Nærings- og handelsdepartementet

Samfunnets sårbarhet som følge av avhengighet til IT

Oktober 2000

Forord

Styringsgruppen for IT-sårbarhetsprosjektet legger med dette frem hovedrapporten fra prosjektet. Prosjektet har basert seg på eksisterende materiale fra etatene som er innhentet gjennom departementene og deres representanter i styringsgruppen. Vurderinger av sårbarheten for de ulike kritiske funksjonene er foretatt av etatene som har ansvar for de respektive funksjonene og av etatenes fagdepartementer.

Styringsgruppen tenker seg at oppfølging av den helhetlige strategien skjer i regi av Nærings- og handelsdepartementet, mens den sektorvise oppfølgingen skjer i regi av fagdepartementene. Utredning av økonomiske og administrative konsekvenser må skje i forbindelse med konkretisering og oppfølging av rapportens forslag til tiltak.

Oslo 30. oktober 2000

1. Innledning

Informasjons- og kommunikasjonsteknologien (IKT) har gitt mennesket store muligheter, gitt økonomisk vekst og nye kanaler for formidling av informasjon. Produksjon av varer og tjenester har blitt enklere, noe som igjen har ført til økt tilbud.

Teknologiutviklingen kan også medføre ulemper. Dagens økonomi og samfunn er blitt helt avhengig av denne teknologien. Teknologien er blitt en integrert del av systemene vi omgir oss med og som er med på å sikre vår velferd. Omfattende svikt i IKT-systemer og infrastruktur kan nå forstyrre vitale samfunnsfunksjoner på en måte som få av oss kan forutse. Selv enkel svikt i IKT-systemer kan føre til omfattende svikt innen viktige sektorer som energiforsyning, telekommunikasjon, drivstofforsyning, helse, betalingsformidling, næringsliv og nasjonens forsvar.

Det er derfor en samfunnsoppgave å tilstrebe at vi har den innsikt og handlekraft som må til for å oppnå mest mulig av godene og minst mulig av ulempene ved denne utviklingen.

1.1. Bakgrunn

Det har de senere år både nasjonalt og internasjonalt blitt satt et stadig økende fokus på samfunnets sårbarhet som følge av teknologiutviklingen. Flere land i den vestlige verden er nå i gang med å gjennomføre nasjonale tiltak innen området som følge av nasjonale analyser. USA er ett eksempel, der det i 1997 ble offentliggjort et arbeide ”Critical Foundations – Protecting Americas Infrastructures”, der samfunnets sårbarhet ble vurdert å være stor. Land som Sveits og Sverige har også kommet et godt stykke på vei.

I 1998 tok Statssekretærutvalget for IT (SSIT) initiativ til et underutvalg som skulle lage en rapport om status for IT-sårbarhetsarbeidet i Norge. Et resultat av dette arbeidet var at det i 1999 ble igangsatt et IT-sårbarhetsprosjekt for å studere området grundigere.

Som følge av en rekke funn og indikasjoner både nasjonalt og internasjonalt, som alle tydet på en utvikling mot økt samfunnssårbarhet, ble det også i 1999 etablert et offentlig utvalg – Sårbarhetsutvalget. Oppgaven til dette utvalget var å studere samfunnets sårbarhet i et bredt perspektiv. Arbeidet med IT-sårbarhetsprosjektet er koordineret med Sårbarhetsutvalgets arbeid innenfor området IKT-sårbarhet.

I Sårbarhetsutvalgets NOU (2000:24) - ”Et sårbart samfunn”, som ble avgitt 4. juli 2000, er det klart uttrykt behov for tiltak for å redusere sårbarheten i samfunnet. Det er også lagt stor vekt på betydningen av IKT-sårbarhet for samfunnets sårbarhet, og utvalget foreslår en nasjonal strategi med et antall tiltak for å redusere denne sårbarheten.

I henhold til mandatet ble en ”Underveisrapport” fra prosjektet oversendt Sårbarhetsutvalget 1. april 2000. ”Underveisrapporten” og Sårbarhetsutvalgets NOU danner utgangspunkt for den strategi og de tiltak som foreslås av IT-sårbarhetsprosjektet, og som er beskrevet i denne rapporten.

