 2025 skjedde Europas største strømbrudd i nyere tid. Kl. 12:33 oppstod ustabilitet i det spanske strømmettet, og få sekunder etter ble rundt 60 millioner mennesker rammet av strømbrudd i Spania og Portugal. Strømbruddet rammet blant annet sykehus, mobilnett, transportsystemer, trafikklys, matbutikker og husstander. Strømmen ble gjenopprettet rundt 12 timer etter utfallet startet i Portugal, og etter 16 timer med utfall i Spania.

I slutten av april 2022 ble tre digitale hovedføringsveier ved Paris kappet. Hendelsen fremstod som et koordinert og målrettet angrep på kritisk digital infrastruktur, og fikk konsekvenser for flere mobil- og bredbåndsnett i Paris og regionene rundt. Under sommer-OL i Paris i 2024 var det en lignende hendelse, der flere sentrale digitale føringsveier ble kuttet. Dette rammet deler av mobil- og bredbåndsnettene og fikk konsekvenser for sendinger fra OL.

Strømbruddet i Sør-Europa, og brudd på kommunikasjonskabler i Paris, viser hvor krevende det er å forebygge mot utfall, både ved tilsiktede og utilsiktede hendelser.

Krigen i Ukraina har gjort det enda tydeligere hvor viktig opprettholdelse av mobilkommunikasjon er under store og langvarige påkjenninger. Den digitale infrastrukturen har vært avgjørende for å opprettholde kritiske samfunnsfunksjoner og støtte forsvaret av landet, gjennom flytting av kunder mellom nett ved langvarige utfall, internasjonal redundans og tilgang til lavbanesatellitter.

Økt avhengighet til den digitale grunnmuren

Den digitale grunnmuren bærer stadig større verdier og flere kritiske tjenester for det norske samfunnet. Sentrale styringssystemer for annen infrastruktur, finanstjenester, helsetjenester, transport- og posisjoneringstjenester, tilgang på nyheter og informasjon fra myndighetene og tilgang til nødnummer, er eksempler på tjenester som den digitale infrastrukturen bærer i dag. Med regjeringens mål om å bli verdens mest digitaliserte land innen 2030, som beskrevet i digitaliseringsstrategien, kreves det en kontinuerlig styrking av den digitale infrastrukturen.

Digitaliseringen gir muligheter til å løse oppgaver på nye og mer effektive måter, men skaper også sårbarheter som kan utnyttes. Stadig flere kritiske tjenester går over mobil-

og bredbåndsnettene. Det pågående arbeidet med å etablere fremtidens nød- og beredskapskommunikasjon over de kommersielle mobilnettene er i gang, og skal erstatte dagens Nødnett.

Forsvarets og totalforsvarets avhengighet

Forsvaret og totalforsvaret blir stadig mer avhengige av mobil- og bredbåndsnett i hele krisespekteret, som en konsekvens av samfunnets digitalisering, automatisering og teknologiske utvikling i både sivil og militær sektor. Effektiv samhandling og understøttelse av Forsvaret fra sivil side forutsetter digital kommunikasjon. Omfattende utfall av elektronisk kommunikasjon (ekom) vil kunne få store konsekvenser for Forsvaret og totalforsvarets operative evne.



Mer ekstremvær

Fiberbrudd og bortfall av strømforsyning er i dag de vanligste årsakene til ekomutfall. Dette skyldes ofte ekstremvær, flom, jordskred eller mindre naturhendelser som trefall over linjer med mer. Forskning peker på at det kan forventes mer ekstremvær i fremtiden som følge av klimaendringer. Hvis ekomnettene ikke styrkes for å møte denne utviklingen (klimatilpasning), er det en risiko for at kvaliteten på nettene svekkes og for flere og mer alvorlige utfall.



Ekstremværet Hans rammet Sør-Norge fra 7. til 9. august 2023 og førte til omfattende skader på infrastruktur og eiendom, særlig i fylkene Innlandet og Viken, og i deler av Vestland og Trøndelag.

I Ål kommune førte ekstremværet til flom og jordskred som medførte tap av hus og infrastruktur, samt at flere områder i kommunen ble evakuert. Under håndteringen av ekstremværet opplevde Ål kommune også utfordringer med kommunikasjonsinfrastruktur. Telenor og Telia sine mobilnett og deler av bredbåndsnettet falt ut fordi steinmasser bragt i bevegelse av flom ødela fiberkablene inn mot kommunesenteret. En femtedel av innbyggerne kunne ikke gjøres rede for. Dette skapte store utfordringer for kommunens evne til å varsle og kommunisere med innbyggerne under evakueringsarbeidet.

Slike hendelser understreker sårbarheten i den digitale infrastrukturen under ekstreme værforhold, og hvor viktig digital kommunikasjon er for effektiv krisehåndtering.

Bildet under er fra flom i Feda i Agder i 2015, og illustrerer utfordringene.



Geografiske forskjeller

Tilgangen til mobil- og bredbåndsnett er bedre i tettbygde enn i spredtbygde strøk. Spredtbygde og sentrale strøk har ulik risiko- og sårbarhetsprofil for digital infrastruktur, og ulike behov for tiltak for å styrke motstandsdyktigheten. Nordområdene er Norges viktigste strategiske satsingsområde. Regjeringen la i august 2025 fram en ny nord-områdestrategi med prioriterte innsatsområder som viderefører og forsterker innsatsen for nordområdene.

Typiske tiltak for spredtbygde strøk er styrket reservestrømskapasitet, styrket redundans og å sikre at flere tilbydere kan levere transmisjon. For sentrale strøk kan et tiltak være å redusere konsentrasjonsrisiko, for eksempel der flere kritiske kommunikasjonskabler og/eller utstyr er samlet på samme lokasjon.



Samarbeid om sikkerhet og beredskap mellom staten og tilbyderne

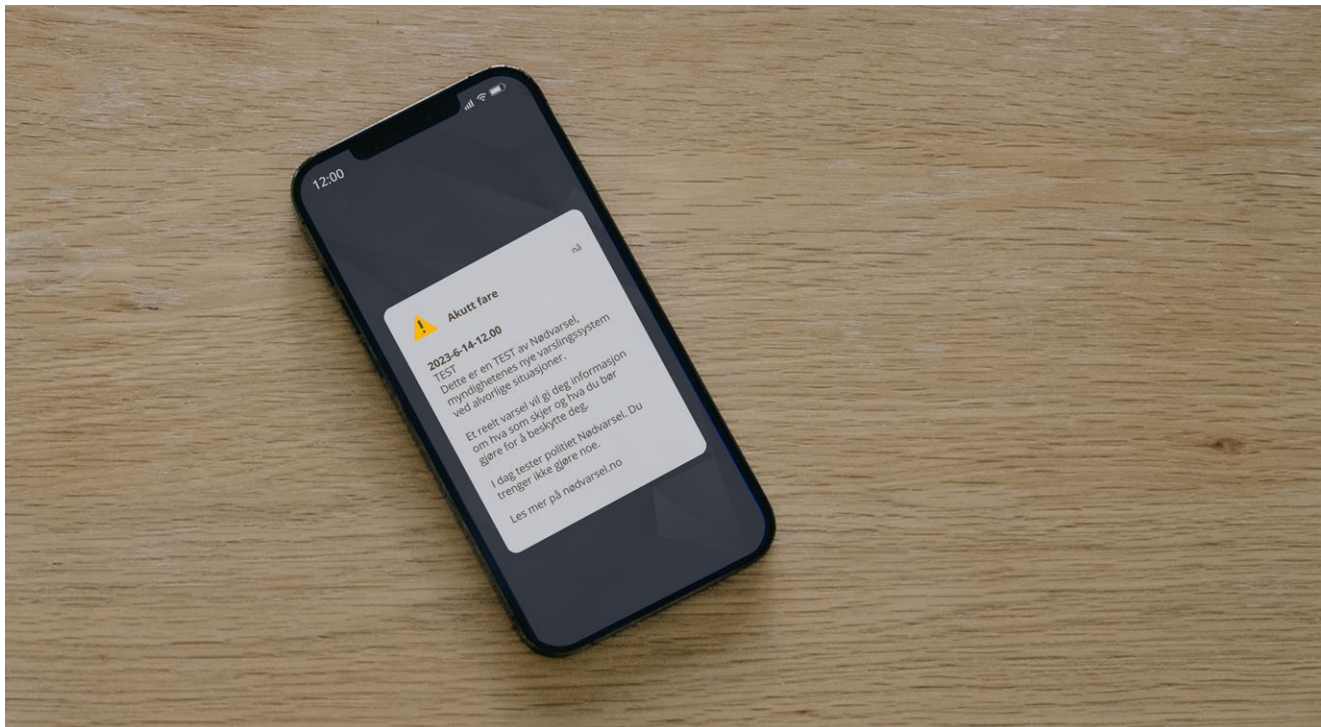
Hvert år investerer ekomtilbyderne betydelige beløp¹ i utbygging og styrking av infrastrukturen. I tillegg bevilger staten årlig tilskuddsmidler for å styrke nettene. Selv om statens bidrag utgjør en liten del av de totale investeringene, har målrettede

