telenor

Justisdepartementet

Postboks 8005 Dep
0030 Oslo

Vår dato
25.10.2006

Vår referanse
G.R.050.3/15/06/TD

Deres dato
26.06.2006

Deres referanse
200604470-RBA-K/LB/BHH

Vår saksbehandler
Tor-Odd Danielsen

TELENORS HØRINGSSVAR VEDRØRENDE NOU 2006:6 – NÅR SIKKERHETEN ER VIKTIGST

Telenor viser til Justisdepartementets brev av 26.06.2006 angående høring av NOU 2006:6 **Når sikkerheten er viktigst**. Vedlagt følger Telenors kommentarer til Infrastrukturutvalgets rapport.

Infrastrukturutvalget har kommet med en omfattende og detaljert rapport med mange gode forslag for å forbedre sikkerhet og beredskap. Telenor er allerede omfattet av noen av de forslag utvalget kommer med og har dermed erfaring med de tiltak utvalget foreslår. Dette er kommentert under de aktuelle kapitlene. På andre områder stiller vi oss bak det som går igjen i mye av det utvalget foreslår, klare retningslinjer, som gjør virksomhetene i stand til å gjennomføre sikkerhets- og beredskapstiltak til beste for det offentlige, næringslivet og landets befolkning.

Det er overraskende for Telenor at utvalget ikke har behandlet kystradiotjenesten i sin rapport. Det stilles spesifikke internasjonale krav for opprettholdelse av denne tjenesten, og Telenor Maritim Radio har spesielle behov i forhold til andre Ekom-leveranser. Blant annet forutsetter samlokalisering med Forsvaret at Sikkerhetslovens krav må gjøres gjeldende.
Telenor forutsetter at Justisdepartementet tar med vurderinger av kystradiotjenestens behov i den videre behandling av utvalgets rapport.

Telenor oversender herved høringskommentarer til infrastrukturutvalgets rapport.

Med hilsen
for Telenor ASA

Per Pundsnes
Vice President Group Risk

Telenor ASA
Hovedkontor

Kontoradresse:
Snarøyveien 30
1331 Fornebu

Postadresse:
1331 Fornebu

Telefon:
810 77 000
Telefaks:
96212242

Bankgiro:
7058 06 93936

Hovedkontor:
Snarøyveien 30
1331 Fornebu
Organisasjonsnummer:
NO 982 463 718 MVA

Telenors kommentarer til utredningen fra Utvalg for sikring av landets kritiske infrastruktur (Infrastrukturutvalget)

Generelle kommentarer

Utvalget skriver i sammendraget i kapittel 1.:

"Tiltak for å sikre kritiske infrastrukturer og kritiske samfunnsfunksjoner krever derfor grundig behandling og høy prioritet. Offentlige myndigheter må stille tydelige krav, føre effektive tilsyn og sikre god beredskap"

Som utvalget skriver i sin oppsummering er aktørene, som besitter kritisk infrastruktur, avhengig av gode retningslinjer for at de skal kunne tilby og levere tjenester med nødvendig sikkerhet til samfunnskritiske brukere. Utvalget uttrykker bekymring for at bedriftsøkonomiske mål om kostnadseffektivisering kan gå på bekostning av kvalitet på tjenester og innsats for å vedlikeholde den underliggende infrastrukturen. Telenor er opptatt av å drive kostnadseffektivt, men dette skjer ikke ved at kvaliteten og vedlikeholdet på den underliggende infrastrukturen forringes.

Ekomloven
Ekomlovens § 2-10, Sikkerhet og beredskap, stiller generelle krav til tilbydere av elektroniske kommunikasjonsnett og -tjenester om nødvendig sikkerhet for brukerne i fred, krise og krig. Utfordringen for tilbyderne er å identifisere hvilke forventninger samfunnet har og hvor store ressurser aktører i et konkurranseutsatt marked skal bruke på å oppnå "tilstrekkelig" sikkerhet. Telenor har tidligere både overfor sektordepartementet (Samferdselsdepartementet) og tilsynsmyndigheten (Post- og teletilsynet) pekt på at dersom disse bestemmelsene fullt ut skal kunne følges opp, er det nødvendig at en del forhold klargjøres.

Bruker med samfunnskritisk funksjon.
Begrepet "bruker med samfunnskritisk funksjon" slik det er brukt i ekomforskriftens § 8.1 er et av de områdene hvor Telenor har behov for en nærmere presisering og klargjøring for å sikre en god etterlevelse. For det første må det avklares hvem som omfattes av dette begrepet og hvorvidt det er alle tjenester til disse brukerne som er samfunnskritisk eller bare noen.

Telenor registrerer at utvalget har gått inn på denne problemstillingen, når de i kapittel 3 har søkt å identifisere det de kaller kritisk infrastruktur. Dette er gjort ved å utarbeide en definisjon og et sett med retningslinjer. Til sammen har dette lagt til rette for en skjønnsmessig vurdering av hva som er kritisk infrastruktur. For begrepsmessig å konkretisere kritisk infrastruktur, skiller utvalget mellom kritisk infrastruktur og kritiske samfunnsfunksjoner og ut fra dette er det utarbeidet en oversikt over de som utvalget mener faller inn under denne definisjonen.

