DET KONGELIGE
SAMFERDSELSDEPARTEMENT

St.meld. nr. 47

(2000-2001)

Telesikkerhet og -beredskap i et telemarked med fri konkurranse

Tilråding fra Samferdselsdepartementet av 11. mai 2001, godkjent i statsråd samme dag.

1 Innledning og sammendrag

1.1 Innledning

Det moderne samfunnet omtales ofte som *informasjonssamfunnet*. Et grunnleggende kjennetegn som særpreger informasjonssamfunnet er evnen til å formidle store mengder informasjon hurtig, over store avstander og til lav pris. Tilgangen til opplysninger, fakta og vurderinger er enorm, og mulighetene for å informere eller rådføre seg med andre blir både flere og enklere.

Utviklingen av informasjonssamfunnet hadde ikke vært mulig uten utviklingen innen og utbredelsen av informasjonsteknologi og telekommunikasjon. Rimelig informasjonsteknologi og telekommunikasjonsteknologi gjør det lønnsomt for markedet å bygge opp nye typer tjenester basert på denne teknologien.

Parallelt med utviklingen innen informasjons- og kommunikasjonsteknologi (IKT) ser vi en økende globalisering innen mange samfunnsområder. Utviklingen innen telekommunikasjon gir oss verdensomspennende nett for telekommunikasjon over nasjonale grenser, og gir dermed nye muligheter for alternativ organisering, lokalisering og styring av virksomheter.

Vi ser en økende gjensidig avhengighet mellom ulike samfunnsområder. Alvorlige forstyrrelser på et område kan få store ringvirkninger for andre funksjoner. I denne sammenheng kan det være interessant å skille mellom:

– funksjoner som svært mange andre funksjoner er avhengig av, og
– funksjoner som selv er avhengig av svært mange andre funksjoner.

Ut fra en slik vurdering vil en kunne finne de funksjonene som er mest viktig for øvrig samfunnsvirksomhet. En vil også se hvilke funksjoner som er sårbare hvis annen samfunnsvirksomhet svikter. En slik vurdering gjenspeiles i figur 1.1.

	Ledelse/informasjon	Kraftforsyning	Telekommunikasjon	Olje og drivstoff	Transport	Arbeidskraft	Vannforsyning	Bank- og pengevesen	Bygg og anlegg	Industri og varehandel	Helse	Ernæring	Brann/redning	Politi/orden
Ledelse/informasjon		XX	XX			X			X				X	XX
Kraftforsyning	X		XX	X	XX	X				X			X	
Telekommunikasjon	X	XX			X	X				X			X	
Olje og drivstoff	X	XX	X		XX				X	X			X	
Transport	X	X	X	XX		XX			XX	X			X	X
Arbeidskraft	XX	XX	XX		X		X	XX			X	XX		
Vannforsyning	X	XX	X							X				
Bank- og pengevesen	XX	XX	XX										X	
Bygg og anlegg	X	X	X	XX	XX	XX		XX		X				
Industri og varehandel	X	XX	XX	XX	XX	XX	X	XX					X	
Helse	X	XX	XX		XX	XX	XX			XX		XX	X	X
Ernæring	X	XX	XX		XX	XX	XX	XX		XX				
Brann/redning	XX	X	XX		XX	X	XX		X					XX
Politi/orden	XX	X	XX		X	X								

Kryss langs kolonnen angir at funksjonen er nødvendig for funksjonene i linjene

Kryss langs linjen angir at funksjonen er avhengig av funksjonene i kolonnene

Figur 1.1 Viktige samfunnsfunksjoners gjensidige avhengighet. To kryss angir sterk avhengighet, ett kryss angir en mer usikker avhengighet.

Kilde: Forsvarets forskningsinstitutt «Beskyttelse av samfunnet», 1997.

Det er spesielt de tre funksjonene kraftforsyning, telekommunikasjon og ledelse/informasjon som skiller seg ut som vesentlige for all samfunnsvirksomhet. Disse finnes ved å se på hvilke funksjoner som har flest kryss langs sin kolonne i figur 1.1. Svikt innen en av disse funksjonene vil kunne medføre svikt i mange andre samfunnsfunksjoner, og de kan således betraktes som bærebjelker som må være intakte for at samfunnet skal fungere. De sterke gjensidige avhengighetene i samfunnet er forhold som bidrar sterkt til det moderne samfunnets sårbarhet, og dette vil sannsynligvis forsterkes de kommende år.

Samtidig med samfunnets økende avhengighet av telesektoren, har telesektoren i løpet av få år gjennomgått store endringer. Utviklingen har gått fra et statlig Televerk med enerett til et konkurransemarked med mange aktører, en utvikling en også finner i de fleste andre land i den vestlige verden. En rask teknologisk utvikling har gitt sterk vekst i teletjenestenes funksjonalitet og kapasitet. Internett har vært viktig i denne utviklingen. Utviklingen har videre ført til en globalisering både med hensyn til eierstrukturer innen telebransjen og i telenettenes utbredelse. Etter murens fall står vi nå også overfor et helt nytt og annerledes trusselbilde enn tidligere der høyteknologiske trusler blir stadig viktigere.

Samlet sett fører denne utviklingen til et mye mer komplekst og uoversiktlig bilde enn tidligere, som setter helt nye krav til myndighetenes rolle. Økt avhengighet av telekommunikasjon, mange nye aktører og rask teknologisk

utvikling gjør det nødvendig for myndighetene å ta i bruk andre virkemidler enn tidligere for å oppnå et sikkert samfunn.

Økt avhengighet og konsekvensene av svikt understreker viktigheten av å iverksette forebyggende tiltak innenfor telesikkerhet og teleberedskap, noe som har blitt demonstrert ved flere anledninger i de siste par år, jf. graveuhellet utenfor Kristiansand sommeren 2000 der bl.a. Kjevik lufthavn mistet teleforbindelsene. Også Telenors teletrafikk i regionen, som omfatter store deler av Aust- og Vest-Agder, ble lammet, og dette gjaldt også nødmeldingstjenesten. Betydningen av og effekten av ikke å ha tiltak som alternative transportnett og separate framføringsveier ble slik klart demonstrert.

Telekommunikasjon er som vist i figur 1.1 et område som mange andre samfunnsfunksjoner er avhengig av. Sårbarhetsreduserende tiltak innenfor denne sektoren vil derfor få betydning for en rekke andre funksjoner og således komme samfunnet som helhet til gode. Robuste telekommunikasjoner vil ha avgjørende betydning for beskyttelse av samfunnet ved at sentrale funksjoner i den normale samfunnsvirksomhet i fred og krig kan opprettholdes. For å sikre samfunnet tilgang til robuste telekommunikasjoner må staten påse at det implementeres sikkerhets- og beredskapstiltak i de offentlige telenett. Samferdselsdepartementet vil i denne meldingen skissere en strategi for telesikkerhet og -beredskap tilpasset en telesektor i fri konkurranse.

1.2 Sammendrag

Hendelser som forårsaker svikt i telekommunikasjon kan ha utspring i mange ulike årsaker. En skiller gjerne mellom villede og ikke-villede hendelser. Ikke-villede hendelser kan være tekniske feil eller ødeleggelser som følge av naturgitte fenomener som storm, flom og lynnedslag etc. Også menneskelig svikt og feiloperasjoner inngår i denne kategorien. Slike hendelser vil skje, men må minimeres både i antall og konsekvens.

Villede hendelser er hendelser som har sin årsak i menneskers bevisste handlinger for å skade eller forårsake problemer på annen måte. Motivet og kapasiteten til de som står bak vil være forskjellig, og vil kunne befinne seg i et spenn fra rene barnestreker til velstrukturerte og omfattende angrep fra høyt kompetente individer.

Grovt sett vil trusselen mot telenettene innbefatte følgende fem hovedkategorier av anslag og virkemidler:

- Anslag med fysiske virkemidler mot infrastruktur
- Anslag med elektroniske virkemidler mot infrastruktur
- Manipulasjon med informasjonssystemer innen telefunksjonen
- Overbelastning av telenettene
- Sosiale trusler mot beslutningstakere i driftsfunksjonen i telenettene

I en normalsituasjon er det mest sannsynlig at virkemidlene vil kunne forekomme enkeltvis eller i enkle kombinasjoner. I mer omfattende situasjoner vil trusselbildet være mer komplekst og kunne omfatte en rekke ulike virkemidler i kombinasjon.

Sannsynligheten for alvorlig og langvarig svikt i teletjenester vurderes ut fra dagens trusselbilde til å være liten overfor fysiske angrep. Logiske angrep ved forsøk på inntrenging i telenettenes IT-systemer anses i dag som en større

reell trussel. Konsekvensene som følge av slike angrep kan raskt bli alvorlige for større eller mindre deler av samfunnet. Dersom sikkerhetspolitiske kriser eller økt terror etc. inntreffer, øker imidlertid den menneskeskapte fysiske trusselen mot teletjenestene, og dermed også sannsynligheten for omfattende, alvorlig og langvarig svikt. Konsekvensene for Totalforsvarets og samfunnets støtte til det militære forsvaret kan i så fall være svært alvorlige.

1.2.1 Telepolitikk og teleberedskap

Hovedmålene for telepolitikken i Norge er å sikre at alle husstander og bedrifter over hele landet får tilgang til grunnleggende teletjenester av høy kvalitet og til lavest mulige priser, samt å legge til rette for størst mulig verdiskapning og effektiv bruk av ressurser som nyttes til utbygging og tjenesteyting innenfor sektoren.

Fra 1. januar 1998 ble de siste eneretter i telesektoren avviklet, og det ble etablert alminnelig konkurranse innenfor alle deler av telemarkedet i Norge. Den markedsmessige og tekniske utviklingen på teleområdet medfører at den samfunnsmessige styringen av sektoren baseres på regulatoriske virkemidler. Gjeldende regulatorisk rammeverk er utformet bl.a. med sikte på å få i stand overgangen fra monopolsituasjonen til en konkurransesituasjon. Regelverket fokuserer på å etablere et konkurranseutsatt marked der nye aktører gis innpass.

Europakommisjonen fremmet 12. juli 2000 utkast til nytt rammeverk på området for elektronisk kommunikasjon. Forslagene er nå til behandling i Det europeiske råd og Europaparlamentet, og forventes å tre i kraft i 2002/2003.

Reguleringsforslagene fra Europakommisjonens side omhandler i liten grad sikkerhet og beredskap, selv om det legges opp til god funksjonalitet og at det skal sikres et høyt nivå for vern av brukerne. I tillegg presiseres det i direktivutkastet om tillatelser at rettsakten ikke er til hinder for at statene sikrer allmenne interesser som er anerkjent i traktaten, herunder beredskaps- og sikkerhetshensyn.

Sikkerhet og beredskap i elektroniske nettverk står på dagsorden i EU. Det europeiske råd vil sammen med Europakommisjonen utarbeide en samlet sikkerhetsstrategi for elektroniske nett. Det antas at det i første omgang er aktuelt å lage en handlingsplan, og at det på sikt eventuelt kan være aktuelt å opprette et europeisk organ som styrer sikkerhetsarbeidet innen sektoren.

For å få operatørene til å investere i tiltak rettet mot telesikkerhet og teleberedskap kan det være nødvendig med regulatoriske virkemidler gjennom lov, forskrifter eller enkeltvedtak. Någjeldende telelov inneholder bestemmelser som på visse vilkår gir telemyndigheten kompetanse til å gi pålegg og fastsette forskrifter om sikringstiltak i telenett og teletjenester.

Telenor har i sin konsesjon krav om leveranse av spesielle samfunnspålagte oppgaver (SSO) som bl.a. omfatter ytelser til Totalforsvaret. Merkostnader forbundet med disse oppgavene er fra og med 1998 blitt dekket gjennom offentlig kjøp av tjenester over statsbudsjettet. Utførelse av spesielle samfunnsoppgaver er pålagt Telenor i kraft av selskapets ledende posisjon på det norske telemarkedet. Prinsipielt, og i henhold til gjeldende telelov med forskrifter, er det ingen hindring for at også andre aktører kan pålegges å utføre spesielle samfunnspålagte oppgaver. I et etablert og velfungerende marked

kan det dessuten være hensiktsmessig og effektivitetsfremmende å la flere aktører konkurrere om samfunnsoppgavene. En forutsetning for å innføre konkurranse om disse oppgavene vil imidlertid være at flere aktører har opparbeidet betryggende evne til å ivareta oppgavene på en tilfredsstillende og kontinuerlig måte i hele eller deler av landet.

1.2.2 Strategi for telesikkerhet og -beredskap tilpasset den nye markedssituasjonen

I et telemarked der flere operatører etter hvert begynner å få en relativt betydelig posisjon, enkelte også med egen infrastruktur, er det ikke tilstrekkelig at kun én operatør er pålagt å levere teleberedskapstjenester. I 1999 hadde Tele2 og Enitel til sammen en markedsandel på over 10 prosent for offentlig telefontjeneste. Vi kan dermed regne med at en del viktige brukere i Totalforsvaret har fasttelefonabonnement hos andre tilbydere enn Telenor, uten at det foreligger spesielle beredskapsforpliktelser. Et nytt konsept for teleberedskap vil innebære at flere operatører i tillegg til Telenor pålegges slike beredskapsforpliktelser. Teleloven gir rettsgrunnlag om sikring av telenett også for andre tilbydere.

Bruken av mobiltelefoner har økt kraftig de senere år, med den konsekvens at samfunnet i større grad er avhengig av mobiltelefon som kommunikasjonsmiddel. Også innenfor Totalforsvaret blir deler av kommunikasjonsbehovet dekket gjennom bruk av mobiltelefon, og det er derfor viktig at mobiltelefon kan brukes også i ulike krisesituasjoner. Det nye konseptet vil også omfatte tiltak rettet mot mobiltelefoni.

Ved utformingen av den nye strategien for telesikkerhet og teleberedskap har Samferdselsdepartementet tatt utgangspunkt i anbefalingene fra Forsvarets forskningsinstitutt (FFI) i prosjektet Beskyttelse av samfunnet 2 (BAS2) om sårbarhetsreduserende tiltak innen telekommunikasjon og det frittstående TIFKOM-prosjektet, jf. nærmere omtale i vedlegg 1. Samferdselsdepartementet har fått nærmere utredet og kvalitetssikret de mest sentrale forslagene i TIFKOM-rapporten. TIFKOM-prosjektets sluttrapport har også vært sendt på bred høring, bl.a. til de øvrige departementene og en rekke aktører i telesektoren. Det er enighet blant høringsinstansene om at rapporten bør få en rask oppfølging. Sårbarhetsutvalget støtter i all hovedsak TIFKOM-prosjektets forslag.

1.2.3 Ulike elementer i en ny strategi for telesikkerhet og -beredskap

I den nye strategien for telesikkerhet og -beredskap vil det inngå en rekke fysiske og teletekniske tiltak, i tillegg til administrative og organisatoriske tiltak.

1.2.3.1 Post- og teletilsynet tillegges ansvar for telesikkerhet og -beredskap

Uansett hvilket nivå som velges for sikkerhet og beredskap i telenettene så vil myndighetene måtte tillegges omfattende oppgaver på området. I regjeringens fornyelsesprogram for offentlig sektor er det uttrykt en klar målsetting om å begrense/redusere antallet tilsynsenheter i statsforvaltningen. På teleområdet finnes det gjennom Post- og teletilsynet allerede et spesialisert til-

synsorgan som gjør det naturlig at også ansvaret for telesikkerhet og -beredskap legges dit. Samferdselsdepartementet har derfor besluttet å delegere et særskilt myndighetsansvar for telesikkerhet og -beredskap til Post- og teletilsynet med følgende ansvarsområder:

– Sette krav til telesikkerhet og teleberedskap, og vurdere investeringer i tiltak for å øke robustheten i telenettene.
– Føre tilsyn med at pålagte tiltak blir iverksatt.
– Bevisstgjøring, kompetanseheving og veiledning overfor operatører, brukere og andre aktører (kurs, seminarer, bedriftsbesøk, etablering av kompetansefora etc.).
– Arrangere samøvelser og utvikle samarbeid mellom teleoperatørene.

Det vil være naturlig og ønskelig å integrere sikkerhets- og beredskapsarbeidet i den øvrige forvaltningen av telesektoren. Ved å legge også myndighetsansvaret for telesikkerhet og -beredskap til Post- og teletilsynet får teleoperatørene ett felles kontaktpunkt mot myndighetene. I Post- og teletilsynet vil det dessuten være god tilgang på relevant fagkompetanse.

Arbeidet med telesikkerhet og -beredskap må innplasseres i eksisterende organisasjon slik at det ikke oppstår noe motsetningsforhold/habilitetsproblematikk i forhold til andre arbeidsoppgaver.

Samferdselsdepartementet regner med at man for å få et kompetent sikkerhets- og beredskapsmiljø bør ha en bemanning på minimum 4-7 personer. Bemanningsstørrelsen må tilpasses ambisjonsnivået for funksjonen. Dessuten må det foretas en nøye avveining mellom den kompetanse tilsynet selv må ha og den kompetanse man kan kjøpe utenfra i tilknytning til de enkelte prosjekter. Departementet mener at man bør foreta en forsiktig og skrittvis oppbygging av dette feltet.

Post- og teletilsynet vil måtte forholde seg til en rekke andre organisasjoner og enheter som har oppgaver relatert til sikkerhet og beredskap. Totalforsvarets råd for sikring av tele- og informasjonssystemer (TRSTI) ble opprettet 1. mars 1998. TRSTI skal i henhold til sitt mandat gi råd til Samferdselsdepartementet i sikkerhets- og beredskapsspørsmål på teleområdet. Departementet mener at TRSTI i fremtiden også bør bli en viktig medspiller for Post- og teletilsynet.

Ansvarsfordelingen mellom Post- og teletilsynet og det myndighetsorgan som etter den nye sikkerhetsloven skal utøve oppgaven som Nasjonal sikkerhetsmyndighet (NSM) er vurdert i samråd med Forsvarsdepartementet. NSM har koordinerings- og kontrollansvaret, i praksis fagmyndighetsansvaret, for alle forebyggende sikkerhetstiltak. Post- og teletilsynet bør kontrollere at de prosedyremessige eller tekniske sikkerhetstiltak som foreskrives i sikkerhetslov med forskrifter, ses i sammenheng med de sikkerhetsmessige krav som det ellers vil være aktuelt å stille for telesektoren.

Sårbarhetsutvalget har i sin utredning bl.a. foreslått at det bør etableres et Senter for informasjonssikring som bør ha som oppgave å koordinere deler av innsatsen for å styrke IKT-sikkerheten og bidra til en mer robust IKT-infrastruktur. Senter for informasjonssikring vil primært være et samarbeidsforum for private og offentlige interessenter, og skal ha som hovedoppgave å varsle deltakerne om trusler og sårbarhet mot IT-systemer. Senteret skal ikke ha myndighetsoppgaver. Ettersom Post- og teletilsynet og Senter for informasjonssikring vil ha ulike, men beslektede ansvarsområder, mener Samferd-

selsdepartementet at tilsynet og senteret vil være komplementære og ikke konkurrerende enheter. Nærings- og handelsdepartementet har våren 2001 etablert et forprosjekt med deltakelse fra flere departementer som bl.a. skal avklare forhold omkring formålet med et slik senter, arbeidsoppgaver, organisering, lokalisering/tilknytning samt økonomiske og administrative konsekvenser. Det legges opp til at regjeringen vil komme tilbake til dette.

1.2.3.2 Tiltak for økt telesikkerhet og -beredskap

Post- og teletilsynet vil få ansvar for å påse at en rekke ulike tiltak for å øke sikkerheten og beredskapen i telenettene blir iverksatt. Det må raskt innføres en ny prioritetsordning i telenettene til erstatning for ordningen med viktig prioritert telefon (VPT) som ble nedlagt fra årsskiftet 2000/2001. En ny *prioritetsordning* må omfatte alle tilbydere av offentlig telefontjeneste både i faste nett og mobilnettene, og skal sikre at forhåndsdefinerte viktige abonnenter får prioritet i situasjoner der nettene eller deler av nettene er overbelastet. En ny prioritetsordning må bl.a. gi øyeblikkelig prioritet til nødnumre fra mobiltelefoner. Prioritetsordningen må være tilpasset den internasjonale teleunions (ITUs) anbefaling om prioritet i telenettene på tvers av landegrensene. En ny prioritetsordning vil for øvrig måtte baseres på nærmere definerte krav utarbeidet av Post- og teletilsynet.

I et kommersielt telemarked er det viktig å sikre viktige installasjoner (sentraler og knutepunkter) til alle tjenesteleverandører av betydning. TIFKOM-prosjektet tilrår at vitalt telekommunikasjonsutstyr bør plasseres i fjellanlegg med god beskyttelse mot fysiske trusler som f.eks. bombing og elektromagnetisk stråling. Dette er utstyr av høy verdi eller utstyr som det tar lang tid å gjenanskaffe ved ødeleggelse og som er viktig for at telenettene skal fungere. TIFKOM-prosjektet foreslår videre at fjellanlegg som Telenor i dag eier bør benyttes til dette formålet ved at de oppgraderes til *sikrede samlokaliseringssentra* hvor også andre teleoperatører kan plassere vitalt telekommunikasjonsutstyr. Det er foreslått samlokalisering i til sammen 15 fjellanlegg, der 10 overtas fra Telenor i tillegg til at det bygges 5 nye anlegg. Forslaget har en kostnadsramme på 1,9 mrd. kr.

Med den sikkerhetspolitiske situasjon vi har i Norge i dag, er det ikke den fysiske trusselen mot telenettene som er mest fremtredende, og det kan derfor stilles spørsmål om hvor mye ressurser det er riktig å bruke på beskyttelse mot fysiske trusler. På denne bakgrunn anbefaler Samferdselsdepartementet at det for eksisterende utstyr og installasjoner som ikke allerede er lokalisert i fjell, ikke stilles krav om at teleoperatører som leverer teletjenester til Totalforsvaret skal sikre vitalt telekommunikasjonsutstyr i fjellanlegg. Post- og teletilsynet får imidlertid i oppgave å legge til rette for at det for fremtidige installasjoner skal finnes en mulighet for samlokalisering i fjellanlegg for de operatører som leverer tjenester til Totalforsvaret. Samlokalisering i det omfang TIFKOM-prosjektet skisserer, og med de kostnader dette medfører, anses uansett for å være urealistisk å gjennomføre, jf. nærmere omtale i kapittel 7.

Post- og teletilsynet bør følge utviklingen i utbygging av teleinfrastrukturen nøye og gjennom pålegg og ulike samarbeidstiltak sørge for *økt redundans* [1)] i telenettene. Samferdselsdepartementet mener det vil bli spesielt viktig å få til et samarbeid mellom operatører med landsdekkende transportnett,

med tanke på etablering av flere sammenkoblingspunkter mellom disse nettene. Et slikt samarbeid behøver ikke koste mer for tjenesteleverandørene. Med bakgrunn i dagens trusselbilde mener departementet det er forsvarlig å prioritere tiltak for å øke redundansen fremfor å benytte ressursene på samlokalisering i fjellanlegg.

TIFKOM-prosjektet anser at det eksisterer et stort behov for statlig koordinering og tilrettelegging av telekommunikasjonsløsninger for de brukergruppene som har behov for ekstra sikkerhet og robuste teletjenester. Ved slik koordinering vil en kunne oppnå betydelige synergieffekter. Det er viktig å få en felles, kostnadseffektiv utnyttelse av sivile og militære sambandsressurser. TIFKOM-prosjektet har pekt på at dersom et eventuelt nytt *felles radiosamband for nødetatene så langt som mulig baseres på Forsvarets digitale nett (FDN)*, som suppleres med sikkerhetsmessig tilfredsstillende kommunikasjonsresurser fra de allmenne nett, kan denne kombinasjonen samlet danne et godt fundament for å sikre prioriterte brukere i Totalforsvaret tilgang til ekstra robuste mobilkommunikasjonsløsninger. Forsvarets tele- og datatjeneste (FTD) er i ferd med å gjennomføre et omfattende arbeid for å kartlegge hvor stor del av et eventuelt landsdekkende radionett for nødetatene som kan etableres med basis i FDN og de økonomiske betingelser knyttet til dette. Det som gjenstår og som må utredes videre når dette arbeidet er avsluttet, er hvilke betingelser Forsvaret stiller til aktuelle brukere av et nytt nødnett dersom FDN skal benyttes.

For å gjøre det enklere å samordne innsatsen fra flere aktører under kriser og ulykker, bør også prioriterte brukere i Totalforsvaret utenom nødetatene politi, helse og brann gis mulighet til være brukere av et eventuelt nytt nødnett. Eventuell utbygging av et nytt nødnett gjør imidlertid ikke at man kan se bort fra sikringstiltak i de offentlige nett. Selv om et radionett for nødetatene tilsynelatende vil være et eget lukket telenett, vil også dette nettet være avhengig av ressurser i de offentlige nett for at det skal fungere etter hensikten.

En rekke andre tiltak vil også være aktuelle for å sikre god sikkerhet og -beredskap i norske telenett. Det må investeres i transportabelt *beredskapsutstyr* for å styrke telekommunikasjonssektorens reparasjonsberedskap og rehabiliteringsevne. Transportabelt beredskapsutstyr skal kunne settes inn i telenettene ved trafikkbrudd eller ved fare for trafikkbrudd på steder hvor brudd vil medføre alvorlige konsekvenser for samfunnet både i fredstid og i krigstid.

Det er videre utarbeidet utkast til *forskrift om sikring av telekommunikasjonsanlegg mot elektromagnetisk puls*. Det vil også bli vurdert å innføre et krav om *nasjonal autonomi* [2)] i telenettene. I tillegg kommer en rekke administrative sikkerhets- og beredskapstiltak som f.eks. *bevisstgjøring, kompetanseheving og veiledning* innen telesikkerhet og -beredskap, utvikling av en *klassifiseringsordning for teleinfrastrukturen*, gjennomføring av *sikkerhetsevaluering av teleinfrastrukturen* i samarbeid med teleoperatørene, samt planlegging og gjennomføring av *samøvelser* for operatørene. Det er også anbefalt å implementere tiltak for å bedre informasjonssikkerheten i telenettene. For å hindre

---

[1)] Med redundans menes omrutingsalternativer eller reserveløsninger i den enkelte operatørs nett eller mellom ulike operatørers nett.

[2)] Nasjonal autonomi innebærer at det skal være mulig å kommunisere innenfor nasjonens grenser uten å være avhengig av driftsstøtte fra utlandet.

at uvedkommende får tilgang til operatørenes drifts-, vedlikeholds- og støttesystemer, bør bl.a. operatørene få krav om å utarbeide en *oversikt over viktige system* og hvordan disse, f.eks. driftssystemet, er koblet mot det øvrige nettverket. Et annet tiltak for økt informasjonssikkerhet er bruk av *betalte hacker-oppdrag* for å avdekke svakheter i operatørenes IT-systemer.

*Internett*antas i løpet av få år å tilby mange av de samfunnskritiske tjenestene som de tradisjonelle teletjenestene i dag utfører. I hvilken grad disse tjenestene på Internett vil overta eller supplere tilsvarende tradisjonelle tjenester gjenstår å se. Utviklingen vil mest sannsynlig medføre at Internett får økende betydning som kommunikasjonskanal for en rekke tjenester som i gitte situasjoner vil være av avgjørende betydning for å opprettholde samfunnsviktige funksjoner. Dette tilsier at samfunnet, ut fra risiko- og sårbarhetshensyn, har et behov for å arbeide systematisk med sikte på å øke Internetts robusthet mot alvorlige tekniske feil, fysisk sabotasje og - ikke minst - logiske angrep fra stater eller organisasjoner med tilgang til etterretningsinformasjon, kunnskap og teknologi.

I fremtiden kan det følgelig bli behov for å iverksette særskilte sikringstiltak for Internett tilsvarende det man i dag gjør for øvrige deler av telesektoren. Post- og teletilsynet må derfor overvåke utviklingen i bruken av Internett og fortløpende vurdere behovet for å implementere tiltak. I kapittel 11.2.1 er det pekt på områder der det kan være aktuelt for en statlig regulatør å gripe inn.

1.2.4 Administrative og økonomiske konsekvenser

1.2.4.1 Finansiering av telesikkerhet og -beredskap

Ordinære driftsutgifter i forbindelse med Post- og teletilsynets sikkerhets- og beredskapsoppgaver vil kunne finansieres med gebyrer fra teleoperatørene på lik linje med Post- og teletilsynets øvrige virksomhet. Etableringskostnaden første år, jf. nedenfor, vil bli dekket over Samferdselsdepartementets beredskapskapittel i statsbudsjettet.

For de øvrige telesikkerhets- og teleberedskapstiltak vil det måtte foretas en nærmere konkret vurdering av hvilke finansielle virkemidler som er best egnet i det enkelte tilfelle. Det er viktig at det ved vurderingen sikres at finansieringen ikke gir utilsiktede konkurransevridninger eller skaper ulik belastning for noen av de berørte parter. Finansiering av konkrete tiltak vil kunne skje gjennom gebyrer, avgifter, egenfinansiering (operatørfinansiering), kundefinansiering eller bevilgninger over statsbudsjettet.

Hvilken finansieringsmåte som passer best vil avhenge av det konkrete tiltak. Endelig valg av regulerings- og finansieringsmåte må besluttes i det enkelte tilfelle.

I tilfeller der det eventuelt kan være hensiktsmessig at tiltak finansieres med bevilgninger over statsbudsjettet, vil Samferdselsdepartementet komme konkret tilbake med bevilgningsforslag i forbindelse med de årlige budsjettforslagene.

I henhold til gjeldende forskrift om offentlig telenett og offentlig teletjeneste har teleoperatører plikt til å ha et minimumsnivå for telesikkerhet i sine nett for å garantere leveringsdyktighet og sikring av kundenes telekommuni-

kasjon. Kostnader for å ivareta denne grunnsikkerheten vil under enhver omstendighet måtte dekkes av operatørene.

1.2.4.2 Tiltak og kostnadsanslag

TIFKOM-prosjektet har foreslått tiltak iverksatt over en 5-årsperiode med en total ramme på 730 mill. kr, som er foreslått dekket over statsbudsjettet. TIFKOM-prosjektets forslag medfører i tillegg kostnader for overtakelse av Telenors fjellanlegg på ca. 1,2 mrd. kr, kostnader for flytting av teleoperatørenes utstyr til samlokaliseringssentra samt andre tiltak TIFKOM-prosjektet ikke har beregnet kostnaden for, herunder eventuell samordning mellom FDN og et eventuelt nytt felles radionett for nødetatene. Med de kostnader vi i dag har oversikt over gir TIFKOM-prosjektets forslag en samlet ramme på ca. 2 mrd. kr over 5 år.

Samferdselsdepartementet legger opp til et vesentlig lavere kostnadsnivå enn det TIFKOM-prosjektet foreslår. Selv om det per i dag ikke foreligger nøyaktige kostnadstall har vi foreløpige, grove anslag som gir et bilde av hvilke kostnadsstørrelser det er snakk om. Beregninger viser at det vil koste i størrelsesorden 5-10 mill. kr å utføre de nye oppgavene i Post- og teletilsynet det første året med en bemanning på 4 personer. Av dette er 3,2 mill. kr rene etableringskostnader. Over en 5-årsperiode er det beregnet at sikkerhets- og beredskapsarbeidet i Post- og teletilsynet vil koste til sammen 20-40 mill. kr dersom bemanningen holdes stabil på 4 personer. De kostnadene vi i dag har oversikt over viser at det minimum vil være behov for i underkant av 200 mill. kr over en femårsperiode. Tabell 12.1 i kapittel 12.3 gir en oversikt over foreløpige kostnadsoverslag.

1.2.4.3 Avvikling av gjeldende SSO-ordning

Det nye konseptet for telesikkerhet og teleberedskap som skisseres i meldingen vil bli en ny ordning med spesielle samfunnspålagte oppgaver (SSO) til Totalforsvaret som skal gjelde for alle samfunnsviktige teleoperatører, og ikke bare for Telenor slik tilfellet er i dag.