¹ Ca. 11,6 milliarder kroner i 2024, jf. <https://nkom.no/statistikk/nokkeltall-og-interaktive-dashbord/ekomstatistikk>

statlige tiltak, der staten finansierer deler av eller hele tiltak, vist seg å ha svært høy samfunnsverdi. I mange tilfeller har disse tilskuddene også fungert som en katalysator for bransjen, og har utløst investeringer fra tilbyderne selv.

Den digitale infrastrukturen er avgjørende for det norske samfunnet, Forsvaret og totalforsvaret. Tiden er inne for økt innsats. Denne sikkerhetsplanen er delt i ulike innsatsområder med tilhørende tiltak. Regjeringen mener det er nødvendig å gjennomføre disse tiltakene for å lykkes med å nå målene i regjeringens nasjonale sikkerhetsstrategi, digitaliseringsstrategi og totalberedskapsmelding, slik at Norge er rustet for utfordringene som er beskrevet ovenfor. Enkelte av tiltakene vil være så omfattende og kostnads-krevende at de strekker seg utover perioden 2026–2030, som denne planen omfatter. Flere av tiltakene forutsetter betydelig statlig- og kommersiell finansiering i perioden for gjennomføring.





Nødvarsel er en tjeneste fra norske myndigheter som politiet i fredstid og sivilforsvaret i krig kan bruke for å varsle befolkningen. Nødvarsel skal brukes ved akutte og alvorlige hendelser med fare for liv og helse. Et nødvarsel inneholder informasjon om hva som skjer, og hva du bør gjøre for å beskytte deg selv.

Systemet er basert på teknologi hvor mobilnettene benyttes til å kringkaste varsler til befolkningens mobiltelefoner. Nødvarsel er anonymt, og myndighetene får ikke tilgang til posisjon eller annen informasjon fra mobiltelefonene.

I 2025 blir det innført ny funksjonalitet i Nødvarsel for å få mer geografisk presis varsling, kjent som Device Based Geo Fencing.

Nødvarsel er et godt eksempel på et samarbeidsprosjekt mellom mobiltilbyderne og staten for å styrke samfunnssikkerhet og beredskap.

(Se www.nødvarsel.no)



2. Tiltak

Regionale forsterkningstiltak for kritisk digital kommunikasjonsinfrastruktur

Regionale risiko- og sårbarhetsanalyser og tiltak

Gode og oppdaterte risiko- og sårbarhetsanalyser for digital infrastruktur, som omfatter hendelser oppover i krisespennt, gir kunnskap for å iverksette tiltak som trygger landet. Slike analyser utgjør fundamentet for at ekomtilbydere og offentlige virksomheter kan iverksette de rette tiltakene for å styrke motstandskraften i den digitale infrastrukturen, slik at den er i stand til å møte nye utfordringer.

Det er siden 2019 gjennomført regionale risiko- og sårbarhetsanalyser av ekominfrastrukturen i Finnmark, Troms, Nordland, Trøndelag, Innlandet og Buskerud. Etter analysen er det identifisert og igangsatt tiltak for å styrke motstandsdyktigheten til den digitale infrastrukturen i alle disse regionene. Tiltakene inkluderer flere digitale føringsveier, blant annet nye fiberforbindelser, og styrking av sårbare punkter i nettene, og gir vesentlig økt beredskap.

Kunnskap fra analysene deles med statsforvaltere i de ulike områdene, noe som bidrar i deres arbeid med samfunnssikkerhet, beredskap og krisehåndtering. Regjeringen vil gjennomføre grundige risiko- og sårbarhetsanalyser i alle landets regioner, og gjennomføre nødvendige tiltak når analysene er gjennomført, jf. Digitaliseringsstrategien.

Elektroniske kommunikasjonstjenester er spesielt viktig på Svalbard, gitt øygruppens beliggenhet og infrastruktur. Regjeringen foreslo i Prop. 47 S (2024-2025) å etablere et nytt sjøfibersamband mellom Svalbard, Jan Mayen og fastlandet. Stortinget sluttet seg til forslaget, jf. Innst. 174 S (2024-2025). Nytt sjøfibersamband har en kostnadsramme på 2,8 mrd. kroner, og skal etter planen være operativt i 2028.

For å styrke kritisk infrastruktur, jf. nasjonal sikkerhetsstrategi, og forberede ekomsektoren på krise og krig, jf. totalberedskapsmeldingen, er det nå nødvendig å styrke og forsere dette arbeidet. I tillegg bør tidligere analyser i Nord- og Midt-Norge, oppdateres i lys av en ny sikkerhetspolitisk situasjon.



REGJERINGEN VIL:

- doble takten for å gjennomføre regionale risiko- og sårbarhetsanalyser og ferdigstille analyser for de resterende regionene i Norge
 - iverksette tiltak for å styrke den digitale infrastrukturen som følge av funn i risiko- og sårbarhetsanalysen
 - gjøre nødvendige oppdateringer for de eksisterende regionale analysene for dagens sikkerhetspolitiske situasjon, og hendelser oppover i krisespennet
-

Regional autonomi og datasentre

Regional autonomi betyr at tjenester fungerer i regionen, uavhengig av tilkobling mot andre regioner, eller resten av verden. Det er utfordrende å få oversikt over verdikjeder til digitale tjenester, og det er hver sektors ansvar å vurdere behovet for autonomi for egne digitale tjenester. På den ene siden går utviklingen i retning av økt kompleksitet i internasjonale verdi- og leverandørkjeder. På den andre siden er skyteknologien skalerbar og geografisk fleksibel.

Digitale tjenester produseres ofte i datasentre, som kan være lokalisert nasjonalt, i naboland, andre europeiske land eller i andre verdensdeler. Norske datasentre og en sterk

digital infrastruktur legger dermed til rette for at kritiske digitale tjenester kan produseres i Norge heller enn i datasentre i utlandet. Dette vil styrke den nasjonale kontrollen og autonomien.

I dagens sikkerhetspolitiske situasjon er det nødvendig å kjenne til de digitale verdikjedene som viktige og kritiske samfunnsfunksjoner benytter eller har avhengigheter til. For å sikre at Norge kan beskytte kritiske tjenester og informasjon, er det et behov for tilstrekkelig datasenterkapasitet, og at datasentrene som disse tjenestene blir levert fra er sikre. Den sikkerhetspolitiske situasjonen gjør også at en sterk digital infrastruktur, geo-redundans og raskt å kunne migrere data eller datasentertjenester ut av landet, blir stadig mer viktig. Tilsvarende kan allierte land ha et ønske om at deres kritiske data eller datatjenester kan leveres fra Norge. Det er viktig å stille krav til sikkerhet ved anskaffelser, blant annet anskaffelser av digitale tjenester og datalagring, og vurdere hvilken grad av autonomi det er behov for, både for digitale bærere som anskaffes og for digitale tjenester. For eksempel er det viktig å vurdere behov for redundans og leverandørdiversitet for anskaffelse av bredbånds- og mobiltjenester til kritiske samfunnsfunksjoner.