Samtidig har Telenor registrert at utvalget i sammendraget fra Kap 3 sier :

" *Utvalget understreker at listen over de kritiske infrastrukturene og kritiske samfunnsfunksjonene ikke er ment å være en endelig og objektiv liste. Det er fordi en liste av nødvendighet vil måtte utarbeides med et formål. Formålet med utvalgets liste er å vurdere overordnede virkemidler for å sikre kritisk infrastruktur og samfunnskritiske funksjoner. Listen er derfor av overordnet karakter. Kapittel 3 har også en gjennomgang av sentrale begreper knyttet til beskyttelse av kritisk infrastruktur og kritiske samfunnsfunksjoner."*

Telenor er enig med utvalget i, **og vil sterkt understreke, at en liste som nevnt vil måtte utarbeides med et formål.**

Mens utvalgets liste er av overordnet karakter og skal nyttes til å dekke samfunnets grunnleggende behov og befolkningens trygghet, er begrepet "brukere med samfunnskritisk funksjon" i ekomforskriften knyttet til videreføring av samfunnets funksjonsevne i krise- eller beredskapssituasjoner.

Dette alene tilsier en mer kritisk vurdering av hvem som kommer inn under det begrepet. Samtidig er det nødvendig å vurdere om dette er et entydig formål eller om en må gå videre, og både se på hva en slik liste skal nyttes til helt konkret, og i hvilke typer kriser/beredskapssituasjoner de enkelte brukere er kritiske for videreføring av samfunnets funksjonsevne. Etter Telenors mening vil det eneste funksjonelle være å snakke om ulike typer lister for ulike typer situasjoner/bruksområder. Dette, blant annet, for å få lister som er håndterbare. Det er neppe håndterbart å prioritere alle med samfunnskritiske funksjoner i alle situasjoner. Det er også viktig å ta med seg at en ikke snakker om et statisk område men om noe som er dynamisk. For eksempel vil det være behov for en løpende overvåking og hyppig justering av hvem som i en gitt situasjon skal ha prioritet i telenettet.

Det sentrale spørsmålet da blir hvordan dette skal praktiseres og hvem som avgjør dette.
Etter Telenors mening må det være et myndighetsorgan som har ansvar her.

Vi registrerer at utvalget i Kap. pkt 5.4.1 tillegger Justisdepartementet ansvar for å :
"*Etablere og videreutvikle oversikt over kritisk infrastruktur og kritiske samfunnsfunksjoner i Norge, gjennom en felles metode og system for utpeking og klassifisering av kritisk infrastruktur og kritiske samfunnsfunksjoner* "

Det er meget viktig at en slik metode/et slikt system kommer i stand snarest mulig fordi dette vil være bakgrunn for nødvendige konkrete tiltak.

Telenor er kjent med at DSB og PT, med bakgrunn i dette utvalgets innstilling, har utarbeidet en liste som kan nyttes ved innføring av en ordning med prioritering i mobilnettet. Telenor skal ikke kommentere denne listen nå, men vil komme tilbake til denne i en annen sammenheng. Det må imidlertid understrekes, slik også DSB og PT har gjort, at en slik oversikt/prioriteringsliste må være dynamisk og krever et apparat på myndighetssiden som kan ivareta denne oppgaven.
Samtidig må det påpekes at en slik liste ikke uten videre kan nyttes for andre formål, jamfør det som er sagt foran om behov for lister til ulike formål. Det er derfor en meget vanskelig og krevende oppgave en står overfor. For å løse denne oppgaven trengs det ytterligere avklaring fra myndighetene og et godt og tillitsfullt samarbeide mellom de ulike infrastruktureiere og myndighetene.

Telenor registrerer at utvalget i pkt 5.3.2 kommenterer betydningen av samarbeide på tvers av offentlig og privat sektor og slutter oss til det utvalget her sier. Samtidig er utvalget flere steder også inne på at man snakker om et område hvor det er behov for skjønn og også det slutter Telenor seg til.

På den annen side må ikke dette føre til at en ikke sørger for nødvendig avklaring av de forhold Telenor her omtaler, med den konsekvens det kan ha for en riktig håndtering av ulike krise og beredskapssituasjoner.

Ansvarsforhold
Det er en forutsetning for en effektiv krisehåndtering at alle aktører kjenner sin rolle og sitt ansvar, og at de krav som en står overfor er avklarte.
For ekomsektoren er dette dessuten blitt forsterket av det forslag til endring i Ekomloven som nå er ute på høring. Skulle det nye forslaget om overtredelsesgebyr, straff og tvangsmulkt i Ekomloven bli vedtatt, gjør dette det umulig å leve med bestemmelser som forutsetter stor grad av skjønn både fra tilbyderne og myndighetenes side.
Telenor har derfor et klart behov for å få avklart hvem som er brukere med samfunnskritisk funksjon i de ulike krise og beredskapssituasjonene, samt hvor disse er lokalisert. Brukernes adresse/lokalisering er avgjørende for at Telenor skal kunne peke ut hvilke av våre anlegg i aksessnettet som må sikres prioritet. Dessuten må det avklares hvilket ansvar den som utpekes som bruker med samfunnskritisk funksjon har, samt hvilket ansvar tilbyderne har.