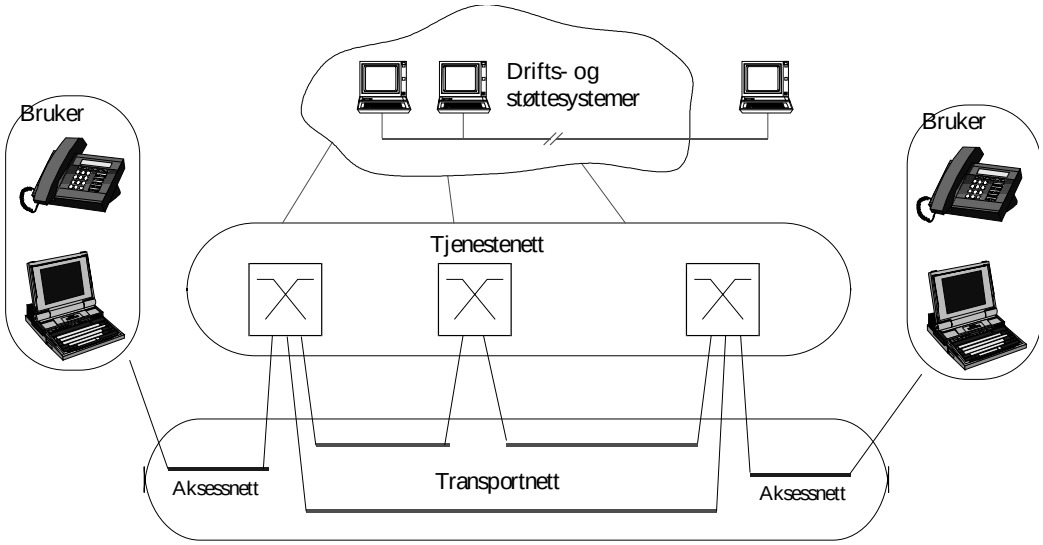
Før den nye SSO-ordningen etableres vil det være hensiktsmessig om staten gjør opp de forpliktelser som staten har påtatt seg gjennom gjeldende SSO-overenskomst med Telenor for 2001. Foreløpige beregninger viser at det koster ca. 80 mill. kr som engangskostnad å innfri disse forpliktelsene. Forut for utfasing av gjeldende SSO-ordning må det gjennomføres samtaler med Telenor for å komme frem til endelig størrelse på kompensasjonen. Samferdselsdepartementet vil komme konkret tilbake til dette med forslag i den ordinære budsjettprosessen. Kostnader for utfasing kommer i tillegg til de kostnader som er skissert i kapittel 12.3.

Inntil det nye konseptet er fullt ut etablert vil det uansett være behov for å videreføre enkelte av de oppgavene Telenor har vært pålagt gjennom SSO-ordningen. Dette gjelder bl.a. administrative og organisatoriske beredskapstiltak samt investeringer i transportabelt reservemateriell som må oppgraderes i takt med utviklingen i telenettene. For 2002 er dette beregnet til å utgjøre ca. 9 mill. kr. Samferdselsdepartementet vil også her komme tilbake med konkret forslag i den ordinære budsjettprosessen.

2 Telenettenes oppbygging og forholdet til sikkerhet og beredskap

2.1 Elementer i telenett

Grunnleggende elementer i telenettene er:
- Aksessnett
- Transportnett
- Tjenestenett
- Drifts- og støttesystemer
- Brukerutstyr



Figur 2.1 Telenettets prinsipielle oppbygning.

Kilde: Forsvarets forskningsinstitutt «Beskyttelse av samfunnet 2/Sårbarhetsreduserende tiltak innen telekommunikasjon», 1999.

Transport- og aksessnett består av en fysisk infrastruktur som tar hånd om all transport av informasjon mellom geografiske punkter. Transportnettet kopler landet som helhet sammen, mens aksessnettet knytter den enkelte bruker til transportnettet. Denne fysiske infrastrukturen omfatter både kabel- og radioforbindelser som er knyttet sammen gjennom et stort antall koplingspunkter.

Det tas i økende grad i bruk optiske fiberforbindelser i *transportnettet*. Fordelen med disse er at de har svært høy kapasitet, samtidig som de kan formidle informasjon med svært god kvalitet (få feil). *Aksessnettet* består i dag hovedsakelig av metallisk kabel for tilknytning av faste terminaler, mens en benytter radioforbindelser for tilknytning av mobile terminaler (f.eks. mobiltelefoner). Det er her viktig å understreke at samtaler mellom mobiltelefonbrukere går via det faste transportnettet. Utviklingen videre går mot at særlig

mellomstore og store bedrifter tilknyttes direkte til transportnettet gjennom høykapasitet optisk fiber. Det bygges for tiden også opp infrastruktur basert på høykapasitet radioaksess til faste brukere i områder med høy befolkningskonsentrasjon.

For å gi brukerne av teletjenester en tilstrekkelig grad av funksjonalitet er det opprettet såkalte *tjenestenett*. Disse består av et nettverk med tjenestenoder, som benytter transportnettet for å formidle informasjon innbyrdes mellom tjenestenodene. De enkelte brukerne av en teletjeneste knyttes fysisk til tjenestenettet gjennom aksessnettet. En av tjenestenettets viktigste funksjoner er å sørge for at brukerens informasjon styres gjennom transportnettet frem til mottakeren. Eksempler på tjenestenoder er telefonsentraler for telefoni og stamnettrutere i Internett-relatert trafikk.

Drifts- og støttesystemer i telenettene består av en rekke ulike typer systemer og teknologier. Felles for disse er at de muliggjør kostnadseffektiv drift av telenettet. Funksjonene er i stor grad bygd opp som egne nettverk av noder og kommunikasjonsveier. Disse kan ses på som separate interne tjenestenett for den enkelte tilbyder av teletjenester. I tillegg kommer også systemer for utvikling og produksjon av teletjenester.

Det er helt grunnleggende for sårbarheten i telenettene hvordan infrastrukturen er bygget opp. Det vil for eksempel si hvorvidt alternative veier finnes, og i hvilken grad sentrale knutepunkter i alle typer nett er sikret mot ulike former for trusler. Et svakt punkt vil kunne påvirke den totale sårbarheten i telenettene. Teletjenester er bygd opp med basis i et antall av enkeltfunksjoner og er derved avhengig av disse enkeltfunksjonene for å kunne fungere. En teletjeneste vil bestå av et komplisert hierarki av nettfunksjoner. Dette vanskeliggjør oppgaven med å kvantifisere teletjenestenes sårbarhet samt å sette opp årsakskjeder ved feil. Helt grunnleggende i slik kjedeproblematikk er likevel at tilnærmet alle funksjoner i utstrakt grad er avhengige av det faste transportnettet for å kunne levere teletjenester, inklusive mobiltelefontjenesten. I takt med digitaliseringen av funksjonene i telenettene er også de IKT-baserte produksjonssystemene i økende grad blitt viktig for telesystemets totale sårbarhet. Mens mange funksjoner tidligere var fordelt til den enkelte teleinstallasjon, er disse nå sentralisert for å møte markedets krav til effektivitet. Dette medfører også at denne kritiske informasjonen nå er mer samlet enn tidligere, noe som gjør den mer utsatt for angrep.

Anvendelsen av teletjenester er i stor endring. Mens teletjenester tidligere i hovedsak besto av enkel telefoni med et telefonapparat som eneste brukerutstyr, er dagens teletjenester tilpasset et svært bredt brukerbehov. Dette spenner fra formidling av tale til ulike typer data og video. Denne utviklingen har medført at også utstyret på brukersiden er blitt betydelig mer sammensatt enn tidligere, som igjen har følger for sårbarheten til systemet sett fra brukerens synsvinkel. Ansvaret for denne delen av sikkerheten må i fremtiden tillegges den enkelte bruker.

2.1.1 Telenettenes produksjonssystemer - avhengighet og sårbarhet

I tillegg til nettinfrastrukturen består telenettene også av ulike typer IKT-baserte produksjonssystemer. Disse sørger for at nettet til enhver tid leverer teletjenester til brukeren på en mest mulig kostnadseffektiv måte. Tilstanden

til den informasjonen som behandles og formidles i disse systemene er svært viktig for telenettets evne til en hver tid å produsere teletjenester, og dermed også for nettets sårbarhet. Produksjonssystemene kan deles inn i følgende typer funksjonsområder:

– Operativ drift og styring
– Driftsstøtte
– Utvikling og produksjon av teletjenester
– Signalering

Funksjonen operativ drift og styring er rettet mot funksjoner i alle typer telenett på komponent-, system- og virksomhetsnivå. Dette dreier seg blant annet om den viktige daglige driften av telenettet, fra time til time. Operativ drift og styring består av en rekke ulike IKT-systemer, som i større eller mindre grad er innbyrdes sammenknyttet. Trenden går imidlertid mot standardisering og ett system basert på en felles informasjonsbase. En felles betegnelse for dette er TMN (Tele Management Network). Eksempler på den informasjon en finner innen funksjonsområdet er informasjon innhentet fra nettet om eventuelle tekniske feil og styreordre til nettkomponenter og -systemer i nettet. Funksjonsområdet er viktig i den daglige normale driften av nettet, i tillegg til at det er svært viktig i situasjoner med svikt i nettet og behov for beslutninger om og iverksettelse av tiltak. Funksjonen inngår som det sentrale elementet i en moderne driftssentral for et telenett. Svikt i funksjonen eller informasjonen som ligger i denne vil være svært alvorlig for avviklingen av teletrafikken.

Driftsstøttesystemer tilbyr informasjon til både planleggere og driftsorganisasjonen, blant annet om telenettets oppbygging, tjenestestatus og den enkelte kunde tilknyttet nettverket. For driftsorganisasjonen er dette informasjon som særlig er viktig i situasjoner med svikt i telenettet, fordi den danner et viktig grunnlag for beslutninger om tiltak. Manglende tilgang til denne typen informasjon i en sviktsituasjon vil kunne føre til en betydelig forlengelse av tiden en tjeneste er gjort utilgjengelig.

I takt med et økende behov for funksjonalitet i teletjenestene, øker også behovet for en effektiv og fleksibel måte å utvikle og tilrettelegge disse på i tjenestenettet. Et eksempel på et slikt system er IN (intelligente nett) innen det tradisjonelle telefoninettet. Gjennom en sentralisert funksjon i nettet kan teleoperatøren utvikle og vedlikeholde avanserte teletjenester, samtidig med at nettets øvrige tjenester er i bruk. Fordi denne typen funksjoner legges inn i en sentralisert plattform tilknyttet alle nodene i et tjenestenett, vil disse kunne utgjøre en sårbarhet i forhold til tjenestene som leveres fra nettet. Svikt som følge av et angrep mot denne funksjonen vil kunne føre til at bruker taper tilgjengelighet til teletjenester.

For å oppnå en effektiv formidling og fremføring av informasjon i et tjenestenett benyttes signalering mellom tjenestenodene, for eksempel mellom telefonsentralene i telefoninettet. Signaleringsinformasjonen som utveksles mellom tjenestenodene er helt vital for at tjenestenettet skal fungere sammen som ett system. Denne signaleringen er ofte implementert som et eget kommunikasjonsnett med egne kanaler. Det mest vanlige systemet i dag er Signaleringssystem nr. 7 (SS7). For at tjenestenettet skal kunne levere tjenester til brukeren er det nødvendig at signaleringsnettet formidler korrekt informasjon til den enkelte noden i nettet til enhver tid. Svikt vil føre til at tjenestenettets tjenester blir gjort utilgjengelig for brukeren. SS7 har i dag svært lite sik-

kerhet innebygget, noe som synes å utgjøre et økende problem for telesikkerheten. Med tiden har det innenfor telefonitjenesten kommet mange aktører som har behov for tilknytting til SS7 for å tilby sine tjenester til markedet. Med et relativt høyt antall større og mindre aktører vil sikkerhetsproblemet øke.

I takt med digitaliseringen av funksjonene i telenettet er avhengigheten av ulike typer IKT-systemer som beskrevet ovenfor blitt svært høy. Disse systemene utgjør samlet sett et meget sammensatt og komplekst system, med flere nettverk som i utgangspunktet er separate, men som i stor grad integreres med hverandre på flere nivåer. Mens funksjonene tidligere var fordelt til den enkelte teleinstallasjon, er disse nå i stedet sentralisert for å møte markedets krav til effektivitet. Gjennom denne sentraliseringen er også mye informasjonen i systemet samlet. Feil i eller angrep mot denne samlede informasjonen vil få betydelig større konsekvenser enn tidligere. Den systeminformasjonen som behandles og formidles i disse IKT-systemene er dermed i ferd med å gjøre telesystemet som helhet mer sårbart.

Hvilke typer informasjon som er mest betydningsfull med hensyn til nettets sårbarhet er vanskelig å vurdere. Forebyggende tiltak bør iverksettes balansert da dette er et svært sammensatt område, med en rask utvikling både innen systemer og trusler.

2.2 Definisjon av begrepene telesikkerhet og teleberedskap

Informasjonsbehandling og informasjonsformidling ved hjelp av telekommunikasjon og datateknikk har lenge vært av vital betydning for samfunnets funksjoner. Denne betydningen har vært sterkt økende i 1990-årene og det er grunn til å tro at vi vil se en akselerert utvikling i samme retning i tiden som kommer. En sentral forutsetning for denne utviklingen er telenett og teletjenester med tilstrekkelig nivå på sikkerhet og beredskap.

Telesikkerhet som begrep omfatter:

– *Tilgjengelighet* - at systemet er sikret mot avbrudd i sin forventede funksjon og at systemet har tilgang til nødvendig datainnhold.
– *Integritet* - at systemet er sikret mot manipulering med systemets funksjon og datainnhold.
– *Konfidensialitet* - at systemets funksjon og datainnhold er sikret mot innsyn.

Tilfeldig svikt eller et tilsiktet angrep mot tele- og IT-systemer vil i større eller mindre grad kunne ramme en eller flere av disse egenskapene.

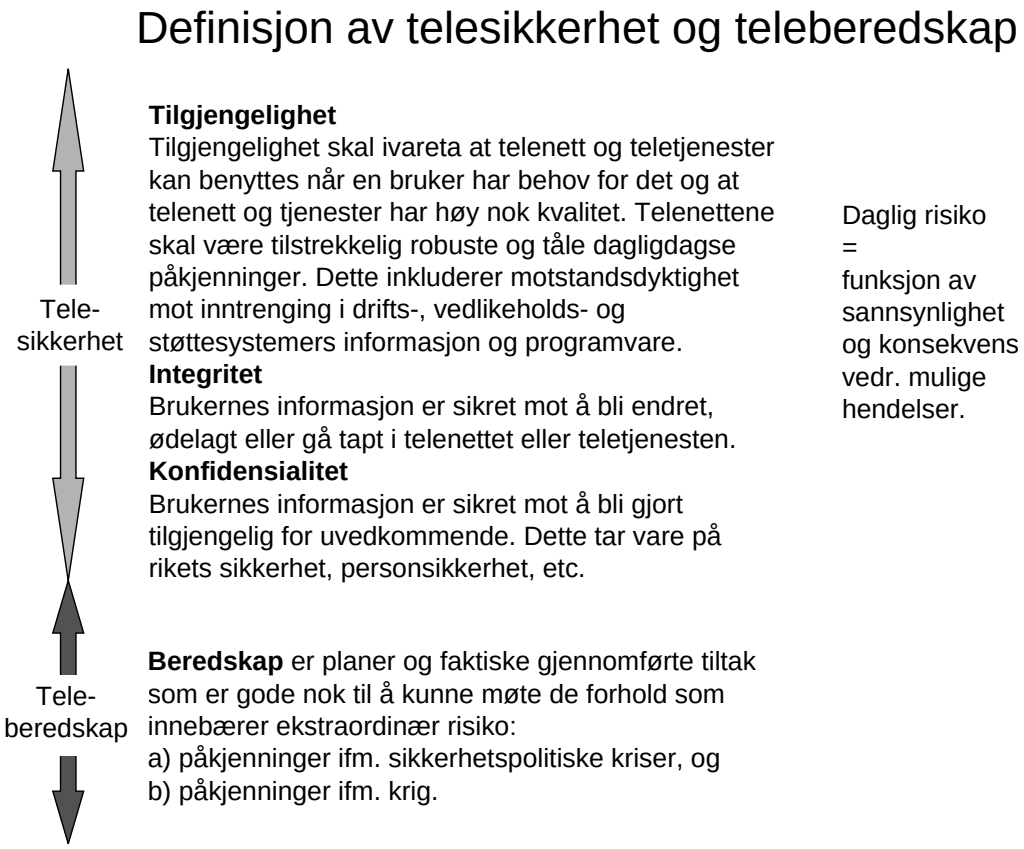
Tilgjengelighet innebærer at telenett og teletjenester kan benyttes når en bruker har behov for det, og at nettet og tjenesten har riktig kvalitet både teknisk og innholdsmessig. At informasjonen til en hver tid er tilgjengelig, er en viktig forutsetning for effektiv tjenesteproduksjon innen telenettene. Mange prosesser er tidskritiske og krever løpende utveksling av informasjon. Mangel på eller forsinket tilgang til informasjon vil også kunne være fatalt ved feilsøkings- og reetableringsarbeider etter en svikt. Sviktende tilgjengelighet vil også kunne føre til langvarig ødeleggelse av utstyr i telenettene. Tilfeldige feiloperasjoner og ulike former for teknisk svikt er ofte en typisk årsak til tap av tilgjengelighet.

Integritet betyr at brukerens informasjon er sikret mot å bli endret, ødelagt eller gå tapt i telenettet eller teletjenesten. IT-systemene som står bak telenettenes tjenesteproduksjon vil være svært følsomme overfor angrep rettet mot informasjonens integritet. Gjennom et «vellykket» integritetsangrep vil en angriper kunne manipulere informasjon knyttet til styring og kontroll med produksjonsprosesser. Illegal styringsinformasjon til prosesser kan i verste fall føre til fysisk ødeleggelse av utstyr. Feiloperasjoner og enkelte former for teknisk svikt kan også ha tilsvarende virkning.

Konfidensialitet innebærer at brukerens informasjon er sikret mot å bli gjort tilgjengelig for uvedkommende. Tiltak som sikrer konfidensialitet (kryptering etc.) vil være av spesielt stor betydning i forhold til informasjon som gjelder rikets sikkerhet, personsikkerhet etc. Konfidensialitetssikring er av mindre betydning i IT-systemer knyttet til produksjon av teletjenester. For den enkelte sluttbruker av telekommunikasjon er derimot konfidensialitetssikring viktig, for eksempel for å hindre at informasjon om personlige forhold, forretningsstrategier eller nasjonens sikkerhetspolitiske disposisjoner avsløres.

For å oppnå nødvendig robusthet og sikkerhet i tele- og IT-systemene, må det iverksettes effektive tiltak for å forebygge, begrense eller håndtere kriser og andre uønskede hendelser så vel i fredstid som i en beredskaps- eller krisesituasjon. Det må med andre ord etableres både planer og gjennomføres faktiske tiltak som er gode nok til å kunne møte forhold som innebærer ekstraordinær risiko, for eksempel påkjenninger i forbindelse med sikkerhetspolitiske kriser og krig. Det er slike tiltak som inkluderes i begrepet *teleberedskap*.

Figur 2.2 gir et bilde av begrepene telesikkerhet og teleberedskap.



Figur 2.2 Definisjon av telesikkerhet og teleberedskap.

Hovedhensikten med et telekommunikasjonsnett er informasjonsformidling i form av tale, bilde, video, tekst e.l. For brukeren er det viktig at den informasjonen som formidles gjennom en teletjeneste er tilgjengelig til rett tid, at informasjonen ikke blir endret underveis, at informasjonen kommer frem til riktig adressat og at uvedkommende ikke kan avlytte.

Samferdselsdepartementet har i denne meldingen valgt å avgrense sikkerhet til å omfatte brukers tilgjengelighet til informasjon gjennom telenettene, og i mindre grad andre former for sikring av brukers informasjon. En sentral årsak til dette er at tjenestetilgjengelighet i all hovedsak ligger i den enkelte teleoperatørs disposisjoner. Når det gjelder integritets- og konfidensialitetsbeskyttelse har brukeren selv god mulighet til å forestå dette blant annet gjennom tilgang til stadig flere produkter på området.

Det vurderes likevel som viktig at telemyndigheten i samarbeid med andre aktuelle myndigheter også følger opp med tiltak rettet mot økt integritet og konfidensialitet i telenettene. Utarbeidelse av veiledere for informasjonssikkerhet for brukere av teletjenester er ett eksempel på en slik oppfølging.

3 Risiko og trusselbilde for norske telenett

Totalt sett vil telekommunikasjonsproblemer som følge av svikt innen hvert enkelt av nettelementene medføre alvorlige konsekvenser for større eller mindre deler av samfunnet, selv om de skulle inntreffe under ellers normale forhold. Supplert med gjensidige avhengigheter i samfunnet vil alvorlige og langvarige forstyrrelser innen telekommunikasjon medføre at de teknologiavhengige prosessene i samfunnet ikke lenger kan utføres etter sin hensikt. Eksempler på generelle samfunnskonsekvenser som følge av svikt i telekommunikasjon kan være tilhørende svikt i:

– informasjon til befolkningen
– alarm- og nødtelefoner
– elektronisk betalingsformidling
– oversikt over vare- og drivstoffbeholdninger
– sentraliserte funksjoner, f.eks. innen kraftbransjen
– offentlige funksjoner, f.eks. innen utbetalinger, helsetjenester
– trafikkavvikling innen samferdselssektoren

3.1 Mulige trusler mot norske telenett

Hendelser som forårsaker svikt i telekommunikasjon kan ha utspring i mange ulike årsaker. En skiller gjerne mellom villede og ikke-villede hendelser. Ikke-villede hendelser kan være tekniske feil eller ødeleggelser som følge av naturgitte fenomener, f.eks. storm, flom og lynnedslag. Også menneskelig svikt og feiloperasjoner inngår i denne kategorien. Et eksempel i denne sammenheng kan være graveuhellet i Kristiansand sommeren 2000 der bl.a. Kjevik lufthavn mistet teleforbindelsene. Også Telenors teletrafikk i regionen, som omfatter store deler av Aust- og Vest-Agder, ble lammet, og dette gjaldt også nødmeldingstjenesten. Slike hendelser vil skje, men må minimeres både i antall og konsekvens.

Villede hendelser er derimot hendelser som har sin årsak i menneskers bevisste handlinger for å skade eller forårsake problemer på annen måte. Motivet og kapasiteten til de som står bak vil være forskjellig, og vil kunne befinne seg i et spenn fra rene barnestreker til velstrukturerte og omfattende angrep fra høyt kompetente individer. I den første delen av dette spennet vil en i hovedsak finne angrep som rammer tilfeldig mot en enkelt infrastruktur, mens den andre ytterligheten vil gjelde angrep som rammer et på forhånd bestemt mål med høy presisjon. Det vil imidlertid også kunne skje at et ustrukturert angrep, som i utgangspunktet synes å være lite og ubetydelig, likevel kan vise seg å få alvorlige konsekvenser fordi angriperen har klart å sette i gang en kjedereaksjon som egentlig ikke var tilsiktet. En slik kjedereaksjon kan innbefatte ulike former for teknisk svikt og feiloperasjon. Mangfoldet av potensielle aktører og typer av virkemidler som på sikt kan representere en trussel mot de norske telenett og deres tjenester er økende.

Grovt sett vil trusselen mot telenettene innbefatte følgende fem hovedkategorier av anslag og virkemidler:

– Anslag med fysiske virkemidler mot infrastruktur

– Anslag med elektroniske virkemidler mot infrastruktur
– Manipulasjon med informasjonssystemer innen telefunksjonen
– Overbelastning av telenettene
– Sosiale trusler mot beslutningstakere i driftsfunksjonen i telenettene

I en normalsituasjon er det mest sannsynlig at virkemidlene vil kunne forekomme enkeltvis eller i enkle kombinasjoner. I mer omfattende situasjoner vil trusselbildet derimot være mer komplekst og kunne omfatte en rekke ulike virkemidler i kombinasjon. Nedenfor gis det en kort gjennomgang av trusler mot telekommunikasjon.

3.1.1 Fysiske trusler

Formålet med bevisst fysisk ødeleggelse av teleinfrastruktur er enten å sette utvalgte fremføringsveier ut av funksjon, eller generelt å redusere nettets struktur og kapasitet og dermed evne til å formidle store trafikkmengder. Målrettede fysiske anslag mot telesystemet kan primært tenkes rettet mot infrastruktur som driftssentraler, telesentraler, koblingspunkter og kabelforbindelser i det fysiske transportnettet. Installasjonene i transportnettet er mest utsatt, fordi disse ofte er fysisk lett tilgjengelig i terrenget. Kabler som ligger i traséer mellom disse installasjonene vil også ofte være lett tilgjengelige.

Driftssentraler, telesentraler og øvrige komponenter i tjenestenettstrukturen er vanligvis relativt godt sikret mot skade i fredstid. Her er en imidlertid inne i en utvikling mot at en får flere mindre tjenestetilknytningspunkter i skap langs vei og i mindre bygninger, som det vil være enkelt å sette ut av funksjon. Disse vil også ofte være forsynt med teleoperatørens logo, slik at det er enkelt å finne frem til de riktige stedene. Ved mer omfattende angrep som flyangrep, terrorangrep og angrep fra regulære kampavdelinger vil imidlertid så godt som alle disse installasjonene være sårbare.

Midler for menneskeskapt fysisk ødeleggelse kan være alt fra enkle kabelklipp og brannstiftelse til bruk av eksplosiver og avanserte avstandsleverte våpen. Utviklingen innen våpenteknologien går mot avstandsleverte våpen med stor presisjon og høy penetrasjonsevne. Det vil forenklet si at en treffer det en sikter på, og våpenet kan om nødvendig trenge gjennom en betongoverdekking på flere meter før det detonerer. For å motvirke trusselen fra slike våpen mot stasjonære installasjoner kreves det i praksis innebygging i fjellanlegg med høy overdekning. Kostnaden for slike våpen er ikke spesielt høy, og vi må regne med at utviklingen går mot økt tilgjengelighet. Dette vil sette store krav til fysisk beskyttelse av viktige punkter i telenettene.

Trusler i form av anslag mot infrastruktur fra sabotasjegrupper og terrorister vil være de mest kostnadskrevende å sikre seg mot. Størstedelen av teleinfrastrukturen er både svært utsatt og sårbar selv overfor enkle våpenvirkninger. Selv beskyttede anlegg i fjell vil være sårbare overfor sabotasjegrupper og terrorister dersom anleggene ikke er tilstrekkelig sikret med overvåking, varslingssystemer og vakthold.

Installasjoner i transportnettet vil også være utsatt for, og sårbare overfor uværsfenomener som lynnedslag, ising (gjelder radiolinje), nedblåsing (gjelder radiolinje) og flom. Lynnedslag utgjør her den mest markerte trusselen, og en opplever stadig at deler av telenettet faller ut på grunn av overspenning

fra lynnedslag. Også ulike former for anleggsarbeid kan utgjøre en trussel mot telenettene, f.eks. ved at kabler skades under gravearbeid.

3.1.2 Elektroniske trusler

Den elektroniske trusselen er en form for fysisk trussel, men skiller seg fra denne ved at det kun er de elektroniske komponentene i systemet som forstyrres eller ødelegges som følge av virkemiddelbruken. En skiller i første rekke mellom *elektromagnetisk jamming* og *elektromagnetiske strålingsvåpen*.

Elektromagnetisk jamming består i at en mot radiobaserte overføringssystemer for informasjon tilfører sterk elektromagnetisk stråling. Denne fører til at informasjonen som overføres i systemet ødelegges. Jamming er normalt ikke fysisk ødeleggende for systemene, og har tradisjonelt hatt mest anvendelse i militær sammenheng. Det finnes også eksempler på at teknikken har vært benyttet i fredstid. Jamming av kringkastingssendere i politisk øyemed har vært anvendt i andre deler av verden. I dagens telekommunikasjon er imidlertid radiobaserte overføringssystemer i tilbakegang på grunn av utviklingen innen optiske fibersystemer. For å kunne jamme informasjonsveiene i et moderne telesystem kreves det uansett betydelige ressurser for å finne de «rette» signalveiene som må jammes for å oppnå en ønsket effekt. I tillegg kreves det at jammeutstyret er godt teknisk tilpasset til det enkelte målet for jammingen. Jamming krever også relativ nær tilstedeværelse. Jammeteknikker vurderes også i fremtiden å være mest aktuelle i militær sammenheng.

Elektromagnetiske strålingsvåpen er en type strålingsvåpen som genererer høyenergi elektromagnetisk stråling med mål å forstyrre funksjonen i eller helt ødelegge elektroniske systemer. Dette er stråling som i intensitet overstiger den normale bakgrunnsstrålingen, som finnes naturlig. Halvledermaterialet som inngår i all informasjonsteknologi er svært følsomt for slik stråling. I kategorien elektromagnetiske strålingsvåpen inngår tradisjonell *elektromagnetisk puls* (EMP) og *«High Power Microwave»* (HPM).

Elektromagnetisk puls (EMP) genereres naturlig gjennom lynnedslag. Andre mindre kraftige kilder for EMP er radiosendere, termostater og koblinger i det elektriske nettet. Alle disse typene EMP er det mulig å sikre seg godt mot. Verre er det med menneskeskapt EMP. Den typen EMP som det gjennom de senest ti-årene er blitt lagt mest vekt på er kjernefysisk generert EMP. Gjenom å avsette en kjernefysisk lading over atmosfæren vil det utvikles en svært kortvarig og kraftig elektromagnetisk puls rettet mot et stort område på jordoverflaten. Denne vil kunne bli så kraftig at elektronisk utstyr ødelegges i stort omfang. Mot denne typen EMP er det kostnadskrevende å iverksette effektive beskyttelsestiltak. I Norge er det i dag i hovedsak Forsvarets mest kritiske systemer som er gitt effektiv EMP-beskyttelse. Også innenfor sivile infrastrukturer med stor viktighet for Totalforsvaret har det vært foretatt en viss grad av sikring, for eksempel i systemer innen kraftforsyningen og i Telenors telenett.

«High Power Microwave» (HPM) er en relativt ny type strålingsvåpen. Her benyttes moderne radarteknologi til å generere en svært kortvarig og intens puls. Denne pulsen vil kunne få tilsvarende virkning som en kjernefysisk EMP. HPM opererer imidlertid på kortere bølgelengder enn EMP, og en angriper vil av fysikalske årsaker måtte befinne seg i nærheten av den instal-

lasjon som skal rammes. Skadeområdet for HPM er dermed også mye mindre enn for EMP. Det er i de senere år skrevet mye i internasjonal sammenheng om denne trusselen, men det er lite som er offentliggjort av målinger og empiri. Det er likevel med bakgrunn i beregninger antatt at forstyrrelse eller ødeleggelse av elektronisk utstyr uten spesiell skjerming kan oppnås med en rekkevidde på et fåtall kilometer. HPM-utstyr er enkelt i oppbygging og teknologi og er derfor også enkelt å fremstille. Det er utviklet relativt lette transportable HPM-våpen som også kan tenkes å bli benyttet i forbindelse med sabotasje- og terroraksjoner. Det er i dag mulig å få kjøpt slikt utstyr over disk i enkelte land.

3.1.3 Logiske trusler og manipulasjon med informasjonssystemer

Logiske trusler dreier seg om et sett med virkemidler direkte rettet mot IKT-systemenes logiske funksjon. Disse datasystemene inngår i dag som viktige komponenter i et telenetts produksjonssystem på alle nivåer. Virkemidler for logiske angrep kan grovt deles inn i *direkte systemangrep* og *programvareangrep*. Begge formene for logiske angrep vil kunne være rettet mot alle egenskapene til et IKT-system; integritet, tilgjengelighet og konfidensialitet. Logiske trusler er i den senere tid blitt mer aktuelle på grunn av IKT-systemenes tilknytning til det åpne globale Internett. Det er i dag ikke kjent i hvilken grad norske teleoperatører har knyttet sine IKT-baserte produksjonssystemer til Internett eller til andre former for inngangsveier. Det er likevel klart at det forekommer, og internasjonale trender viser også at dette i fremtiden vil forekomme i økende grad. Dette skjer som en direkte følge av globaliseringen innen bransjen og behovet for kostnadseffektiv drift.

3.1.3.1 Direkte systemangrep

Gjennom ulike metoder vil en angriper gjennom eksterne tilkoblinger i sann tid kunne sørge for at et IKT-basert produksjonssystem får en bestemt og på forhånd planlagt oppførsel. Eksempler på eksterne tilkoblinger er Internett. Ett eksempel på virkning av en slik inntrenging er at angriperen gjennom direkte fjernstyringsfunksjoner vil kunne stenge ned knutepunkt i transportnettet og dermed hindre informasjonsfremføring i et bestemt område. Angriperen kan også velge å angripe en eller flere telefonsentralers funksjon og forårsake at en tjeneste blir gjort utilgjengelig for større eller mindre brukergrupper.

Angrepet kan også innebære å sørge for at et driftssystem ikke lenger kan yte sine tjenester, for eksempel gjenom sletting av data- og programlager med påfølgende nedkjøring av datamaskinene i driftssystemet. Dersom dette kombineres med fysiske anslag mot den fysiske infrastrukturen i telenett, som kontrolleres fra det samme driftssystemet, vil virkningen kunne bli omfattende og relativt langvarig.

For å trenge inn i et system utenfra benyttes en rekke teknikker. Det finnes i dag flere verktøy tilgjengelig på Internett som kan hjelpe en inntrenger. Disse er til dels markedsført som sikkerhetsprodukter, fordi de også kan hjelpe en systemeier med å analysere egen sårbarhet. Med en kombinasjon av flere tilsvarende og andre teknikker vil det være mulig også å trenge seg igjennom forsvarsmekanismer som brannmurer og lignende.

Denne typen logiske angrep karakteriseres ved å gi svært presise virkninger gitt at angriperen klarer å forsere alle systemhindre og får kontroll med systemet. Denne betingelsen er såpass vesentlig at *innsidere* ofte er en ressurs av avgjørende betydning for at en angriper skal lykkes med å komme inn i systemene. Innsideren kan ha ulike motiver for å hjelpe den utenforstående, som kan spenne fra ren godtroenhet til et sterkt ønske om å skade den virksomheten man er ansatt i. Mange av virksomhetene som er utsatt for angrep er ofte store og uoversiktlige å ha full kontroll over. Det er ofte lagt opp til lite beskyttelse mot indre trusler innen den enkelte virksomheten. Den dyktige innsideren har derfor ofte godt arbeidsrom.