For å sikre at staten skal kunne ivareta styringsevne og handlingsfrihet over hele krisespennet er det viktig å ha tilgang til både egne og kommersielt drevne datasentre med tilpasset sikkerhetsnivå. Relevante beredskapsaktører i totalforsvaret må kunne ha tilgang til datasenterkapasitet under nasjonal teknisk og juridisk kontroll i fred, krise og krig, med autorisert personell og statlig styringsmulighet. Det er derfor viktig med datasentre på norsk jord. Regjeringen la i juni 2025 frem en ny datasenterstrategi som blant annet vektlegger at datasenternæringen skal bidra til et sikrere og mer forberedt Norge.

For ekomsektoren er det behov for å kartlegge situasjonen rundt regional autonomi for de ulike ekomtjenestene, og kartlegge hvilke datasentre som er til stede i hver region. Det skal vurderes hvordan styrket regional autonomi kan oppnås for ulike ekomtjenester, og det skal identifiseres tiltak som er nødvendige for å styrke autonomien, og vurdere behov for å redusere avhengigheten til enkelte sentrale lokasjoner for tjenesteproduksjon av kritiske tjenester. Målet med arbeidet er å øke motstandsevnen for kritisk infrastruktur i fred, krise og krig, som både nasjonal sikkerhetsstrategi og totalberedskapsmeldingen peker på.

Regional produksjon av ekomtjenester betyr at nettverk, nettverksutstyr og tjenesteproduksjon er regionalt tilgjengelig, og fungerer uavhengig av tilkobling mot sentrale lokasjoner. I tillegg vil grad av regional autonomi avhenge av tilgangen til personell og kompetanse for tjenesteproduksjon, drift og vedlikehold og regionale reservelager med kommunikasjonskabler og tekniske reservedeler, for å opprettholde og gjenopprette ekomnett og -tjenester.

REGJERINGEN VIL:

- kartlegge dagens situasjon for regional autonomi for ekomnett og -tjenester
 - vurdere tiltak for å styrke regional autonomi for digital kommunikasjon, slik at kritiske kommunikasjonstjenester kan opprettholdes selv ved større utfall i andre regioner
 - styrke regionale reservelagre for å styrke evnen til å gjenopprette ekomnett og -tjenester i krise og krig
 - at Norge skal ha robuste datasentre som sikrer både nasjonal og regional autonomi av datasentertjenester
-



Stortinget har vedtatt en ny ekomlov som trådte i kraft 1. januar 2025. Ekomloven § 3-1 setter krav til sikkerhet og beredskap, og åpner dessuten opp for å inngå avtale om eller pålegge tiltak

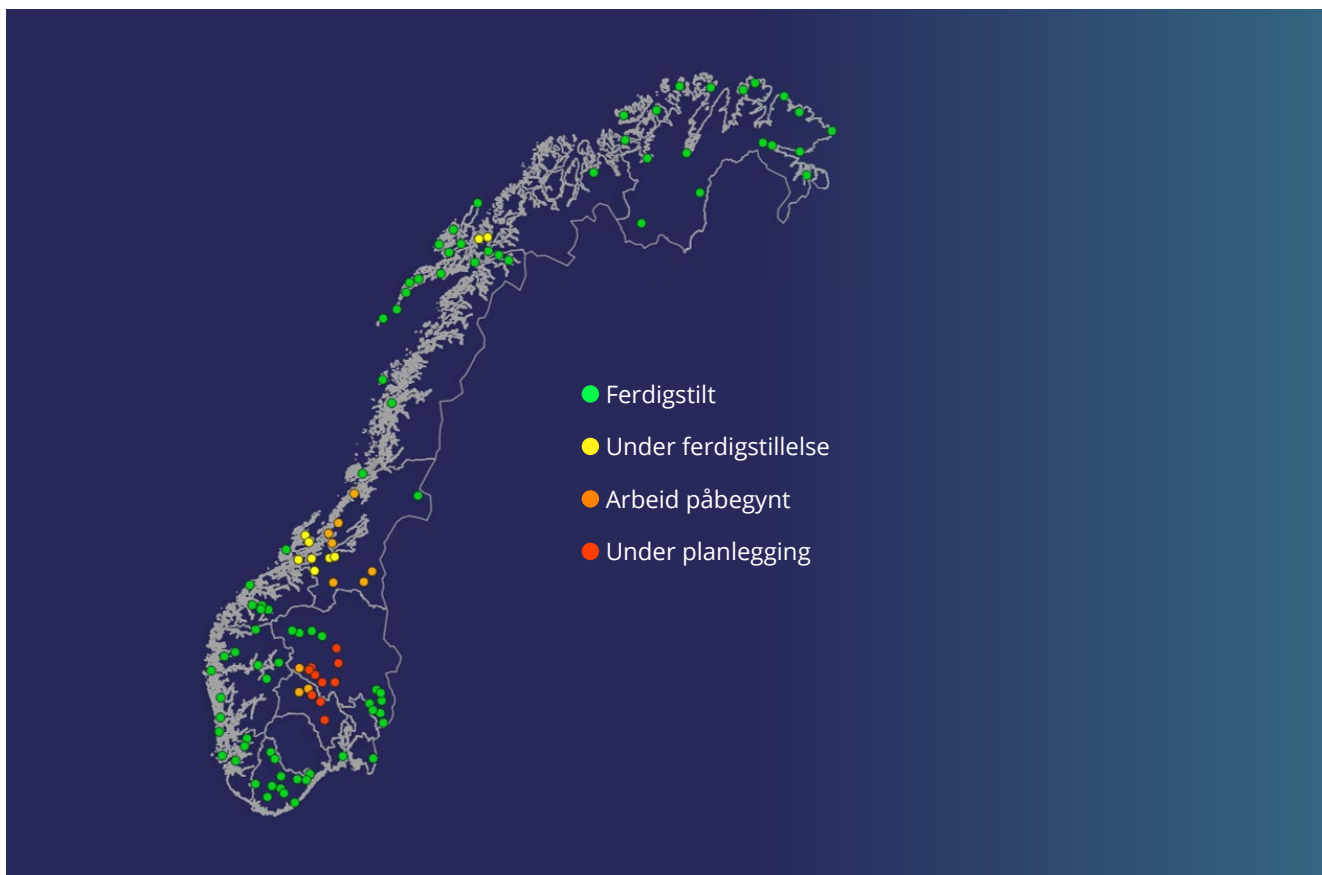
- Ekomloven § 3-1 første ledd setter krav om at tilbyder skal tilby ekomnett og -tjenester med forsvarlig sikkerhet for brukerne i fred, krise og krig, opprettholde forsvarlig beredskap, og sikre forsvarlig vern av kommunikasjon og data. Myndighetene kan etter ekomloven § 3-1 femte ledd fatte enkeltvedtak for å sikre at tilbyder gjennomfører tiltak som gir forsvarlig sikkerhet, beredskap og vern av kommunikasjon og data. Tilbyder skal dekke kostnadene ved slike tiltak.
- Etter ekomloven § 3-1 sjette ledd kan myndighetene pålegge tilbyder å iverksette tiltak som går utover kravet til forsvarlig sikkerhet etter ekomloven § 3-1 første ledd for å sikre oppfyllelse av nasjonale behov for sikkerhet, beredskap og funksjonalitet i ekomnett og -tjenester. Myndighetene kan etter bestemmelsen treffe vedtak og/eller inngå avtale med tilbyder, og myndighetene dekker ved slike tiltak tilbyders merkostnader.

Økt motstandsevne for mobilnettene

Regjeringen vil i samarbeid med mobiloperatørene styrke motstandsevnen i mobilnettene og gjennomføre tiltak for økt beredskap. Tiltakene som skal gjennomføres for mobilnettene, skal sees i sammenheng med de regionale analysene.