Telenors forslag
Etter Telenors mening må det slås utvetydig fast at det er utpekt myndighetsorgan som klargjør hvem som er bruker med samfunnskritisk funksjon og i hvilke sammenhenger virksomheten er samfunnskritisk. (Det forutsetter selvsagt at involverte virksomheter trekkes inn i denne vurderingsprosessen, jamfør det som er sagt foran om godt og tillitsfullt samarbeide).
I enkelte tilfeller må det også klargjøres hvilke deler av virksomheten som er samfunnskritisk. Spesielt ved prioritering er dette nødvendig fordi ikke alle telekommunikasjonsopplegg for en virksomhet er like samfunnskritiske.
Når myndighetene har klargjort dette må involverte parter varsles, i ekomsektoren for eksempel tilbyderne og brukerne med samfunnskritisk virksomhet.

Selv om elektronisk kommunikasjon er definert som kritisk infrastruktur, vil vi peke på at Telenor og andre tilbydere i det alt vesentlige er underleverandører til aktørene i en krise og beredskapssituasjon. Det må ikke herske noen tvil om at det er de virksomheter som blir utpekt til å ha en samfunnskritisk funksjon som har ansvaret for å sikre at de har trygge og sikre telekommunikasjonsopplegg i en krise og beredskapssituasjon.
Følgelig må det, når myndighetene har utpekt bruker med samfunnskritisk funksjon, være den virksomhet som er utpekt som har ansvaret for å varsle og sikre seg nødvendige leveranser hos sine underleverandører, herunder sin Ekomleverandør.
Utvalget har berørt dette i sin innstilling når det gjelder offentlige virksomheter og vi tillater oss å sitere fra punkt 6.6.4 :

"Etter utvalgets mening bør det derfor være et krav at det ved offentlige innkjøp skal vurderes sikkerhets- og beredskapsmessige konsekvenser ved bortfall av de varer og tjenester som leveres. Det må herunder også stilles krav til sikkerhet og beredskap i forhold til underleverandører."

Tilsvarende krav bør etter Telenors mening også gjelde overfor private virksomheter som utpekes som brukere med samfunnskritisk funksjon.

Dette berøres også i pkt 6.6.1.1 hvor utvalget både sier at underleverandørene ikke må lide urimelig økonomisk tap på bakgrunn av myndighetenes prioriteringer i krisesituasjoner samt i forbindelse med drift og leveransesikkerhet sier at det bør være opp til den enkelte infrastrukturvirksomhet å inngå avtaler med sine underleverandører som sikrer tilgang på kritiske underleveranser under alle forhold også i beredskapssituasjoner.

Krav om ytelser som går ut over det som er standard ytelser fra underleverandøren må også brukerne med samfunnskritisk funksjon betale særskilt for.
Når tilbyderne er varslet av brukerne og det er inngått avtale om hvilke kommunikasjonsløsninger som er samfunnskritiske i de ulike situasjonene og hvilke særskilte ytelser en ønsker å kjøpe, skal tilbyderne registrere dette og ivareta de forpliktelser som følger av avtalen og lov/forskrift.

Vi er innforstått med at etter Ekomloven er det Staten som dekker tilbydernes reelle merkostnader. En avtale om dette er inngått mellom Post og teletilsynet og Telenor. Slik Telenor ser det omfatter den generelle sikkerhetstiltak og spesielle tiltak overfor Totalforsvaret.
Avtalen omfatter ikke leveranser til de private eller andre statlige aktørene som kan bli omfattet av begrepet bruker med samfunnskritisk funksjon. Det er grunn til å anta at flere av disse for hele eller deler av sin virksomhet kan ha behov for særskilte tiltak som ekstra sikring av telekommunikasjonsløsningene eller prioritet i ulike situasjoner.

Etter vår mening er det tvilsomt om det er riktig at Staten ved Post og teletilsynet skal inngå avtale med Telenor eller andre tilbydere om å dekke opp alle disse aktørenes særskilte behov. Mer naturlig er det at det etableres et ordinært kunde/leverandørforhold mellom disse aktørene og deres tilbydere og at eventuelt behov for støtte blir et forhold mellom disse brukerne og myndighetene.
I den sammenheng mener vi det vil være riktig at også disse aktørene må omfattes av utvalgets uttalelse i punkt 10.1.4.3 om økonomiske virkemidler hvor det heter :

"Utvalget mener kjøp av tjenester og tilskudd til spesielle oppgaver for sikring av kritisk infrastruktur vil være et nødvendig virkemiddel sammen med regulatoriske bestemmelser. Det vises i denne sammenheng også til utvalgets forslag om en tilskuddsordning, jf. kapittel 6.6.3."

Kommentarer til enkeltkapitler

Telenors kommentarer til utvalgets anbefalinger knyttet til enkeltkapitlene i rapporten.