3.1.3.2 Programvareangrep

Programvare for datamaskiner består av en samling av svært mange, men enkle logiske operasjoner i sekvens som styrer datamaskinens enkeltfunksjoner. Et vanlig program for kontordatamaskiner vil kunne inneholde mange millioner logiske operasjoner og kombinasjoner av slike, der feil i kun én operasjon vil føre til feilfunksjon. Moderne dataprogrammer er nå så store og komplekse at dette også er et problem for programmereren. Programvarepålitelighet er derfor blitt et eget fagområde.

Denne kompleksiteten kan benyttes av en angriper til å gi de IKT-baserte produksjonssystemene bestemte logiske funksjoner som er uheldig for totalsystemets funksjonsevne. Det finnes en rekke ulike teknikker for slike angrep. Noen av disse er kort beskrevet nedenfor.

Datavirus består av et kodesegment med logiske «feil»-operasjoner som fordobler seg selv ved å knytte seg opp mot filer. Viruset åpnes når man benytter seg av den infiserte filen. Virus er for de som blir rammet en meget stor utgiftskilde. Ser man verden under ett, kostet virusangrep i 1999 samfunnet 100 mrd. kr, ifølge Computer Economics Research. Av disse utgiftene kan anslagsvis 1 milliard føres tilbake til norske bedrifter og offentlig virksomhet. Et virus kan spre seg raskt. Hvis man sender et virus fra ett sted til femti mottakere, der hver enkelt mottaker igjen sender det til 50 nye mottakere, vil det etter fem generasjoner spredning ha nådd frem til 312 millioner brukere. Typisk for virusangrep er at de også treffer mange som nødvendigvis ikke trenger å være i målgruppen for angrepet.

Trojanske hester er programmer som ligger skjult i andre programmer inntil de aktiveres. De kan aktiveres av den som har sendt dem ut gjennom en på forhånd bestemt mekanisme eller på et forhåndsdefinert tidspunkt. De vil da kunne utføre en uønsket handling, for eksempel sletting av filer eller harddisker, eller sende (lekke) informasjon tilbake til utsenderen.

De som er med og utvikler programvare kan legge inn *bakdører* som brukeren ikke kjenner til. Dette kan gjøres av det firma som utvikler programmet eller av en enkelt programmerer. De som kjenner til de logiske funksjonene i en slik bakdør har blant annet mulighet til å komme seg inn på en datamaskin uten å gå gjennom sikkerhetsmekanismer, som passord eller andre autentiseringsmekanismer. Dette kan for eksempel være et problem der sentralt IT-personell har sluttet i sitt arbeid og gått over til en konkurrent.

Flere store nettsteder på Internett er blitt utsatt for det som kalles *«Distributed Denial-of-Service attack» (DDoS-angrep)*. Det vil si at angriperne bruker

flere kraftige datamaskiner til samtidig å sende store mengder forespørsler mot den datamaskinen og de tjenestene de ønsker å angripe. Dette vil føre til at den angrepne datamaskinen i verste fall bryter sammen, som igjen fører til tap av tjenestetilgjengelighet. DDoS-angrep er en mer omfattende avart av enklere *«Denial of Service Attacks»* (DoS).

Disse teknikkene synes så langt mest å ha vært benyttet til å skape blind og tilfeldig forvirring og skade hos mange brukere med tett tilknytning til Internett. Av teknikkene som er beskrevet ovenfor vurderes imidlertid trojanske hester, bakdører og beslektede teknikker å være de farligste fordi disse kan være svært vanskelige å beskytte seg mot. Programvare blir mer og mer kompleks og vanskelig å vite innholdet av, noe som i særlig grad gjelder programvare som inngår i telenettenes produksjonssystemer. Dette gjelder både masseprodusert programvare som Microsoft Windows og spesielle programvaresystemer, som for eksempel benyttes til fjernkontroll av komponenter innen teleinfrastrukturen. Dette øker alvoret som ligger i problemet.

En kombinasjon av teknikker for programvareangrep og direkte systemmanipulering anses å være svært kraftige virkemidler i et angrep mot vitale IKT-systemer. De virkemidlene som er beskrevet ovenfor utgjør imidlertid bare et utvalg. I fremtiden vil en måtte forvente en utvikling mot stadig mer raffinerte teknikker og kombinasjoner av slike.

3.1.4 Overbelastning av telenett

Tjenestenettene i telenettene er dimensjonert på en måte som innebærer at det er mindre sambandsressurser tilgjengelig enn det som må til for at alle skal kunne benytte disse samtidig. Moderne tjenestenett har en jevnt over god trafikkavviklingsevne gjennom bruk av robuste og godt dimensjonerte reguleringsfunksjoner. Dette fører til at overbelastning av en tjeneste sjelden skjer i en normal samfunnstilstand der bruken av teletjenester fordeler seg over døgnet. Overbelastning av en teletjeneste som følge av økt teletrafikk under en ekstraordinær situasjon er derimot meget realistisk. Både under flommen på Østlandet i 1995 og ved Åsta-ulykken 6. januar 2000 resulterte dette i svikt i tilgjengelighet.

Tjenestenett kan på tilsvarende måte også overbelastes ved at noen, f.eks. gjennom logiske angrep mot sentrale drifts- og tjenesteproduksjonssystemer, bevisst tilfører mer trafikk enn det nettet har kapasitet til å formidle. Dette er eksempel på et såkalt DoS-angrep, jf. kapittel 3.1.3.2, som gjennomføres for å blokkere tilgjengelighet i kommunikasjonsnettverk. Resultatet vil bli det samme som for fysiske angrep, ved at den legitime trafikken vil blokkeres. Teknisk svikt eller skade etter fysiske angrep mot forbindelser i nettet vil føre til at nettets evne til å formidle trafikk reduseres. Når nettet er degradert til et visst nivå vil trafikken etter hvert bli blokkert og stoppe opp.

3.1.5 Sosiale trusler

Ovenfor er det beskrevet en rekke ulike typer virkemidler som enkeltvis eller i kombinasjon effektivt vil kunne føre til alvorlige virkninger for tilgjengeligheten til teletjenester. Imidlertid inngår også mennesket som en viktig ressurs som beslutningstaker både i planlegging og i den daglige operative drift av et telenett. Derfor er også den menneskelige faktor viktig med hensyn til sårbar-

het i disse systemene. Eksperten kan med eller uten eget vitende påvirkes til å gjøre gale ting.

Den sosiale trusselen må dermed tas i betraktning ved implementering av sårbarhetsreduserende tiltak i telenettene.

3.2 Trusselen mot norske telenett

Et angrep må være fundert i et motiv og en intensjon om å utrette skade. Dette kan dekke hele spekteret fra ren underholdningsverdi for angriperen, via økonomisk vinning til et ønske om å skade en fremmed makts interesser. En angriper med en gitt intensjon må samtidig ha kapasitet til å gjennomføre angrepet gjennom å beherske de nødvendige fysiske, elektroniske, logiske og sosiale virkemidler. Systemet som angripes må også være sårbart overfor den kapasitet en angriper innehar.

I tabell 3.1 er det er vist en enkel sammenstilling med fem utvalgte aktørgrupper. Her er mulig intensjon koblet opp mot den kapasitet disse kan forventes å ha i dag. Det må imidlertid understrekes at det finnes et utall mulige aktørgrupper og varianter av slike, og det vil ikke være mulig å presentere alle. Kapasitet for fysiske og elektroniske virkemidler er i tabellen slått sammen og benevnt fysiske virkemidler.

Tabell 3.1: Villede trusler mot IKT-systemer - mulighet for svikt.

Aktørtype	Motiv/intensjon	Kapasitet		
		-Fysisk-	-Logisk-	-Sosial-
1. Underholdning	Tilfeldig rettet skadeverk - underholdning	-	L	-
2. Kriminell - individ	Egen økonomisk vinning	L	L	-
3. Organisert kriminalitet	Økonomisk vinning	L	M	L
4. Terroristgruppering	Promotere/skape oppmerksomhet om sak	M	H/M	H/M
5. Statlig / nasjon	Skade på eller overtagelse av annen stats territorium	H	H	H

(Antydning av kapasitet: -=ubetydelig, L=liten, M=middels, H=høy)

Utviklingen innen de tre første aktørgruppene viser at trusselbildet er blitt bredere. Tidligere ble det fokusert mest på den interne trusselen, det vil si den utro medarbeideren som misbrukte dataanlegget innen virksomheten. På grunn av at systemene nå er knyttet sammen i globale kommunikasjonsnettverk, må også den eksterne trussel legges til. Dermed blir også gruppen av mulige angripere betydelig større.

Innen den førstnevnte aktørgruppen vil man finne aktører med begrenset kapasitet i anvendelse av fysiske virkemidler som krever tilstedeværelse. I første omgang vil de også ha en begrenset kapasitet til å gjennomføre strukturerte logiske angrep mot IKT-systemer. Angrep fra disse vil ofte ramme tilfeldig, og så langt synes angriperne å ha vært mest interessert i utfordringen i å komme seg inn i systemet. En mulig trend kan gå mot at denne typen aktører

med tiden går sammen i nettverk og blir mer strukturerte og målrettede. I så fall vil også kapasiteten øke betydelig.

De to neste aktørgruppene fra tabellen kjennetegnes ved at deres mål og intensjon i stor grad vil være begrenset til utvalgte målgrupper og enkeltvirksomheter. Deres kapasitet vil dekke både logiske og fysiske virkemidler. Disse aktørene vil ha som primært mål å søke økonomisk utbytte fra eller økonomisk skade utvalgte virksomheter. Slike aktører kan med tiden få betydelig kapasitet til logiske angrep. Virksomheter innen telesektoren har i lengre tid vært utsatt for ulike typer vinningskriminalitet og er bevisst på risikoen ved dette.

Når det gjelder terroristorganisasjoner og sub-statlige aktører, hersker det mer tvil. Tradisjonelt har slike organisasjoner primært rettet sine virkemidler inn mot mennesker og menneskeliv, og har kun i liten grad vært interessert i samfunnsinfrastrukturer som telekommunikasjon som mål. Det kan likevel ikke utelukkes at det kan oppstå nye typer grupperinger og organisasjoner som i større grad vil bruke virkemidler mot infrastruktur. Angrep mot telenettene i det moderne samfunnet vil i mye sterkere grad enn tidligere kunne være et middel for å oppnå former for kaos, også med tap av menneskeliv.

Statlige aktører må både i dag og i fremtiden forventes å inneha en svært høy kapasitet i hele spekteret av virkemidler. Det foreligger allerede i dag sterke indikasjoner på at enkelte stormakter innehar en betydelig kapasitet på logiske virkemidler. Det er også kjent at en rekke andre mindre stater er i ferd med å bygge opp kapasitet på området.

Utviklingen mot at de IKT-baserte produksjonssystemene innen telenettene i økende grad knyttes sammen med det verdensomspennende Internett fører også til at det blir vanskeligere å identifisere angripere. Logiske angrep kan utføres fra hvor som helst i verden gjennom dette nettet. En angriper kan ganske effektivt skjule hvem han er og dermed også hvilke motiver han har for et angrep. Angriperen har også mulighet til å flytte ansvaret over på en annen som del av en strategi for å forvirre den som angripes. Derfor kan det være vanskelig for en virksomhet som blir angrepet å umiddelbart fastslå årsaken til angrepet. På samme måte kan også stater få store problemer med å identifisere angriperens geografiske utgangspunkt, da man kan rute angrepene via flere land og gjennom datamaskiner i nettet som anonymiserer angriperen. På denne måten er det svært vanskelig å bedømme om det er «barnestreker» eller et direkte angrep fra et annet land det er snakk om. Under Golfkrigen i 1991 opplevde USA logiske angrep mot sin IKT-infrastruktur som de i første omgang oppfattet kom fra en bestemt ikke vennligsinnet makt. Dette viste seg etter en tids etterforskning å komme fra en gruppe «underholdningshackere» i USA.

3.3 Risikovurdering for norske telenett

Sannsynligheten for alvorlig og langvarig svikt i teletjenester vurderes ut fra dagens trusselbilde å være liten overfor fysiske og elektroniske angrep. Logiske angrep ved forsøk på inntrenging i telenettenes IT-baserte produksjonssystemer anses i dag som en større reell trussel, og konsekvensene av

slike angrep kan være alvorlige for større eller mindre deler av samfunnet. Dersom sikkerhetspolitiske kriser eller økt terror etc. inntreffer, øker imidlertid den menneskeskapte fysiske trusselen mot telenettene og dermed sannsynligheten for omfattende og langvarig svikt. Konsekvensene for Totalforsvarets og samfunnets støtte til det militære forsvaret kan i så fall være svært alvorlige.

Det anses som usannsynlig at ikke-statlige aktører skal kunne tilegne seg så store ressurser at det vil kunne representere en så stor trussel for Norge at det blir krigslignende tilstander. Dette betyr imidlertid ikke at disse aktørene kan avskrives helt, ettersom de kan utføre fysiske og logiske angrep styrt fra større statlige aktører. Selv om de ikke-statlige aktørene ikke representerer den største trusselen for Norges suverenitet, vil disse aktørene likevel kunne forstyrre samfunnsmaskineriet og medføre alvorlige konsekvenser for de personer og organisasjoner som rammes. Dagens trusselbilde tilsier at det er den logiske trusselen som utgjør størst risiko mot telenettene. Selv om det er størst sannsynlighet for at telenettene skal bli utsatt for logiske angrep kan konsekvensene som følge av fysiske angrep være så store at vi ikke kan se bort fra trusselen om fysiske angrep. Ikke minst er det viktig å merke seg at konsekvensen av et logisk angrep mot f.eks. et driftssystem er av betydelig kortere varighet enn et fysisk angrep mot det samme systemet.

Vi kan heller ikke glemme trusselen fra tilfeldige, ikke-villede hendelser. Dette kan være både tekniske feil eller ødeleggelser som følge av naturgitte fenomener, f.eks. storm, flom, lynnedslag, og menneskelig svikt og feiloperasjoner, slik som når en gravemaskin under arbeid kutter kabler og dermed setter telenettene ut av funksjon. Slike hendelser vil kunne skje, men så lenge man i telenettene har tatt høyde for beskyttelse mot villede menneskeskapte trusler vil man samtidig være beskyttet også mot ikke-villede hendelser.

4 Telepolitikk og teleberedskap

Hovedmålene for telepolitikken i Norge er å sikre at alle husstander og bedrifter over hele landet får tilgang til grunnleggende teletjenester av høy kvalitet og til lavest mulige priser, samt å legge til rette for størst mulig verdiskapning og effektiv bruk av ressurser som nyttes til utbygging og tjenesteyting innenfor sektoren.

4.1 Sikring av effektiv og virksom konkurranse

Fra 1. januar 1998 ble de siste eneretter i telesektoren avviklet, og det ble etablert alminnelig konkurranse innenfor alle deler av telemarkedet i Norge. Den markedsmessige og tekniske utviklingen på teleområdet medfører at den samfunnsmessige styringen av sektoren baseres på regulatoriske virkemidler. Gjeldende regulatorisk rammeverk er utformet bl.a. med sikte på å få i stand overgangen fra monopolsituasjonen til en konkurransesituasjon. Regelverket fokuserer på å etablere et konkurranseutsatt marked der nye aktører gis innpass. Gjeldende regelverk regulerer derfor tilbydere med sterk markedsstilling strengere enn andre tilbydere. Dette medfører blant annet at tilbydere med sterk markedsstilling i en rekke tilfeller skal stille nett og tjenester til rådighet for andre på objektive, oversiktlige og ikke-diskriminerende vilkår. Tilbydere av offentlig telenett for tilbud om overføringskapasitet eller offentlig telefontjeneste med sterk markedsstilling må ha konsesjon. Tilbydere som ikke har sterk markedsstilling har plikt til å forhåndsregistrere seg hos telemyndigheten før de starter sin virksomhet. Tilbydere som ønsker å ta i bruk radiofrekvenser må som hovedregel ha konsesjon før frekvensene tas i bruk.

For å forenkle telekommunikasjonslovgivningen, tilpasse lovgivningen den nye markedssituasjonen som åpningen av telemarkedet har medført og tilpasse lovgivningen den gradvise integrasjonen mellom medie-, tele- og IT-sektorene, er det nødvendig med et nytt regulatorisk rammeverk. Det nye rammeverket må sørge for at tilstrekkelig konkurranse oppnås i alle segmenter av markedet og samtidig sikre at grunnleggende forbrukerrettigheter blir ivaretatt. Europakommisjonen fremmet 12. juli 2000 utkast til nytt rammeverk på området for elektronisk kommunikasjon. Forslagene er:

- Forslag til Europaparlaments- og rådsdirektiv om et alminnelig regulatorisk rammeverk for elektronisk kommunikasjonsnett og -tjenester
- Forslag til Europaparlaments- og rådsdirektiv om tillatelser til etablering og drift av elektroniske kommunikasjonsnettverk og -tjenester
- Forslag til Europaparlaments- og rådsdirektiv om samfunnspålagte tjenester og forbrukerrettigheter relatert til elektroniske kommunikasjonsnettverk og -tjenester
- Forslag til Europaparlaments- og rådsdirektiv om tilgang til, og samtrafikk av, elektroniske kommunikasjonsnettverk og tilhørende elementer
- Forslag til Europaparlaments- og rådsdirektiv om ivaretagelse av personvern på området for elektronisk kommunikasjon

I tillegg ble følgende to forslag fremmet

– Forslag til Kommisjonsdirektiv om konkurranse i markedet for elektroniske kommunikasjonstjenester (2000/xx/EC)
– Forslag til Europaparlaments- og rådsvedtak om et regulatorisk rammeverk for frekvensforvaltning innenfor fellesskapet (KOM(2000)407)

Forslagene er nå til behandling i Det europeiske råd og Europaparlamentet, og forventes å tre i kraft i 2002/2003. Reguleringsforslagene fra Europakommisjonens side omhandler i liten grad sikkerhet og beredskap, selv om det legges opp til god funksjonalitet og at det skal sikres et høyt nivå for vern av brukerne. I tillegg presiseres det i direktivutkastet om tillatelser at rettsakten ikke er til hinder for at statene sikrer allmenne interesser som er anerkjent i traktaten, herunder beredskap og sikkerhetshensyn. Sikkerhet og beredskap i elektroniske nettverk står likevel på dagsorden i EU. Det europeiske råd vil sammen med Europakommisjonen utarbeide en samlet sikkerhetsstrategi for elektroniske nett. Det antas at det i første omgang er aktuelt å lage en handlingsplan, og at det på sikt eventuelt kan være aktuelt å opprette et europeisk organ som styrer sikkerhetsarbeidet innen sektoren.

4.2 Leveringsplikt og spesielle samfunnspålagte oppgaver (SSO)

For å sikre alle husstander og bedrifter over hele landet tilbud av grunnleggende teletjenester er Telenor i kraft av selskapets ledende posisjon på det norske telemarkedet, gjennom konsesjonsvilkår pålagt landsdekkende leveringsplikt (USO - Universal Service Obligations) for enkelte nærmere definerte tjenester. USO-forpliktelsen omfatter offentlig taletelefoni, katalogtjenester, telefonautomater, nødtjenester, og tjenester for funksjonshemmede og brukere med særskilte behov. Videre skal brukerne være i stand til å opprette tilgang til Internett. Telenor skal i tillegg levere spesielle samfunnspålagte oppgaver (SSO) som bl.a. omfatter ytelser til Totalforsvaret og nød- og sikkerhetstjenester knyttet til kystradioen. Merkostnader forbundet med SSO blir dekket gjennom offentlig kjøp av tjenester (kompensasjon for dokumenterte merkostnader) over statsbudsjettet.

Prinsipielt er det intet til hinder for at andre aktører kan konkurrere også om å levere de tjenestene som omfattes av USO-forpliktelsen, eller utføre spesielle samfunnspålagte oppgaver. I et etablert og velfungerende marked kan det være hensiktsmessig og effektivitetsfremmende å la flere aktører konkurrere om samfunnsoppgavene. En forutsetning for å innføre konkurranse om disse oppgavene vil imidlertid være at flere aktører har opparbeidet betryggende evne til å ivareta oppgavene på en tilfredsstillende og kontinuerlig måte i hele eller deler av landet.

4.3 Liberaliseringens betydning for teleberedskapen

Liberaliseringen av telesektoren har ført til flere tilbydere med egen infrastruktur. Fra et konkurranseperspektiv er dette positivt. Fra et sikkerhetsmessig perspektiv har utviklingen av konkurranse i telesektoren både positive og negative sider, som fordrer at myndighetene må gå gjennom og eventuelt endre ivaretakelsen av teleberedskapen i Norge i dag.

Økende konkurranse har medvirket til lavere priser og økende bruk av teletjenester. Prispresset medfører et tilsvarende kostnadspress som kan

innebære risiko for nedprioritering av kvalitets- og sikkerhetstiltak både fra tilbyders og brukers side. Sikkerhet i telenettene kan imidlertid være et virkemiddel i konkurransen, da det må antas at en rekke kunder som har strenge krav til sikkerhet vil foretrekke en tilbyder som kan dokumentere god sikkerhet i nettene. Fra et sikkerhetsmessig perspektiv vil det være positivt med egen infrastruktur hos flere tilbydere, dersom infrastrukturen kobles sammen slik at det blir flere alternative veier å sende trafikken hvis en del av nettet settes ut av drift.

Det må sikres at konkurransens negative sider for telesikkerhet og teleberedskap blir håndtert så godt som mulig, og at de positive sidene blir tatt vare på.

4.4 Regulatoriske virkemidler

For å få operatørene til å investere i tiltak rettet mot telesikkerhet og teleberedskap kan det være nødvendig med regulatoriske virkemidler gjennom lover, forskrifter eller enkeltvedtak. Slike regulatoriske virkemidler bør utformes slik at de blir fremtidsrettede og ikke får tilbakevirkende kraft. For eksempel kan en forskrift for fysisk sikring gjelde alle nye anlegg og større endringer av eksisterende anlegg.

Ulempen med bruk av lov og forskrift som virkemidler er at det kan ta tid før en oppnår full effekt av kravene. På sikt antas likevel lov- og forskriftsregulering å være effektivt for å sikre at nyinstallasjoner planlegges med tilstrekkelig telesikkerhet og teleberedskap.

Någjeldende telelov inneholder bestemmelser som på visse vilkår gir telemyndigheten kompetanse til å gi pålegg og fastsette forskrifter om sikringstiltak i telenett og teletjenester. I henhold til gjeldende forskrift om offentlig telenett og offentlig teletjeneste har teleoperatører plikt til å ha et minimumsnivå for telesikkerhet for å garantere leveringsdyktighet og sikring av kundenes telekommunikasjon.

4.5 Strategi for telesikkerhet og -beredskap tilpasset den nye markedssituasjonen

Svikt i telekommunikasjon kan få meget alvorlige konsekvenser for samfunnet så vel i fredstid som i krise- og beredskapssituasjoner. Økt avhengighet av telekommunikasjon og konsekvensene av svikt understreker viktigheten av å iverksette effektive, forebyggende tiltak. Sårbarhetsreduserende tiltak innenfor denne sektoren får dessuten ringvirkninger for en rekke andre funksjoner, og vil således i stor grad komme samfunnet som helhet til gode. Robuste telekommunikasjoner vil ha avgjørende betydning for beskyttelse av samfunnet ved at sentrale funksjoner i den normale samfunnsvirksomhet kan opprettholdes både i fred og ved krig.

Grovt sett vil trusselen mot telenettene innbefatte fem hovedkategorier av anslag og virkemidler. Disse fem er anslag med fysiske virkemidler mot infrastruktur, anslag med elektroniske virkemidler mot infrastruktur, manipulasjon med informasjonssystemer innen telefunksjonen, overbelastning av telenettene og sosiale trusler mot beslutningstakere i driftsfunksjonen i telenettene.

Sannsynligheten for alvorlig og langvarig svikt i teletjenester vurderes ut fra dagens trusselbilde å være liten overfor fysiske angrep. Logiske angrep ved forsøk på inntrenging i telenettenes IT-systemer anses i dag som en større reell trussel mot telenettene.

Selv om det er størst sannsynlighet for at telenettene skal bli utsatt for logiske angrep, kan konsekvensene som følge av fysiske angrep være så store at vi ikke kan se bort fra denne trusselen. Ikke minst er det viktig å merke seg at konsekvensen av et logisk angrep mot f.eks. et driftssystem er av betydelig kortere varighet enn et fysisk angrep mot det samme systemet. For å redusere risikoen mot norske telenett og teletjenester blir det derfor viktig å implementere tiltak som beskytter telenettene mot begge disse typene trusler, i tillegg til elektroniske trusler, overbelastning av nettene og sosiale trusler.

Som et generelt utgangspunkt kan det sies at operatørene sikrer seg mot hendelser som rammer aktørene i markedet ulikt, og som kan true produkt- og tjenestekvaliteten og dermed få betydning for den enkeltes konkurranseposisjon. Operatørene vil som hovedregel ikke sikre seg mot hendelser som rammer alle likt, eksempelvis gjelder dette både krig og større naturgitte hendelser som storm og flom. For Norge som nasjon er dette en lite tilfredsstillende løsning ettersom nasjonen også er avhengig av tilgang til teletjenester og telenett under naturkatastrofer, kriser og krig. Når operatørene ikke vil ivareta dette hensynet på egenhånd må staten involvere seg og sikre nødvendig robusthet utover det som er kommersielt interessant. Staten bør derfor i forkant sørge for at det iverksettes både skadeforebyggende og skadebøtende tiltak. Staten kan gjøre dette gjennom pålegg til bransjen eller ved kjøp av tjenester.

Som nevnt ovenfor er Telenor eneste tilbyder med teleberedskapsforpliktelser ved at selskapet gjennom konsesjon er pålagt å yte spesielle samfunnspålagte oppgaver (SSO) til Totalforsvaret. I et telemarked der andre operatører etter hvert begynner å få en posisjon på markedet vil det ikke være tilstrekkelig at kun én operatør er pålagt å levere teleberedskapstjenester. I 1999 hadde bl.a. Tele2 og Enitel til sammen en markedsandel på over 10 prosent for offentlig telefontjeneste. Vi kan dermed ikke lenger være sikre på at alle viktige brukere i Totalforsvaret har fasttelefonabonnement hos Telenor, og derigjennom også har en teleoperatør med visse beredskapsforpliktelser.

Dette betyr at SSO-ordningen slik den i dag er lagt opp ikke sikrer en tilfredsstillende beredskap i telesektoren, og at det må etableres et nytt SSO-konsept til erstatning for det vi har. En ny strategi for teleberedskap vil innebære at flere operatører i tillegg til Telenor vil få beredskapsforpliktelser. I praksis betyr dette at det settes krav som omfatter alle samfunnsviktige teleoperatører. Teleloven gir rettsgrunnlag om sikring av telenett også for andre tilbydere. Ansvaret for iverksettelse og daglig oppfølging av en ny ordning bør ivaretas av en organisatorisk enhet med høy teknisk og regulatorisk kompetanse.

Någjeldende SSO-ordning og den nye strategien atskiller seg dessuten ved at fremtidige teleberedskapstiltak også vil innbefatte tiltak rettet mot mobiltelefoni. Bruken av mobiltelefon har økt kraftig de senere år, med den konsekvens at samfunnet i større grad er avhengig av mobiltelefon som kommunikasjonsmiddel. Også innenfor Totalforsvaret blir deler av kommunika-

sjonsbehovet dekket gjennom bruk av mobiltelefon, og det er derfor viktig at mobiltelefon kan brukes også i ulike krisesituasjoner.

Ved utformingen av den nye strategien for telesikkerhet og teleberedskap har Samferdselsdepartementet tatt utgangspunkt i anbefalingene fra Forsvarets forskningsinstitutt (FFI) i prosjektet Beskyttelse av Samfunnet 2/Sårbarhetsreduserende tiltak innen telekommunikasjon (BAS2) og det frittstående prosjektet Teleberedskap i fritt konkurransemarked (TIFKOM), jf. vedlegg 1. Samferdselsdepartementet har fått nærmere utredet og kvalitetssikret de mest sentrale forslagene i TIFKOM-rapporten. TIFKOM-prosjektets sluttrapport har også vært sendt på bred høring, bl.a. til de øvrige departementene og en rekke aktører i telesektoren. Det er enighet blant høringsinstansene om at rapporten bør få en rask oppfølging. Det regjeringsoppnevnte Sårbarhetsutvalget støtter i all hovedsak TIFKOM-prosjektets forslag.

Å legge et særskilt myndighetsansvar knyttet til telesikkerhet og -beredskap til Post- og teletilsynet vil være et avgjørende organisatorisk og administrativt grep innenfor den nye strategien. For øvrig vil det være snakk om fysiske og teletekniske tiltak av både skadeforebyggende og skadebøtende karakter. Når myndighet for telesikkerhet og -beredskap er delegert til Post- og teletilsynet vil tilsynet i første omgang få i oppgave å arbeide videre med de tiltakene som omtales i kapittel 6-11. Det understrekes imidlertid at tilsynets nye oppgaver, som skisseres i kapittel 6-11, ikke må anses som uttømmende. Ytterligere oppgaver og tiltaksområder vil kunne komme til underveis som følge av den teknologiske og markedsmessige utviklingen innen sektoren. I kapittel 12 redegjøres det nærmere for de administrative og økonomiske konsekvensene som følger av strategien for telesikkerhet og -beredskap tilpasset et telemarked i fri konkurranse.

5 Organisering av arbeidet med telesikkerhet og -beredskap

5.1 Tilknytning, oppgaver og bemanning

Uansett hvilket nivå som velges for sikkerhet og beredskap i telenettene så vil myndighetene måtte tillegges omfattende oppgaver på området. I regjeringens fornyelsesprogram for offentlig sektor er det uttrykt en klar målsetting om å begrense/redusere antallet tilsynsenheter i statsforvaltningen. På teleområdet finnes det gjennom Post- og teletilsynet allerede et spesialisert tilsynsorgan som naturlig også bør få ansvaret for telesikkerhet og -beredskap.

På denne bakgrunn har Samferdselsdepartementet besluttet å delegere et særskilt myndighetsansvar for telesikkerhet og -beredskap til Post- og teletilsynet med følgende ansvarsområder:

- Sette krav til telesikkerhet og teleberedskap, og vurdere investeringer i tiltak for å øke robustheten i telenettene, f.eks. investeringer for å øke omrutingsmulighetene i telenettene, etablering av sikrede samlokaliseringssentra som flere operatører gis tilgang til, samt investeringer for å styrke telenettenes reparasjonsbehov og rehabiliteringsevne.
- Føre tilsyn med at pålagte tiltak blir iverksatt.
- Bevisstgjøring, kompetanseheving og veiledning overfor operatører, brukere og andre aktører (kurs, seminarer, bedriftsbesøk, etablering av kompetansefora etc.).
- Arrangere samøvelser og utvikle samarbeid mellom teleoperatørene.

Det vil være naturlig og ønskelig å integrere sikkerhets- og beredskapsarbeidet i den øvrige forvaltningen av telesektoren. Ved å legge også myndighetsansvaret for telesikkerhet og -beredskap til Post- og teletilsynet får teleoperatørene ett felles kontaktpunkt mot myndighetene. I Post- og teletilsynet vil det dessuten være god tilgang på relevant fagkompetanse. Dette er for øvrig i tråd med tilbakemeldingene fra høringen av TIFKOM-prosjektets sluttrapport.

Arbeidet med telesikkerhet og -beredskap må innplasseres i eksisterende organisasjon slik at det ikke oppstår noe motsetningsforhold/habilitetsproblematikk i forhold til andre arbeidsoppgaver.

Samferdselsdepartementet regner med at man for å få et kompetent sikkerhets- og beredskapsmiljø i Post- og teletilsynet bør ha en bemanning på minimum 4-7 personer. Bemanningsstørrelsen må tilpasses ambisjonsnivået for funksjonen, og departementet mener det bør være en gradvis og forsiktig oppbygging av dette feltet. Dessuten må det foretas en nøye avveining mellom den kompetanse tilsynet selv må ha og den kompetanse man kan kjøpe utenfra i tilknytning til de enkelte prosjekter. Beregninger viser at det vil koste i størrelsesorden 5-10 mill. kr å utføre de nye oppgavene i Post- og teletilsynet det første året med en bemanning på 4 personer. Av dette er 3,2 mill. kr rene etableringskostnader.

5.2 Finansiering av virksomheten

Med hjemmel i teleloven § 10-1 har Samferdselsdepartementet (jf. funksjonsfordelingsforskriften) fastsatt forskrift om gebyr til inntekt for Post- og teletilsynets virksomhet. Post- og teletilsynet kan ta inn gebyr for konsesjoner, tillatelser, tildelinger, for kostnader til planleggings-, registrerings-, standardiserings-, tilsyns- og annen forvaltningsvirksomhet i medhold av loven.

Sikring av telenett utføres med hjemmel i teleloven § 7-7. Det må antas at sikkerhetsrelatert virksomhet i hovedsak er å betrakte som «andre forvaltningstjenester», dvs. «annen forvaltningsvirksomhet», fordi sikkerhet inngår som en del av den tradisjonelle forvaltningen. Dette må være utgangspunktet så langt sikkerhetsvirksomheten er å betrakte som offentligrettslig virksomhet. Driftskostnader som påløper som følge av oppgaver relatert til telesikkerhet og -beredskap kan dermed finansieres ved gebyrer fra teleoperatørene.