Doblet utbyggingstakt for programmet for forsterket ekom

I 2014 innførte Nasjonal kommunikasjonsmyndighet (Nkom) krav om minimum reservestrømkapasitet² på 2-4 timer for alle basestasjoner. Samme år ble programmet for forsterket ekom startet opp. Programmet etablerer 72 timers reservestrømkapasitet på basestasjonene i ett utvalgt område som er viktig for beredskapen i kommunen. Det er sentrale tettsted i kommunene som dekkes, og vanligvis området der kommunenes kriseledelse samles. I tillegg er det ofte sentrale trafikknutepunkt, andre offentlige myndigheter og overnattingsmuligheter i det utvalgte området. Normalt etableres en alternativ digital føringsvei (transmisjonslinje) til basestasjonene i det utvalgte området for å sikre redundans. En gjennomgang av utfallshistorikk viser at utbyggingen av forsterket ekom har ført til en betydelig reduksjon i antall utfall i de utbygde områdene.



² Vedtak om minstekrav til reservestrømkapasitet i landmobile nett, Post- og teletilsynet, juni 2014



Valget av kommuner som skal forsterkes, er basert på risikovurderinger der det legges vekt på en kombinasjon av isolasjonsrisiko, utfallsstatistikker og synergier med andre regionale forsterkingstiltak. Programmet har blitt svært godt mottatt lokalt, både i kommunene, hos fylkesberedskapssjefene og i DSB, da det i vesentlig grad forbedrer kommunens beredskap, kriseledelsesevne og befolkningens muligheter for kommunikasjon.

Siden oppstart i 2014 er 102 kommuner forsterket eller er under forsterking pr. 31.12.2024. 10 nye kommuner er planlagt for 2025.

Lokale bidrag til programmet for forsterket ekom kan øke takten på utbyggingen ytterligere. Regjeringen vil se på muligheten for frivillig samfinansiering med kommuner, og på den måten sikre at enda flere kommuner får forsterket ekom totalt sett.

REGJERINGEN VIL:

- doble utbyggingstakten for programmet for forsterket ekom, og gi 100 nye kommuner forsterket ekom innen 2030
 - se på muligheten for at kommuner kan samfinansiere forsterket ekom, slik at flere kommuner kan få forsterket ekom innen 2030
-

Styrket beredskap til 100 tettsteder og utvalgte basestasjoner

En gjennomgang av rapporterte utfall i mobilnettene i perioden 2019-2024, viser at en økning av reservestrøm fra 4 timer til 8-12 timer, kombinert med flere digitale føringsveier til lokasjoner som er spesielt utsatt for hyppige og langvarige strømutfall, vil redusere antall utfall med 50-70 % i de berørte områdene.

Det er ønskelig å styrke reservestrømkapasiteten og samband til basestasjoner i utsatte områder for å styrke motstandsdyktigheten mot langvarig strømutfall. Tiltaket skal sikre nok reservestrømkapasitet til at tjenester opprettholdes i 8-12 timer ved strømbryt og hindre at et enkelt fiberbryt resulterer i tjenesteutfall.

Målsettingen er å styrke reservestrøm for 300 basestasjoner innen 2030. Dette er viktig for befolkningens mulighet til kommunikasjon, og for å øke effektiviteten til rettemannskap, nødetater og andre aktører under langvarige strømutfall og hendelser. Det er primært basestasjoner som dekker større områder og der alle tilbydere er til stede, som skal prioriteres. Tiltaket vil også komme fremtidens nødnett til gode.

Det nøyaktige antallet basestasjoner som bør forsterkes og hvor lang reservestrømkapasitet som bør bygges, skal avgjøres basert på ROS-analyser.

I tillegg til å forsterke utsatte kommuner gjennom programmet for forsterket ekom, er det behov for å styrke flere isolasjonsutsatte tettsteder, som er sårbare for utfall og



vanskelige å nå ved langvarige strømbrudd. Målet er å gi 100 nye tettsteder 12-24 timers reservestrøm innen 2030.

Tiltakene vil sees i sammenheng med ekomtilbydernes behov for å fornye eksisterende reservestruømløsninger, og det må skje gjennom en kostnadsdeling mellom tilbyderne og staten.

REGJERINGEN VIL:

- styrke beredskapen på 300 basestasjoner i Norge med 8-24 timers reservestrøm og sikre flere digitale føringsveier i utsatte områder der alle tre mobiltilyderne er til stede
 - styrke mobildekningen for 100 nye tettsteder med 12-24 timers reservestrøm og flere digitale føringsveier
-

Ny bransjestandard for fysisk sikkerhet for kommunikasjonskabler

Gjennom arbeidet med risiko- og sårbarhetsanalyser er det avdekket sårbarheter knyttet til manglende fysisk sikring av viktige og kritiske kommunikasjonskabler, blant annet transportnettkabler.

For å sikre nettutstyr mot uønskede ytre fysiske påvirkninger, stiller klassifiseringsforskriften krav til nettilbyder om å klassifisere alle sine anlegg i forhold til viktigheten



anlegget har for offentlige elektroniske kommunikasjonstjenester og sikre anlegget deretter. Forskriften stiller ikke tilsvarende krav til elektroniske kommunikasjonsnett.

Bransjen inviteres til å utarbeide en bransjestandard for viktige og kritiske kommunikasjonskabler, slik at kravet i ekomloven til å ivareta forsvarlig sikkerhet, overholdes. Regjeringen vil nedsette en arbeidsgruppe med representanter fra ekomtilbydere og Nkom som får i oppdrag å utarbeide en omforent bransjestandard for fysisk sikring av kritiske kommunikasjonskabler.

REGJERINGEN VIL:

- at kommunikasjonskabler som bærer viktig og kritisk digital kommunikasjon skal ha forsvarlig fysisk sikring
 - at bransjen og Nkom i samråd utarbeider en felles bransjestandard for fysisk sikring av kommunikasjonskabler som er viktige for transportnett og andre kritiske tjenester
-

Sikkerhet for undersjøiske kommunikasjonskabler

Beskyttelse av kritisk undervannsinfrastruktur er en prioritet for regjeringen. Undersjøiske kommunikasjonskabler er avgjørende for nasjonal og global datatrafikk, og bærer over 99 % av den internasjonale datatrafikken. Dagens sikkerhetspolitiske situasjon med krigen i Ukraina, skadene på undersjøiske kabler i Østersjøen og andre havområder og sabotasjen av Nord Stream-rørledningene i 2022, viser hvor viktig det er å beskytte undervannsinfrastruktur på norsk sokkel.

Norge har siden 2022 styrket innsatsen for å øke sikkerheten til undersjøiske kommunikasjonskabler og elektroniske kommunikasjonstjenester i norske farvann gjennom tett samarbeid mellom sivile myndigheter, bransjeaktører og forsvarssektoren. Noen av tiltakene som benyttes er:

- Undersøkelser av viktige undersjøiske kommunikasjonskabler
- Bruk av teknologi for å overvåke undersjøiske kommunikasjonskabler
- Eiere av kritiske undersjøiske kommunikasjonskabler underlegges sikkerhetsloven

Et tett nasjonalt og internasjonalt samarbeid mellom myndigheter, bransjen og forsvarssektoren, har avgjørende betydning for økt sikkerhet for undersjøisk infrastruktur i våre havområder. Norge og flere andre land ved Nordsjøen har derfor etablert et samarbeid for å øke sikkerheten for energi- og ekinfrastrukturen i Nordsjøen. Videre har norske myndigheter sammen med operatører av sjøkabler i norske farvann etablert et nasjonalt samarbeidsorgan, Norsk Sjøkabelforening, med mål om økt sikkerhet for sjøkabler gjennom samarbeid, bevisstgjøring og gjensidig informasjonsutveksling.

Etter norsk og tysk initiativ har NATO opprettet et maritimt senter for sikring av kritisk undersjøisk infrastruktur.

Regjeringen ser behov for videre styrking av sikkerheten og beredskapen for kritisk undersjøisk infrastruktur. Alvoret i den sikkerhetspolitiske situasjonen gjør det også nødvendig med tiltak for å kunne beskytte denne infrastrukturen i det øvre krisespennet, blant annet å forbedre rettekapasitet.