Kapittel 5 Ansvar for beskyttelse av kritisk infrastruktur og kritiske samfunnsfunksjoner

5.4.1 Forslag til tydeliggjøring av Justis og politidepartementets rolle
Telenor har en god dialog med både eget sektordepartement og tilsyn med hensyn til sikkerhets- og beredskapssaker relatert til Telenors totalforsvarsansvar. En samling av alle sektorer under et departement vil kunne føre til at fokus på sektorvise sikkerhetstiltak vil bli mindre enn i dag. Dette kan svekke heller enn styrke sikkerheten. En samling av ansvaret for sikkerhet og beredskap for alle sektorer under Justisdepartementet bør derfor vurderes nøye før iverksetting.
Utvalgets forslag til en bedre koordinering av trussel-, risiko- og sårbarhetsinformasjon på tvers av departementene er et godt forslag. Det vil kunne medføre en samordning av kravene til retningslinjer slik at eiere av kritisk infrastruktur får en bedre mulighet til å etablere sikkerhetstiltak som fungerer og tilfredsstiller de forventninger offentlige og private brukere har.

5.4.2 Forslag knyttet til tydeliggjøring av nasjonale mål/akseptnivå
Forslaget til Objektsikkerhetsforskrift, som var ute på høring, adresserte krav til ROS-analyser for virksomheter som besitter samfunnskritisk infrastruktur. Utgivelse av en nøktern objektsikkerhetsforskrift, som også ivaretar private rettssubjekter muligheter til å gjennomføre sikkerhetstiltakene, vil kunne bidra til å ivareta de forslag utvalget har til tydeliggjøring av nasjonale mål og akseptnivå for sikring av samfunnskritisk infrastruktur. Det er her viktig med retningslinjer og krav samtidig som myndighetene ikke pålegger konkurransevridende tiltak utover virksomhetenes kommersielle sikkerhetstiltak.

5.4.4 Forslag knyttet til prinsipper for god sikkerhetskultur
Forskrift om sikkerhetsadministrasjon under Sikkerhetsloven stiller allerede krav om de forslag utvalget knytter til prinsipper om god sikkerhetskultur. Private rettssubjekter som besitter kritisk infrastruktur eller samfunnskritisk funksjon bør derfor vurderes underlagt Sikkerhetsloven.
Det er i den forbindelse meget viktig at dette ikke samtidig påfører virksomhetene ulemper og kostnader som virker konkurransevridende i forhold til nasjonale og internasjonale konkurrenter.

Kapittel 6 Virkemidler

6.6.3 Forslag knyttet til etablering av tilskuddsordning
Telenor har god erfaring med dagens tilskuddsordningen for å ivareta sikkerhets- og beredskapskrav for totalforsvaret. Ordningen er rettet mot gjennomføring av tiltak som ikke er forretningsmessig begrunnet. Dette medfører økt sikkerhet for basistjenester i telenettet og bidrar til økt sikkerhet for alle som benytter elektronisk kommunikasjon da de fleste tilbydere benytter Telenors nett i større eller mindre grad. Erfaringen har vist at det har vært vanskelig å få kunder både fra offentlige og private virksomheter til å dekke kostnader ved sikkerhetsprodukter. Tilskuddsordning kan være et alternativ for at kritiske samfunnsfunksjoner får økt sikkerhet for leveranse av tjenester. Det bør også være et alternativ å kjøpe høyere leveransesikkerhet, eksempelvis prioritet. Her bør myndighetene gå foran og etablere krav som tilsier at de samfunnskritiske virksomhetene må bestille høyere kvalitet og sikkerhet på de tjenestene de behøver slik utvalget anbefaler i kapittel 6.6.4.

6.6.6 Forslag knyttet til samarbeid og informasjonsdeling

Samarbeid og informasjonsdeling på tvers og mellom virksomheter er viktig for å oppnå høy og ensartet sikkerhetsnivå. Det er dog viktig at det ikke blir for mange fora for samarbeid og informasjonsdeling. Det anbefales at JD tar en gjennomgang av allerede eksisterende møteplasser og samordner med andre departementer slik at virksomhetene ikke involveres i et stort antall, men møtes i de riktige fora. Samordning mellom sektorene bør ivaretas av myndighetene og virksomhetene bør samarbeide og utveksle informasjon med aktører med felles utfordringer. Eksempelvis var Totalforsvarets Råd for sikring av tele- og informasjonssystemer (TRSTI) et forum for virksomhetene med totalforsvarsansvar under Samferdselsdepartementet. Det var overraskende for de fleste deltakende virksomheter at det ble nedlagt. TRSTI er ennå ikke senere erstattet av annet relevant forum.

Kapittel 7 Sikkerhetsloven og den forebyggende sikkerhetstjenesten

7.5.1 Forslag knyttet til objektsikkerhet

Sikkerhetsloven skal ligge til grunn for å etablere samt ivareta en forebyggende sikkerhetstjeneste. Telenor er bekymret for Sikkerhetslovens manglende fokusering på sammenhengen mellom sikring av objekter for å beskytte den samfunnsvitale funksjonen objektene representerer, og sikring av informasjon om objektene, deres oppbygning og sammenheng med andre tilsvarende objekter. Dette er informasjon som enkeltvis ikke vil være sikkerhetsgradert, men i sum oppfattes å være sikkerhetsgradert. Tilgangen til systemer som kan være skadelig eller ødeleggende for funksjonaliteten til objektene kan eventuelt benyttes til sabotasje.