Når det gjelder de øvrige tiltakene i telesikkerhet og -beredskap vil det bli nødvendig å vurdere alternative modeller for finansiering. Finansiering av konkrete tiltak vil kunne skje gjennom gebyrer, avgifter, egenfinansiering (operatørfinansiering), kundefinansiering eller bevilgninger over statsbudsjettet, jf. kapittel 12. Valg av finansieringsmåte vil avhenge av type tiltak og må derfor avgjøres konkret i forbindelse med beslutning om implementering av det enkelte tiltak. Det er viktig at det ved vurderingen sikres at finansieringen ikke gir utilsiktede konkurransevridninger.

5.3 Forholdet mellom Post- og teletilsynet og andre organer

Som ansvarlig for arbeidet med sikkerhet og beredskap i telesektoren vil Post- og teletilsynet måtte forholde seg til en rekke andre organisasjoner og enheter som har oppgaver relatert til sikkerhet og beredskap. Nedenfor følger en kort gjennomgang av tilsynets forhold til Totalforsvarets råd for sikring av tele- og informasjonssystemer (TRSTI) og to andre organisasjoner som er under planlegging, Nasjonal sikkerhetsmyndighet (NSM) og Senter for informasjonssikring.

5.3.1 Totalforsvarets råd for sikring av tele- og informasjonssystemer (TRSTI)

På beredskapssiden er det allerede skjedd enkelte endringer som følge av den endrede markedssituasjonen i telesektoren ved at den tidligere Totalforsvarets sambandsnemnd (TSBN), som ble ledet av Telenor, ble erstattet av et nytt råd fra 1. mars 1998. I likhet med TSBN skal også det nye rådet, Totalforsvarets råd for sikring av tele- og informasjonssystemer (TRSTI), gi råd til Samferdselsdepartementet i sikkerhets- og beredskapsspørsmål. I tillegg til at rådets ledelse og sekretariat er flyttet fra Telenor til Post- og teletilsynet, er representasjonen i det nye rådet bedre tilpasset den nye markedssituasjonen ved at ElTele Øst, Tele2, Enitel og NetCom er representert i tillegg til Telenor. Ved siden av de sivile nettoperatørene har TRSTI representanter fra ulike enheter i Forsvaret, Direktoratet for sivilt beredskap (DSB) samt sektorene kringkasting, luftfart, og bank- og finans. Samferdselsdepartementet deltar i rådet som observatør.

I rådets instruks heter det bl.a. at TRSTI skal utrede og foreslå forebyggende og skadebøtende tiltak basert på trusselbildet og risiko- og sårbarhetsvurderinger. Rådet skal innenfor rammen av gjeldende beredskaps-, tele-, data- og kringkastingslovgivning på eget initiativ og på forespørsel bl.a.:

- Utarbeide forslag til generelle sikrings- og beredskapskrav som bør stilles til nettutbyggere.
- Utarbeide forslag til policy og retningslinjer for prioritert bruk av tele- og informasjonssystemer/-tjenester innenfor Totalforsvaret, herunder komme med forslag til retningslinjer og policy for tilknytning og drift av slike systemer.
- Utarbeide forslag til tiltak for å sikre tilgjengelighet til prioriterte tele- og informasjonssystemer i Totalforsvaret.
- Gi bidrag til utarbeidelsen av langtidsplaner innenfor det sivile beredskap innen tele- og informasjonssektoren som er koordinert med aktuelle sikringstiltak i Forsvarets langtidsplanlegging.
- Foreslå beredskapstiltak innenfor sivile og militære tele- og informasjonssystemer med anslag over tiltakenes kostnad og forslag til prioritering innenfor gitte budsjettrammer. Forholdet mellom militære og sivile systemers bruksområder, herunder utnyttelse av Forsvarets sambandsnett for den sivile del av Totalforsvaret, belyses særskilt.
- Behandle saker om og gi høringsuttalelser til forslag til beredskapsrelaterte bestemmelser (i lov, forskrift eller konsesjonsdokument) rettet mot ulike operatører/aktører innenfor tele- og informasjonssektoren.
- Gi råd om nasjonal iverksetting av tiltak i samsvar med forslag fra den sivile kommunikasjonskomiteén i NATO.
- Foreslå utredning av viktige problemstillinger innenfor rådets virkefelt, herunder forskningsprosjekter.

Til støtte for rådets arbeid er det etablert en egen permanent arbeidsgruppe. Også denne gruppen har ledelse og sekretariat fra Post- og teletilsynet.

I høringsuttalelsene i forbindelse med TIFKOM-prosjektet kom det bl.a. forslag om å opprette en ressursgruppe med representanter fra sivile myndigheter, Forsvaret og teleoperatørene. Samferdselsdepartementet mener en slik ressursgruppe allerede finnes i form av TRSTI. Samferdselsdepartementet mener TRSTI bør bli en viktig medspiller som rådgivende organ også for Post- og teletilsynet. Bl.a. vil Post- og teletilsynet gjennom TRSTI ha et egnet forum for å få i stand tett samarbeid med telebransjen ved utredning og implementering av tiltak.

5.3.2 Forholdet til Nasjonal sikkerhetsmyndighet (NSM)

Ansvarsfordelingen mellom Post- og teletilsynet og det myndighetsorgan som etter sikkerhetsloven skal utøve oppgaven som Nasjonal sikkerhetsmyndighet (NSM) er nærmere utredet i samarbeid med Forsvarsdepartementet.

I sikkerhetsloven § 8 heter det at Nasjonal sikkerhetsmyndighet (NSM) skal koordinere de forebyggende sikkerhetstiltak og kontrollere sikkerhetstilstanden. NSM er også utøvende organ i forholdet til andre land og internasjonale organisasjoner. NSM har koordinerings- og kontrollansvaret, i praksis fagmyndighetsansvaret, for alle forebyggende sikkerhetstiltak som skal motvirke spionasje, sabotasje og terrorhandlinger som kan tenkes å skade rikets sikkerhet eller vitale nasjonale sikkerhetsinteresser. Dette fagmyndighetsan-

svaret har tverrsektoriell gjennomslagskraft i offentlig forvaltning og de deler av næringslivet som omfattes av loven. Fagmyndighetsansvaret vil derfor også gjelde innen telesektoren, men avgrenset til de deler som genererer eller behandler skjermingsverdig informasjon eller som råder over infrastruktur (skjermingsverdige objekter) som kan utsettes for sabotasje eller terrorhandlinger.

Post- og teletilsynet bør, avgrenset til telesektoren, ha som oppgave å utvikle løsninger for å kontrollere at de prosedyremessige eller tekniske sikkerhetstiltak som foreskrives i sikkerhetslov med forskrifter, ses i sammenheng med andre sikkerhetsmessige krav som stilles. Disse må på en koordinert måte ivaretas i sektoren. Post- og teletilsynet bør som en konsekvens av dette gi nødvendige råd og skriftlige veiledninger, eller om det foreligger behov og juridisk hjemmel, instrukser innen telesektoren. Post- og teletilsynet bør videre søke å identifisere sikkerhetsbehov innen telesektoren, som ikke er dekket av andre regelsett og tekniske løsninger, og fremme forslag til hvordan slike risikoer bør reduseres.

Forsvarsdepartementet har uttalt at etablering av et organ med spesielt ansvar for telesikkerhet og -beredskap vil bidra vesentlig innen dette felt i samfunnet generelt og i Totalforsvaret spesielt. Særlig er det viktig å få etablert en organisasjon som kan koordinere mellom det store antall teleoperatører i markedet og brukere med behov for tjenester med mer sikkerhet og beredskap enn det som det allmenne telenettet kan levere.

For øvrig er det i St.prp. nr. 45 (2000-2001) Omlegging av Forsvaret i perioden 2002-2005 foreslått at NSM etableres som et eget direktorat direkte underlagt Forsvarsdepartementet. Direktoratet vil benevnes Direktoratet for forebyggende sikkerhet.

5.3.3 Forholdet til et planlagt Senter for informasjonssikring

Det regjeringsoppnevnte Sårbarhetsutvalget har i sin utredning bl.a. foreslått at det bør etableres et Senter for informasjonssikring som bør ha som oppgave å koordinere deler av innsatsen for å styrke IKT-sikkerheten og bidra til en mer robust IKT-infrastruktur. Senter for informasjonssikring skal være et ressurs- og kompetansesenter for offentlige og private aktører. Det er foreslått at Senter for informasjonssikring bl.a. skal være det koordinerende og operative meldings- og håndteringssenter for sikkerhetsbrudd i norske nettverk innen næringsliv, statsforvaltning, utdanning, forskning og forsvar, og bidra til at sikkerhetsbrudd håndteres effektivt på tvers av sektorer og organisatoriske skiller. Senteret skal ikke ha myndighetsoppgaver.

Sårbarhetsutvalget har anbefalt at senteret i første omgang konsentrerer seg om et sett av kjerneoppgaver. Aktivitetsnivået kan deretter økes i løpet av en innkjøringsfase og vurderes løpende i forhold til brukernes behov. Utvalget ser det som en krevende oppgave å få etablert partnerskapet og den nødvendige tillit mellom aktørene. Det er fremhevet som viktig at senteret ikke dupliserer eksisterende aktiviteter.

For å komme raskt i gang er det våren 2001 igangsatt et forprosjekt av Nærings- og handelsdepartementet med deltakelse fra flere departementer. Forprosjektet skal bl.a. avklare forhold omkring formålet med et slikt senter, arbeidsoppgaver, organisering, lokalisering/tilknytning samt økonomiske og

administrative konsekvenser forbundet med etableringen av et Senter for informasjonssikring. Det legges opp til at regjeringen vil komme tilbake til dette.

Mens Post- og teletilsynet er et sektorspesifikt forvaltningsorgan med ansvar for å ivareta bl.a. sikkerhets- og beredskapstiltak i telesektoren, er Senter for informasjonssikring tenkt å skulle omfatte flere samfunnssektorer, der telesektoren vil være én av mange sektorer som bør være deltaker. Slik Samferdselsdepartementet ser det er det derfor ingen konflikt mellom Post- og teletilsynet og Senter for informasjonssikring ettersom de to enhetene vil ha ulike roller. Ansvarsområdene til de to enhetene vil imidlertid være nært beslektet, og det blir derfor viktig å få til et godt samarbeid mellom de to enhetene. På den måten kan man trekke veksler på den kunnskap som finnes og det arbeid som utføres i den enkelte enhet.

5.4 Samferdselsdepartementets konklusjon

Samferdselsdepartementet vil utvide Post- og teletilsynets myndighetsansvar til å omfatte også oppgaver i tilknytning til telesikkerhet og teleberedskap. Disse oppgavene må innplasseres i eksisterende organisasjon slik at det ikke oppstår noe motsetningsforhold/habilitetsproblematikk i forhold til andre arbeidsoppgaver.

Samferdselsdepartementet regner med at man for å få et kompetent sikkerhets- og beredskapsmiljø i Post- og teletilsynet bør ha en bemanning på 4-7 personer. Beregninger viser at det vil koste i størrelsesorden 5-10 mill. kr å utføre de nye oppgavene i Post- og teletilsynet første år, med en bemanning på 4 personer. Av dette er 3,2 mill. kr rene etableringskostnader. Samferdselsdepartementet går inn for at etableringskostnadene dekkes over Samferdselsdepartementets beredskapskapittel i statsbudsjettet, mens drift finansieres ved gebyrer fra teleoperatørene, på lik linje med Post- og teletilsynets øvrige virksomhet.

Når det gjelder investeringer i konkrete tiltak, vil det bli nødvendig å vurdere alternative modeller for finansiering. Finansiering vil kunne skje gjennom gebyrer, avgifter, egenfinansiering (operatørfinansiering), kundefinansiering eller bevilgninger over statsbudsjettet, jf. kapittel 12. Det er viktig at det ved vurderingen sikres at finansieringen ikke gir utilsiktede konkurransevridninger.

6 Prioritet i telenettene

Kapasiteten i telenettene er dimensjonert med mindre sambandsressurser tilgjengelig enn det som må til for at alle skal kunne benytte disse samtidig. En slik samtidig bruk er normalt heller ikke nødvendig ut fra et bruksmønster som fordeler seg over hele døgnet. Ved alvorlige hendelser, som større ulykker i et område, er det derimot sannsynlig at behovet for bruk av tjenestenettene vil øke sterkt i visse perioder. Dette kan medføre at ikke alle som ønsker det får tilgang til å bruke telenettene. Et felles behov for de prioriterte brukerne i Totalforsvaret, herunder nødetatene, er å bli sikret fremkommelighet i telenettene også i situasjoner der nettene blir overbelastet og ikke kan håndtere trafikkavvikling. For å sikre prioriterte brukere i Totalforsvaret tilgang til nettene også i kritiske situasjoner der mange ønsker å benytte telefon, må det implementeres spesielle prioriteringsmekanismer i telenettene.

6.1 Ordningen med viktig prioritert telefon (VPT)

Prioritet i telenettet er tidligere ivaretatt gjennom en ordning kalt viktig prioritert telefon (VPT). Ordningen er nå nedlagt med virkning fra årsskiftet 2000/2001. VPT-ordningen fungerte slik at dersom nettet befant seg i (eller det var fare for) en overbelastning, så kunne man manuelt fra en driftsterminal kutte summetonen til alle abonnenter bortsett fra de som hadde prioritet (dvs. VPT-abonnentene). Ordningen omfattet kun Telenors fastnett-abonnenter, og ved iverksettelse av ordningen kunne kun Telenor-abonnenter med prioritet initiere samtaler, mens alle andre abonnenter fremdeles kunne motta samtaler. Abonnenter tilknyttet andre operatørers nett hadde fortsatt mulighet til å ringe etter at VPT var iverksatt, så sant det var kapasitet i nettene og kundene ikke hadde fast forvalg (kunder med fast forvalg mistet summetonen på lik linje med Telenors abonnenter uten VPT).

Alternativt kunne også mobilnettene benyttes såfremt det var kapasitet i nettene. Ved iverksettelse av VPT ville derfor trolig alle Telenor-kunder som ikke var VPT-abonnenter samt abonnenter med fast forvalg i stedet forsøke å benytte mobiltelefonen. Et sannsynlig scenario kunne dermed vært at kapasiteten i mobilnettene ble sprengt og forårsaket sperr i nettene. Iverksettelse av VPT kunne med andre ord fått store konsekvenser dersom mobilnettene ble overbelastet.

Som nevnt ovenfor omfattet VPT-ordningen kun Telenors fastnett-abonnenter, og var således ikke tilpasset dagens telemarkedet med mange tilbydere av telefontjeneste samt økende bruk av mobiltelefon. Under Åsta-ulykken i januar 2000 ble mobilnettene overbelastet. Dette var et tilfelle der det virkelig hadde vært behov for å benytte en prioritetsfunksjon i nettene, men VPT kunne ikke benyttes her i og med at den omfattet kun fastnett-abonnenter. VPT kunne derimot bidratt til å forverre situasjonen ytterligere ved at trykket på mobilnettene kunne blitt enda større. Dette illustrerer at den gamle VPT-ordningen ikke var anvendelig i de situasjonene der det i dag er størst behov for prioritet. Det er også et åpent spørsmål om VPT-ordningen etter gammel modell kunne blitt anvendt i tilfelle krig. Med tanke på dagens sikkerhetspoli-

tiske situasjonen anbefalte Samferdselsdepartementet Justisdepartementet å legge ned VPT-ordningen f.o.m. 1. januar 2001. Justisdepartementet fulgte anbefalingen. I denne forbindelse kan det nevnes at de svenske telemyndighetene har gjort det samme ved at det gamle VPT-konseptet Telia hadde er lagt ned.

6.2 Ny prioritetsordning i telenettene

Ettersom prioriterte brukere i Totalforsvaret også i fremtiden vil ha behov for prioritet i telenettene, tilsier nedleggelsen av VPT-ordningen at man starter arbeidet med innføring av en ny prioritetsordning som skal gjelde både for fast- og mobiltelefoni og for alle teleoperatørene. Dette er i samsvar med TIFKOM-prosjektet som, på bakgrunn av svakhetene til den gamle ordningen, foreslo at VPT burde erstattes av en ny og bedre prioritetsordning for å sikre viktige brukere i Totalforsvaret prioritet under krise, beredskap og krig.

Det bør etableres en prioritetsordning som fungerer slik at alle abonnenter har et elektronisk «flagg» som indikerer prioritet. I en slik løsning vil nettet dynamisk og løpende overvåke trafikkbelastningen, og dersom en øvre grense blir nådd, vil kun de med prioritet bli gitt anledning til å ringe. Fordelen med en slik løsning fremfor VPT er bl.a. at den virker kontinuerlig uten at det må iverksettes noen manuelle tiltak før tjenesten er aktiv. Dette kalles derfor en sanntidsprioritetsordning.

Totalforsvarets råd for sikring av tele- og informasjonssystemer (TRSTI) har sluttet seg til en anbefaling om innføring av prioritert tjenesteaksess. I tillegg har Forsvarets forskningsinstitutt i BAS2-prosjektet foreslått at det bør innføres en ny sanntidsprioritetsordning i telenettene i Norge. Også alle de seks europeiske landene TIFKOM-prosjektet besøkte har innført et system for prioritet i telenettene.

6.2.1 Prioritet i fastnett

Teknisk sett er det mulig å gi brukere prioritet, og i regi av TRSTI har det pågått et arbeid for å kartlegge nærmere mulighetene for å implementere en slik tjeneste i de norske telenettene. Under TRSTIs arbeid er det kommet frem at det i det faste nettet er lagt et grunnlag for innføring av prioritert tjenesteaksess ved at alle abonnenter nå er tilknyttet digitale sentraler. Telenor har tidligere spesifisert og fått levert nødvendig funksjonalitet for såkalt «sambandsreservering» og «prioritert trafikk» i begge sentraltypene for å innføre et nytt prioritetssystem. Funksjonen er ikke testet og aktivert. Denne funksjonaliteten innebærer at en viss kapasitet i alle sambandsbunter reserveres for prioriterte brukere og at sentralene har mekanismer som beskytter mot overbelastning. Spesifikasjonene ble utarbeidet etter anbefalinger fra Totalforsvarets sambandsnemd (TRSTIs forløper, jf. kapittel 5.3.1) og vil i hovedsak tilfredsstille anbefalingene i BAS2- og TIFKOM-prosjektet. Prioriterte brukere i Totalforsvaret kan få tilgang til prioritet i fastnett, enten ved å ringe fra et telefonnummer som på forhånd er gitt prioritet, eller ved å taste en bestemt PIN-kode som vil gi prioritet i nettene fra et hvilket som helst telefonnummer. I tillegg bør det også være mulig å få aksess i fastnett via andre nett, f.eks. dedikerte nødnett, og samtidig opprettholde den prioriteten som dette nettet gir brukeren.

Som nevnt er denne prioritetsfunksjonen i fastnett imidlertid ikke tatt i bruk, og for å kunne iverksette denne funksjonen har Telenor opplyst at prioritert tjenesteaksess også må koordineres med øvrige tilbydere av offentlig telefontjeneste i Norge, dvs. at det både i samtrafikkgrensesnittet i signaleringssytem nr. 7 og i kommersielle samtrafikkavtaler må innarbeides en slik tjeneste hos alle operatørene. Tidsplanen for iverksetting av tjenesten må imidlertid tilpasses øvrig oppgradering av sentralene, og normalt tar det derfor 18 måneder fra beslutning om innføring til funksjonaliteten kan tas i bruk. Høsten 2002 er antydet som et mulig tidspunkt for implementering, forutsatt at det tidlig i 2001 tas en beslutning om innføring av prioritert tjenesteaksess.

Kostnadene ved å innføre ordningen er svært usikre fordi man ikke har testet og aktivert programvaren. Telenor har antydet at det for hvert av sentralsystemene (S12 og AXE) vil koste ca. 10 mill. kr å innføre prioritert tjenesteaksess. Disse kostnadene vil dekke bl.a. prosjektgjennomføring, test, eventuell tilpasning av funksjonen, implementering, driftsopplæring etc., og gjelder så fremt det er tilstrekkelig kapasitet i sentralene. Dersom også kapasiteten i sentralene må økes, kan kostnaden for innføring av prioritert tjenesteaksess komme opp mot 100 mill. kr for det ene sentralsystemet. I tillegg er det anslått at det vil koste ca. 6 mill. kr å oppdatere de administrative systemene som skal håndtere prioritert tjenesteaksess.

6.2.2 Prioritet i mobilnettene

Av kommersielle grunner ønsker verken Telenor eller NetCom å innføre et system for prioritert tjenesteaksess i GSM-nettene. Innvendingene er bl.a. frykt for at ikke-prioriterte brukere skal oppfatte en slik ordning som redusert tjenestekvalitet og at ordningen kan virke konkurransevridende. Samferdselsdepartementet er av den oppfatning at så lenge prioritetsordningen kun benyttes i krisesituasjoner og i forbindelse med ulykker vil kommersielle brukere ha forståelse for den type sambandsreservering. Skulle det derimot vise seg at prioriterte brukere i Totalforsvaret benytter seg av prioritetsfunksjonen også i det daglige, vil dette åpenbart kunne oppfattes som redusert tjenestekvalitet for andre kunder. Som en del av ordningen må det derfor utarbeides klare retningslinjer for når den kan benyttes, samt at det må være mulig å iverksette sanksjoner ved misbruk av ordningen. Samferdselsdepartementet har for øvrig vanskelig for å se hvordan en prioritetsordning som implementeres av alle mobiloperatørene vil virke konkurransevridende.

Det er allerede spesifisert en prioritetsfunksjon i GSM-standarden, men teknisk sett er full implementering problematisk fordi ikke alle utstyrsleverandørene som benyttes kan tilby denne funksjonaliteten per i dag. Dette skaper problemer med hensyn til å innføre tjenesten. Både Telenor og NetCom har imidlertid opplyst at det likevel er teknisk mulig å implementere en løsning med noe redusert funksjonalitet i forhold til standarden.

En slik løsning innebærer at brukerne inndeles i ulike prioritetsklasser og at prioriterte brukere kan utstyres med egne SIM-kort eller en PIN-kode som tastes for å få tilgang til prioritet i mobilnettene. Når det er flere som ønsker å bruke mobilnettene enn det er kapasitet til vil prioriterte brukere få tilgang til ledige talekanaler på nærmeste basestasjon så snart det blir ledig kapasitet. Den reduserte funksjonaliteten innebærer med andre ord at en prioritert bruker vil få prioritet til å initiere en samtale på nærmeste basestasjon, men ikke

prioritet for samtalen videre i nettene. Den skisserte løsningen muliggjør dermed ikke ende-til-ende prioritet for samtaler fra mobiltelefon.

Mobiloperatørene har uttalt at innføring av en redusert funksjonalitet for prioritert tjenesteaksess i mobilnettene muligens må kombineres med en økning av kapasiteten i radionettet. Grunnen til dette er at den reduserte løsningen ikke gir mulighet for at prioriterte samtaler kan bryte allerede pågående samtaler. Dermed kan prioriterte brukere i Totalforsvaret risikere å ikke få tilgang til mobilnettene i krisesituasjoner selv om de er med i prioritetsordningen. Post- og teletilsynet har uttalt at man i dag ikke kan se behov for økt kapasitet i radionettet.

Telenor og NetCom har på forespørsel fra Samferdselsdepartementet antydet at det vil koste ca. 10 mill. kr å oppgradere hvert av mobilnettene for innføring av en redusert funksjonalitet for prioritert tjenesteaksess, og at årlige driftskostnader vil komme på anslagsvis 2 mill. kr. Eventuell utbygging av reservekapasitet på basestasjonene kommer i tillegg. Telenor har antydet at kostnader for å utvide med radioressurser reservert for prioriterte brukere vil beløpe seg til ca. 250 mill. kr.

6.2.2.1 Øyeblikkelig prioritet til nødnumre

En annen nyttig funksjonalitet som kan tenkes innført sammen med prioritert tjenesteaksess i mobilnettene er øyeblikkelig prioritet til nødnumre. Dette innebærer at dersom man fra mobiltelefon forsøker å nå et nødnummer samtidig som all kapasiteten i nettet er i bruk, vil allerede pågående samtaler bli brutt for at samtalen til et nødnummer skal komme gjennom. En slik funksjonalitet kalles «instantan prioritet», og Samferdselsdepartementet mener funksjonaliteten bør søkes implementert som en del av prioritert tjenesteaksess i mobilnettene. Det er foreløpig ikke beregnet hva det vil koste å implementere instantan prioritet.

6.2.2.2 Nasjonal roaming i mobilnettene

Nasjonal roaming innebærer at en mobiloperatør med eget nett får anledning til å bruke nettet til en annen nasjonal mobiloperatør for sine kunder. Dette er først og fremst aktuelt i områder der vedkommende ikke selv har dekning. Slik kan mobiloperatører oppnå en større dekningsgrad enn det de kan oppnå ved egen utbygging.

Ved bygging av eget mobilnett basert på f.eks. DCS 1800 eller UMTS, vil det av frekvenstekniske årsaker antakelig ikke være økonomisk forsvarlig å bygge ut nettet til samme dekningsgrad som f.eks. et GSM 900 nett. Nasjonal roaming vil for samfunnet som helhet kunne bidra til at det ikke bygges mobilnett med større dekning enn det som er samfunnsmessig forsvarlig, og legge til rette for en mer miljøvennlig utbygging. Nasjonal roaming vil også kunne bidra til mer effektiv konkurranse.

I Norge er mobiloperatører med sterk markedsstilling pålagt å gi DCS 1800-operatører uten slik markedsstilling tilgang via nasjonal roaming. Kunden vil i slike tilfeller ikke ha noe abonnementsforhold til den mobiloperatøren som leverer nasjonal roaming, men vil i stedet bli belastet for bruken av dette nettet via den ordinære regningen fra DCS 1800-operatøren.

For å sikre at prioriterte brukere i Totalforsvaret til enhver tid kan nås i de områder hvor det er mobildekning, mener Samferdselsdepartementet det bør innføres nasjonal roaming i GSM-nettene for prioriterte brukere i Totalforsvaret. På denne måten kan disse brukerne ha kundeforhold til kun én av de tilgjengelige mobiloperatørene, samtidig som de har maksimal mobilkommunikasjonsdekning. Nasjonal roaming muliggjør også at prioriterte brukere i Totalforsvaret kan motta prioriterte samtaler over et større geografisk område. Nasjonal roaming er ikke implementert i GSM-nettene i dag fordi telemyndigheten har hatt et ønske om å fremme konkurransen mellom mobiloperatørene. For å opprettholde denne målsettingen skal nasjonal roaming kun benyttes i krisesituasjoner. Nasjonal roaming for prioriterte brukere i Totalforsvaret kan raskt settes i drift i krisesituasjoner, og vil bidra til økt beredskap. Det er heller ikke behov for store investeringer i nettet for å gjøre nasjonal roaming tilgjengelig for prioriterte brukere i Totalforsvaret.

Ifølge mobiloperatørene Telenor og NetCom kan nasjonal roaming etableres i dagens GSM-nett uten spesielle tekniske vanskeligheter. Prioriterte brukere utstyres med egne SIM-kort og innføring av systemet må innarbeides i samtrafikkavtalene mellom mobiloperatørene. Administrasjon og retningslinjer for en slik ordning må beskrives nærmere, og dette vil være en naturlig oppgave for Post- og teletilsynet.

6.2.2.3 Alternativ til prioritert tjenesteaksess i mobilnettene

Ettersom mobiloperatørene av kommersielle grunner ikke ønsker å innføre prioritert tjenesteaksess, er det foreslått at det alternativt kan anskaffes mobile basestasjoner som i en krisesituasjon kan etableres relativt raskt for å øke kapasiteten i et område. NetCom har etablert slike løsninger på ett døgns varsel. En kontinuerlig landsdekkende beredskap vil være avhengig av antallet slike enheter og geografisk utplassering. Samferdselsdepartementet er av den oppfatning at det i de situasjoner det vil være størst behov for prioritet i nettene, f.eks. ved større ulykker, ikke vil være tilstrekkelig at reservekapasitet kan etableres på ett døgns varsel. Departementet finner derfor ikke en slik løsning tilrådelig. Den internasjonale teleunions anbefaling om innføring av prioritetsmekanismer som skal virke på tvers av landgrensene kan for øvrig ikke oppfylles ved en slik løsning, jf. kapittel 6.3.

6.3 Prioritet på tvers av landegrensene - International Emergency Preference Scheme (IEPS)

Det er ikke bare under nasjonale kriser det er behov for prioritetsmekanismer i telenettene. Kriser kan involvere flere nasjoner, og i slike situasjoner vil beslutningstakere i flere land ha behov for å kommunisere med hverandre. Selv om det enkelte land har implementert prioritetsfunksjoner nasjonalt betyr ikke det at ordningen vil virke internasjonalt også. For at man skal være sikker på at disse beslutningstakerne når frem til sine kolleger i andre land, er det viktig at prioritetsfunksjonene i det enkelte land også vil gjelde på tvers av landegrensene. I NATO har man sett behovet for en slik prioriteringsmekanisme, og for NATO er dette spesielt viktig ved håndtering av sikkerhetspolitiske kriser og krig der flere nasjoner er involvert. På denne bakgrunn har NATOs sivile kommunikasjonskomité CCPC utarbeidet forslag til hvordan en

internasjonal prioritetsordning kan fungere. CCPCs forslag ble oversendt til den internasjonale teleunionen (ITU) som i mars 2000 ga en anbefaling om prioritert tjenesteaksess over landegrensene.

ITU-rekommendasjonen E.106, «Description of an International Emergency Preference Scheme» (IEPS), gjelder både faste nett og mobiltelefonsystemer. Formålet med rekommendasjonen er å beskrive et system som sikrer prioriterte brukere tilgang til internasjonale telefonforbindelser ved internasjonale krisesituasjoner. Systemet skal fungere selv om det ikke er nasjonal krise der brukeren oppholder seg. Det er viktig å merke seg at ITU-rekommendasjonen spesielt nevner at internasjonale og nasjonale ordninger for å sikre prioritet bør kunne operere uavhengig av hverandre, men samtidig må de være kompatible. En prioritert bruker av en nasjonal ordning trenger ikke være IEPS-bruker, mens en IEPS-bruker sannsynligvis trenger begge ordninger implementert. ITU-rekommendasjonen er svært generell og kan betraktes som en anbefaling til nasjonale myndigheter og nettoperatører om å inngå avtaler på tvers av landegrensene for å støtte formidling av prioriterte samtaler. Det legges opp til at det må inngås bilaterale avtaler mellom myndigheter og teleoperatører for å sikre IEPS-brukere tilgang til teletjenester på tvers av landegrensene.

ITU-rekommendasjonen åpner for ulike former for aksess til IEPS. Aksess kan f.eks. skje fra forhåndsbestemte abonnentlinjer tilsvarende opplegget rundt VPT-ordningen, fra brukere med spesiell prioritet, f.eks. ved bruk av PIN-kode, eller aksess fra dedikerte nødnett. IEPS kan derfor ses på som en anbefaling om kompatibilitet mellom ulike systemer og er ikke en detaljert spesifikasjon av et nytt prioritetssystem.

Det sentrale i IEPS-anbefalingen er at samtaler fra prioriterte brukere må «markeres» med prioritet i telefonsentralen. Denne prioritetsmarkeringen må følge samtalen fra ende-til-ende, dvs. fra abonnent A til abonnent B gjennom alle nett, også når samtalen rutes fra et land til et annet.

6.3.1 Nasjonale konsekvenser

IEPS-anbefalingen kan benyttes som et grunnlag for å sikre prioritet for samtaler som transporteres over forskjellige telenett nasjonalt. Det var bl.a. et problem med den gamle VPT-ordningen at den kun var et tilbud til Telenors kunder, og at prioriteringen opphørte dersom man valgte å flytte abonnementet på telefontjenester til en av de andre teleoperatørene. Som nevnt i avsnitt 6.2.2 kan det bli vanskelig å innføre prioritert tjenesteaksess i mobilnettene ettersom den prioritetsfunksjonen som er spesifisert i GSM-standarden ikke støttes av alle utstyrsleverandørene. I utgangspunktet er det derfor bare mulig å innføre en løsning med noe redusert funksjonalitet, og som kun gir prioritet på radiogrensesnittet, dvs. at den prioriterte brukeren vil få prioritet til å initiere en samtale på nærmeste basestasjon, men ikke prioritet videre i nettene. Denne løsningen muliggjør med andre ord ikke ende-til-ende prioritet for samtaler fra mobiltelefon, og er således ikke i samsvar med IEPS-anbefalingen.