REGJERINGEN VIL:

- styrke sikkerhet og robusthet for sjøkabler gjennom økt nasjonalt og internasjonalt samarbeid
 - gjennomføre risiko- og sårbarhetsanalyser for ekinfrastruktur på norsk sokkel for å identifisere sårbarheter, og sørge for å iverksette nødvendige tiltak for å redusere sårbarheter som identifiseres
 - kartlegge og vurdere behov for økt rettekapasitet for sjøkabler i Norge i krise og krig
-

Nasjonal kontroll med kritisk digital infrastruktur

De fleste viktige og kritiske samfunnsfunksjoner er avhengige av at kritisk digital kommunikasjon fungerer i hele krisespennet. For å sikre dette er det viktig at staten har nødvendig grad av nasjonal kontroll. Nasjonal kontroll innebærer styringsevne til å ta effektive beslutninger gjennom for eksempel regulering, eierskap eller avtaler, og handlefrihet til å gjennomføre beslutninger mest mulig uavhengig av utenlandske aktører og innsatsfaktorer. Dette er tydeliggjort i rapporten som Lysne III-utvalget leverte til regjeringen i februar 2025.³

Oppdaterte oversikter over virksomheter som leverer kritisk infrastruktur og utarbeidelse av målbilder over kritisk kommunikasjonsinfrastruktur, er forutsetninger for å sikre nasjonal kontroll. Målbildene skal beskrive en tilstand som er nødvendig å nå for å sikre nasjonal kontroll. Målbildene vil danne utgangspunkt for å vurdere nåsituasjonen, identifisere gap og gi grunnlag for å gjennomføre målrettede tiltak.

Regjeringen har blant annet igangsatt et arbeid for å etablere en nasjonal skytjeneste. Formålet er å sikre økt nasjonal kontroll med kritisk digital infrastruktur, viktige samfunnsfunksjoner og digitale verdier. I anskaffelsen skal det stilles krav til nasjonal kontroll med skytjenesten som leverandører må tilfredsstille og gi garantier for. I tillegg skal regelverket for skytjenester tydeliggjøres.

³ Nasjonal kontroll med kritisk digital kommunikasjonsinfrastruktur



Styrket nasjonal kontroll med kritisk infrastruktur er et uttalt mål for regjeringen i Nasjonal sikkerhetsstrategi. Regjeringen vil analysere behovet for å styrke personellressurser og kompetanse lokalisert i Norge som er nødvendig for utbygging, drift og overvåking, feilretting og gjenoppretting av kritisk digital kommunikasjonsinfrastruktur.

REGJERINGEN VIL:

- utarbeide en oversikt over virksomheter som leverer kritisk digital kommunikasjonsinfrastruktur i Norge, og sikre at denne oppdateres jevnlig
 - etablere og vedlikeholde målbilder over kritisk kommunikasjonsinfrastruktur som er nødvendige for å sikre tilstrekkelig nasjonal kontroll
 - iverksette tiltak som bedrer nåsituasjonen knyttet til nasjonal kontroll, herunder planlegge en nasjonal skytjeneste for å sikre økt nasjonal kontroll med kritisk digital infrastruktur, viktige samfunnsfunksjoner og digitale verdier
 - i samarbeid med aktørene kartlegge behovet for kritisk kompetanse og ressurser som er nødvendig for utbygging, drift og overvåking, feilretting og gjenoppretting av kritisk kommunikasjonsinfrastruktur
-



Satellittbasert kommunikasjon – dekning og beredskap

Det siste tiåret har det blitt investert betydelig i de norske mobilnettene, og Norge har en mobildekning i verdensklasse. I dag har 99,9 % av befolkningen mobildekning fra minst én mobiloperatør, og omtrent 85 % av landarealet er dekket av enten 4G eller 5G. Til tross for dette er det fortsatt store områder hvor folk ferdes som ikke har mobildekning, og som heller ikke kan forvente å få dekning fremover basert på kommersiell utbygging. De gjenværende områdene uten dekning er ofte enten svært kostbare å bygge ut eller ligger i vernede områder som begrenser mulighetene for utbygging (for eksempel naturreservater).

Dekning fra lavbanesatellitter vil langt på vei kunne løse problemet med manglende dekning. I tillegg til å gi ekstra dekning, gir satellittbasert kommunikasjon økt robusthet og er en beredskapsløsning dersom de landbaserte ekomnettene skulle falle helt eller delvis ut av ulike årsaker.

Flere satellittoperatører tester direktekommunikasjon fra vanlige smarttelefoner til satellitt. Foreløpige resultater er lovende, men det er ennå for tidlig å kunne konkludere med i hvilken grad en slik løsning vil kunne oppfylle kravene til driftsstabilitet, kvalitet, kapasitet, dekning, robusthet og sikkerhet. Direktekommunikasjon fra smarttelefoner til satellitt kan gi et stort løft ift. å øke dekningen og tilgjengeligheten utover 4G/5G.

Flere ekomtilbydere har inngått avtaler med lavbanesatellittoperatører for å kunne tilby direktekommunikasjon med smarttelefoner. Nkom er i dialog med relevante mobil-leverandører og norske nødetater om mulighetene for å innføre funksjoner på mobiltelefoner som gjør det mulig å sende meldinger til nødetatene via satellitt, i områder uten noen mobildekning. Per mai 2025 er det 17 land som har denne funksjonen tilgjengelig.

I dagens sikkerhetspolitiske situasjon, er det viktig for virksomheter som har ansvar for eller understøtter kritiske samfunnsfunksjoner å vurdere reserveløsninger for digital kommunikasjon. Med økt utvikling av satellittbasert kommunikasjon de siste årene, er det stadig flere beredskapsaktører som velger satellittbaserte reserveløsninger, som kan ivareta digital kommunikasjon dersom bakkenettene blir utilgjengelige.

REGJERINGEN VIL:

- legge til rette for at satellittbasert kommunikasjon effektivt kan benyttes for dekning og som beredskapstiltak for digital kommunikasjon
 - legge til rette for at meldinger kan sendes til nødetatene via satellitt for befolkningen i områder uten mobildekning
 - utrede løsninger for direktekommunikasjon mellom mobil og satellitt i Norge
 - at virksomheter som har ansvar for eller understøtter kritiske samfunnsfunksjoner vurderer å anskaffe satellittbaserte reserveløsninger for digital kommunikasjon i kriser og krig
-

Økt robusthet for posisjonerings- og tidstjenester

Samfunnet er i stor grad avhengig av gode og pålitelige posisjonerings- og tidstjenester. Mange av de digitale tjenestene som folk bruker hver dag, har en avhengighet til presis tid og posisjon. Det gjelder blant annet mobilkommunikasjon, karttjenester og finansielle tjenester, som mange av de digitale tjenestene benytter i sine verdikjeder. Utvikling av stadig mer høyeffektive, raske og robuste digitale tjenester øker behovet for presis tids-synkronisering. Global Navigation Satellite System (GNSS) er en fellesbetegnelse for satellittbaserte systemer for posisjonering, navigasjon og tid (PNT) med global dekning. Det har stor internasjonal nytteverdi med satellittbasert distribusjon av høypresist PNT-signal til alle land-, luft- og sjølokasjoner i Norge. Samtidig er GNSS-signaler følsomme for forstyrrelser, som demonstrert under jammehendelser og jammetester. Deres satellittbaserte tjenester faller bort, vil det få alvorlige konsekvenser for samfunnet, Forsvaret og totalforsvaret. Regjeringen ser behov for å vurdere å etablere alternative løsninger under norsk kontroll, både for posisjoneringstjenester og tidstjenester.



Det har over lengre tid vært daglige forstyrrelser av GPS (Global Positioning System) i luftrommet over Øst-Finnmark knyttet til jamming. Nye målinger gjennomført av Nasjonal kommunikasjonsmyndighet (Nkom), viser at GPS-signalene i Øst-Finnmark sporadisk blir utsatt for manipulasjon ned til 150 meters høyde.

Spoofing: er en teknikk hvor signaler bevisst manipuleres slik at brukerne kan få feil informasjon om posisjon, navigasjon og tid inn i sine systemer.