En sikkerhetstjeneste som skal ivareta forebyggende innsats for å sikre vitale nasjonale sikkerhetsinteresser, må, som et av flere forebyggende tiltak, ha fokus mot de konsekvensene en insider ville kunne medføre ved å ha tilgang til informasjon eller systemer som kan sette de kritiske samfunnsfunksjonene ut av spill. Vital informasjon kan finnes i ulike/flere ugraderte systemer, men kan i sum utgjøre helhet som kan innebære behov for sikkerhetsgradering. Mulighet for manipulering av vitale funksjoner kan skje gjennom bruk av driftsstøttesystemer som enkeltvis ikke vil inneholde sikkerhetsgradert informasjon, men der konsekvensen av bruk kan føre til stopp i samfunnskritiske systemer.

Grunnet Sikkerhetslovens mangel på krav om beskyttelse av samfunnskritiske funksjoner og de elementer om inngår for å ivareta disse, er det er i dag ikke mulig å foreta sikkerhetsklarering av personale som gis tilganger som nevnt over. Telenor opplever dette som uheldig og som et hinder for å ivareta en helhetlig og forebyggende sikkerhetstjeneste. Ovennevnte objekter og informasjons eller støttesystemer, er gitt solide sikringstiltak for å hindre eller strengt regulere tilganger.
Den manglende faktoren medfører at kontroll med personer som gis tilganger til data-/støttesystemene, som er vitale for objektenes funksjon, ikke kan gjennomføres. Telenor mener derfor at det er nødvendig å gjennomføre personkontroll av personale som gjennom sine systemtilganger kan få mulighet til å utøve ødeleggende aktivitet overfor samfunnskritiske systemer slik at dette vil hindre gjennomføringen av og opprettholdelse av oppgaver tillagt vitale nasjonale sikkerhetsinteresser.
Infrastrukturutvalgets rapport har etter Telenors oppfatning for liten fokus på dette helt sentrale området.

7.5.2 Forslag knyttet til sikkerhetslovens virkeområde

Sikkerhetsloven er et godt verktøy for å opprettholde sikkerhet og beredskap for samfunnskritisk infrastruktur. Etter privatiseringen har Telenor, etter avtale med Samferdselsdepartementet, forholdt seg til sikkerhetslovens krav. For å få dette til å fungere i Telenor, som i stor grad er innrettet på leveranser som normalt ikke berøres av Sikkerhetslovens krav, er det viktig å skille mellom informasjon som omfattes og informasjon som ikke omfattes av Sikkerhetsloven.
Med den graderte informasjonsmengden som behandles i dag mener Telenor at dette fungerer i vår virksomhet.

Kapittel 8 Ivaretakelse av sikkerhets- og beredskapshensyn ved omreguleringer og omorganiseringer

8.5.1 Forslag knyttet til innføring av kontrollpunkter ved omreguleringer og omorganiseringer

Ivaretakelse av sikkerhets og beredskapskrav i forbindelse med privatiseringen og forskjellige omorganiseringer er i Telenor godt ivaretatt.
Kundene forventer høy leveransesikkerhet, konfidensialitet og integritet av informasjonen som formidles i våre nett. En liste over kontrollpunkter, slik utvalget foreslår, er et godt hjelpemiddel, men må alltid tilpasses den virksomhet og de lovpålagte krav som gjelder slik at virksomheten som er berørt får entydige retningslinjer å forholde seg til.

8.5.2 Forslag til å holde sikkerhets- og beredskapsmessige oppgaver som en integrert del av virksomheten

Utvalget har også anbefalt at oppgaver som angår sikkerhets- og beredskapsmessige oppgaver ikke skal løsrives fra den ordinære driften. Dette vil være en vurderingssak, da det ikke uten videre er slik at egne tjenester fungerer bedre enn innkjøpte tjenester. Under forutsetning av at kravene til sikkerhet og beredskap inkluderes i kontrakten med leverandører og følges opp med kontroll og revisjon, vil dette kunne fungere like godt som om dette var en del av den ordinære driften.

Kapittel 9 Offentlig eierskap

I dette kapittelet drøfter utvalget blant annet om offentlig eierskap er en forutsetning for å sikre kritisk infrastruktur. Utvalget har ikke fremsatt nye forslag i kapittel 10 knyttet til offentlig eierskap innenfor sektoren elektronisk kommunikasjon. Telenor anser dette riktig da det etter vår oppfatning ikke er forhold som tilsier at det bør innføres særskilte krav om at det offentlige skal eie hva som er definert som kritisk infrastruktur innenfor ekomsektoren.

Telenor ønsker likevel å kommentere utvalgets generelle vurderinger av offentlig eierskap som virkemiddel for å ivareta sikkerheten i kritisk infrastruktur.