I arbeidet med å innføre en ny ordning for prioritert tjenesteaksess må det tas hensyn til de anbefalinger som gis i ITU-rekommendasjonen, slik at det nye systemet blir kompatibelt med IEPS. Bl.a. bør Post- og teletilsynet påse at Telenor innarbeider prioritert tjenesteaksess i samtrafikkavtalene med andre nettoperatører og tjenesteleverandører, slik at øvrige aktører som tilbyr

offentlig telefontjeneste blir integrert i et nytt prioritetssystem. Den prioritetsordningen som kan innføres i mobilnettene muliggjør ikke ende-til-ende-prioritet slik IEPS anbefaler. Dersom det satses på den reduserte løsningen, vil det bety at det uansett må investeres i ny funksjonalitet når IEPS innføres. Den prioritetsfunksjon som allerede er spesifisert i GSM-standarden muliggjør imidlertid ende-til-ende-prioritet, men kan, som nevnt ovenfor, ikke innføres per i dag fordi én av utstyrsleverandørene ikke tilbyr denne funksjonaliteten. Post- og teletilsynet bør sammen mobiloperatørene ta initiativ overfor denne leverandøren for å søke å få levert prioritet i henhold til GSM-standarden.

Dersom dette ikke lar seg gjøre kan det i første omgang bli aktuelt å innføre en todelt prioritetsfunksjon for GSM, ved at den gjeldende GSM-standarden innføres der det er mulig, mens det i de delene av nettene som har utstyr fra den ene leverandøren innføres en redusert prioritetsfunksjon. Den reduserte løsningen kan som nevnt ikke bryte samtaler og det kan dermed ta lengre tid å få initiert en prioritert samtale, men bortsett fra dette vil ikke brukerne merke at det er to ulike prioritetsmekanismer implementert i nettene. Samferdselsdepartementet mener dette er en bedre løsning enn å implementere en redusert funksjon i hele mobilnettet.

Når det gjelder prioritetsordninger i telenettene, bør det bemerkes at det i dag er sterkt fokus på prioritet for talekommunikasjon. I tiden fremover vil imidlertid behovet for prioritet av datakommunikasjon øke. Dette vil medføre at det også kan være behov for muligheten til å prioritere innen datakommunikasjon slik at viktig informasjon får høyere prioritet enn f.eks. spill. Dette er en problemstilling Post- og teletilsynet vil måtte arbeide videre med, også fordi ITU-rekommendasjonen om IEPS omhandler prioritet for datakommunikasjon.

6.4 Administrative rutiner

Felles for ovennevnte prioritetsordninger, og uavhengig av valg av teknisk løsning, er den administrative siden knyttet til prioritert tjenesteaksess. Før tjenesten kan fungere tilfredsstillende og oppfylle den hensikt den er tiltenkt må alle forhold rundt det administrative være på plass. Her er det mange erfaringer fra den gamle VPT-ordning som vil være nyttige i utformingen av det administrative rammeverk også for en ny prioritetsordning. TIFKOM-prosjektet har anbefalt at den administrative siden, dvs. vedlikehold av informasjon om hvem som anses som prioritere brukere, og videreformidling av denne informasjonen til operatørene bør koordineres av Direktoratet for sivilt beredskap (DSB), mens Post- og teletilsynet bør ha som ansvar å veilede brukere. DSB er allerede bedt om, som en forberedelse til innføring av en eventuell ny prioritetsordning, å utarbeide forslag til klare retningslinjer og rutiner for utvelgelse av personer som bør ha prioritet, samt effektive rutiner for innmelding av endringer og kontinuerlig oppdatering av abonnentlistene. I denne forbindelse vil det også bli fremskaffet en komplett oversikt over de personer som tidligere hadde VPT-abonnement. DSB startet dette arbeidet like over nyttår 2001.

6.5 Samferdselsdepartementets vurderinger og konklusjoner

Samferdselsdepartementet vil arbeide for at det blir implementert en funksjon for prioritert tjenesteaksess både i faste nett og mobilnettene, for å sikre at forhåndsdefinerte viktige abonnenter får prioritet i situasjoner der nettene eller deler av nettene er overbelastet. En ny prioritetsordning vil bli implementert basert på krav utarbeidet av Post- og teletilsynet. Krav til en ny prioritetsordning som skal gjelde for alle tilbydere av offentlig telefontjeneste både i faste nett og mobilnettene vil bl.a. være:

- Det må være en sanntidsprioritetsordning.
- Øyeblikkelig prioritet til nødnumre fra mobiltelefoner inkluderes, dvs. en oppringing til et nødnummer kan avbryte allerede pågående samtaler.
- Nasjonal roaming i GSM-nettene innføres for prioriterte brukere i Totalforsvaret.
- Prioritetsordningen tilpasses ITUs IEPS-anbefaling. Det betyr at den reduserte løsningen for prioritet i mobilnettene ikke kan innføres. Post- og teletilsynet bør sammen med mobiloperatørene ta initiativ overfor denne leverandøren for å søke å få levert prioritet i henhold til GSM-standarden. Dersom dette ikke lar seg gjøre kan det i første omgang bli aktuelt å innføre en todelt prioritetsfunksjon for GSM, ved at den gjeldende GSM-standarden innføres der det er mulig, mens det i de øvrige delene av nettene innføres en redusert prioritetsfunksjon.
- Telenor innarbeider prioritert tjenesteaksess i samtrafikkavtalene med andre nettoperatører og tjenesteleverandører, slik at øvrige aktører som tilbyr offentlig telefontjeneste blir integrert i et nytt prioritetssystem.
- Post- og teletilsynet tar initiativ overfor de operatørene som skal bygge ut tredje generasjons mobilnett (UMTS) slik at det i disse nettene på et tidlig tidspunkt kan legges til rette for implementering av en prioritetsordning som muliggjør ende-til-ende-prioritet i henhold til IEPS-anbefalingene.

Når det gjelder prioritetsordninger i telenettene, er det i dag sterkt fokus på prioritet for talekommunikasjon. I tiden fremover vil imidlertid behovet for prioritet av datakommunikasjon øke slik at viktig informasjon får høyere prioritet enn f.eks. spill. Dette er en problemstilling Post- og teletilsynet vil måtte arbeide videre med.

7 Samlokalisering i fjellanlegg

Telenettene består av en del vitalt utstyr som er avgjørende for at telenettene skal fungere tilfredsstillende. Dette er utstyr av høy verdi og som det er vanskelig å gjenanskaffe ved ødeleggelse. Dersom slikt utstyr blir ødelagt, vil funksjonaliteten i telenettene bli degradert, og i verste fall vil telekommunikasjonen falle ut. Et logisk angrep mot slikt utstyr vil sette utstyret midlertidig ut av funksjon, mens et fysisk angrep kan medføre permanent ødeleggelse. Dersom man ønsker å sette telenettene ut av funksjon for et lengre tidsrom, kan dette altså mest effektivt oppnås gjennom fysisk angrep mot vitalt utstyr. Utstyr av høy verdi eller utstyr som det tar lang tid å gjenanskaffe ved ødeleggelse kan beskyttes mot ytre fysiske og elektromagnetiske påkjenninger ved at utstyret blir plassert i fjellanlegg.

Et fjellanlegg er dimensjonert etter bomberomsforskriftene, offentlig tilfluktsrom, klasse A. Et slikt anlegg er beskyttet mot krigshandlinger med konvensjonelle våpen og ABC-våpen, og er således sikret mot både trykk, gass og elektromagnetisk stråling. Ettersom det i fjellanleggene vil være plassert utstyr som er svært viktig for telenettenes funksjon vil disse anleggene være svært attraktive mål for en fiende som ønsker å sette telenettene i Norge ut av funksjon. Fjellanleggene er derfor også utstyrt med overvåknings- og varslingsfunksjoner og reaksjonsmuligheter dersom det viser seg at noen er i ferd med å ta seg inn i et anlegg.

7.1 Nasjonale samlokaliseringssentra i fjellanlegg

Telenor er i dag eier av en rekke fjellanlegg rundt om i landet, slik at en del av teleinfrastrukturen allerede er lokalisert i fjellanlegg og således er sikret mot fysiske trusler. Disse anleggene ble bygd av det gamle Televerket i perioden 1965 til 1992. Televerket har i hovedsak finansiert byggingen over eget budsjett ved bevilgninger over statsbudsjettet, men i noen tilfeller ble det også bevilget midler til dette formål over Samferdselsdepartementets beredskapsbudsjett. I tillegg til at anleggene benyttes av Telenor til kommersielle formål er selskapet gjennom konsesjon pålagt å opprettholde disse anleggene ut fra totalforsvarsformål. Inntil telemonopolet opphørte 01.01.1998 måtte Telenor selv dekke Totalforsvarets andel av kostnadene for fjellanleggene, som en motytelse for enerettsområdet. Fra og med 1998 har imidlertid Telenor fått kompensert Totalforsvarets andel av kostnaden for fjellanleggene ved at dette tiltaket inngår i SSO-ordningen, jf. kapittel 4.2 og 4.5.

Samferdselsdepartementet anser det viktig på sikt å sørge for at infrastrukturen til alle tjenesteleverandører av betydning er tilfredsstillende sikret. Et av hovedforslagene til TIFKOM-prosjektet er at vitalt telekommunikasjonsutstyr, dvs. utstyr av høy verdi eller utstyr som det tar lang tid å gjenanskaffe ved ødeleggelse og som er viktig for at telenettene skal fungere, bør plasseres i fjellanlegg for å være godt beskyttet mot fysiske trusler og elektromagnetisk stråling. TIFKOM-prosjektet har foreslått at Telenors fjellanlegg bør benyttes til dette formålet ved at de oppgraderes til sikrede samlokaliseringssentra hvor også andre teleoperatører kan plassere vitalt telekommunikasjonsutstyr.

I tillegg har prosjektet foreslått at det skal bygges enkelte helt nye samlokaliseringssentra. Slik vil man kunne oppnå beskyttelse mot fysiske trusler og samtidig være i stand til å utnytte mangfoldet i markedet uten at samlokalisering medfører økt sårbarhet.

I tillegg til at man gjennom samlokalisering samlet vil oppnå et høyere fysisk sikkerhetsnivå, vil det bli lettere å implementere andre tiltak, som f.eks. forberedte sammenkoblingspunkter mellom de ulike operatørenes nett. Operatørene ser også kommersielle fordeler ved samlokalisering. Derfor er det flere som tilbyr samlokalisering i såkalte «telehotell» på kommersielle betingelser i dag. Disse telehotellene er ikke nødvendigvis sikret på samme nivå som fjellanleggene. Det er derfor viktig å komme denne utviklingen i forkjøpet gjennom utvikling av gode, sikre alternativer. Post- og teletilsynet bør vurdere nærmere hvilke sikkerhetskrav som bør stilles til slike anlegg.

7.2 Modeller for samlokalisering i fjellanlegg

Samlokaliseringssentraene kan tenkes etablert på to ulike måter. Det ene alternativet er at staten overtar eierskapet til fjellanleggene og setter bort driften av disse til en operatør (eller annen egnet virksomhet) som igjen leier ut anleggene til teleoperatører. Det andre alternativet går ut på at Telenor fremdeles eier anleggene, men leier dem ut til andre operatører.

7.2.1 Staten overtar eierskapet til Telenors fjellanlegg

Fordelen med staten som eier av fjellanleggene er at andre operatører vil oppfatte stedet som nøytral grunn, og mange teleoperatører har fremhevet dette som viktig dersom de skal ønske å flytte inn i et samlokaliseringssenter. Ved en slik løsning vil da Telenor kunne leie sitt arealbehov i fjellanlegg på lik linje med andre operatører.

Statlig overtakelse av fjellanleggene ved ordinært kjøp vil imidlertid innebære et betydelig kapitalbehov for staten ved at det er anslått at fjellanleggene har en samlet markedsverdi på tilnærmet 1,2 mrd. kr.

Dersom staten skal overta fjellanleggene kan dette enklest skje gjennom en kapitalnedsettelse der staten innløser aksjer tilsvarende anleggenes verdi. Et slikt alternativ vil ikke medføre et finansieringsbehov for staten. Ved statlig overtakelse av anleggene må det ved prisfastsettelsen tas hensyn til at staten tidligere har gitt direkte investeringstilskudd til Telenor ved byggingen av noen av fjellanleggene. Det må også tas hensyn til den kompensasjon Telenor gjennom SSO-ordningen har mottatt for investeringer i fjellanleggene.

7.2.2 Telenor beholder eierskapet til fjellanleggene

Dersom Telenor beholder eierskapet til fjellanleggene og leier ut arealer som samlokaliseringssentra, bør det eventuelt skilles ut en egen enhet fra Telenor som kan ta seg av administrasjon og utleie av fjellanleggene slik at det skapes større distanse til de øvrige delene av Telenor. Staten kan alternativt leie arealer fra Telenor, for så å fremleie disse til andre operatører og Telenor.

I Sverige har man satset på samlokalisering av teleoperatører i fjellanlegg basert på en modell der én operatør eier og står for utleie og drift av anleggene. Den svenske Post- och telestyrelsen har finansiert og tatt initiativ til

utbyggingen av flere fjellanlegg til samlokaliseringsformål. Utbyggingen har skjedd etter forutgående anbudskonkurranser blant svenske konsulenter og entreprenører. De ferdigstilte anleggene har blitt overdratt fra Post- och telestyrelsen til Telias eiendomsselskap. Dette eiendomsselskapet er forpliktet til å drive fjellanleggene som «operatørhotell», der operatører kan leie arealer som bare de selv får adgang til, dvs. at hver operatør bare har adgang til sine egne avgrensede lokaler med systemer og utstyr. Driften av fjellanleggene skal være kostnadseffektiv, og leien er basert på drifts- og vedlikeholdskostnader, ettersom alle investeringskostnader allerede er betalt av Post- och telestyrelsen. Leien pr. kvadratmeter er derfor svært lav og attraktiv. En annen fordel med «operatørhotell»-konseptet er at fysiske sammenkoblinger mellom ulike operatørers nett blir enkelt og kan skje i beskyttede omgivelser

7.2.3 TIFKOM-prosjektets anbefaling vedrørende valg av modell for samlokalisering i fjellanlegg

TIFKOM-prosjektet har anbefalt at Norge i likhet med Sverige bør ha tilbud til teleoperatørene om samlokalisering i fjellanlegg. TIFKOM-prosjektet mener de viktigste begrunnelsene for ønsket om samlokalisering i fjellanlegg bør være:

– høyt telesikkerhets- og beredskapsnivå,
– et realiserbart samlokaliseringskonsept som ikke er konkurransevridende, og
– grunnlag for et godt samarbeid mellom operatørene.

Selv om prosjektet primært anbefaler en løsning der staten overtar eierskapet til anleggene, gis det samtidig uttrykk for at selve eierskapet er av underordnet betydning så lenge formålet med samlokalisering oppnås.

TIFKOM-prosjektet har foreslått at samlokalisering i fjellanlegg bør skje i to trinn. I trinn 1 overtar staten ti fjellanlegg fra Telenor, oppgraderer fem av disse anleggene til samlokaliseringssentra, samt bygger to helt nye fjellanlegg for samlokalisering. I trinn 2 oppgraderes ytterligere fem anlegg til samlokaliseringssentra og det bygge tre nye anlegg for samlokalisering.

Prosjektet anbefaler at trinn 1 gjennomføres i løpet av en femårsperiode, mens det på lang sikt bør være et mål å gjennomføre også trinn 2. Samlet kostnad for trinn 1 og 2 inklusiv kostnader for overtakelse av fjellanleggene fra Telenor er anslagsvis 1,9 mrd. kr. I tillegg kommer kostnader for flytting av operatørenes utstyr inn i samlokaliseringssentraene.

7.3 Sentrale forutsetninger for innføring av samlokalisering i fjellanlegg

For at det skal være mulig å gjennomføre samlokalisering i fjellanlegg, er det en rekke forutsetninger som må være oppfylt. Samferdselsdepartementets utgangspunkt er at samlokalisering bør være frivillig. TIFKOM-prosjektet har dessuten fremhevet viktigheten av gunstig leiepris slik at operatørene får insitament til å benytte seg av sikrede samlokaliseringssentra. Subsidierte leiepriser kan utgjøre et problem i forhold til EU-regelverket for offentlig støtte. Et annet forhold som det bør tas hensyn til er at eventuell etablering av sikrede samlokaliseringssentra representerer en sentralisering av viktig utstyr og

funksjoner i telenettene. Dette vil være negativt for sårbarheten i telenettene, og fordrer at man samtidig gjennomfører tiltak for å redusere denne økte sårbarheten. Disse problemstillingene vil det bli redegjort nærmere for i det følgende.

7.3.1 Forutsetninger for at teleoperatørene skal ønske å flytte inn i samlokaliseringssentra i fjell

Samferdselsdepartementet har gjennomført en kartlegging av teleoperatørenes interesse for å plassere viktig teknisk utstyr i sikrede samlokaliseringssentra. Resultatene fra denne undersøkelsen viser at operatørene kun ønsker å flytte inn i et samlokaliseringssenter i de tilfeller der fjellanleggets lokalisering sammenfaller med deres utbyggingsplaner. Dersom staten overtar eierskapet til flere fjellanlegg og det på et senere tidspunkt viser seg at operatørene ikke ønsker å leie arealer, kan man i verste fall risikere at staten sitter med svært dyre arealer som samfunnet ikke får noen nytte av. Operatørene er for øvrig av den oppfatning at staten må dekke alle de kostnader som påløper som følge av en eventuell flytting fra dagens lokaliteter og inn i fjellanlegg.

Operatørene har dessuten satt som forutsetning at arealene i fjellanlegg må ha spesielt gunstige leiepriser. En modell for å oppnå gunstige leiepriser er at staten dekker kostnadene for overtakelse og ombygging av fjellanleggene. Operatørenes utlegg vil da bli begrenset til å dekke drifts- og vedlikeholdskostnader, og dette vil gi teleoperatørene insitament til å foretrekke å plassere sitt utstyr i sikrede samlokaliseringssentra, jf. den svenske modellen beskrevet i kapittel 7.2.2.

Lokalisering i fjellanlegg har utvilsomt en del ulemper av ikke-sikkerhetsmessig art ved at det bl.a. kan være vanskelig å få personell til å jobbe i disse anleggene over tid. Man må derfor kompensere disse bedre enn om de hadde hatt et annet arbeidssted. Selv om anleggene stort sett finnes i tilknytning til byer, så er de lokalisert utenfor allfarvei, og dette kan også gjøre det problematisk å skaffe kvalifisert personell. Den usentrale beliggenheten kan dessuten medføre at avstanden til teleoperatørenes øvrige virksomhet blir stor. Operatørene får dermed ekstraordinære kablingsutgifter for å innlemme fjellanleggene i sine nett.

På et tidlig tidspunkt ble det uttrykt en viss interesse for en atskillig mer begrenset modell som ville innebære samlokalisering i 1-2 fjellanlegg der flere operatører kunne plassere back-up drifts- og overvåkingsutstyr. En grundigere undersøkelse avdekket imidlertid at den interessen som først kom til uttrykk likevel ikke var tilstede i tilstrekkelig grad. De store og etablerte operatørene ønsker ikke et slikt tilbud ettersom de har etablert andre løsninger for å ivareta denne funksjonen. De relativt nyetablerte operatørene har imidlertid uttrykt en viss interesse for et tilbud om å plassere utstyr i et felles reservesenter for drifts- og overvåkingsutstyr. Forutsetningen er at reservesenteret etableres i et fjellanlegg i nærheten av andre lokaliteter operatøren har. Alle de operatørene som har uttrykt en viss interesse, ønsker plass i Oslo-området, samtidig som kablingsdistansen må være liten. Dette kan være et problem med tanke på eksisterende utvalg av fjellhaller i Oslo-området.

Med de forutsetningene operatørene har for å skulle ønske å flytte inn i fjellanlegg, kan det se ut som det blir vanskelig å få til samlokalisering i sikrede anlegg hvis det skal skje på frivillig basis. Alternativet vil da være å stille

som krav at de operatørene som skal levere teletjenester til Totalforsvaret skal ha vitalt telekommunikasjonsutstyr i fjellanlegg, jf. kapittel 10.2 om klassifisering av teleinfrastrukturen.

7.3.2 Mulige problemstillinger i forhold til EUs regelverk for offentlig støtte

At staten eventuelt dekker investeringskostnadene for overtakelse og ombygging av aktuelle fjellanlegg, medfører behov for avklaring av spørsmålet om ulovlig subsidiering i henhold til EUs regelverk for offentlig støtte. Denne problemstillingen er forelagt Nærings- og handelsdepartementet.

Nærings- og handelsdepartementet mener at det foreligger ulovlig støtte etter artikkel 61(1) i EØS-avtalen dersom en markedsaktør får en økonomisk fordel som andre markedsaktører ikke får tilgang til. Forbudet omfatter støtte i enhver form som vrir eller truer med å vri konkurransen på EØS-markedet. Dette innebærer at tilbakesalg av eiendom til offentlige myndigheter over markedspris, utleie fra det offentlige til kommersielle aktører under markedspris og offentlig kompensasjon for bestemte utgifter kan utgjøre støtte som anses ulovlig i medhold av artikkel 61(1) i EØS-avtalen.

7.3.2.1 Unntak for anvendelse av EØS-avtalens bestemmelser

Dersom man skulle komme til at det foreligger offentlig støtte etter artikkel 61(1) i EØS-avtalen, kan avtalens artikkel 59(2) gi grunnlag for unntak for anvendelse av avtalens bestemmelser, deriblant statsstøttereglene. EØS-avtalens bestemmelser om offentlig støtte gjelder både for offentlige foretak og for foretak som EFTA-statene gir særlige eller eksklusive rettigheter, jf. artikkel 59(1) EØS. Foretak som er blitt tillagt oppgaven å utføre tjenester av allmenn økonomisk betydning kan imidlertid unntas etter artikkel 59(2) EØS i den utstrekning anvendelsen av disse reglene rettslig eller faktisk hindrer dem i å utføre de særlige oppgaver som er tillagt dem.

Det avgjørende her er hvorvidt telesikkerhet og teleberedskap er oppgaver som myndighetene anser for å være i allmennhetens interesse, og som av den grunn må tilsikres borgerne under tilsyn av det offentlige. Dette vilkåret må utvilsomt anses som oppfylt.

Det er etter artikkel 59(2) EØS også et vilkår at det offentlige positivt har gitt foretaket i oppgave å utføre den aktuelle funksjon. Det er imidlertid ikke avgjørende hvorvidt dette skjer gjennom konsesjonsbehandling, i lovs form eller på annen måte. Med hjemmel i teleloven § 7-7 kan Samferdselsdepartementet gi pålegg om at private aktører skal utføre særlige oppgaver knyttet til teleberedskap og telesikkerhet.

Markedspris på utleie vil trolig gjøre det umulig og uinteressant for aktuelle markedsaktører å flytte inn i fjellanleggene. Dette er etter Nærings- og handelsdepartementets oppfatning et argument for at leieprisene bør kunne fastsettes til et nivå som gjør at det er interessant for potensielle leietakere å flytte inn i fjellanleggene.

Dersom vilkårene for å anvende artikkel 59(2) er oppfylt, må leieprisen på fjellanleggene ikke settes lavere enn nødvendig for at markedsaktørene skal finne det interessant å flytte inn.

Når det gjelder forholdet til EU-regelverket om statsstøtte, har man i Sverige lagt til grunn at bygging av fjellanlegg er et tiltak som er begrunnet ut fra forsvarsformål, og således er unntatt fra EU-regelverket om statsstøtte i medhold av en bestemmelse i EU-traktaten tilsvarende EØS-avtalens artikkel 123. Artikkel 123 er en unntaksbestemmelse for at EØS-avtalen ikke skal hindre EFTA EEA-landene i å treffe tiltak på områder knyttet til offentlig orden og forsvar.

7.3.2.2 Plikt til å notifisere støtteordninger

Dersom man velger en løsning som innebærer støtte etter EØS-avtalen artikkel 61(1), er norske myndigheter gjennom EØS-avtalen og overvåknings- og domstolsavtalen mellom EFTA-landene forpliktet til å notifisere nye støtteordninger og endringer i eksisterende støtteordninger til EFTAs overvåkningsorgan. Unnlatelse av dette kan medføre at EFTAs overvåkningsorgan finner en støtteordning ulovlig på prosessuelt grunnlag. Notifiseringsplikten gjelder også støtteordninger som faller inn under unntaksbestemmelsen i EØS-avtalen artikkel 59(2).

7.3.3 Tiltak som må gjennomføres sammen med samlokalisering

Samlokalisering representerer en sentralisering av viktig utstyr og funksjoner, og vil således være negativt for sårbarheten i telenettene dersom man ikke samtidig gjør noe med kablingsstrukturen i og inn til fjellanleggene. Dette kan ivaretas gjennom følgende tiltak:

– Forberedte sammenkoblingspunkter mellom de enkelte operatørenes nett i samlokaliseringssentraene. Disse sammenkoblingspunktene skal ikke være operative for kommersiell bruk, men kan benyttes i en krisesituasjon.
– Transportnettløsninger med omrutingsmuligheter inn til samlokaliseringssentraene ved at det finnes minimum to separate kabelinnføringer i fjellanleggene.

TIFKOM-prosjektet har estimert kostnadene for disse to tiltakene til 120 mill. kr, dersom ti av Telenors fjellanlegg oppgraderes til samlokaliseringssentra, samt at det bygges fem helt nye anlegg for samlokalisering.

Ettersom det i samlokaliseringssentraene vil være plassert utstyr som er svært viktig for telenettenes funksjon, vil disse anleggene være svært attraktive mål for en fiende som ønsker å sette telenettene i Norge ut av funksjon. Samlokaliseringssentraene må derfor utstyres med overvåknings- og varslingsfunksjoner og reaksjonsmuligheter dersom det viser seg at noen er i ferd med å ta seg inn i et anlegg. Dette er viktig for å hindre at sabotører og terrorister får tid til å ta seg inn i et anlegg og gjøre skade.

7.4 Samferdselsdepartementets vurderinger og konklusjoner

Samlokalisering i fjellanlegg er et tiltak som skal beskytte vitale installasjoner i telenettene mot fysiske trusler slik som f.eks. bombing og elektromagnetisk stråling. Med den sikkerhetspolitiske situasjon vi har i Norge i dag er det ikke den fysiske trusselen mot telenettene som er mest fremtredende, derimot står telenettene overfor en stadig økende logisk trussel, dvs. trusler mot informa-

sjonssystemene i telenettene. Samlokalisering vil ikke beskytte telenettene mot logiske trusler i nevneverdig grad, og det kan derfor stilles spørsmål om hvor mye ressurser det er riktig å bruke på beskyttelse mot fysiske trusler.

Ettersom det utstyret som plasseres i fjellanlegg er av vital betydning for telenettenes funksjonalitet og er vanskelig å gjenanskaffe på kort varsel, kan vi ikke se bort fra behovet for denne type fysiske sikringstiltak. Samferdselsdepartementet mener imidlertid at det omfanget av samlokalisering i fjellanlegg som TIFKOM-prosjektet skisserer er for omfattende og for ressurskrevende i forhold til den nytten en kan forvente å få ut av et slikt tiltak. Departementet mener dessuten det vil bli særdeles vanskelig å få operatørene til frivillig å flytte eksisterende utstyr inn i fjellanlegg, samtidig som det vil bli meget kostbart for staten eventuelt å skulle dekke alle de kostnader som påløper ved en mulig flytting fra dagens lokaliteter og inn i fjellanlegg.

På bakgrunn av ovenstående anbefaler Samferdselsdepartementet at det for *eksisterende* utstyr og installasjoner som ikke allerede er lokalisert i fjell, ikke stilles krav om at teleoperatører som leverer teletjenester til Totalforsvaret skal sikre vitalt telekommunikasjonsutstyr i fjellanlegg. Post- og teletilsynet bør imidlertid få i oppgave å legge til rette for at det for *fremtidige* installasjoner skal finnes en mulighet for samlokalisering i fjellanlegg for de operatører som leverer tjenester til Totalforsvaret.

Post- og teletilsynet bør bl.a. gjennomføre en nærmere kartlegging av hvilke fjellanlegg som er mest aktuelle som samlokaliseringssentra, samt hvilke investeringer som er nødvendige for å klargjøre anlegg for samlokalisering. Post- og teletilsynets arbeid på dette området bør skje i nært samarbeid med de operatører som er aktuelle for samlokalisering. Før etablering av et tilbud om samlokalisering i Telenors fjellanlegg må Post- og teletilsynet i samarbeid med Telenor og øvrige operatører komme frem til hvilken modell for samlokalisering som er å foretrekke. Det omfanget som velges for samlokalisering må ta utgangspunkt i en vurdering av de andre operatørenes alternative sikkerhetsløsninger til samlokalisering i fjellanlegg.

Post- og teletilsynet bør for øvrig være spesielt oppmerksom når det gjelder introduksjon av nye teletjenester slik at det tidligst mulig kan legges til rette for fornuftig samlokalisering. Ved at staten legger til rette for samlokalisering i fjell, sikres det at samlokalisering i telenettene skjer i lokaliteter med tilstrekkelig sikkerhet.

8 Redundans [3)] i telenettene

I dag er teleoperatørene lokalisert på flere forskjellige steder, og det betyr at dersom man skal klare å sette alle teleoperatører ut av funksjon vil en angriper måtte slå til mot en rekke forskjellige steder. På denne måten er mangfoldet i markedet en faktor som kan være med på å redusere sårbarheten i telenettene, og utfordringen blir dermed å utnytte denne på best mulig måte.

I denne sammenhengen bør man imidlertid skille mellom tilbydere av offentlig telefontjeneste og overføringskapasitet (leide samband). I den første kategorien er avhengigheten av Telenor svært stor siden trafikken i praksis oppstår og termineres gjennom Telenors sentraler, og et utfall av viktige noder i Telenors nett vil dermed også ramme de øvrige operatørene. Denne risikoen er redusert ved at viktige komponenter i Telenors nett i dag er sikret i fjellanlegg. Mangfoldet i tilbudet av overføringskapasitet øker derimot robustheten i telenettet ved at flere aktører kan levere sambandslinjer mellom ulike deler av landet. Utfordringen består i å etablere et system for samarbeid og omruting av trafikk mellom de ulike operatørenes nett ved alvorlige uhell eller i krisesituasjoner. Dersom et viktig knutepunkt i en operatørs nett settes ut av spill slik at det blir umulig å rute teletrafikk fra en del av nettet til en annen, vil en mulig løsning være å rute trafikken via en annen operatørs nett forbi skadestedet. Dette forutsetter imidlertid at det på forhånd er etablert sammenkoblingspunkter mellom de to operatørenes nett.

Problemet i dag er at hver enkelt operatør bygger ut nett kun dersom det er kommersielt interessant. På samme måte vil det være med sammenkoblingspunkter mellom ulike operatørers nett, slike punkter etableres kun dersom det er kommersielt interessant. De nettløsninger som er interessante i ren kommersiell virksomhet anses ikke å være tilstrekkelig i krisesituasjoner. Samferdselsdepartementet mener derfor det bør iverksettes tiltak som kan øke antallet omrutingsmuligheter i telenettene, dvs. at redundansen i telenettene må økes.

8.1 Nettstruktur i offentlig telenett

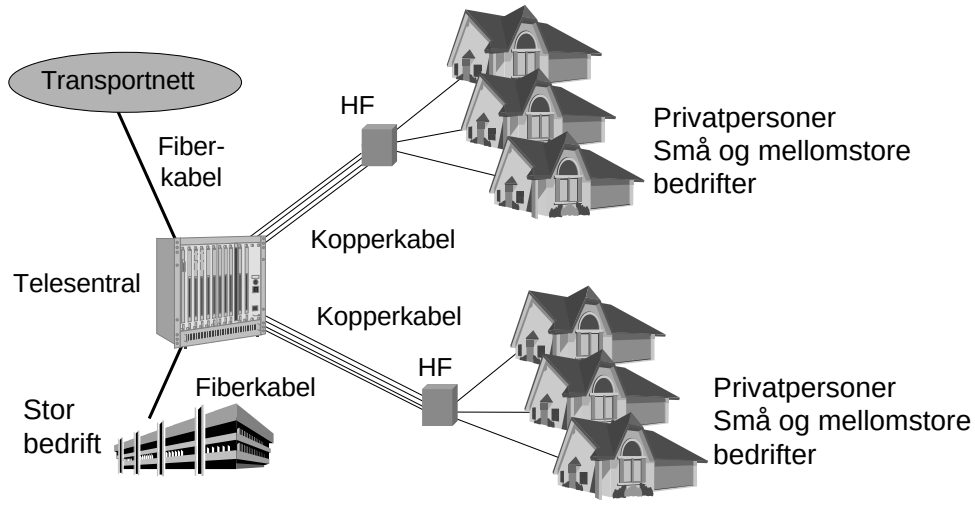
For å illustrere hvordan redundansen i nettene kan økes tar vi utgangspunkt i nettstrukturen i offentlig telenett. Som det ble redegjort for i kapittel 2 inndeles vanligvis offentlig telenett i

– aksessnett, dvs. forbindelsen til den enkelte bruker, og
– transportnett, dvs. interne forbindelser mellom ulike deler av et telenett.

Med aksessnett menes den siste delen av fastnettet, dvs. fra abonnentsiden av endesentralen og frem til abonnenten. Avstanden fra telesentral til bruker kan være fra noen hundre meter til noen få kilometer. Transportnettet er nett mellom telesentraler og gir forbindelser innen og mellom regioner. Mens det i aksessnettet er kapasitet som er eksklusiv for den enkelte bruker, har trans-

[3)] Med redundans menes omrutingsalternativer eller reserveløsninger i den enkelte operatørs nett eller mellom ulike operatørers nett.