Jamming: er å sende ut radiostøysignaler som har til hensikt å forstyrre, blokkere eller hindre mottak av GPS-signaler. Det brukes for eksempel hvis man ønsker å beskytte informasjon om hvor man befinner seg.

GNSS er forkortelse for Global Navigation Satellite Systems. Et av de mest brukte GNSS-systemene er GPS.

Styrke evnen til å motstå GNSS-forstyrrelser

Den årlige Jammetesten på Andøya, der myndigheter, industri og academia samles, samarbeider om, og gjennomfører, testing og utprøving av systemers motstandsevne mot GNSS-forstyrrelser, har gitt gode resultater. Regjeringen vil legge til rette for å videreføre denne årlige testen. Arbeidet er svært viktig for å gi økt kunnskap og utvikling av robuste og motstandsdyktige systemer mot forstyrrelser i mottakersystemene for GNSS.

Arbeidet med utvikling av systemene for automatisert monitorering av GNSS-båndene, og andre prioriterte deler av frekvensspektrumet i Norge, vil bli styrket – herunder automatisert kontinuerlig monitorering, deteksjon og analyse av utnyttelsen av frekvensspektrumet og forstyrrelser mot dette. Arbeidet med karakterisering, lokalisering og stans av kilder til forstyrrelser vil forsterkes og automatiseres spesielt ved hjelp av KI og andre (matematiske) algoritmer.

For å styrke arbeidet med GNSS-forstyrrelser skal Nkoms regionskontor i Nord-Norge flyttes fra Lødingen til Tromsø, med kort reisetid til strategisk viktige områder på Svalbard og i Øst-Finnmark samt gode muligheter for samarbeid med relevante samarbeidsaktører.

Presis tid for digitale systemer og 5G-posisjonering

Distribusjon av robust og høypresis tid er avgjørende for videre utvikling innenfor flere områder som mobilkommunikasjon, kraftsektoren, transport, kringkasting, bank og finans, forsvar, seismologi, romindustri, forskning, helse, datasentre, nød- og beredskapskommunikasjon m.m. For å sikre en motstandsdyktig digital infrastruktur, vil regjeringen vurdere å etablere en alternativ nasjonal infrastruktur for distribusjon av et presist og sporbart tid-/klokkesignal. Tiltaket er utpekt av Totalberedskapskommisjonen som et viktig sårbarhetsreducerende virkemiddel.

5G-posisjonering kan være et nasjonalt alternativ til internasjonale posisjoneringssystemer. Det skal vurderes hvordan 5G-posisjonering kan etableres i Norge, og hvilke effekter et slikt tiltak kan ha for sikkerhet og beredskap i krise og krig.

REGJERINGEN VIL

- styrke arbeidet med å detektere, analysere og fjerne kilder til forstyrrelser av GNSS-signaler i Norge
 - styrke totalforsvarets evne, både sivil side og Forsvaret, til å motstå slike forstyrrelser, blant annet med jammetester
 - styrke Nkoms tilstedeværelse i Nord-Norge gjennom å flytte Nkoms regionkontor til Tromsø
 - vurdere å etablere en nasjonal tjeneste for distribusjon av nøyaktig tid, som tilleggstjeneste og redundans til GNSS
 - vurdere mulighet for styrket nasjonal kontroll for posisjoneringstjenester med bruk av 5G-posisjonering
-

Styrket nordisk samarbeid om digital sikkerhet og beredskap

Oppover i krisespennet er kritisk infrastruktur, som mobil- og bredbåndsnett, et mål for sabotasje. I tillegg til tiltak for styrket nasjonal kontroll og styrket regional autonomi som skal gjennomføres i denne planen, vil det være et viktig løft for den digitale sikkerheten og beredskapen med tettere samarbeid på tvers av landegrensene i Norden. For eksempel vil det styrke sikkerheten for mobil- og bredbåndsnettene i Norge dersom digital trafikk kan omdirigeres via nordiske nabolands nett ved utfall som rammer nett på norsk side.

Samarbeid med nordiske naboland om sikkerhet og beredskap, med mulighet for gradert samhandling og kommunikasjon styrkes gjennom NATO medlemskap. Det kan bidra til bedre beredskap og legge forholdene bedre til rette for tettere samarbeid i Norden for sikkerhetsklarering av ressurser som utfører arbeid på kritisk digital infrastruktur.

REGJERINGEN VIL:

- arbeide for å styrke nordisk samarbeid, inkludert bruk av digitale føringsveier på tvers av landegrensene for å styrke motstandsdyktigheten til den digitale grunnmuren i nordområdene
 - arbeide for et tettere samarbeid i Norden for sikkerhetsklarering og adgangsklarering for å kunne benytte kritisk kompetanse og ressurser på tvers av landegrensene
-

Øvelser i ekomsektoren – gode hver for oss, best sammen

Ekomsektoren består av over hundre ekomtilbydere, som tilbyr mobilnett og -tjenester, bredbåndsnett og -tjenester og satellittkommunikasjon. Et fåtall av disse er underlagt norsk sikkerhetslov, grunnet betydningen infrastrukturen som deres selskap forvalter har for nasjonal sikkerhet.

Selskapene som er underlagt sikkerhetsloven, deltar i sektorens rådsstruktur for krisehåndtering, som omfatter strategisk, taktisk og operative nivåer i sektoren. Digitaliserings- og forsvaltningsdepartementet (DFD) leder strategisk sikkerhetsråd for ekomsektoren, på strategisk nivå. Nkom leder ekom beredskapsråd, på taktisk og operasjonelt nivå.

I fredstid skal ekomtilbydere konkurrere, men i kriser og krig der store deler av infrastrukturen settes ut av spill, vil det være nødvendig å samarbeide for å holde kritisk digital kommunikasjon oppe. Ekommyndigheten er derfor en pådriver for nødvendig sikkerhetssamarbeid innenfor sektoren. Det skal også legges til rette for samarbeid



mellom sektorer som har kritiske avhengigheter, for eksempel mellom kraft- og ekomsektoren.

Et viktig ledd i slikt samarbeid er øvelser. Det gjennomføres regelmessig øvelser både organisert av myndighetene og hos ekomtilbyderne. Regjeringen vil at det gjennomføres minst en årlig øvelse, eller trening, innenfor ekomsektoren, og ev. med andre myndigheter, som omfatter både strategisk, operasjonelt og taktisk nivå. Målet for øvelsene er styrket samarbeid og samhandling for mer effektiv håndtering av hendelser i kriser og krig. Øvelsen kan gjennomføres i regi av andre øvelser, for eksempel tverrsektorielle øvelser, inkludert øvelser mellom sivil og militær sektor.

REGJERINGEN VIL:

- at det gjennomføres minst en årlig øvelse innenfor ekomsektoren og ev. med andre myndigheter for å styrke samarbeidet og samhandlingen ved hendelser oppover i krisespennet
-

Styrke motstandsevnen mot digitale angrep på kritisk digital infrastruktur

I takt med den raske digitaliseringen i samfunnet, blir utfordringer knyttet til digitale angrep stadig mer komplekse. Angrepene spenner fra ikke-statlige aktører som typisk handler ut fra økonomiske incentiver, til avanserte statligstøttede trusselaktører, og statlige aktører, med hensikt å drive politisk etterretning, politisk destabilisering, sabotasje eller spionasje. Videre stiller overgangen til nye teknologier, som kunstig intelligens og kvanteteknologi, økte krav til oppdatert situasjonsforståelse og evne til å forebygge og håndtere nye trusselområder. Økt innsats og bedre kunnskap på området er nødvendig for møte denne utviklingen. I tillegg vil regjeringen at kunstig intelligens skal benyttes for å styrke motstandsevnen mot digitale angrep.

Nkoms EkomCERT er den norske ekomsektorens digitale responsmiljø i Norge og utgjør en operativ enhet med kontaktflater nasjonalt og internasjonalt. EkomCERTs samfunnsoppdrag er å bistå ekomtilbyderne med å forebygge og håndtere cyberhendelser. Dette skjer gjennom tett samarbeid mellom aktører og NSMs nasjonale responsmiljø, og ved å gi råd til bransjen rundt sikring og beste praksis. En viktig forutsetning for å kunne levere er at Nkom og sektoren har kapasitet og de riktige verktøyene.