Telenor anser at det er en svakhet ved utredningen i kapittel 9 at utvalget synes å fokusere mye på risikoer ved privat eierskap, mens det er få vurderinger av tilsvarende risikoer ved offentlig eierskap. Telenor kan ikke se at utvalget tilstrekkelig begrunner hva som gjør offentlig eierskap mer egnet til å ivareta sikkerhetshensyn enn privat eierskap. Også ved et offentlig eierskap vil det kunne oppstå risiko for at sikkerheten ikke ivaretas tilstrekkelig. Uten sammenligning for øvrig er det mange eksempler på at offentlig eid infrastruktur av budsjettmessige årsaker ikke har blitt tilstrekkelig vedlikeholdt. Offentlig eierskap er derfor ikke i seg selv en garanti for at sikkerhetshensyn alltid vil bli tilstrekkelig ivaretatt. Etter Telenors oppfatning burde de sikkerhetsmessige risikoer som offentlig eierskap representerer også vært vurdert nærmere.

Utvalget gir under punkt 9.3 uttrykk for en bekymring for at bedriftsøkonomiske mål om kostnadseffektivisering kan gå på bekostning av kvalitet på tjenester og innsats for å vedlikeholde den underliggende infrastrukturen. Telenor er, som andre private aktører, opptatt av å drive kostnadseffektivt. På lang sikt vil det ikke være kostnadseffektivt å forringe kvaliteten og vedlikeholdet av den underliggende infrastruktur. Kostnadseffektivisering innenfor ekomsektoren skjer i det vesentlige gjennom utvikling av nye tjenester og tekniske plattformer samt automatisering av administrative prosesser og støttefunksjoner etc. Det er avgjørende av forretningsmessige grunner at kvalitetsmål til oppetid, feilretting, og kvalitet på tjenester nås. Både privatkunder og bedriftskunder forventer høy kvalitet og oppetid på tjenestene. Dersom det, ut i fra samfunnsmessige beredskaps- og sikkerhetshensyn, er behov for økte sikkerhetstiltak i infrastrukturen utover det som nivået som er etablert for å dekke kunders krav til kvalitet, må dette sikres gjennom at det offentlige tar ansvar for å dekke kostnadene ved slike økte sikkerhetskrav, jfr vårt forslag under generelt.

Telenor er videre ikke enig i utvalgets generelle uttalelser om at "*det offentlige bør eie virksomheter som har ansvar for å legge premissene for de strategiske beslutningene som skal sikre at infrastrukturen blir utviklet, driftet og vedlikeholdt.*" Sikkerhetshensyn både kan og bør ivaretas gjennom regulering. Regulatoriske krav kan da stilles til eiere av kritisk infrastruktur på en slik måte at hensynet til sikkerhet blir ivaretatt når beslutninger om utvikling, drift og vedlikehold fattes. Når dette er sagt må det samtidig gjøres en vurdering av kostnadssiden ved innføring av krav til sikkerhet. Kostbare tiltak for å ivareta offentlige sikkerhetshensyn bør ikke ensidig belastes private aktører.

Utvalget drøfter også spørsmålet om utskilling av kritisk infrastruktur og videre om infrastrukturen i så fall bør være privat eller offentlig eid. Utvalget uttaler at et argument mot vertikalt skille mellom nett og nettbasert tjenesteproduksjon er tap av eventuelle synergieffekter mellom oppstrøms- og nedstrømsvirksomheten. Som utvalget videre peker på er dette fremholdt som et viktig argument mot å skille ut fastnettet som en egen offentlig eller privat eiet virksomhet. Telenor stiller seg fullt ut bak dette argumentet. Telenor kan ikke se at det foreligger verken sikkerhetsmessige eller konkurranserettslige hensyn som taler for en utskilling. Sikkerhetsmessige aspekter kan og blir, utover det som følger av forretningsmessige grunner, ivaretatt gjennom offentlig regulering. Videre er konkurransehensyn fullt ivaretatt gjennom den særskilte konkurranseregulering under Ekomlovgivningen samt den generelle konkurranselovgivningen.
Utskilling av faste telekommunikasjonsnett ville også fått store konsekvenser på kostnadssiden. I en vurdering fra OECD[1] som riktignok tar for seg utskilling av det faste aksessnettet (local loop) konkluderer OECD i rapporten side 32 med følgende:

> *Vertical separation is a significant intervention in the marketplace, with substantial and – unlike behavioural regulation, which can be reversed – irreversible costs. It should not be undertaken lightly. Seeming simple in concept, structural separation of the local loop is in practice complex with uncertain outcomes and many questions to be answered. The benefits of structural separation of the local loop are uncertain while the costs are certain and appear potentially large. There is little evidence that the benefits of structural separation of the local loop are sufficiently in excess of costs. Accordingly, it would seem more sensible to persevere with the current regulatory approach (with appropriate improvements and argumented by sanctions). Only if regulatory authorities cannot show that the benefits are in excess of the*

[1] *The benefits and costs of structural separation of the local loop*, DSTI/ICCP/TISP(2002)13/FINAL, 3. Nov 03.

costs, and that alternative regulatory approaches would not work, should consideration be given to the structural separation of the local loop.

Telenor støtter konklusjonen fra OECD. Selv om OECD her har vurdert utskilling av det faste aksessnettet og utvalget primært behandler spørsmålet om utskilling av Telenors stamnett, legger Telenor til grunn at de samme hensyn mot utskilling gjør seg gjeldende for stamnettet.