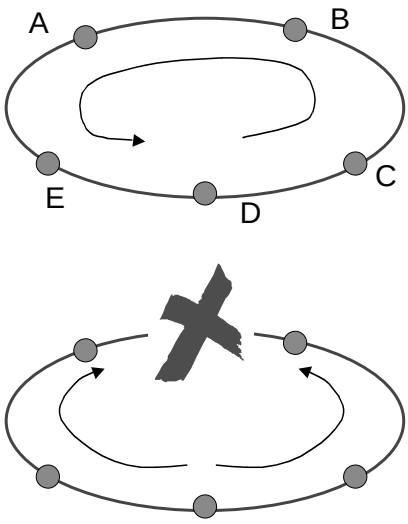
portnettet kapasitet som er en fellesressurs for alle brukere. Figur 8.1 illustrerer strukturen i aksessnettet. Nærmest telesentralen er det mange forbindelser i hver kabel, og i hovedfordeler (HF på figuren) splittes forbindelsene opp i mindre kabler frem til bedrifter og boliger. De største bedriftene er tilknyttet telesentralen over fiberkabel.



Figur 8.1 Aksessnettet er forbindelsen mellom en telesentral og brukerne.

Telenor er dominerende eier av aksessnett, men andre aktører har begynt å bygge aksessnett spesielt i de største byene og til de største brukerne. I denne utbyggingen benyttes det i stor grad fiberkabel. I noen tilfeller brukes også radiokommunikasjon i aksessnettet. Enkelte selskaper har fått tildelt radiofrekvenser fra Post- og teletilsynet for dette formålet, og etablerer en sentral basestasjon som har fri sikt til antenner hos aktuelle brukere. Basestasjonen er tilkoblet en telesentral via kabel- eller radioforbindelse. I områder med stor konsentrasjon av brukere vil det dermed kunne være flere parallelle aksessnett basert på fiberkabel og radiosystemer, mens det spesielt i spredtbygde områder av landet bare er tilgang til Telenors aksessnett. For å øke konkurransen i markedet har telemyndigheten bestemt at Telenors konkurrenter nå kan få tilgang til Telenors tradisjonelle aksessnett.

Transportnettet er basert på fiberkabel eller radiolinjeforbindelser med meget stor kapasitet. I dag er det flere aktører som har transportnett som dekker store deler av landet. Telenor har i henhold til sin konsesjon leveringsplikt for telefontjenester og overføringskapasitet over hele landet, og har dermed også transportnett mellom alle byer og tettsteder i hele landet. Øvrige eiere av transportnett har bygd ut nett i hovedsak mellom de største byene og tettstedene, det vil si strekninger hvor de mener det er tilstrekkelig trafikk fra egne og andre tjenesteleverandørers tjenester til å gjøre utbyggingen økonomisk lønnsom. Enitel har transportnett som dekker store deler av Sør-Norge og Jernbaneverket Bane Tele har fiberkabel langs jernbanetraséene. Andre mindre operatører eier transportnett i deler av landet. Transportnett bygges som regel i ringstruktur. Dette gjør det mulig å rute om trafikk, slik at feil ett sted i ringen ikke fører til alvorlige konsekvenser for brukerne, jf. figur 8.2. Transportnett bygges også i nivåer, med lokale, regionale og interregionale nett som koples sammen i knutepunkter felles for flere nivåer.



Kommunikasjon mellom sentralene A - E går normalt "en vei" i en ringstruktur i transportnettet

Ved brudd i ringen kan trafikken legges om slik at den samme kapasiteten benyttes, men nå i begge retninger

Figur 8.2 Ringstruktur gir muligheter for omruting av trafikk når brudd oppstår.

8.2 Redusert sårbarhet gjennom økt redundans i telenettene

Med redundans menes her overkapasitet og muligheter for omruting av teletrafikk slik at man har flere muligheter å komme fram i telenettene på, for på den måten å redusere konsekvenser av feil og brudd. Telenett bygges som hovedregel slik at det skal kunne fungere også om enkle feil oppstår i sentraler og overføringssystem. Nye tekniske løsninger, som f.eks. ringstruktur i transportnettet, bidrar til at det nå finnes muligheter for å rute trafikk utenom kabelbrudd og stasjoner som rammes av feil. Alle eiere av transportnett i Norge benytter i dag digital teknologi.

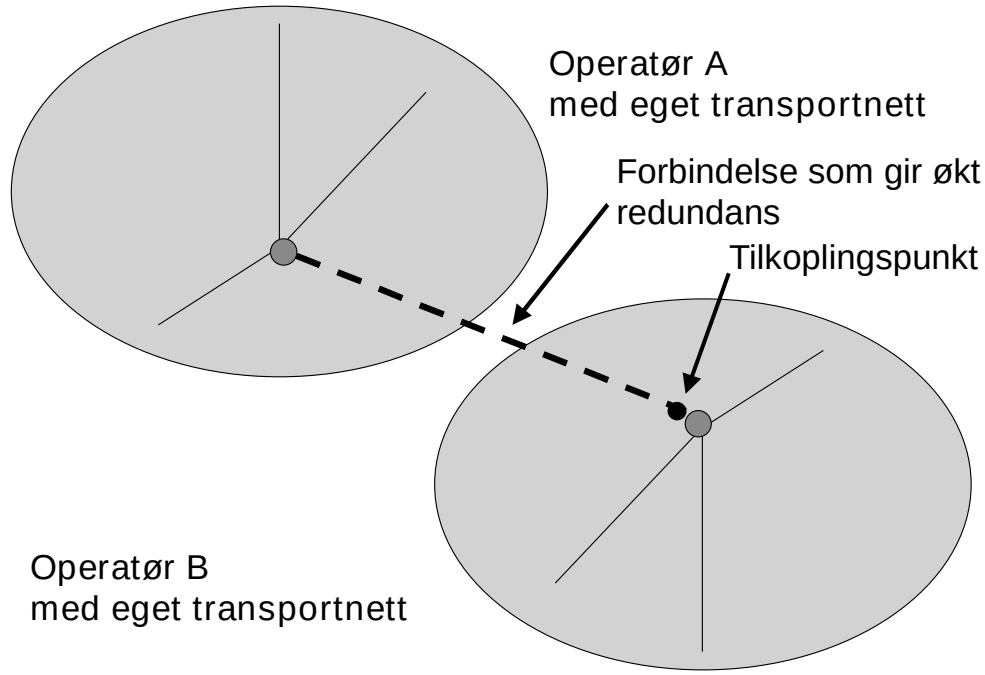
Denne nye digitale teknologien gir muligheter for at omlegging av kapasitet i transportnettet foretas via dataterminal eller automatisk via støttesystem som registrerer når feil eller brudd oppstår og omruting er forberedt. Slik omlegging er aktuell når nettet utvides for økt kapasitet eller med nye kabel- eller radiosystemer, eller når det er tekniske feil i nettet.

Mens nett er under utbygging eller endring, kan det imidlertid være begrensede muligheter for å foreta omkoblinger til reservekapasitet eller andre tiltak for å unngå at feil og brudd gir brudd i trafikkavviklingen, eller det kan være umulig å få til en omkobling. Dette kom ikke minst fram under to graveuhell medio 2000 som rammet Telenors telenett.

I det ene tilfellet ble en kabel utenfor Bergen skadet, slik at flyplassen på Flesland mistet teleforbindelsene, med det resultat at flytrafikken ble lammet. Et kabelbrudd i Kristiansand førte tilsvarende til at Telenors teletrafikk i regionen, inklusiv nødmeldingstjenesten, ble lammet og flyplassen på Kjevik mistet teleforbindelsene. Fordi mobiloperatøren NetCom brukte transportnettet til Jernbaneverket Bane Tele for kommunikasjon mellom mobilsentral og basestasjoner, kunne likevel NetComs kunder bruke mobiltelefon i Kristian-

sand-området, mens Telenors kunder ikke kunne ringe i verken fastnett eller mobilnett. Eksempelvis fikk man på flyplassen på Kjevik lånt mobiltelefoner med abonnement hos NetCom, slik at man fikk nok kommunikasjon til at noen fly kunne sendes av gårde. Dersom det hadde vært etablert sammenkoblingspunkter mellom Telenors nett og nettet til Jernbaneverket Bane Tele, kunne samtaler i Telenors nett blitt rutet via Bane Teles nett, jf. figur 8.3. Effekten av ikke å ha alternative transportnett og separate framføringsveier kom klart frem under dette uhellet.

Siden det i store deler av landet er tre parallelle transportnett og disse nettene benytter samme teknologi, er det også teknisk mulig å koble trafikk fra et transportnett over i et annet transportnett. Kapasiteten i transportnett har økt sterkt ved at man de senere årene har oppgradert gjennom utbygging basert på fiberkabel. Det vil derfor ikke være tekniske problemer med å fremskaffe kapasitet for sammenkobling av ulike operatørers transportnett. Satt i system vil slik sammenkobling både redusere sårbarheten i landets totale teleinfrastruktur og kunne redusere hver netteiers kostnader knyttet til egen utbygging.



Figur 8.3 Sammenkobling av transportnett for økt redundans.

Aksessnettet er i hovedsak bygget uten redundans. Dette innebærer at brudd på en kabel, f.eks. på grunn av graving og anleggsarbeid, fører til at alle brukere med tilkobling til telesentral via denne kabelen mister forbindelsen til telenettene. I nye og oppgraderte aksessnett med fiberkabel på mange strekninger, vil det ofte være redundans for fiberkabel men ikke for tradisjonell kobberkabel. Brukere som er svært avhengige av teletjenester vil imidlertid kunne bestille ekstra forbindelser i aksessnettet, mot å dekke kostnadene for

dette. Kostnadene vil ofte være store og i praksis virke som hinder for at brukerne på eget initiativ sørger for slike ekstra forbindelser.

8.3 Samferdselsdepartementets vurderinger og konklusjoner

Transportnett og aksessnett bygges som regel med kritisk vurdering av kostnader forbundet med anlegg og drift. Driftssikkerhet og sikring mot skader i normale og unormale situasjoner kan bli lavt prioritert når konkurranse i markedet er en rammebetingelse og kundene i liten grad er villige til å betale for økt sikkerhet.

Post- og teletilsynet bør derfor følge opp utviklingen i utbygging av teleinfrastrukturen. Gjennom pålegg med hjemmel i regelverk kan Post- og teletilsynet bidra til samarbeid om tiltak for økt redundans i telenettene. Samferdselsdepartementet mener det vil bli spesielt viktig å få til et samarbeid mellom operatører med landsdekkende transportnett, med tanke på etablering av flere sammenkoblingspunkter mellom disse nettene. Et slikt samarbeid behøver ikke koste mer for tjenesteleverandører. Følgende oppgaver er aktuelle for et tilsynsorgan innen telesikkerhet og -beredskap:

- oppfølging av utbyggingen av transportnett, med sikte på å øke sikkerheten gjennom at ulike operatørers transportnett kan gi reservekapasitet for hverandre.
- oppfølging av utbyggingen av aksessnett, slik at viktige brukere i størst mulig grad kan nytte flere alternativer for tilkobling til tjenesteleverandør, og at kapasitet i en operatørs aksessnett kan være reserve for andre tjenesteleverandører.
- vurdering av muligheter for å etablere løsninger for sammenkobling av telenett, slik at mulighetene for omkobling av trafikk fra et nett til et annet sikres. Dette kan spesielt være av betydning i faser med utbygging og oppgradering av nett, hvor ringstruktur i operatørens eget nett i en periode ikke er tilgjengelig.

Dersom redundansen i telenettene er god gjennom transportnett bygd med ringstruktur samtidig som det finnes flere sammenkoblingspunkter mellom de ulike nettene, utnytter man mangfoldet i markedet til å redusere sårbarheten i telenettene totalt sett. Med dagens trusselbilde mener departementet det er forsvarlig å prioritere tiltak for å øke redundansen fremfor å benytte ressursene på samlokalisering i fjellanlegg. I motsetning til fjellanlegg som hovedsakelig er ment for beskyttelse i forbindelse med sikkerhetspolitiske kriser og krig, vil økt redundans være av betydning over hele utfordringsspekteret fra normalsituasjon til krig. Dette ble ikke minst demonstrert under uhellet i Kristiansand i 2000, der forberedte sammenkoblingspunkter mellom telenett kunne medført at graveskaden hadde fått mindre konsekvenser for samfunnet.

9 Kommunikasjon for prioriterte brukere i Totalforsvaret

Enkelte brukergrupper vil ha behov for telekommunikasjonsløsninger med ekstra robusthet i forhold til det som er tilgjengelig i de allmenne telenett. Dette har ført til at f.eks. Forsvaret har bygget ut et eget nett, Forsvarets Digitale Nett (FDN), og nødetatene politi, brann og helse vurderer utbygging av et felles mobilt radionett.

Mange av de brukerne i samfunnet som har behov for ekstra robuste telekommunikasjoner inngår også i det som kan kalles prioriterte brukere i Totalforsvaret. Prioriterte brukere i Totalforsvaret er brukere som ut fra sin funksjon og rolle i gitte kritiske situasjoner må gis kommunikasjonsmessig prioritet i de allmenne nett og/eller tilgang til andre telenett og teletjenester for at de skal kunne ivareta sine oppgaver.

TIFKOM-prosjektet har påpekt at det eksisterer et stort behov for statlig koordinering og tilrettelegging av telekommunikasjonsløsninger for de brukergruppene som har behov for ekstra sikre og robuste teletjenester. Ved slik koordinering vil en kunne oppnå betydelige synergieffekter. En mulig koordinert løsning for disse prioriterte brukerne kan være at Forsvarets digitale nett (FDN) og et eventuelt nytt landsdekkende radionett for nødetatene samordnes. Dersom et eventuelt nytt felles radiosamband for nødetatene så langt som mulig baseres på FDN, som suppleres med sikkerhetsmessig tilfredsstillende kommunikasjonsressurser fra de allmenne nett, kan denne kombinasjonen samlet danne et godt felles fundament for de brukergrupper som har behov for ekstra robuste telekommunikasjonsløsninger. Hvorvidt en slik samordning av FDN og et eventuelt nytt nett for nødetatene kan gjennomføres praktisk og funksjonelt, herunder med hvilken økonomisk konsekvens, er imidlertid ikke behandlet i TIFKOM-rapporten.

Samferdselsdepartementet etablerte derfor en arbeidsgruppe som fikk i oppgave å utrede og verifisere tekniske, funksjonsmessige og økonomiske premisser for en mulig samordning av FDN og et nytt nett for nødetatene.

9.1 Eventuelt nytt radionett for nødetatene

For å kunne være i stand til å utføre sine oppgaver på tilfredsstillende vis, er nødetatene avhengig av sikrere samband enn publikum generelt. Nødetatenes samband må fungere i ekstremsituasjoner der offentlige telenett har redusert tjenestekvalitet eller ikke fungerer. Ettersom de dedikerte radiokommunikasjonssystemene nødetatene i dag har er basert på analog teknologi og ikke tilfredsstiller nødetatenes krav til sambandsløsning, arbeides det med å få etablert et nytt landsdekkende radionett som skal være felles for alle de tre nødetatene. Et nytt nett for nødetatene er tenkt basert på TETRA-standarden (TErrestrial Trunked RAdio). TETRA er en leverandøruavhengig standard for digital gruppeorientert radiokommunikasjon, definert av European Telecommunications Standards Institute (ETSI). Mulighet for gruppekommunikasjon, direkte kommunikasjon mellom brukere, kryptering av samtaler og data samt

sambandslederfunksjon, er kritiske krav til funksjonaliteten i et nytt radiosamband for nødetatene.

Arbeidet med å utrede grunnlaget for etableringen av et nytt felles radionett for nødetatene har vært organisert som et prosjekt under ledelse av Justisdepartementet [4)] . Prosjektet har hatt i oppgave å:

- Utrede beslutningsgrunnlag for eventuell realisering av et nytt felles radionett for nødetatene basert på TETRA-standarden.
- Utrede muligheter for, og konsekvenser av, en utvidelse av nødsambandet til å omfatte instanser med bl.a. nødrelaterte oppgaver og beredskapsoppgaver.
- Utarbeide grunnlag for en prosjektspesifikasjon som underlag for en anbudsforespørsel.
- Vurdere alternative former for finansiering og eierskap.

Et nytt nødnett er forutsatt å få like god radiodekning som mobilnettene i byer og langs veier, bedre flatedekning på landsbasis, samt at det vil være mulig å kommunisere i områder der det normalt ikke bor mennesker, men hvor det like fullt kan skje ulykker. Investeringskostnaden for et landsdekkende nødnett, inkludert utbygging i tunneler, er foreløpig estimert til 5,3 mrd. kr. Kostnadselementer som brukerutstyr, drift i investeringsfasen og merverdiavgift er tatt med i totalbeløpet.

9.2 Forsvarets digitale nett (FDN)

Forsvarets digitale nett (FDN) er et landsdekkende telenett som er etablert for å dekke Forsvarets behov for teletjenester. FDN dekker i dag alle Forsvarets installasjoner over hele landet samt enkelte deler av offentlig forvaltning, og totalt antall brukere i FDN er ca. 50 000.

FDN har innebygget egenskaper som er viktige for å oppnå høy tilgjengelighet for brukerne, selv i situasjoner med betydelig degradering av transportnettet. De viktigste av disse egenskapene finner en i funksjoner for oppsetting og ruting av samband og i prioritetsfunksjonen. FDN har automatisk omruting av trafikk ved brudd, i tillegg til at rutingsfunksjonen sørger for at det kan settes opp samband så lenge det er mulige veier igjen i et degradert transportnett. Få gjenværende veier gjør imidlertid at nettet er i stand til å formidle mindre trafikk. En prioritetsfunksjon i fire nivåer er da med på å sikre at de aller viktigste brukerne har samband helt til det ikke lenger er forbindelser i nettet.

Forsvarets tele- og datatjeneste (FTD) disponerer for øvrig en rekke transportable systemer for reetablering av traseer, forsterkninger eller knutepunkter. Med slikt utstyr kan FTD ved hjelp av radiolinjer eller satellitt raskt etablere kommunikasjon til og fra steder utenom FDN.

9.3 Mulig samordning mellom FDN og et nytt radionett for nødetatene

Et eventuelt nytt landsdekkende nødnett kan tenkes realisert på ulike måter; i offentlig telenett, i FDN, som et eget fysisk nett, eller en blanding av alle tre

[4)] Sju departementer er med i prosjektets styringsgruppe.

typer løsninger. Beregning av kostnadene ved realisering av et nytt nødnett har tatt utgangspunkt i utbygging i Telenors nett. Denne løsningen ble valgt fordi Telenor hadde planleggingsverktøy og innsikt til å kunne foreta den nødvendige kostnadsberegning med tilstrekkelig grad av nøyaktighet. Telenors kostnadsberegninger for etablering av nødnettet gir en maksimalverdi for kostnadene, bl.a. fordi Telenor er pålagt å ha «åpne og ikke-diskriminerende vilkår» for leide samband og samlokalisering, jf. forskrift om offentlig telenett og offentlig teletjeneste (teleforskriften). På disse og andre områder vil det være mulig ved eventuell utbygging å velge leverandører og løsninger som kan gi lavere kostnader for nødnettet.

Kort oppsummert er konklusjonen til den arbeidsgruppen Samferdselsdepartementet nedsatte at realisering av et landsdekkende nødnett med basis i FDN blir mer aktuelt jo større krav som stilles til sikkerheten i det nye nødnettet.

Dersom prioriterte brukere i Totalforsvaret skal sikres tilstrekkelig robuste telekommunikasjonsløsninger gjennom en samordning av Forsvarets digitale nett (FDN) og et eventuelt nytt landsdekkende radionett for nødetatene, er det imidlertid en forutsetning at Forsvaret stiller FDN tilgjengelig som kommunikasjonsbærer i det nye nettet.

Forsvarsdepartementet vurderer sikkerhetsmessige forhold ved bruk av FDN fra andre enn Forsvaret til å være tilfredsstillende. Alle FDN-installasjoner kan i prinsippet benyttes i forbindelse med etablering av nød- og beredskapsnett for nødetatene dersom man etablerer praktiske løsninger som ivaretar sikkerheten. Forsvarsdepartementet har imidlertid understreket at sivil utnyttelse av FDN generelt bør begrenses til prioriterte brukere innenfor Totalforsvaret. Forsvarsdepartementet forutsetter videre at Forsvaret til enhver tid står fritt til å vurdere hvilke aktører som i fremtiden bør falle inn under denne kategorien. Forsvarsdepartementet forutsetter også at kostnadene forbundet med ovennevnte samordning belastes de aktuelle brukere, og ikke medfører økte kostnader for Forsvaret.

Det foreligger ikke en fullstendig kostnadsberegning for utbygging av et nytt nødnett med basis i FDN som kan sammenlignes med beregningene fra Telenor. Dette kan først skje etter en fullstendig radioplanlegging av utbygging med basis i FDN. Forsvarets tele- og datatjeneste (FTD) er i samarbeid med Telenor i ferd med å gjennomføre et omfattende arbeid med å kartlegge hvor stor del av et landsdekkende radionett for nødetatene som kan etableres med basis i FDN og de økonomiske betingelser knyttet til dette. Det som gjenstår og som må utredes videre når dette arbeidet er avsluttet, er hvilke betingelser Forsvaret stiller til aktuelle brukere av et eventuelt nytt nødnett dersom FDN skal benyttes.

9.4 Nødnett også for andre prioriterte brukere i Totalforsvaret?

Dersom det skulle vise seg at det ikke er hensiktsmessig å realisere et nytt nødnett med basis i FDN, kan det uansett løsning være interessant å inkludere også andre prioriterte brukere i Totalforsvaret, som brukere i et eventuelt nytt, felles radionett for nødetatene. Ved ulykkes- og krisesituasjoner vil det ofte være flere enn nødetatene helse, politi og brann som har en sentral rolle på ulykkesstedet, eksempelvis kan dette gjelde Forsvaret, Sivilforsvaret og

vegmannskaper. Et felles sambandssystem er et virkemiddel for å oppnå bedre samarbeid og mer effektiv utnyttelse av ressursinnsatsen til de ulike aktørene. De aktørene det er snakk om vil normalt også være definert som prioriterte brukere i Totalforsvaret, og vil således være naturlige brukere av et eventuelt felles nett for nødetatene og øvrige deler av Totalforsvaret.

TETRA-prosjektet har i sin utredning kartlagt en rekke virksomheter som involveres i hendelser knyttet til nød, redning og beredskap, og har estimert antall brukere utover nødetatene til 36 000. Dette inkluderer både offentlig og privat virksomhet. Samferdselsdepartementet har på forespørsel vurdert eventuelle telepolitiske, konkurransemessige og regulatoriske føringer for og konsekvenser av en eventuell kommersiell bruk av et offentlig finansiert nødnett, og har konkludert med at kommersiell bruk er mulig dersom denne bruken skilles ut økonomisk i forhold til nødetatenes bruk av nettet. TETRA-prosjektet har derfor forutsatt at også andre brukere innenfor nød, redning og beredskap kan tilknyttes et eventuelt nytt nødnett. På det nåværende tidspunkt er det ikke mulig å tallfeste kostnader for eventuelt å inkludere prioriterte brukere i Totalforsvaret som nødnett-brukere, men foreløpige beregninger viser at investeringskostnaden kun i liten grad vil bli påvirket om antallet brukere økes.

Det er viktig å være klar over at et nødnett bare vil bli brukt av et begrenset utvalg aktører innen Totalforsvaret, mens øvrige samfunnskritiske funksjoner fortsatt vil være avhengig av et robust og velfungerende offentlig telenett. Det vil dermed fortsatt være behov for å investere ytterligere i sikkerheten i de offentlige nettene, også etter etableringen av et landsdekkende nødnett.

Et nødnett vil for øvrig være tjent med et robust offentlig telenett ettersom nødnettet må nytte framføringsveier og radiopunkter i offentlig telenett. For at nettet totalt skal ha den sikkerhet og tilgjengelighet som er forutsatt fra nødetatene, må framføringsveier og radiopunkter i offentlig telenett gis økt sikkerhet i forhold til dagens situasjon. Dette vil også gjelde dersom nødnettet realiseres med basis i FDN, og FDN suppleres med kapasitet fra kommersielle operatører i stedet for ny utbygging.

Et utvidet nødnett vil heller ikke gjøre en prioritetsordning i de offentlige telenettene overflødig. Grunnen er at en ny prioritetsfunksjon bl.a. må implementeres dersom Norge ønsker å bidra til at prioritet i telenettene på tvers av landegrensene blir mulig i fremtiden. For øvrig vil en samtale initiert fra et nødnett få automatisk prioritet i de andre telenettene etter implementering av en ny prioritetsfunksjon som skissert i kapittel 7.

9.5 Samferdselsdepartementets vurderinger og konklusjoner

Prioriterte brukere i Totalforsvaret bør sikres tilgang til telekommunikasjonsløsninger med den robusthet som er nødvendig for at disse gruppene skal kunne utføre sine oppgaver både i krise- og beredskapssituasjoner. For å oppnå dette bør man utnytte de militære og sivile sambandsressurser som allerede finnes i samfunnet. Ved en eventuell utbygging av et nytt radionett for nødetatene bør det tas hensyn til at Forsvaret allerede har et telenett med høy sikkerhet.

Forsvarets tele- og datatjeneste (FTD) er i ferd med å gjennomføre et omfattende arbeid for å kartlegge hvor stor del av et eventuelt landsdekkende

radionett for nødetatene som kan etableres med basis i FDN og de økonomiske betingelser knyttet til dette. Det som gjenstår og som må utredes videre når dette arbeidet er sluttført, er hvilke betingelser Forsvaret stiller til aktuelle brukere av et nytt nødnett dersom FDN skal benyttes.

Uavhengig av om et eventuelt nytt radionett for nødetatene realiseres med basis i FDN eller ikke, bør også prioriterte brukere i Totalforsvaret utenom nødetatene politi, helse og brann gis mulighet til være brukere av nødnettet. Dette vil gjøre det enklere å samordne innsatsen fra flere aktører under kriser og ulykker, noe som vil øke samfunnsnytten av et slikt nytt nett. TETRA-prosjektet har i sin utredning forutsatt at andre brukere innenfor nød, redning og beredskap kan tilknyttes et eventuelt nytt nødnett, og har gjennomført en første kartlegging av andre virksomheter som involveres i hendelser knyttet til nød, redning og beredskap. Samferdselsdepartementet mener at Post- og teletilsynet og TETRA-prosjektet i fellesskap bør utrede videre forutsetninger for å inkludere prioriterte brukere i Totalforsvaret som brukere av et eventuelt nytt radionett for nødetatene, med spesifisering av krav til sikkerhet, eventuell bruk av FDN som integrert del av nettet, og økonomiske forutsetninger mv.

Utbygging av et radionett for nødetatene gjør imidlertid ikke at man kan se bort fra sikringstiltak i de offentlige nett. Selv om et nødnett tilsynelatende vil være et eget lukket telenett, vil også dette nettet være avhengig av ressurser i de offentlige nett for å fungere etter hensikten. I tillegg vil det være en rekke brukere som ikke får tilgang til et nødnett, men som like fullt har behov for sikre og robuste telekommunikasjoner.

10 Andre telesikkerhets- og teleberedskapstiltak

Fra kapittel 5 og utover har Samferdselsdepartementet presentert og vurdert hovedelementene i en ny strategi for telesikkerhet og teleberedskap tilpasset markedssituasjonen. I tillegg til forslagene om å legge et særskilt myndighetsansvar for telesikkerhet og -beredskap til Post- og teletilsynet, prioritert tjenesteaksess i fast- og mobilnett, samlokalisering i fjellanlegg, økt redundans i telenettene samt eventuell samordning av Forsvarets digitale nett (FDN) og et nytt radionett for nødetatene, er det en rekke andre tiltak som også vil bidra til god sikkerhet og beredskap i norske telenett. Dette dreier seg først og fremst om mindre omfattende administrative og organisatoriske tiltak, og ikke i så stor grad fysiske og teletekniske tiltak. Nedenfor følger en kort gjennomgang av andre tiltak som Samferdselsdepartementet mener vil ha betydning for å øke sikkerheten og beredskapen i telenettene.

10.1 Bevisstgjøring, kompetanseheving og veiledning

Brukerens behov for å sikre seg robuste kommunikasjonsløsninger øker som en konsekvens av den økende avhengigheten av tele- og datakommunikasjon. Bevisstgjøring, kompetanseheving og veiledning om telesikkerhet og -beredskap vil være en viktig oppgave for Post- og teletilsynet. Brukerne må lære seg å stille krav til kvaliteten på de teletjenester som kjøpes, der robustheten inngår som en viktig faktor. Det er langt fra alle brukere som har mulighet til å sette seg inn i problemstillingen eller er i stand til å vurdere hva som kreves for å gjøre kommunikasjonsløsningene robuste nok. Post- og teletilsynet bør derfor ha som en av sine oppgaver å bevisstgjøre brukere med hensyn til robusthet, samt å tilrettelegge for enklere gjennomføring av sårbarhetsreduserende tiltak. Post- og teletilsynet bør bl.a. assistere og gi retningslinjer innen beredskapsplanlegging, slik at brukerne blir best mulig i stand til å møte Totalforsvarets behov ved fredskriser og krig. Post- og teletilsynet bør også kunne kontaktes for å få råd ved anskaffelser av telekommunikasjonstjenester og -utstyr.

Teleberedskap er i kapittel 2.2 definert til å være planer og faktisk gjennomførte tiltak som er gode nok til å kunne møte forhold som innebærer ekstraordinær risiko. Innen kritiske samfunnsfunksjoner er det viktig at det utarbeides planer for hvordan telekommunikasjonsbehovet skal ivaretas også utenfor normalsituasjonen. Samtidig må det gjennomføres tiltak slik at det blir mulig å iverksette planene i en krise- eller krigssituasjon. Planer og tiltak må jevnlig revideres for å avstemmes med det aktuelle risikobildet innen telekommunikasjon ettersom trusselbildet endres i takt med teknologien. Post- og teletilsynet bør være et kompetansesenter som aktivt veileder og gir råd innen telesikkerhet og teleberedskap. Selv om Post- og teletilsynet tilbyr en slik tjeneste, vil det uansett være den som søker råd som selv har ansvaret for at sikkerheten og beredskapen innen telekommunikasjon er tilfredsstillende og at planer og tiltak blir fulgt opp.

10.2 Klassifisering av teleinfrastrukturen

Som grunnlag for vurdering av sikringstiltakenes omfang er det fornuftig å ta utgangspunkt i en klasseinndeling av telekommunikasjonsinfrastrukturen avhengig av hvilken betydning infrastrukturen har for telenettenes funksjon. For teleinfrastruktur som vurderes å ha vesentlig betydning for at telekommunikasjonen skal fungere vil det f.eks. være en rekke krav knyttet til telesikkerhet og -beredskap, mens teleinfrastruktur som ikke er avgjørende for at telenettene skal fungere vil få færre sikringskrav. I en klassifiseringsordning bør det legges opp til at det er mulig å oppgradere eller nedgradere anlegg fra opprinnelig sikringsklasse.

På bakgrunn av en gjennomgang av risiko og sårbarhet knyttet til de offentlige telenett bør Post- og teletilsynet i samarbeid med teleoperatørene spesifisere hvilken sikringsklasse de ulike systemer og nettelementer faller inn under. Krav til sikkerhetstiltak innen ulike sikringsklasser må utarbeides av tilsynet i samarbeid med teleoperatørene. Klassifiseringsordningen bør bl.a. inneholde en sikringsklasse for nett og anlegg som ikke får spesielle krav til telesikkerhet og teleberedskap.

TIFKOM-prosjektet har anbefalt at man følger en modell fra danske telemyndigheter, der man har delt det nasjonale telenettet inn i fire sikringsklasser. I Danmark har man benyttet følgende inndeling:

Sikringsklasse 1:	Omfatter teleanlegg av særlig vesentlig betydning for landsdekkende og internasjonal telekommunikasjon. Det vil si anlegg til bruk for offentlige telenett eller teletjenester, som ikke kan erstattes av andre anlegg innenfor samme telenett eller teletjeneste.
Sikringsklasse 2:	Omfatter teleanlegg av vesentlig betydning for landsdekkende samfunnsviktig telekommunikasjon. Det vil si anlegg til bruk for offentlige telenett eller teletjenester, som kun delvis kan erstattes av andre anlegg innenfor samme telenett eller teletjeneste.
Sikringsklasse 3:	Omfatter teleanlegg av vesentlig betydning for regional samfunnsviktig telekommunikasjon. Det vil si anlegg til bruk for offentlige telenett eller teletjenester, som har betydning for de regionale totalforsvarsenheter.
Sikringsklasse 4:	Omfatter teleanlegg uten betydning for samfunnsviktig telekommunikasjon. Det vil si øvrige anlegg til bruk for offentlige telenett eller teletjenester.