Behovet for nasjonal kompetanse for sikkerhet og forsvar av de digitale verdiene i samfunnet øker i takt med digitaliseringen.

REGJERINGEN VIL

- at bransjen og Nkom i samråd utreder mulighetsrommet for bruk av kunstig intelligens for å styrke motstandsevnen mot og håndteringen av digitale angrep mot kritisk digital kommunikasjonsinfrastruktur
 - styrke nasjonal kompetanse for digitalt forsvar av kritisk infrastruktur
-

Styrket digital egenberedskap

Med egenberedskap menes beredskapstiltak som en person eller virksomhet skal sørge for, slik at samfunnets motstandsdyktighet øker ved hendelser oppover i krisespennet. Digital egenberedskap er tiltak for å sørge for tilgang på digitale nett og tjenester, blant annet batterier og reservestrøm for å lade mobiltelefonen. Tilgang på digitale nett og -tjenester er viktig blant annet for å kunne varsle om nødsituasjoner, for eksempel kunne ringe nødnummer og motta viktig melding fra myndighetene, for eksempel nødvarsler.

Digital egenberedskap for befolkningen

Ved hendelser oppover i krisespenntet er det viktig med digital egenberedskap som gjør befolkningen forberedt på å ta i bruk alternative løsninger når de vanlige digitale tjenestene, eller strømkilder som trengs for å opprettholde disse, ikke er tilgjengelig. Nkom har utarbeidet 5 råd for digital egenberedskap, og skal holde disse oppdatert og kommunisere de ut til befolkningen.

Digital egenberedskap for offentlige og private virksomheter

For å sikre mest mulig normal aktivitet i offentlige og private virksomheter ved hendelser oppover i krisespenntet, er det behov for å oppdatere råd for digital egenberedskap for offentlige og private virksomheter, inkludert for staten og kommuner. Rådene skal peke på mulige tiltak for å opprettholde viktige og kritiske samfunnsfunksjoner og nødvendig kommunikasjons- og samhandlingsbehov ved hendelser, i krise og i krig.

Pilot for styrket lokal involvering med digital beredskap

De regionale beredskapslagene med reservestrom og transportable basestasjoner benyttes fortrinnsvis av teleselskapene for feilretting og gjenoppsettelse. Forsvaret benytter også slike løsninger for taktisk dekning. Ved hendelser høyt oppe i krisespenntet, kan behovet for rask gjenoppsettelse være stort, og tilgang på slike ressurser bli begrenset.



For å vurdere muligheten for styrket lokal involvering, skal det gjennomføres en pilot som involverer kommuner eller andre relevante lokale ressurser, og som bygger opp erfaringer om digital egenberedskap for kommunene. Målet er å styrke den lokale evnen til å gjenopprette mobildekning, i de tilfeller der tilgang på normal rettekapasitet er begrenset. Piloten kjøres i samråd med utvalgte kommuner, og i tett dialog med lokale beredskapsråd, og teleselskapene.

Resultat fra piloten vil inngå i rådene for egenberedskapen.

REGJERINGEN VIL:

- styrke arbeidet med digital egenberedskap for å ivareta kommunikasjon og samhandling ved hendelser oppover i krisespennet
 - utarbeide råd for digital egenberedskap for offentlige og private virksomheter
 - gjennomføre en pilot der kommunene selv kan gjenopprette mobildekning ved utfall, med mål om å styrke den lokale beredskapsevnen i kommunene
-





3. Gjennomføring av sikkerhetsplanen

Sikkerhetsplanen er delt i ulike innsatsområder med tilhørende tiltak. For å sikre en helhetlig oppfølging av planen, og at tiltakene får nødvendig prioritet hos tilbyderne, etableres et program med en styringsstruktur med berørte parter. Programstrukturen skal sørge for at innsatsområdene og tiltakene sees i sammenheng regionvis.

Flere av tiltakene forutsetter betydelig statlig og kommersiell finansiering gjennom perioden for gjennomføring.

Organisering av gjennomføringen av sikkerhetsplanen

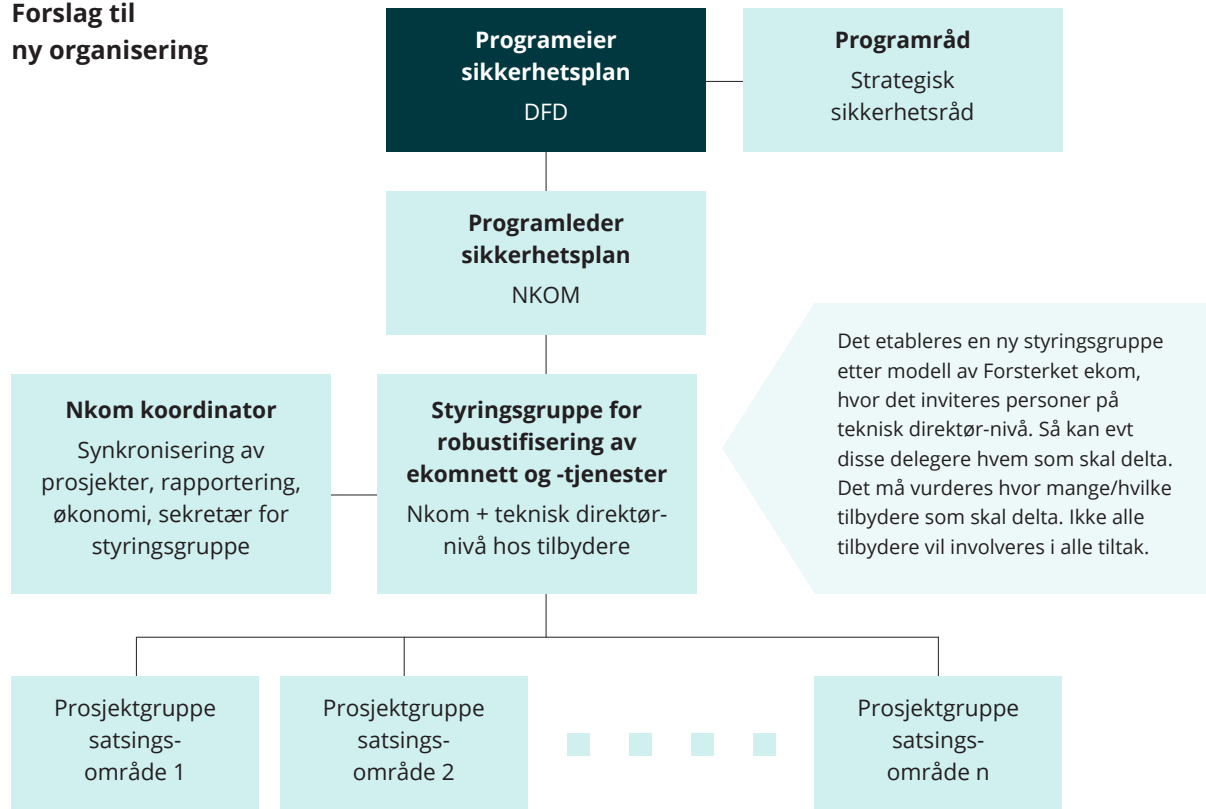
Det opprettes et program for gjennomføringen av sikkerhetsplanen som eies av DFD og som Nkom leder.

Strategisk sikkerhetsråd for ekomsektoren vil i praksis fungere som et programråd. Programrådet følger de store linjene for sikkerhetsplanen. For å sikre eierskap til gjennomføringen i hele verdikjeden i ekomsektoren, vil de eksisterende beredskapsrådene som ledes av DFD og Nkom, benyttes i gjennomføringen av sikkerhetsplanen. Ekom beredskapsråd får anledning til å gi innspill til gjennomføringen av sikkerhetsplanen, blant annet basert på erfaringer med hendelser og teknologisk utvikling som kan bidra til styrket beredskap.