Kapittel 10 Kartlegging av kritisk infrastruktur og sektorvise anbefalinger

10.1.1 Overordnet beskrivelse av infrastruktur og samfunnsfunksjon

Prinsippskissen og den overordnede beskrivelsen av nettet er ikke prinsipielt feil men det blir misvisende at det kan forstås slik at radiolinje og kabel er likestilt i Transportnettet. Det alt overveiende av trafikken går i kabel.

Drifts- og støttesystemene

Utvalget hevder at etter hvert som operatører vokser i markedet, vil ønsket om å redusere kostnader ved driftsfunksjonene kanskje medføre en utvikling med sentralisering av drifts- og støttesystemer. Videre at det vil være en potensiell fare for at operatørens evne til å opprettholde tilgjengeligheten ved større feil- eller krisesituasjoner svekkes. Telenor mener at ønsket om sentralisering og reduksjon av kostnader ofte er større hos mindre leverandører i markedet og at det derved ikke har noe med størrelse å gjøre.

Vedrørende nasjonal autonomi

Ekomforskriftens §8-3 krever at tilbyder som leverer nødvendige kommunikasjonstjenester til bruker med samfunnskritisk funksjon eller leverer overføringskapasitet og samtrafikk til tilbyder som omfattes av ovennevnte, skal opprettholde nødvendig tjenestetilbud for disse uten driftsstøtte og elektroniske kommunikasjonstjenester lokalisert i andre land. Post- og teletilsynet kan i krise- og beredskapssituasjon pålegge tilbyder å utføre drift og vedlikehold av tjenestetilbudet med personell og tekniske løsninger som er lokalisert på norsk territorium. Det er sagt at dette trer i kraft når departementet bestemmer.

Et slikt krav vil kunne legge hindringer i veien for en effektiv drift av nett og tjenester og medføre økte kostnader for de som omfattes av dette – og dermed både konkurransevridning og dyrere teletjenester. Telenor støtter derfor utvalgets forslag om at kravet om autonom drift – slik det er utformet i forskriften, frafalles. Telenor tar det for gitt at kostnadene for eventuelle nasjonale reserveløsninger fullt ut dekkes av staten.

Forslag knyttet til regulering av brukere av Internett

Begrepet "sikkerhetsprogramvare" er lite definert og upresist. Slik programvare kan være virusbeskyttelse, spambeskyttelse, brannmur, sikkerhetstiltak rettet mot barn osv.
Det kan være klienter som installeres på en PC med Internettaksess, men også programvare for mobiltelefoner. Annen forbrukerelektronikk benytter også internettprotokoller, eksempelvis spillkonsoller, SetTop-bokser, PDAer, kameraer, komfyrer, etc.
Begrepene "tilfredsstillende sikkerhetsinnstillinger og gode veiledninger" vil være gjenstand for like mange tolkninger som det finnes utstyrsleverandører. En mer spesifikk tilnærming vil imidlertid være en uoverkommelig oppgave for et statlig organ, og vil i tillegg være et mål som kontinuerlig

endrer seg. I beste fall kan dette uttrykkes til en norm for bransjen, ikke et pålegg. Vil dette medføre at usikrede trådløse aksesspunkt vil være å regne som ulovlige?

"Oppdatert sikkerhetsprogramvare" er et upresist begrep. Oppkobling til Internett er i dag mulig fra et stort antall typer forbrukerelektronikk. Oppdatert programvare blir uten mening i denne sammenhengen - flere av apparatene har ikke et grensesnitt der slik oppdatering er mulig.
Å oppdatere sikkerhetsprogramvaren krever faktisk Internettoppkobling.
Sikkerhetsprogramvare for PC skjuler i sin natur sin identitet - nettopp for å ikke selv kompromitteres av trusler. I beste fall kan Internett Service Providere kontrollere at sikkerhetsprogramvare som er formidlet fra dem er installert (og kanskje oppdatert), men en konsekvens av det vil være at sluttbruker ikke fritt kan velge sikkerhetsprogramvare. Mangfoldet av apparater som benytter Internett er et problem. Det finnes f. eks ikke mulighet for den jevne bruker til å installere sikkerhetsprogramvare på et stereoanlegg.
I stedet for at Internettleverandøren skal kontrollere og verifisere alle klienter før tilgang gis, bør leverandører være pliktig til å koble fra eller stoppe skadelig trafikk etter de blir varslet eller har funnet ut at en av deres kunder/klienter blir misbrukt eller misbruker sitt abonnement. Kontroll av enkeltklienter er tilnærmet umulig i de fleste tilfeller, da det kan være mange klienter bak en internettforbindelse. Det vil være bedre å gi leverandører tilgang/pålegg om å sette ut utstyr som detekterer usikrede maskiner ut i fra trafikken som går på nettet, enn å gi leverandøren tilgang til å gå igjennom alle data som ligger på kundenes maskiner/klienter.

Tjenester, formater og enheter som brukes på Internett styres av et internasjonalt marked og man vil ikke klare å la en offentlig instans i Norge lage oppdaterte regler og disse vil heller ikke bli mulig å håndheve. Til tross for at bruken av Internett har blitt stadig viktigere for vitale samfunnsfunksjoner (bl.a. innenfor helsevesenet), er Internett fortsatt en ikke-prioritert ekomtjeneste.