10.3 Sikkerhetsevaluering av offentlige telenett

Ved en klassifisering av teleinfrastrukturen i sikringsklasser vil med all sannsynlighet sikringsklasse 1 omfatte teleanlegg av særlig vesentlig betydning for landsdekkende og internasjonal telekommunikasjon. Dette vil med andre ord være anlegg til bruk for offentlige telenett eller teletjenester som ikke kan erstattes av andre anlegg innenfor samme telenett eller teletjeneste, og som er avgjørende for at telekommunikasjonssystemene skal fungere. Ettersom tilgjengelighet til telekommunikasjon kan ha betydning for rikets sikkerhet, må det antas at deler av telenettene kan sies å være såkalte skjermingsverdige objekter, dvs. eiendom som må beskyttes mot sikkerhetstruende virksomhet av hensyn til rikets eller alliertes sikkerhet eller andre vitale nasjonale sikkerhetsinteresser. Telenettene kan i tillegg inneholde skjermingsverdig eller sik-

kerhetsgradert informasjon, dvs. informasjon som skal merkes med sikkerhetsgrad etter reglene i lov om forebyggende sikkerhetstjeneste (sikkerhetsloven).

Spørsmålet om f.eks. telesystemer skal defineres som skjermingsverdige, avklares gjennom en forutgående sikkerhetsevaluering, der det tas stilling til om det er grunnlag for sikkerhetsgradering, og i tilfelle hvilken sikkerhetsgradering (BEGRENSET, KONFIDENSIELT, HEMMELIG eller STRENGT HEMMELIG) som skal benyttes. En eventuell gradering må ses i forhold til den skade en eventuell kompromittering, ødeleggelse eller infiltrasjon av systemet vil kunne påføre Norge eller våre internasjonale samarbeidspartnere.

Dersom informasjon eller et objekt defineres som skjermingsverdig, vil dette medføre at sikkerhetslovens pålegg må følges. Dette vil innebære krav når det gjelder personellsikkerhet, men også når det gjelder f.eks. håndtering av sikkerhetsgradert informasjon og sikkerhetsmessige anskaffelser. TIF-KOM-prosjektet har foreslått at det bør innføres krav om sikkerhetsklarering av personell for å bedre telesikkerhet og -beredskap i det samlede nasjonale telenettet. Som det fremgår av ovenstående vil altså krav om sikkerhetsklarering av personell kun være ett av flere tiltak som kan komme til å måtte iverksettes dersom informasjon eller et objekt defineres som skjermingsverdig.

Samferdselsdepartementet foreslår at Post- og teletilsynet får i oppdrag å foreta en samlet sikkerhetsevaluering av offentlige telenett. En slik evaluering må gjøres i samarbeid med operatørene og kan ses i sammenheng med utforming av krav til sikringstiltak differensiert på sikringsklasser, jf. kapittel 10.2.

10.4 Samøvelser

Ved en eventuell krise som involverer telesektoren vil det med stor sannsynlighet være behov for at flere operatører samarbeider for å få situasjonen under kontroll. På denne måten kan man ved større utfordringer mot samfunnet utnytte det mangfoldet som et konkurranseutsatt marked medfører. Det er i den forbindelse nødvendig at det øves på samspill mellom konkurrerende aktører i krise- og krigssituasjoner, og at Post- og teletilsynets krisehåndteringsevne på samme tid opparbeides.

Post- og teletilsynet får i oppgave å planlegge og arrangere øvelser for alle aktørene i telesektoren som anses som viktige i beredskapssammenheng. Under samøvelsene møtes operatørene for å opparbeide kompetanse og praktisk erfaring i hvordan man best mulig kan samarbeide og utnytte ressursene innen telekommunikasjonssektoren under ulike samfunnstilstander.

Under samøvelsene vil ulike hendelser bli simulert, og aktørenes evne til å håndtere utfordringen blir øvd. I løpet av en samøvelse vil deltakerne få en gjennomkjøring av rutiner, prosesser og prosedyrer av både teknisk og organisatorisk art som ved siden av å være viktig for den enkelte operatørs krisehåndteringskompetanse også vil ha betydning for evnen til effektivt samarbeid med andre operatører. En samøvelse vil øke kompetansen hos involverte parter ved at man får et bedre begrep om hvilke skadebøtende tiltak som har best effekt i ulike situasjoner. Bedre kunnskap på dette området vil også bidra til at man ved implementering av nye sikkerhets- og beredskapstiltak i nettene vil være bedre i stand til å prioritere mellom ulike forebyggende tiltak. Samø-

velser kan dessuten gi operatørene erfaringsgrunnlag for å utvikle nye tiltak som kan øke robustheten i telenettene.

I Sverige gjennomføres regelmessige øvelser med operatørene, der driftspersonell trenes opp i å håndtere masseutfall av noder og kommunikasjonsveier. I Nederland pågår trening og organiserte øvelser for simulerte krisesituasjoner annet hvert år. I Finland er det utarbeidet et samarbeidskonsept for personell fra de tre største operatørenes hoveddriftssentraler. I krisesituasjoner skal de samarbeide under kommando av Forsvarsministeriet. Det blir avholdt regelmessige samøvelser annet hvert år.

I utgangspunktet mener TIFKOM-prosjektet at det kan være hensiktsmessig med samøvelser én gang i året, og at det hvert fjerde år bør arrangeres samøvelser av et større omfang. Telekommunikasjonssektoren er en sektor i endring som følge av at det stadig introduseres ny teknologi på markedet, noe som kan tale for hyppige øvelser. Samferdselsdepartementet mener imidlertid at det i første omgang vil være tilstrekkelig med samøvelser hvert annet år, slik det også gjøres i andre land. Hyppigheten av øvelser bør imidlertid evalueres etter at de første samøvelsene er avholdt.

10.5 Beredskapsutstyr

For å styrke telekommunikasjonssektorens reparasjonsberedskap og rehabiliteringsevne bør det etableres beredskapslagre med transportabelt beredskapsutstyr. Formålet med dette er at transportabelt beredskapsutstyr skal kunne settes inn i telenettene ved trafikkbrudd eller ved fare for trafikkbrudd på steder hvor brudd vil medføre alvorlige konsekvenser for samfunnet både i fredstid og i krigstid. I ekstreme situasjoner som naturkatastrofer, kriser og krig vil det mest sannsynlig være behov for beredskapsutstyr ut over det som er kommersielt interessant for operatørene.

Alle aktører som anses viktige i beredskapssammenheng bør derfor ha et minimum av transportable enheter som raskt kan erstatte ødelagte punkter. Forsvarets forskningsinstitutt har i BAS2-rapporten konkret nevnt behovet for transportable transmisjonsterminaler, transportable nødstrømsaggregater og transportable tjenestenoder. I tillegg er det behov for utstyr som f.eks. multipleksere, fiber, feltutstyr, master og transportable basestasjoner. Transportable basestasjoner bør inkluderes som et del av beredskapsopplegget spesielt rettet mot mobiloperatørene.

I Sverige er det ca. ti operatører som regnes for å være viktige i teleberedskapssammenheng. Disse operatørene ble bl.a. spurt om hvor mange nødstrømsaggregater de hadde behov for av ulike typer. Post- och telestyrelsen har betalt for innkjøp, mens operatørene må bære drifts- og vedlikeholdskostnader selv. Post- och telestyrelsen inngår kommersielle avtaler med 10 års varighet med hver operatør for bruk av slike nødstrømsaggregater. Antall nødstrømsaggregater er nå distribuert i Sverige tilsvarende behovet ved større utfall av kraftforsyning som kan skje ved alvorlige snøstormer og uværssituasjoner eller ved større sabotasjeaksjoner.

Transportabelt reservemateriell inngår som en del av Telenors spesielle samfunnspålagte oppgaver til Totalforsvaret, og Samferdselsdepartementet mener dette tiltaket bør videreføres også i det nye konseptet.

10.6 Forskrift om beskyttelse av telekommunikasjonsanlegg mot elektromagnetisk puls (EMP-forskriften)

I kapittel 3.1.2 er det gitt en beskrivelse av de elektroniske truslene mot telenettene. Et av de elektroniske virkemidlene er elektromagnetisk stråling mot teleinstallasjoner for å forstyrre eller ødelegge de elektroniske komponentene i telenettene. Elektromagnetisk puls (EMP) kan forårsake stor skade i elektronisk utstyr dersom den er kraftig nok. EMP genereres naturlig gjennom lynnedslag, og andre mindre kraftige kilder for EMP er radiosendere, termostater og koblinger i det elektriske nettet. Alle disse typene EMP er det mulig å sikre seg godt mot. Verre er det med menneskeskapt EMP som kan genereres ved bruk av spesielle EMP-våpen og ved detonasjon av kjernevåpen over atmosfæren. Kjernefysisk generert EMP vil kunne bli så kraftig at elektronisk utstyr vil ødelegges i stort omfang, og mot denne typen EMP er det kostnadskrevende å foreta effektive beskyttelsestiltak. I Norge er det i dag i hovedsak Forsvarets mest kritiske systemer som er gitt effektiv EMP-beskyttelse. Også innenfor sivile infrastrukturer med stor viktighet for Totalforsvaret har det vært foretatt en viss grad av sikring, for eksempel i systemer innen kraftforsyningen og i Telenors telenett.

Det er utgitt retningslinjer for sikring av viktige IKT-installasjoner i Totalforsvaret mot elektromagnetiske strålingsvåpen. I tillegg har Totalforsvarets råd for sikring av tele- og informasjonssystemer (TRSTI) tatt initiativ til utarbeidelse av en forskrift om beskyttelse av telekommunikasjonsanlegg mot elektromagnetisk puls (EMP-forskriften). Et forskriftsutkast har vært ute på høring, og bare et fåtall av høringsinstansene hadde merknader til utkastet til forskrift med kommentarer.

I forskriftsutkastet er det foreslått at internkontrollprinsippet, som bygger på risiko- og sårbarhetsanalyser gjennomført av den enkelte anleggseier, skal legges til grunn ved vurdering av hvilke telekommunikasjonsanlegg som bør EMP-sikres. Ettersom det legges opp til at den enkelte må bekoste EMP-sikringen selv, mener man at det kan være fare for at EMP-sikringen i mange tilfeller ikke blir i henhold til forskriften. Dette anses for å være uheldig, og det er derfor foreslått å være en forutsetning at Post- og teletilsynet kan gi objektive og faglige råd i forkant av en eventuell EMP-sikring. Dette vil være en naturlig oppgave for Post- og teletilsynet. Det legges opp til at forskriften skal fastsettes av Post- og teletilsynet etter at tilsynets arbeid med telesikkerhet og -beredskap er kommet i gang.

10.7 Nasjonal autonomi [5)]

Tidligere hadde Norge, som mange andre land, ett nasjonalt telenett. Dette nettet var «autonomt» i den forstand at nettet både eiermessig og driftsmessig var uavhengig av andre telenett selv om det var tilknyttet andre nett gjennom internasjonale samtrafikkavtaler. Liberaliseringen av telesektoren og den generelle globaliseringen har endret dette bildet ved at nye telenett i dag ofte blir etablert på tvers av landegrensene.

[5)] Nasjonal autonomi innebærer at det skal være mulig å kommunisere innenfor nasjonens grenser uten å være avhengig av driftsstøtte fra utlandet.

I moderne telenett er det mulig å sentralisere driftsfunksjonene i langt større grad enn tidligere. I prinsippet vil en operatør kunne overvåke driften av hele sitt landsdekkende nett fra ett sentralt senter i utlandet. Knutepunkt i nettene som er vitale for telenettenes funksjon kan også ligge utenfor Norges grenser, og informasjon for håndteringen av tjenesten kan hentes fra sentraliserte noder i utlandet. Dette reduserer muligheten til å ha nasjonal kontroll med telenettet, samtidig som vi er utsatt for sårbarheten i andre lands telenett i tillegg til vår egen.

I det norske markedet har vi fått aktører som definerer hele Norden som sitt hjemmemarked og som bygger ut sammenhengende telenett i alle nordiske land. Driftsteknisk er det mulig å administrere telenettet i hvert land fra et sentralt driftssenter, noe som også skjer i praksis ved at disse operatørenes driftssentre i Norge typisk bare er bemannet i ordinær arbeidstid. På kveldstid og nattetid overføres gjerne overvåkingen av nettet til et sentralt driftssenter utenfor landets grenser.

Etter hvert som de nye aktørene opparbeider betydelige markedsandeler øker også deres betydning i forhold til Totalforsvaret. For Totalforsvaret betyr dette at det ikke lenger bare er Telenors virksomhet som er avgjørende for befolkningens tilgang til telekommunikasjonstjenester. Riktignok er produksjonen av teletjenester hos de nye aktørene i stor grad fortsatt avhengig av Telenors infrastruktur. I en krisesituasjon vil det imidlertid være av stor betydning at telesystemene til andre operatører enn Telenor også fungerer tilfredsstillende. En viktig målsetting er at operatører som tilbyr offentlig telefontjeneste i Norge må kunne opprettholde tjenestetilbudet til sine kunder i en situasjon hvor forbindelsene til utlandet blir brutt. Nasjonal autonomi innebærer at det skal være mulig å kommunisere innenfor nasjonens grenser uten å være avhengig av driftsstøtte fra utlandet. For å sikre Norges suverenitet i enhver samfunnstilstand anbefaler TIFKOM-prosjektet at Post- og teletilsynet bør stille nasjonal autonomi som krav til operatørene, dvs. at det *skal være mulig* å kommunisere som normalt innen nasjonens grenser dersom all kommunikasjon mot utlandet blir brutt.

Myndighetskrav i form av spesielle forskrifter eller konsesjonsbestemmelser kan være et mulig virkemiddel for å oppnå nasjonal autonomi. I det regulatoriske rammeverket som er etablert for telesektoren er det også et siktemål å unngå for mange nasjonale særbestemmelser. Det kan derfor være hensiktsmessig å vurdere andre virkemidler som bl.a. innebærer et sterkere samarbeid mellom myndighetene og de viktigste teleselskapene på dette området.

Av kommersielle grunner er det naturlig at selskaper som f.eks. opererer telenett i alle nordiske land søker å rasjonalisere driften mest mulig. Samtidig krever nærhet til kundene lokal tilstedeværelse når det gjelder kundebehandling, service, feilretting etc. Det er således en avveining av ulike hensyn som avgjør hvilken driftsstruktur selskapene velger. I denne prosessen er det viktig at også beredskapshensyn får en sentral plass i selskapenes planlegging. Dette behøver ikke nødvendigvis å innebære dublering av funksjoner og utstyr, men kan eventuelt også oppnås gjennom omdisponeringer i driftsorganisasjonen med sterkere vekt på lokal beredskap ved krisesituasjoner. Mer-

kostnadene er sannsynligvis svært marginale i forhold til de omfattende investeringene som i dag foretas i telesektoren.

Post- og teletilsynet får i oppgave å utrede nærmere forutsetningene for og konsekvensene av å innføre et krav om nasjonal autonomi for alle samfunnsviktige teleoperatører.

10.8 Sikkerhet i telenettenes IKT-baserte produksjonssystemer

Sikkerhet har blitt en stadig mer aktuell problemstilling ettersom viktige driftsfunksjoner i telenettene i stadig større grad sentraliseres, og i tillegg baserer seg på kommersielt tilgjengelige datamaskintyper. Dersom disse systemene i tillegg har tilknytning til f.eks. Internett, vil dette gi mulighet for uautorisert tilgang til sentrale systemer for telenettenes funksjon. Konkurransen i markedet vil imidlertid sørge for at driftssikkerhet vil gi et konkurransefortrinn for den enkelte aktør. Driftssikkerheten vil derfor generelt være god under normale driftsforhold. Konkurransemarkedet vil derimot være lite opptatt av å beskytte seg mot de større utfordringene, f.eks. mot en aktør som har høy angrepskapasitet. Dette kan for eksempel være en stor terror- eller statlig organisasjon. Den enkelte aktør i markedet har således ikke insentiv til å bruke ressurser på disse utfordringene ettersom de ikke vil få en klar kommersiell fordel av slike tiltak.

I forbindelse med sikkerheten i IT-systemene for teleoperatørene, er inntrykket til TIFKOM-prosjektet at det største problemet er at nye systemer og systemelementer kobles direkte på det eksisterende nettverket uten at operatørene nødvendigvis ser konsekvensene av hva dette kan føre til. Etter hvert som flere systemer og elementer kobles på, risikerer man å miste oversikten. Uten oversikt og kontroll over IT-systemenes oppbygning blir det dermed vanskelig å beskytte et slikt nettverk.

For å hindre at uvedkommende får tilgang til operatørenes drifts-, vedlikeholds- og støttesystemer, mener Samferdselsdepartementet at Post- og teletilsynet bør stille krav til operatørene om at det skal utarbeides en oversikt over hvordan viktige system, f.eks. driftssystemet, er koblet mot det øvrige nettverket. Dersom dette ikke er kjent, er faren stor for at viktige systemer heller ikke er beskyttet bedre enn resten av nettverket. Samtaler TIFKOM-prosjektet har gjennomført med operatørene har imidlertid avdekket at dette var et område som var i fokus i forbindelse med operatørenes forberedelser til overgangen til år 2000.

Når man har oversikt over hvordan nettverkene er oppbygd er grunnlaget lagt for å beskytte viktige delsystem bedre enn det nettverket det er koblet opp mot. Dette kan gjøres ved at delsystemet separeres fra resten av nettverket med en enhet, f.eks. en brannmur. Segmentering av nettverkene blir viktigere etter hvert som flere nettverk kobles sammen, og krav om bedre beskyttelse av viktige delsystemer er et annet krav Post- og teletilsynet bør stille til operatørene.

10.9 Red teams

Det vil være behov for en rekke ulike typer tiltak for å sikre informasjonen innen telenettets IKT-baserte produksjonssystemer. Et eksempel på et viktig

tiltak vil være å ta i bruk såkalte «red teams». Et «red team» er en gruppe mennesker som har fått i oppdrag å trenge inn i en bedrifts datasystemer for å avdekke mulige svakheter i informasjonssystemenes sikkerhet. Dette kan med andre ord beskrives som et betalt hacker-oppdrag.

For å avdekke svakheter i informasjonssystemene i telenettene bør det etableres «red teams» som skal foreta autoriserte inntrengingsforsøk hos den enkelte operatør. Slike betalte hacker-oppdrag kan kombineres med ekstern revisjon eller internkontroll der klare krav og kriterier til informasjonssikkerhet blir testet og analysert. Resultatet av de inntrengingsforsøkene «red teams» gjør skal formidles til den enkelte operatør og Post- og teletilsynet slik at forebyggende tiltak kan iverksettes. Den kompetansen «red teams» må ha for å kunne avdekke svakheter i systemene til teleoperatørene må være på høyde med «profesjonelle hackere». I Norge etableres det miljøer som kan tilby konsulenttjenester innen dette feltet.

I Sverige har Post- och telestyrelsen gjennomført et prosjekt som har analysert trusselbildet for operatørenes drifts- og overvåkningssystemer. Dette prosjektet har vært gjennomført som en inntrengingsanalyse utført av to parallelt arbeidende «red teams». Det er operatørene selv som eier resultatene av disse analysene, mens Post- och telestyrelsen bare får muntlige oppsummeringsrapporter. Etter en slik gjennomgang blir det operatørene selv som må foreslå tiltak for å bedre de eventuelle svakhetene som er blitt avdekket og som må stille krav til sine leverandører, men Post- och telestyrelsen har møter med operatørene og diskuterer tiltakene med dem. I utgangspunktet er det operatørene selv som skal dekke kostnadene forbundet med disse tiltakene, men det kan bli aktuelt for Post- och telestyrelsen å delfinansiere tiltak som må iverksettes hos operatørene.

Samferdselsdepartementet mener «red teams» bør tas i bruk også i norske telenett for å avdekke svakheter i informasjonssystemenes sikkerhet. Post- og teletilsynet får i oppgave å utarbeide et opplegg basert på den svenske modellen som er skissert ovenfor. Dersom «red teams» skal benyttes på datasystemer som er definert som skjermingsverdige objekter eller inneholder skjermingsverdig informasjon, er det spesielle krav til hvem som kan utføre slike inntrengingstester. I slike situasjoner bør Nasjonal sikkerhetsmyndighet kontaktes i forkant for å avklare eventuelle problemer. Bruk av «red teams» vil være basert på frivillighet fra operatørenes side, og vil være et tilbud til de som ønsker det.

11 Sårbarhet i Internett

Både brukere, leverandører og produsenter av informasjon, som TV, radio, aviser, biblioteker, skoler, offentlige institusjoner og bedrifter ønsker at informasjonstilbudet skal være lettest mulig tilgjengelig. Det er derfor en betydelig drivkraft hos informasjonsprodusenter og nettoperatører om å gi all informasjon en standardisert form, som lett lar seg transportere elektronisk over ulike typer nett og på en enkel måte være tilgjengelig på ulike typer brukerutstyr. Internett, på grunn av sin teknologi og betydelige utbredelse, ligger vel til rette for å fylle dette behovet.

I det arbeid som er gjort i regi av Forsvarets forskningsinstitutt og TIF-KOM-prosjektet har det i liten grad vært foretatt vurderinger av Internett. Fokus har vært på den tradisjonelle telefontjenesten og infrastruktur i offentlig telekommunikasjon. Selv om den underliggende teleinfrastrukturen blir gjort mer robust kan likevel sårbarheten ved anvendelse av Internett fortsatt være stor. På denne bakgrunn har Samferdselsdepartementet i samarbeid med Post- og teletilsynet gitt konsulentfirmaet Scandpower i oppdrag å kartlegge nærmere situasjonen på dette området, samt å fremme forslag til sårbarhetsreduserende tiltak som spesielt bør rettes mot Internett.

11.1 Utviklingen i bruken av Internett

En kommunikasjonsprotokoll er et sett av regler som styrer kommunikasjonen mellom ulike enheter i et nett, og som bl.a. definerer grensesnittet mellom nettene og de tjenester nettene skal formidle. Det sentrale med Internett-protokollene er at de tillater overføring og integrering av mange ulike typer tjenester. Gjennom Internett-protokollene er det åpnet en mulighet for å bruke ett felles grensesnitt eller én protokoll for å overføre alle typer informasjon og tjenester. Samtidig vil alle typer underliggende infrastruktur kunne benyttes som overføringssamband. Internett-teknologien gjør det mulig å knytte sammen ulike typer fysiske nett og infrastrukturer i store sammenhengende infrastrukturer. Internett fremstår for brukerne som ett enhetlig nett, men er ingen egen fysisk infrastruktur. Internett er et tjenestenett som benytter ulike typer infrastruktur som opprinnelig ble bygget ut for andre tjenester (for en stor del teletjenester).

Internetts teknologiske grunnlag muliggjør på en enkel måte innføring av et utall tjenester. I det tradisjonelle telenettet som er beskrevet i kapittel 2 er det i dag ikke lagt til rette for tilsvarende muligheter. I løpet av forholdsvis kort tid har derfor Internett blitt en dominerende formidlingskanal for store deler av den digitale informasjonsoverføringen, og det er mye som tyder på at denne utviklingen vil fortsette.

Scandpower mener det må kunne antas at Internett i løpet av få år vil tilby mange av de samfunnskritiske tjenestene som teletjenestene i dag utfører. I hvilken grad disse tjenestene på Internett vil overta eller supplere tilsvarende tjenester i telenettet, er usikkert, men utviklingen vil mest sannsynlig medføre at Internett får økende betydning som kommunikasjonskanal for en rekke tjenester som i gitte situasjoner vil være av avgjørende betydning for å opprett-

holde samfunnsviktige funksjoner. Dette tilsier at samfunnet, ut fra risiko- og sårbarhetshensyn, har et behov for å arbeide systematisk med sikte på å øke Internetts robusthet mot alvorlige tekniske feil, fysisk sabotasje og - ikke minst - logiske angrep fra stater eller organisasjoner med tilgang til etterretningsinformasjon, kunnskap og teknologi, jf. kapittel 3.1.3.

Nedenfor er det gitt noen illustrerende eksempler på hva man i fremtiden kan forvente av Internett-baserte anvendelser, fordelt på typiske «asynkrone» tjenester, dvs. tjenester som kan tolerere en viss forsinkelse i overføringskjeden, og «synkrone» tjenester, som er mer kritiske med hensyn til forsinkelser.

Typiske asynkrone anvendelser:

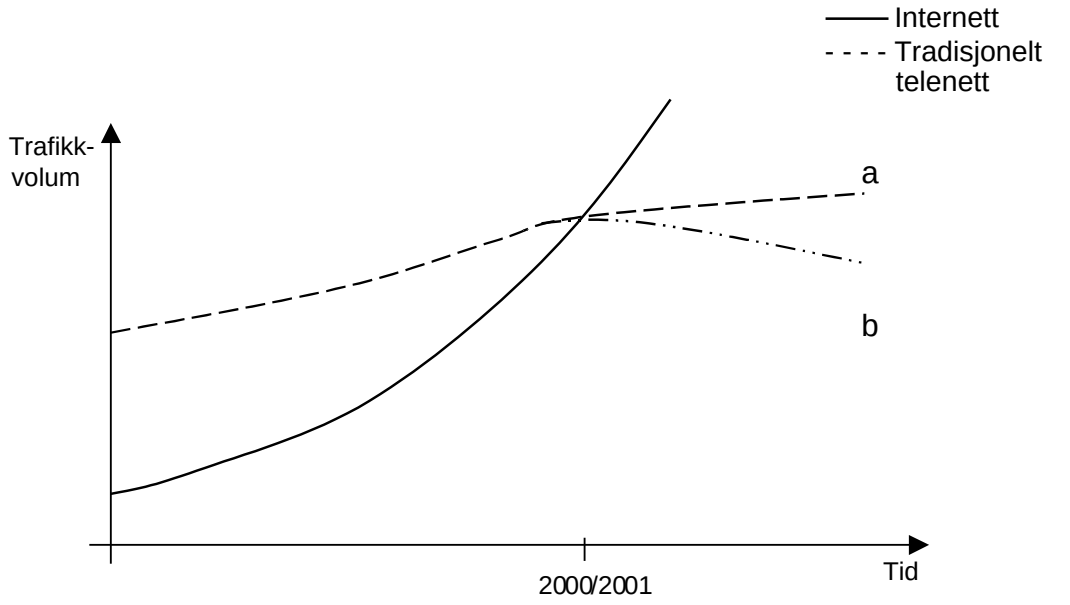
- Store deler av betalingstransaksjonene skjer via Internett (denne utviklingen er allerede i dag et faktum). Pris og overføringssikkerhet vil avgjøre om Internett overtar også de betalingstransaksjoner som i dag går over telenettene (f.eks. fra betalingsterminaler i forretninger).
- I enkelte bransjer er Internett-handel dominerende. Dette gjelder bl.a. aksjehandel (allerede i dag er størstedelen av aksjehandelen fra privatpersoner og mindre bedrifter Internett-basert) og store deler av engroshandelen, samt handel med standardiserte varer som bøker, musikk osv.
- Mange virksomheter, både private og offentlige, baserer store deler av sin informasjonsinnhenting og -distribusjon på Internett (denne utviklingen er allerede i dag et faktum).
- En stor del av den interne databehandlingen i både privat og offentlig sektor er satt bort til et lite antall store EDB-sentra. Internett er et viktig kommunikasjonsmiddel mellom de ansatte og dataanlegget.
- Logistikksystemer (for eksempel styring av reservedeler) vil i stor grad være Internett-baserte.
- Enkleste måte å få tilgang til komplett og utfyllende offentlig informasjon er via Internett.
- Overvåking og styring av et stigende antall tekniske anlegg og innretninger vil skje via Internett.
- Bedrifter, organisasjoner og enkeltstudenter benytter i økende grad nettbaserte opplærings- og studietilbud. E-læring vil stadig mer inngå som del av det ordinære tilbudet ved offentlige og private utdanningsinstitusjoner.

Typiske synkrone tjenester:

- Flere aktører tilbyr telefontjenester over Internett. Drivkrefter i dette vil være muligheten for samtidig overføring av tale og data (dokumenter, bilder, tegninger osv.), enkel oppsetting av nettmøter og kanskje også den antatt lavere prisen som brukeren må betale.
- Overføring av video og andre kringkastingstjenester. For slike anvendelser vil man også se at Internett brukes til bestilling og kommunikasjon fra brukerne til informasjonsleverandørene, mens «returoverføring» av video, bilder, lyd og lignende kan gjøres over andre etablerte bredbåndsnett.

Figur 11.1 illustrerer utviklingen av trafikkvolumet i Internett og i det tradisjonelle telenettet. I Internett forventes en fortsatt dobling av trafikk hver 6. til 12. måned, mens volumveksten i telenettet vil avta og enten stoppe opp (a), eller gå ned (b). Krysningspunktet mellom trafikkvolumet i det tradisjonelle telenettet og Internett er i 2000-2001. Scandpower har her trukket to konklusjoner. Den ene er at den samfunnsmessige betydningen av Internett vil øke betraktelig i forhold til bruk av standard telefon. Dette vil selvsagt ha en brem-

sende effekt på utviklingen av det tradisjonelle telenettet. Om trafikkvolumet her vil avta etter hvert, vil avhenge av om Internett - i global skala - kan demonstrere sin brukbarhet også for telefontjenester.



Figur 11.1 Historisk og antatt trafikkutvikling i hhv. telenett og Internett.

Ved siden av USA, er Norden det området som har størst tetthet av Internettbrukere. I Norge regner man med at 40-50 % av befolkningen har tilgang til Internett enten privat eller via jobben. I første rekke gir denne tilgangen adgang til tjenester som Web, e-post og overføring av filer, og etter hvert også telefontjenester.

Med de skisserte anvendelsesområdene, vil viktige deler av samfunnet raskt komme i ubalanse og til dels kunne stoppe opp dersom Internett settes ut av drift eller alvorlig forstyrres over lengre tid, f.eks. fordi en kompetent inntrenger manipulerer den kommunikasjonen som skjer i nettet.

11.2 Sårbarhetsreduserende tiltak for Internett

Den teknologi som Internett er basert på, gir i utgangspunktet et robust nett i forhold til de fleste typer fysiske trusler. Internett-teknologi med pakkesvitsjing skal i teorien motvirke alvorlige konsekvenser av tekniske feil, uhell, fysisk sabotasje e.l. Denne robustheten er imidlertid avhengig av at de mulighetene som Internett-teknologien gir blir bevisst utnyttet av Internett-operatørene. Dette gjelder spesielt med hensyn til å planlegge de fysiske transmisjonsveiene slik at enkeltfeil ikke slår ut alle forbindelser mellom rutere i Internett. Dersom Internett-operatørene ikke er bevisste på dette området, er Internett like sårbart som det tradisjonelle telenettet når det gjelder kabelbrudd e.l. i alle deler av nettene.

Internett må anses som sårbart overfor logiske anslag. I og med at signalerings- og driftsfunksjoner i prinsippet er åpent tilgjengelige for alle brukere og Internett-operatører, vil det kunne tenkes situasjoner hvor en kompetent organisasjon kan manipulere disse nettfunksjonene, og derigjennom skape betydelige forstyrrelser i nettet. Et annet sårbarhetselement er anslag mot de ende-til-ende tjenester som tilbys gjennom Internett, f.eks. finanstransaksjo-

ner og informasjonssystemer. I utgangspunktet er det brukernes ansvar å sikre slike tjenester ved hjelp av kryptering e.l., men også på dette området er det lett å se scenarier hvor samfunnets stabilitet kan settes i fare, f.eks. ved en alvorlig inntrenging og manipulering med betalingsformidling eller bankkonti, eller såkalte oversvømmelsesangrep mot databaser og informasjonssystemer.

I Norge har det frem til sommeren 2000 vært bare ett sammenkoblingspunkt mellom de ulike Internett-operatørene. Dette sammenkoblingspunktet har vært drevet av Universitetet i Oslos sentrale IT-avdeling. Dette punktet, «Norwegian Internet eXchange» (NIX), kobler sammen ca. 30 uavhengige Internett-operatører. Driftsstabiliteten til selve utstyret har vært svært god, men NIXen er et sårbart punkt dersom tilhørende kabler (transportsystemer) skades. Avdelingen som driver NIXen tok derfor initiativet til installasjon av nok en NIX i Oslo, kalt NIX2. Dette har i betydelig grad økt tilgjengeligheten og gjort det totale norske Internett mindre sårbart for kabelbrudd og liknende.

11.2.1 Forslag til sårbarhetsreduserende tiltak

Internett er en teleinfrastruktur som reguleres av teleloven, og er dermed Samferdselsdepartementets ansvarsområde. I tillegg har Nærings- og handelsdepartementet interesser i dette området. Det er så langt lagt til grunn at tjenestetilbyderne selv skal være sentrale i ordninger for administrasjon og drift av infrastrukturen som benyttes ved tjenester på Internett.

Det har ikke vært foretatt en samlet gjennomgang og vurdering av på hvilken måte telelovgivningen får anvendelse på Internett. Som en del av det pågående arbeidet med regelverksgjennomgang på teleområdet vil det imidlertid bli vurdert om det er områder innen Internett der det kan være behov for å sikre samfunnsmessige interesser via lovregulering, eventuelt om det er mer hensiktsmessig med andre former for regulering. Samferdselsdepartementet vil starte planleggingen av en utredning som vil ha som hensikt å skaffe bedre oversikt over Internett-markedet.

Etter hvert som Internett også tilbyr samfunnskritiske tjenester, vil det bli et økende behov for at statlige myndigheter regulerer og overvåker viktige funksjoner i Internett. Nedenfor følger en gjennomgang av eksempler på områder der det i fremtiden kan være aktuelt for en statlig regulatør å gripe inn.