For mer regelmessig og tettere oppfølging av gjennomføringen av sikkerhetsplanen, etableres det en styringsgruppe for alle områdene, som bygger på erfaringer fra organiseringen i programmet for forsterket ekom.

Det opprettes ulike prosjektgrupper for alle satsingsområdene. De bestående prosjektgruppene opprettholdes der det passer inn i denne strukturen.

Forslag til ny organisering



Programstrukturen etableres på strategisk og operasjonelt nivå med mål om å sikre prioritet og fremdrift, sikre raske avklaringer og vurdere om det er behov for å justere kursen, for eksempel ved videre utvikling i den sikkerhetspolitiske situasjonen eller teknologisk innovasjon og mulighetsrom.

Programstrukturen er forankret i Strategisk sikkerhetsråd, som er øverste ledd i rådsstrukturen i ekomsektoren.

Ordliste

Digitale føringsveier	Digitale føringsveier er fysiske traseer som brukes til å føre og beskytte elektronisk kommunikasjonsinfrastruktur, som for eksempel, fiberkabler, strømledninger eller annen IKT-relatert infrastruktur.
Ekom	Elektronisk kommunikasjon (ekom) er kommunikasjon som bruker elektroniske signaler og nettverk for å overføre informasjon, som lyd, tekst, bilder og data, blant annet mobil-, bredbåndsnett og satellitt-kommunikasjon.
EkomCERT	EkomCERT er det nasjonale digitale responsmiljøet for den norske ekomsektoren, etablert og driftet av Nasjonal kommunikasjonsmyndighet (Nkom). EkomCERT fungerer som et Computer Emergency Response Team (CERT) og har som hovedoppgave å håndtere, koordinere og forebygge alvorlige digitale hendelser som påvirker elektronisk kommunikasjon i Norge.
Ekominfrastruktur	Ekominfrastruktur er den fysiske infrastrukturen som muliggjør elektronisk kommunikasjon – som rør, kabler, master, antenner, skap og teknisk utstyr.
Ekomnett	Ekomnett er et system for overføring av signaler og data, for eksempel tale, tekst, lyd, bilde. Eksempler på ekomnett er mobilnett, bredbåndsnett og satellittnett.
Ekomsektoren	Ekomsektoren omfatter alle aktører som er involvert i overføring og håndtering av elektronisk kommunikasjon i samfunnet.
Ekomtilbyder	En ekomtilbyder er en person eller virksomhet som tilbyr elektroniske kommunikasjonstjenester eller ekomnett til andre. Eksempler er mobiloperatører og bredbåndsløseleverandører.
GNSS	GNSS står for Global Navigation Satellite System, og er et satellitt-basert system som gir posisjons-, navigasjons- og tidsinformasjon til brukere over hele verden. Kjente GNSS-systemer er GPS (USA), GLONASS (Russland), Galileo (EU) og BeiDou (Kina).

Jamming	Jamming er en bevisst handling som har som mål å forstyrre eller blokkere radiokommunikasjon eller signaler ved å sende ut kraftige forstyrrende signaler på samme frekvens eller kanal.
Lavbanesatellitt	En lavbanesatellitt (på engelsk ofte kalt LEO-satellitt – Low Earth Orbit satellite) er en satellitt som går i bane rundt jorden i relativt lav høyde, typisk 500-1500 kilometer over jordoverflaten.
Nasjonal kontroll	Nasjonal kontroll innebærer styringsevne til å ta effektive beslutninger gjennom for eksempel regulering, eierskap eller avtaler, og handlefrihet til å gjennomføre beslutninger mest mulig uavhengig av utenlandske aktører og innsatsfaktorer.
Nasjonal skytjeneste	Nasjonal skytjeneste er en skybasert IT-plattform som tilbys innenfor et lands grenser og under nasjonal kontroll, med mål om å sikre datatrygghet, digital suverenitet og tilgjengelighet for offentlig sektor og kritiske samfunnsfunksjoner.
PNT	PNT står for Positioning, Navigation, and Timing – det vil si posisjonerings-, navigasjons- og tidstjenester.
Regional autonomi	Regional autonomi betyr at tjenester fungerer i regionen, uavhengig av tilkobling mot andre regioner, eller resten av verden. Regional autonomi innebærer også at en region har mulighet for å kontrollere, drifte og vedlikeholde elektronisk kommunikasjonsnettverk innen sitt geografiske område.
ROS-analyser	ROS-analyse står for Risiko- og sårbarhetsanalyse, og er en systematisk gjennomgang for å identifisere mulige uønskede hendelser, vurdere hvor sannsynlige de er, og hvilke konsekvenser de kan ha for mennesker, miljø, verdier og samfunnsfunksjoner.
Spoofing	Spoofing er en teknikk hvor signaler bevisst manipuleres slik at brukerne kan få feil posisjonsinformasjon inn i sine systemer.
Transportnett	Transportnett er den delen av et elektronisk kommunikasjonsnett som sørger for kommunikasjonen mellom sentrale knutepunkter – ofte mellom byer, regioner eller datasentre.

Foto

Forsiden

Illustrasjonsfoto datasenter. Foto: iStock

Telemast. Foto: Telenor Towers

Illustrasjonsfoto smarttelefon. Foto: Anders Martinsen

Side 1

Basestasjon på Hardangervidda. Foto: Amund Ringen Jøråsen/Telenor

Side 2

Illustrasjonsfoto Telemast. Foto: Telenor Norge

Illustrasjonsfoto oljeplattform. Foto: iStock

Illustrasjonsfoto tastatur. Foto: iStock

Illustrasjonsfoto mennesker. Foto: iStock

Side 5

Test av militær dekningsforlengelse. Foto: Henning Huuse/Telia

Side 6

Flom i Feda i Agder, 2015. Foto: Anders Martinsen

Side 7

Illustrasjonsfoto Telemast. Foto: Anders Martinsen

Side 8

Test av mobile basestasjoner. Foto: Henning Huuse/Telia

Side 9

Test av mobil befolkningsvarsling. Foto: DSB

Side 10

Illustrasjonsfoto jernbane. Foto: Nkom

Illustrasjonsfoto mobiltelefon. Foto: Adobe Stock

Illustrasjonsfoto satellitt. Foto: Space Norway

Fiberbrudd i Ål kommune. Foto: Nkom

Side 12

Longyearbyen, Svalbard. Foto: Sophie Cordon/Visit Svalbard

Side 15

Forsterket ekom. Illustrasjon: Nkom

Side 16

Lillesand. Foto: Anders Martinsen

Side 17

Illustrasjonsfoto basestasjon. Foto: Telia Norge

Side 18

Fiberbrudd i Ål kommune under ekstremværet Hans 2023. Foto: Nkom

Side 21

Fjernstyrt tårn. Foto: Øystein Løwer/Avinor

Side 22

Illustrasjonsfoto satellitt. Foto: Space Norway/FFI

Side 24

Andøya i Nordland. Foto: David Jensen

Side 27

Jammetest på Andøya. Foto: Nkom

Side 29

Egenberedskap. Foto: Daniel Fatnes/DSB

Side 30

Illustrasjonsfoto mobiltelefon. Foto: Adobe Stock

Side 31

Illustrasjonsfoto drone. Foto: Anders Martinsen

Illustrasjonsfoto person. Foto: iStock

Illustrasjonsfoto tastatur. Foto: Muha Ajjan/Unsplash

Skader på strømstolper. Foto: Anders Martinsen

Side 37

Illustrasjonsfoto smarttelefon. Foto: Anders Martinsen



Utgitt av: Digitaliserings- og forvaltningsdepartementet

Bestilling av publikasjoner:
Departementenes sikkerhets- og serviceorganisasjon
publikasjoner.dep.no
Telefon: 22 24 00 00
Publikasjoner er også tilgjengelige på:
www.regjeringen.no

Publikasjonskode: D-2013 B
Foto: oversikt s. 36
Design: TIBE Oslo
Trykk: Departementenes sikkerhets- og serviceorganisasjon
09/2025 – opplag 100