Forslag knyttet til organiseringen av IT-sikkerhetsarbeidet
Telenor støtter utvalgets forslag om å legge det overordnede ansvaret for IT-sikkerhet til ett departement. I dag er det for mange departementer involvert. Slik utvalget beskriver i kapittel 10 er koordineringsansvaret delt mellom Justis- og politidepartementet, Forsvarsdepartementet, Moderniseringsdepartementet og Samferdselsdepartementet. Ansvaret er delt mellom disse ut fra fagansvar i medhold av lov- og forskriftsverk samt kongelige resolusjoner. Dette blir veldig uryddig for aktørene i bransjen.

Vedrørende kraft
Kraft er en kritisk ressurs også for en Ekomtilbyder. Det er dermed helt essensielt at vi har en stabil kraftforsyning. Utviklingen på dette området de senere år skaper bekymring. Vi opplever oftere og oftere at vi står ovenfor en trussel om at det kan bli rasjonering/kraftutkopling.
Samtidig registrerer vi at kraftleverandørene har begrensede muligheter til å foreta en selektiv kraftforsyning. Kraftnettene har ikke den fleksibiliteten som er ønskelig for å kunne få en samfunnsmessig optimal utnyttelse av knappe kraftressurser. Nettselskapene bør ved rehabilitering og utbygging pålegges å legge til rette for bedre selektivitet i nettene.
I likehet med at staten dekker reserveløsninger for drift av telenett/-tjenester bør også staten dekke merkostnadene som nettselskapene får ved et slikt krav.

Forslag knyttet til strømrasjonering
Telenor støtter utvalgets presisering av at kraftbransjens distribusjonsnett må tilpasses slik at reell prioritering overfor samfunnsvitale enkeltbrukere lar seg gjennomføre.

Når det gjelder bruken av reserveaggregater er det viktig å skille mellom bruk av slike ressurser under normalsituasjon i krafttilgangene, og når kraftbransjen har behov for å gjennomføre rasjoneringstiltak. Anlegg som er utrustet med reserveaggregater kombinert med batterireserve, vil normalt ha mindre/"liten" driftskapasitet på batterireserven som følge at reserveaggregatet i hovedsak vil ivareta kraftbehovene hvis nettkraften skulle falle bort. Reserveaggregater er som regel kun installert i samfunnsvitale teleanlegg. Hvis det oppstår teknisk feil med påfølgende stopp i aggregatet i løpet av perioden med manglende nettkraft, vil utladningstiden på batterireserven kombinert med alarm normalt føre til at reparasjonstiltak blir iverksatt før den kraftbrukende funksjonen stopper opp. Teknisk feil og stopp i aggregat samtidig med pågående kraftrasjonering, der påtrykket mot driftsressurser i området vil være svært høyt, kan føre til at den kraftbrukende funksjonen stopper opp som følge at reparasjonstiltak ikke lot seg iverksette i tide.

Løsningen på problemstillingen er at nettkraft fortsatt fremføres til den vitale virksomheten, uten at nettkraften brukes. Kraftbehovet ivaretas gjennom reserveaggregat. Hvis det eventuelt skulle oppstå stopp i aggregatet, vil den vitale virksomheten kunne benytte den nettbaserte kraften, og slik sikre opprettholdav den samfunnsvitale funksjonen.

Telenor støtter utvalgets oppfordring til myndighetene om å arbeide videre med løsninger som kan ivareta levering av elektrisk kraft til prioriterte brukere ved rasjonering. Telenettet er i stor grad sikret med aggregater. I aksessnettet nærmest kundene vil det dog alltid være mangler som fører til brudd i leveransene ved lengre eller mer omfattende bortfall av nettkraft.

Kapittel 11 Kartlegging av kritiske samfunnsfunksjoner og sektorvise anbefalinger

11.6 Forslag knyttet til kriseledelsesapparatet

Telenor stiller seg bak utvalgets forslag knyttet til kriseledelsesapparatet. Spesielt fokus bør settes på tidsmessige og funksjonelle samband og involvering av eiere av samfunnskritisk infrastruktur i regelmessige øvelser for å finne og korrigere svakheter.

11.6.2.5 Forslag knyttet til varsling av befolkningen

Telenor vil presisere at i tillegg til at NRK P1 er utpekt som beredskapskanal som formidler av myndighetenes informasjon ved nasjonale kriser og katastrofer, så er RDS i P1 (med P2 som redundans) **bæreren** av styringen av tyfonanleggene.

Ved opprettelsen av Norkring ble NRKs beredskapsansvar redusert til kontribusjon av informasjon og produksjon av program. Norkring har overtatt ansvaret for distribusjonen.
Beredskapssamarbeidet mellom NRK og Norkring er nedfelt i en egen beredskapsavtale som regulerer forholdet mellom NRK og Norkring i forbindelse med planlegging og gjennomføring av tiltak for å sikre at informasjon når befolkningen under krise- eller katastrofesituasjoner i fredstid, og ved sikkerhetspolitiske kriser, beredskap og i krig.

Korreksjon vedr. DAB (Digtal Audio Broadcasting):
"...I løpet av 2006 skal det nye bakkenettet dekke 80 % av landet..."
Skal være: ...I løpet av 2007 skal det nye bakkenettet dekke 80 % av landet...