- Det har vist seg å være vanskelig å skaffe oversikt over hvem som tilbyr Internett-baserte overføringstjenester, dvs. de Internett-operatørene som tilbyr nett-tilknytning, signaloverføring og grunnleggende tjenester som e-post, web, filoverføring osv. Det bør derfor finnes en oversikt over Internett-tilbydere.
- I dag går all Internett-trafikk i Norge via to nasjonale sammenkoblingspunkter (NIX og NIX2). Dette er svært sårbare punkter for Internett-trafikken i Norge, ved at svikt her kan medføre store problemer for trafikkavviklingen mellom de ulike Internett-operatørene. Geografisk plassering, eierskap, fysisk og logisk sikring av NIXene er viktige faktorer i en nasjonal sårbarhetsstrategi for Internett.
- Dersom viktige samfunnsinstitusjoner som alarmsentraler, sykehus, politi, statlige etater etc. overfører større deler av sin kommunikasjon med omverdenen til Internett, vil det bli behov for å bevisst velge Internett-ope-

ratører med tilstrekkelig robusthet i nettet. Det vil i denne forbindelse være behov for retningslinjer og rådgivning med hensyn til det minimumsnivå for sikkerhet som en Internett-operatør må oppvise for å kunne ha ulike kritiske samfunnsinstitusjoner som abonnenter.
- Antall alternative transmisjonsveier mellom noder og nett, og hvordan disse veiene rutes i transmisjonsnettet, er av avgjørende betydning for Internetts sårbarhet. Denne problemstillingen har store likhetstrekk med tilsvarende sårbarhetsaspekter i tradisjonelle teletjenester.
- Etter hvert som antall Internett-operatører øker, vil det bli behov for retningsgivende standardavtaler mellom operatørene, for å sikre problemfri samtrafikk, forsvarlig kvalitet og kapasitet, samt like konkurransevilkår.

11.3 Samferdselsdepartementets vurderinger

Dersom Scandpower får rett i sin antagelse om at Internett i løpet av få år vil tilby mange av de samfunnskritiske tjenestene som de tradisjonelle teletjenestene i dag utfører, vil det være behov for å iverksette særskilte sikringstiltak for Internett tilsvarende det man i dag gjør i telesektoren for øvrig. Post- og teletilsynet må derfor overvåke utviklingen i bruken av Internett og fortløpende vurdere behovet for å implementere sikkerhets- og beredskapstiltak.

12 Administrative og økonomiske konsekvenser

12.1 Finansiering av telesikkerhet og -beredskap - ulike modeller

Det finnes ulike måter å finansiere de tiltak som er foreslått satt i verk, f.eks. egenfinansiering, kundefinansiering, bevilgninger over statsbudsjettet, avgiftsfinansiering, gebyrfinansiering og kombinasjoner av disse.

12.1.1 Egenfinansiering

Operatørene kan selv foreta investeringer i økt telesikkerhet og -beredskap, enten fordi de ved lov eller forskrift er pålagt å garantere et gitt robusthetsnivå som en del av betingelsene for å drive telekommunikasjon i Norge, eller fordi de selv ut fra kommersielle hensyn er tjent med et mindre sårbart telenett. Aktører i telebransjen vil oppfatte pålegg om gjennomføring av tiltak ulikt og ha forskjellig forståelse av nytteverdien. Noen vil kunne mene at de blir mer urimelig belastet enn sine konkurrenter, ved å påstå at pålegg har en konkurransevridende effekt.

Ved *egenfinansiering* pålegges teleaktørene selv å finansiere de nødvendige telesikkerhets- og teleberedskapstiltak. I Danmark, Nederland og til dels Storbritannia finansieres slike tiltak i all hovedsak ved at de offentlige myndigheter stiller krav til operatørene, hvorpå operatørne selv må dekke kostnader for å imøtekomme kravene.

Egenfinansiering egner seg best hvis kostnadene for de aktuelle beredskapstiltakene er lave og relativt jevnt fordelt på alle operatørene, slik at konkurranseforholdene ikke påvirkes. Kostnadene for de aktuelle telesikkerhets- og teleberedskapstiltak kan heller ikke være så store at de truer virksomhetens økonomiske overlevelsesevne. Det bør derfor etableres en refusjonsordning dersom kravene medfører urimelige utgifter for operatørene. Denne modellen brukes bl.a. innen kraftforsyningen i Norge, der Norges vassdrags- og energidirektorat (NVE) med hjemmel i energiloven kan pålegge aktørene tiltak og utbedringer for å øke robustheten i kraftforsyningen. Ifølge loven skal tiltak som kommer etter pålegg fra myndighetene finansieres av den enkelte virksomhet. Loven åpner likevel for at NVE, dersom slike pålegg medfører vesentlige utgifter uten at det samtidig oppveies av motsvarende fordeler, kan gi vederlag for gjennomførte tiltak.

Egenfinansiering vil medføre minimale kostnader for staten. Det er imidlertid uvisst hvor effektiv en ordning med egenfinansiering vil være. En slik ordning vil uansett kreve en aktiv tilsynsfunksjon, og dersom operatører ikke følger opp krav kan det forsinke måloppnåelsen.

12.1.2 Kundefinansiering

Kundefinansiering innebærer at de brukergrupper som stiller spesielle krav til telesikkerhet og -beredskap selv finansierer kostnadene forbundet med implementering av tiltakene. De aktører som i utgangspunktet kan sies å være kunder av telesikkerhets- og teleberedskapstiltak er totalforsvarsaktører med spe-

sielle sikringskrav som går utover de standarder telekommunikasjonsoperatørene og tjenesteleverandørene holder ut fra kommersielle hensyn. Dette kan gjelde bl.a. Forsvaret, Sivilforsvaret, nødetatene, andre med oppgaver relatert til redning og beredskap samt enkelte aktører i privat sektor med spesielle ansvarsområder. I tillegg har staten ansvar for å pålegge telesikkerhets- og teleberedskapstiltak i de allmenne nett, og er dermed den største telesikkerhets- og teleberedskapskunden overfor teleoperatørene.

Kundefinansiering er en oversiktlig løsning, og den eksisterer innenfor dagens administrative rammer. Et faremoment og en utfordring ved å basere seg på kundefinansiering er at tilnærmingen kan virke ansvarspulveriserende og dermed forsinke iverksetting av tiltak. Dersom etterspørsel av et tiltak medfører store kostnader, kan resultatet bli at kunden vil nedtone viktigheten av tiltaket. Kundefinansiering egner seg der spesielle brukere etterspør tjenester som ikke tilbys allmennheten. Kundefinansiering krever at de operatører som tilbyr disse spesielle tjenestene med høy telesikkerhet og -beredskap er garantert å få merkostnadene sine dekket.

12.1.3 Finansiering ved bevilgninger over statsbudsjettet

Ved direkte *bevilgninger over statsbudsjettet* vil de administrative konsekvensene bli små fordi rammeverket for slike bevilgninger allerede eksisterer. Et eksempel er dagens SSO-ordning, jf. kapittel 4.5, hvor det bevilges midler for Telenors ytelser til Totalforsvaret. Et argument for en slik finansieringsform er at avhengigheten av telesektoren er så betydelig, og svikt i telekommunikasjon representerer en så vesentlig risiko for samfunnet generelt, at investeringer i økt telesikkerhet og -beredskap bør fordeles på alle skattebetalere.

Overføringer over statsbudsjettet til disse formål vil uansett måtte konkurrere med andre samfunnsviktige oppgaver, og dermed kunne gi større usikkerhet i forhold til fremtidige investeringer enn andre finansieringsmodeller. Statsbudsjettfinansiering gir gode muligheter for staten til å styre beredskapstiltakene.

12.1.4 Avgiftsfinansiering

Avgiftsfinansiering innebærer at en årlig teleoperatøravgift øremerkes telesikkerhets- og teleberedskapsformål. En avgift kan tenkes knyttet til det enkelte telefonabonnement eller relateres til forbruk av teletjenester. Avgiftsfinansiering gjør det mulig å relatere kostnadene forbundet med økt telesikkerhet og -beredskap til de som kjøper telesektorens produkter og tjenester, slik at man kan fordele kostnadene på samtlige telebrukere.

Beregninger viser at en årlig avgift på 50 kroner per abonnement, vil gi en årlig inntekt på rundt 270 mill. kroner. En generell «teleberedskapsavgift» som innføres med basis i abonnement eller telebruk vil ikke være konkransevridende, fordi nye operatører/tjenesteleverandører i starten vil ha få abonnenter og/eller liten tjenesteproduksjon og dermed betale en lav «teleberedskapsavgift». Hovedutfordringen ved å knytte avgiften til et abonnement er hvordan man skal definere et abonnement og hvilke typer abonnement det skal beregnes avgift på. I dag er det mulig å ha abonnement hos flere operatører på forskjellige type tjenester. Definisjon av avgiftsgrunnlaget må derfor

utarbeides i samarbeid med teleoperatørene for å unngå utilsiktet konkurransevridning.

Innkreving av avgifter representerer en utgiftspost i seg selv, og det vil være betydelige kostnader forbundet med å etablere en helt ny avgiftsinnkrevingsordning. Etablering av avgiftsfinansiering egner seg derfor ikke for å finansiere mindre beredskapstiltak.

12.1.5 Gebyrfinansiering

Post- og teletilsynet er selvfinansierende. Med hjemmel i teleloven § 10-1 har Samferdselsdepartementet (jf. funksjonsfordelingsforskriften) fastsatt forskrift om gebyr til inntekt for Post- og teletilsynets virksomhet. Post- og teletilsynet kan ta inn gebyr for konsesjoner, tillatelser, tildelinger, for kostnader til planleggings-, registrerings-, standardiserings-, tilsyns- og annen forvaltningsvirksomhet i medhold av loven.

Sikring av telenett utføres med hjemmel i teleloven § 7-7. Driftskostnader som påløper som følge av Post- og teletilsynets oppgaver relatert til telesikkerhet og -beredskap kan finansieres ved gebyrer fra teleoperatørene, jf. kapittel 5.2.

Investeringer i konkrete tiltak kan også vurderes finansiert med gebyrer, forutsatt at tiltakene har rettsgrunnlag i teleloven eller annen telelovgivning, og er del av det offentliges forvaltningsvirksomhet. Det er usikkert hvor langt hjemmelsgrunnlaget rekker når det gjelder dekning av investeringer i konkrete tiltak. Før det eventuelt innføres gebyrer for dette formålet må det derfor vurderes nøye om gebyrene ligger innenfor lovens rammer, herunder om gebyrene er forholdsmessige.

12.1.6 Kombinasjonsmodell

Det er også mulig å tenke seg en *kombinasjonsmodell* hvor offentlige myndigheter og teleoperatørene går sammen om å finansiere de foreslåtte telesikkerhets- og teleberedskapstiltakene. Denne modellen forutsetter at staten bevilger midler over statsbudsjettet, samtidig som operatørene sier seg villige til gjennom egne midler og/eller avgiftsmidler å finansiere telesikkerhets- og teleberedskapstiltak som i utgangspunktet er definert som uinteressante ut fra et kommersielt perspektiv. Ettersom offentlige midler øremerket telesektoren representerer et inntektspotensial for teleoperatørene og tjenesteleverandørene, vil denne modellen gi et insentiv til operatørene om også å bidra med midler til sikkerhets- og beredskapstiltak.

Kombinasjonsmodellen er foretrukket av Forsvarets forskningsinstitutt i BAS2-studien, og denne modellen er allerede implementert i Sverige. Der har man siden midten av 90-tallet målbevisst arbeidet for å sikre svenske telenett mot trusler i hele utfordringsspekteret fra fred til krig, ved at staten bevilger midler over statsbudsjettet mens operatørene betaler tilsvarende beløp i avgifter øremerket til sikkerhet og beredskap. Denne ordningen omfatter alle tjenesteleverandørene av betydning, så vel som alle teletjenester som disse tilbyr i markedet. Erfaringer fra Sverige viser at denne løsningen ikke bare har falt gunstig ut for operatørene, men også for myndighetene, ved at tiltak iverksettes i den takt myndighetene ønsker. Denne modellen krever høy teknisk kompetanse hos Post- og teletilsynet for at tilsynet skal kunne fungere som profe-

sjonell kunde på statens vegne. I tillegg vil det være en utfordring å forvalte investeringsmidlene på en rettferdig måte for å unngå konkurransevridning.

12.1.7 Samferdselsdepartementets vurdering av finansieringsmodellene

Som det fremgår av ovenstående er det flere måter å finansiere telesikkerhets- og teleberedskapstiltak på. Gjennomgangen viser for øvrig at valg av finansieringsmåte vil avhenge av type tiltak og derfor må avgjøres konkret i forbindelse med beslutning om implementering av det enkelte tiltak. Det er viktig at de finansieringsløsninger som velges bidrar til klare ansvarsforhold, og at Post- og teletilsynet gis nødvendig handlekraft, slik at arbeidet med telesikkerhet og -beredskap ikke blir forsinket eller at de mål som er satt ikke nås.

Den finansieringsmodellen som velges i det enkelte tilfelle bør ikke virke konkurransevridende eller skape for stor og ulik belastning for noen av de berørte parter.

12.2 Finansiering av foreslåtte telesikkerhets- og teleberedskapstiltak

De tiltak TIFKOM-prosjektet har foreslått iverksatt over en 5-årsperiode har en total kostnadsramme på 730 mill. kr som er foreslått dekket over statsbudsjettet. I tillegg kommer kostnader ved overtakelse av Telenors fjellanlegg på ca. 1,2 mrd. kr, kostnader ved eventuell flytting av teleoperatørenes utstyr til samlokaliseringssentra samt andre tiltak man ikke har beregnet kostnadene for, herunder eventuell samordning mellom Forsvarets digitale nett (FDN) og et eventuelt nytt radionett for nødetatene. Med de kostnader det i dag er oversikt over, gir TIFKOM-prosjektets forslag en samlet ramme på ca. 2 mrd. kr over 5 år.

Den ambisjonen Samferdselsdepartementet legger opp til er vesentlig lavere. Selv om det per i dag ikke foreligger nøyaktige kostnadstall, har vi foreløpige, grove anslag som gir et bilde av hvilke kostnadsstørrelser det er snakk om jf. kapittel 12.3.

Beregninger viser at det vil koste i størrelsesorden 5-10 mill. kr å utføre de nye oppgavene i Post- og teletilsynet det første året med en bemanning på 4 personer. Av dette er 3,2 mill. kr rene etableringskostnader. Over en 5-årsperiode er det beregnet at sikkerhets- og beredskapsarbeidet i Post- og teletilsynet vil koste til sammen ca. 20-40 mill. kr dersom bemanningen holdes stabil på 4 personer. Ordinære driftsutgifter i forbindelse med Post- og teletilsynets sikkerhets- og beredskapsoppgaver vil kunne finansieres med gebyrer fra teleoperatørene på lik linje med Post- og teletilsynets øvrige virksomhet. Samferdselsdepartementet forutsetter at etableringskostnaden første år på 3,2 mill. kr dekkes over Samferdselsdepartementets beredskapskapittel i statsbudsjettet.

For de øvrige telesikkerhets- og teleberedskapstiltak vil det som nevnt måtte foretas en nærmere konkret vurdering av hvilke finansielle virkemidler som er best egnet i det enkelte tilfelle. Det er viktig at det ved vurderingen sikres at finansieringen ikke gir utilsiktede konkurransevridninger. Finansiering av konkrete tiltak vil kunne skje gjennom gebyrer, avgifter, egenfinansiering

(operatørfinansiering), kundefinansiering eller bevilgninger over statsbudsjettet.

I tilfeller der det eventuelt kan være hensiktsmessig at tiltak finansieres med bevilgninger over statsbudsjettet, vil Samferdselsdepartementet komme konkret tilbake med bevilgningsforslag i forbindelse med de årlige budsjettforslagene.

I henhold til gjeldende forskrift om offentlig telenett og offentlig teletjeneste har teleoperatører plikt til å ha et minimumsnivå for telesikkerhet i sine nett for å garantere leveringsdyktighet og sikring av kundenes telekommunikasjon. Kostnader knyttet til å ivareta denne grunnsikkerheten vil under enhver omstendighet måtte dekkes av operatørene.

12.3 Foreslåtte tiltak med foreløpige kostnadsoverslag

I kapittel 6-11 er det foreslått en rekke telesikkerhets- og teleberedskapstiltak som bør implementeres for å heve robusthetsnivået i de offentlige telenett. Enkelte av disse tiltakene er kostnadsberegnet, mens det for andre tiltak ikke er angitt noen kostnad. Dette skyldes at ikke all nødvendig grunnlagsinformasjon foreligger eller at det gjenstår en nærmere utredning av tiltaket. De beregningene som allerede foreligger kan uansett gi et bilde av hvilke kostnadsstørrelser det er snakk om. Tabell 12.1 viser en samlet oversikt over de tiltak som er omtalt i meldingen med tilhørende kostnadsoverslag der det er mulig. Der annet ikke er oppgitt gjelder tallene for en femårsperiode.

Tabell 12.1: Foreløpig kostnadsoverslag i mill. kr (- angir at kostnad foreløpig ikke er beregnet).

Drift av sikkerhets- og beredskapsfunksjonen i Post- og teletilsynet (PT)	40
Prioritet i fast- og mobilnett, redusert løsning	50
Prioritet i fast- og mobilnett, ende-til-ende	-
Samlokalisering i fjellanlegg	-
Redundans i telenettene	Samarbeid mellom operatørene -
Samordning av FDN og eventuelt	
nytt radionett for nødetatene	-
Bevisstgjøring, kompetanseheving	
og veiledning	Inngår i kostnad for drift i PT
Klassifisering av teleinfrastrukturen	Inngår i kostnad for drift i PT
Sikkerhetsevaluering av offentlig telenett	Inngår i kostnad for drift i PT
Samøvelser	20
Beredskapsutstyr	50
EMP-forskriften	Inngår i kostnad for drift i PT
Nasjonal autonomi	-
Sikkerhet i telenettenes IKT-baserte produksjonssystemer	Administrativt tiltak hos operatørene
«Red teams»	15
Sårbarhetsreduserende tiltak i Internett	-
Sum (foreløpig)	175

Som det fremgår av tabell 12.1, er det av de større tiltakene kun investering i ny prioritetsordning i telenettene som er kostnadsberegnet. Foreløpige tall viser at implementering av «sambandsreservering» og «prioritert trafikk» i Telenors fastnett, samt innføring av en redusert løsning som ikke muliggjør ende-til-ende-prioritet i mobilnettene, jf. kapittel 6.2, har en kostnad på ca. 50 mill. kr. I tillegg kommer eventuell utvidelse med radioressurser reservert for prioriterte brukere som kan beløpe seg til ca. 250 mill. kr (fremgår ikke i tabellen). Dersom man skal få etablert en prioritetsordning som muliggjør ende-til-ende prioritet i mobilnettene vil det påløpe ytterligere kostnader, men det finnes foreløpig ikke kostnadsberegninger for dette.

Det vil senere også måtte påregnes betydelige utgifter i tilknytning til eventuell tilrettelegging for begrenset samlokalisering i fjellanlegg. Det legges bl.a. opp til at Post- og teletilsynet skal gjennomføre en nærmere kartlegging av hvilke fjellanlegg som er mest aktuelle som samlokaliseringssentra, samt hvilke investeringer som er nødvendig for å klargjøre anlegg for samlokalisering. Først da vil det være mulig å beregne kostnad for samlokalisering.

Når det gjelder redundans vil man i første omgang søke å øke redundansen gjennom økt samarbeid mellom operatørene med transportnett, jf. kapittel 8.

Kostnader ved utbygging av et eventuelt nytt felles radionett for nødetatene med basis i Forsvarets digitale nett (FDN) vil avhenge av Forsvarets tele- og datatjenestes utredning for å kartlegge hvor stor del av et landsdekkende radionett for nødetatene som kan etableres med basis i FDN og de økonomiske betingelser knyttet til dette, jf. kapittel 9.3.

Bevisstgjøring, kompetanseheving og veiledning, klassifisering av teleinfrastrukturen og sikkerhetsevaluering av offentlig telenett er administrative og organisatoriske tiltak som vil være en del av Post- og teletilsynets oppgaver og som således er inkludert i kostnadene for drift av sikkerhets- og beredskapsfunksjonen.

Samøvelser mellom flere operatører er beregnet å koste 20 mill. kr over 5 år.

Investering i beredskapsutstyr er et tiltak som videreføres fra gjeldende SSO-ordning, jf. kapittel 10.5. Ved å legge tallene fra gjeldende SSO-overenskomst til grunn, vil det for beredskapsutstyr til Telenor være snakk om en samlet kostnad på 30 mill. kr over en 5-årsperiode. En ny ordning må gjelde også for andre operatører, og basert på de tallene som gjelder for Telenor er det rimelig å anta at det kan anslås en samlet kostnad for dette tiltaket på ca. 50 mill. kr over 5 år.

Oppfølging av EMP-forskriften er også et administrativt og organisatorisk tiltak som vil være en del av Post- og teletilsynets oppgaver og som således er inkludert i kostnadene for drift av sikkerhets- og beredskapsfunksjonen.

Nasjonal autonomi er annet tiltak der Post- og teletilsynet skal utrede nærmere forutsetningene for og konsekvensene av å innføre et krav om nasjonal autonomi for alle samfunnsviktige teleoperatører.

Sikkerhet i telenettenes IKT-baserte produksjonssystemer vil være et administrativt tiltak som operatørene må besørge.

Etablering og bruk av «red teams» er kostnadsberegnet til 15 mill. kr over 5 år.

Når det gjelder sårbarhetsreduserende tiltak i Internett, er dette et område der Post- og teletilsynet er forutsatt å overvåke utviklingen i bruk og fortløpende vurdere behovet for å implementere sikkerhets- og beredskapstiltak.

12.4 Avvikling av gjeldende SSO-ordning

Det nye konseptet for telesikkerhet og -beredskap som skisseres i meldingen vil bli en ny ordning med spesielle samfunnspålagte oppgaver (SSO) til Totalforsvaret som vil gjelde for alle samfunnsviktige teleoperatører og ikke bare for Telenor slik tilfellet er i dag.

Før den nye beredskapsordningen etableres vil det være hensiktsmessig om staten innfrir de forpliktelser som staten har påtatt seg gjennom gjeldende SSO-overenskomst med Telenor for 2001. Foreløpige beregninger viser at dette vil koste ca. 80 mill. kr som engangskostnad. Forut for utfasing av gjeldende SSO-ordning må det gjennomføres samtaler med Telenor for å komme frem til endelig størrelse på kompensasjonen. Samferdselsdepartementet vil deretter måtte komme tilbake til dette med forslag i den ordinære budsjettprosessen. Kostnader forbundet med utfasing kommer i tillegg til de kostnader som er skissert i kapittel 12.3.

Inntil det nye konseptet er fullt ut etablert vil det uansett være behov for å videreføre enkelte av de oppgavene Telenor har vært pålagt gjennom SSO-ordningen. Dette gjelder bl.a. en del administrative og organisatoriske beredskapstiltak samt investeringer i transportabelt reservemateriell som må oppgraderes i takt med utviklingen i telenettene. For 2002 er dette beregnet til å utgjøre ca. 9 mill. kr. Samferdselsdepartementet vil også her komme tilbake med et konkret forslag i den ordinære budsjettprosessen.

Samferdselsdepartementet

t i l r å r :

Tilråding fra Samferdselsdepartementet av 11. mai 2001 om telesikkerhet og -beredskap i et telemarked med fri konkurranse blir sendt Stortinget.

Vedlegg 1

Utredninger vedrørende sårbarhet, sikkerhet og beredskap i telekommunikasjon

I1994 ble det besluttet å starte et samarbeidsprosjekt mellom Forsvarets forskningsinstitutt (FFI) og Direktoratet for sivilt beredskap (DSB) med bakgrunn i at den sivile beredskapssektor i vid forstand trengte et mer helhetlig grunnlag for ressursallokering og et bedre system for den langsiktige planlegging. Figur 1.1 i kapittel 1.1 er hentet fra dette forskningsprosjektet som konkluderte med at spesielt de tre funksjonene kraftforsyning, telekommunikasjon og ledelse/informasjon skiller seg ut som nødvendige for all samfunnsvirksomhet. Svikt innen en av disse funksjonene vil kunne medføre svikt i de fleste andre samfunnsfunksjoner. Dette er områder som ifølge FFI bør være gjenstand for økt satsing når det gjelder beredskap.

Prosjektet «Beskyttelse av samfunnet» (BAS) ble etterfulgt av nytt prosjekt med oppdrag å utrede sårbarhet og sårbarhetsreduserende tiltak innen telekommunikasjon. Dette prosjektet fikk betegnelsen BAS2 - «Beskyttelse av samfunnet 2», og ble gjennomført i perioden september 1997 - februar 1999. BAS2-prosjektet ble gjennomført etter oppdrag fra Justisdepartementet, Samferdselsdepartementet og DSB.

For å følge opp FFIs anbefalinger i BAS2-prosjektet, foreslo Totalforsvarets råd for sikring av tele- og informasjonssystemer (TRSTI), etter oppdrag fra Samferdselsdepartementet, at det burde nedsettes et nytt prosjekt som skulle bearbeide FFIs anbefalinger for å fremskaffe grunnlag for et stortingsfremlegg om telesikkerhet og -beredskap i et fritt konkurransemarked (forkortet til TIFKOM).

Beskyttelse av samfunnet 2 - Sårbarhetsreduserende tiltak innen telekommunikasjon (BAS2)

Som nevnt ovenfor har samfunnets avhengighet av velfungerende telekommunikasjoner dannet utgangspunkt for Forsvarets forskningsinstitutts (FFIs) analyse av sårbarhet og sårbarhetsreduserende tiltak innen området offentlig telekommunikasjon. FFI har i BAS2-prosjektet konkludert med at fremtidens samfunn i økende grad vil være avhengig av informasjonsformidling og teletjenester for å kunne fungere. Kommersiell og teknologisk utvikling vil samtidig, dersom den får gå upåvirket, føre til en svært høy grad av sårbarhet innen offentlig telekommunikasjon. FFI mener samfunnet og Totalforsvaret er altfor avhengige av telekommunikasjon til at en kan tillate at markedsutviklingen alene kan få legge premissene for sikkerheten i de offentlige nett. En forutsetning for en videreføring av totalforsvarskonseptet er å sikre kritisk informasjonsbehandling innen Totalforsvaret. Dette dreier seg både om tiltak for å sikre et solid fundament for offentlig telekommunikasjon, så vel som at brukerne innen Totalforsvaret gjennomfører ulike typer tiltak for å sikre sitt eget kritiske behov for informasjonsutveksling. FFI ga en anbefaling om strategi for robust telekommunikasjon, hvorpå brukerens ansvar for sikkerhet ble påpekt.

Et vesentlig element i FFIs anbefalte strategi for sikring av telenettene er satsning på mangfoldet mellom ulike teleoperatører for å redusere sårbarheten. BAS2-prosjektet anbefalte sikring av det offentlige telenettet fremfor i utstrakt grad å satse på tjenester fra alternative nett som Forsvarets nett

(FDN) og mobil satellittkommunikasjon. De foreslåtte tiltakene dekker visse grunnleggende behov for Totalforsvaret, men er på ingen måte gode nok i situasjoner der samfunnet står overfor større menneskeskapte utfordringer. Strategien innebærer at avgjørende og vitale punkter i telenettet er fysisk beskyttet i fjellanlegg, og hvor hensynet til grunnsikkerhet er ivaretatt. Bl.a. er det foreslått samlokalisering i fjellanlegg, investering i transportabelt reservemateriell og sammenkoblingspunkter mellom de ulike operatørene nett. Strategien har en samlet kostnad på 750 mill. kr og er anbefalt gjennomført i løpet av en 5-årsperiode. FFI mener strategien vil representere en betydelig forbedring av sikkerheten i telenettet i forhold til i dag, og fremhever at en årlig kostnad på ca. 150 mill. kr i fem år ikke er særlig høy når en til sammenligning årlig bevilger rundt 25 mrd. kr til Forsvaret.

På lang sikt anbefaler imidlertid BAS2-prosjektet at det bør siktes mot å øke robustheten i telenettet ytterligere. FFIs langsiktige strategi går langt i å sikre infrastruktur mot fysiske og elektroniske våpenvirkninger, dog uten å anbefale full EMP-sikring av nettet. I tillegg inneholder denne strategien en anbefaling om innføring av prioritert tjenesteaksess for alle teleoperatører. Kostnadsrammen for den langsiktige strategien er 2,2 mrd. kr.

For å gjennomføre de strengt påkrevde offentlige inngrep i utviklingen av det sivile telemarkedet, trengs det politisk forståelse, både for telenettets sårbarhet og for samfunnets avhengighet av telekommunikasjon. FFI mener det også trengs et statlig organ med overordnet ansvar for sikkerhet innen norsk telekommunikasjon, som har kompetanse, myndighet og midler til å oppdatere, implementere og følge opp konkrete, langsiktige planer. Rask teknologisk utvikling og et samfunn i stadig endring krever et dynamisk organ som kan følge opp den løpende utviklingen og iverksette tiltak, dvs. bygge sårbarhetsreduserende tiltak inn i den videre utviklingen av telekommunikasjonssektoren.

BAS2-rapporten hadde hovedfokus rettet mot myndighetens ansvar for å sørge for at Totalforsvaret og samfunnet skal ha tilgang til et robust fundament for telekommunikasjon i et moderne telemarked. Utviklingen har imidlertid ført til at brukerens ansvar for å sikre seg robuste kommunikasjonsløsninger øker, ikke minst fordi det moderne telemarkedet gir brukeren nye valgmuligheter og at brukerutstyret er i ferd med å bli svært komplekst. Som konkrete eksempler på anvendelsesrettede tiltak fra brukernes side, nevner FFI at brukeren selv må sørge for tilstrekkelig nødstrømsforsyning til eget teleutstyr, som telesentraler, datanettkomponenter og annet terminalutstyr. Et annet eksempel er at en sørger for å ha alternative traséer for tilknytning til nærmeste telesentral, det vil si alternative aksessnettforbindelser.

FFI fremhever at stor avhengighet av teletjenester også i fremtiden vil være forbundet med en betydelig grad av risiko, selv med de tiltak som foreslås gjennomført. Det er derfor viktig at man ved utviklingen av organisasjoner minimerer risiko med hensyn til at en eller flere teletjenester kan falle bort i kortere eller lengre tidsrom. Det påpekes at det også er nødvendig å være forberedt på at en slik situasjon kan oppstå, og utvikle beredskapsplaner, alternative rutiner og gjennomføre øvelser.

Teleberedskap i fritt konkurransemarked (TIFKOM)

Samferdselsdepartementet har hatt som målsetting å bruke FFIs utredning som utgangspunkt og underlagsmateriale for å utarbeide en nasjonal strategi for telesikkerhet og -beredskap tilpasset et telemarked i fri konkurranse. For å følge opp FFIs anbefalinger, foreslo derfor Totalforsvarets råd for sikring av tele- og informasjonssystemer (TRSTI), etter oppdrag fra Samferdselsdepartementet, at det burde nedsettes et nytt prosjekt med oppdrag å bearbeide FFIs anbefalinger for å fremskaffe grunnlag for et stortingsfremlegg om telesikkerhet og -beredskap i et telemarked med fri konkurranse.

Det nye prosjektet fikk betegnelsen «Teleberedskap i fritt konkurransemarked» (TIFKOM) og ble opprettet i september 1999, med Post- og teletilsynet som prosjektansvarlig forvaltning. TIFKOM-prosjektet ble utført av en prosjektgruppe bestående hovedsakelig av eksterne konsulenter som har innhentet informasjon om telesikkerhet og -beredskap fra teleoperatørene og berørte statlige myndigheter. I tillegg ble en rekke europeiske land besøkt for å få ideer og forslag til å utvikle norske løsninger innenfor telesikkerhet og -beredskap, samt å fremskaffe sammenligningsgrunnlag for vurdering av de tiltak som foreslås. De landene som ble besøkt var Sverige, Danmark, Finland, Storbritannia, Nederland og Sveits. TIFKOM-prosjektets sluttrapport ble overlevert Samferdselsdepartementet 30. mars 2000, og ble umiddelbart sendt ut på bred høring til alle departementer, teleoperatører, Forsvaret og andre relevante myndigheter.

TIFKOM-rapporten gir innledningsvis en beskrivelse av samfunnets avhengighet av og behov for telekommunikasjon, samt sårbarhet og konsekvenser ved tap av telekommunikasjon. I likhet med BAS2-prosjektet konkluderer TIFKOM-prosjektet med at det er behov for tiltak for å styrke robustheten i de norske telenettene, og prosjektet gir bl.a. anbefaling om hvilket ambisjonsnivå en bør legge seg på for å sikre samfunnet den nødvendige robusthet i de samlede nasjonale telenett. Behovet for ekstra telesikkerhet og -beredskap utover det som finnes i telenettene i dag fremheves. TIFKOM-rapporten omhandler hvilke krav som må stilles til markedsaktørene i alminnelighet, og rapporten identifiserer også særlig behov for sikre telekommunikasjoner knyttet til såkalte prioriterte brukere innenfor Totalforsvaret, som har mer spesielle krav til telesikkerhet og -beredskap enn andre aktører. De konkrete forslagene fra TIFKOM-prosjektet blir omtalt nærmere og vurdert fra kapittel 5 i meldingen og utover.