1.2. Mandatet

IT-sårbarhetsprosjektet ble igangsatt i november 1999 og organisert med en styringsgruppe og en prosjektgruppe. Regjeringen ga styringsgruppen følgende mandat:

1. Styringsgruppen har i oppgave å lede prosjektet med ansvar for fremdrift, faglig innhold og anbefalinger.
2. Det gjøres en gjennomgang av aktuelle samfunnssektorer for å identifisere kritisk infrastruktur der IT i særlig grad er tatt i bruk, og for å gi et samlet trusselbilde.
3. Samfunnskritiske funksjoners og virksomheters sårbarhet for svikt i IT-systemer skal kartlegges.
4. Behovet for risiko- og sårbarhetsanalyser ut fra et IT-perspektiv og øvrige utredningsbehov skal identifiseres.
5. Det skal utarbeides en overordnet strategi for arbeidet med sårbarhet og IT: Strategien skal bl.a inneholde informasjon og debattskapende tiltak og partnerskap mellom offentlige og private aktører. Erfaringene fra arbeidet med år 2000 gir et grunnlag man kan bygge videre på i strategiarbeidet.
6. Prosjektet skal foreslå konkrete tiltak for å redusere samfunnets IT-sårbarhet.
7. Prosjektet skal etablere kontakt og samarbeid med Sårbarhetsutvalget ledet av Kåre Willoch, og det regjeringsoppnevnte forsvarspolitiske utvalg (FPU).
8. Styringsgruppen avgir endelig rapport med forslag til strategi og tiltak, og sluttfører prosjektet innen 1. oktober 2000. Det skal gis innspill til Sårbarhetsutvalget vedrørende skisse til strategi, IKT-kritisk infrastruktur og preliminær trusselvurdering innen 1. april 2000. Innen 1. oktober 2000 sluttfører styringsgruppen sitt arbeid med IT-sårbarhetsprosjektet og avgir endelig rapport.

Styringsgruppen ble sammensatt med følgende departementsrepresentanter:

- Rolf Borgerud, Arbeids- og administrasjonsdepartementet
- Alfred Ehrenclou, Sosial- og helsedepartementet
- Kjell G. Skar, Samferdselsdepartementet
- Karianne Skar Sørdahl, Samferdselsdepartementet
- Sven Lilleby, Forsvarsdepartementet
- Jørgen Dyrhaug, Forsvarsdepartementet
- Torgeir Jonvik, Finansdepartementet
- Berit Hjelstuen, Olje- og energidepartementet
- Roger Sundkjer, Olje- og energidepartementet
- Jens Nyhagen, Justisdepartementet
- Christian Baklund, Justisdepartementet
- Bjørn Tørmo, Nærings- og handelsdepartementet
- Eivind Jahren, Nærings- og handelsdepartementet (leder)

Prosjektgruppen ble forankret i Nærings- og handelsdepartementet og har bestått av:

- Vigdis Olsen, Nærings- og handelsdepartementet (prosjektleder fra prosjektets oppstart til 1. juli 2000)
- Steinar Roppen Olsen, Nærings- og handelsdepartementet (fra prosjektets oppstart til 1. mai 2000)
- Kjell Olav Nystuen, Forsvarets forskningsinstitutt (prosjektleder fra 1. juli 2000 til 30. oktober 2000)

Denne rapporten utgjør IT-sårbarhetsprosjektets sluttrapport. En kortversjon inngår som vedlegg til hovedrapporten. Kortversjonen vil bli oversatt til engelsk, og vil også bli distribuert separat.

1.3. Begrepsavklaring

Sårbarhet: Begrepet sårbarhet betegner en egenskap ved funksjoners utforming, gjennomføring eller drift, som gjør funksjonene følsomme overfor ødeleggelse eller å bli gjort funksjonsudyktige som følge av en trussel.

IKT-sårbarhet: Egenskap ved funksjoner som gjør dem følsomme overfor ødeleggelse eller å bli gjort funksjonsudyktige som følge av en trussel som rammer funksjonenes IT-systemer.

Trussel: En trussel mot et system er et sett med mulige utfordringer som kan føre til svikt i systemet. Disse utfordringene kan ha utgangspunkt i mennesker ondsinnethet, eller være av tilfeldig naturlig art. Den førstnevnte kategorien vil være en kombinasjon av angriperens mulige *intensjon* for en handling, og den *kapasitet* vedkommende måtte inneha for å kunne gjennomføre handlingen.

Risiko: Risiko er vanligvis definert som en kombinasjon av sannsynligheten for at en hendelse skal inntreffe, og konsekvensen av den svikt som oppstår, det vil si skadeomfanget av hendelsen[1].

IKT-avhengighet: En beskrivelse/beregning av i hvilken grad et gitt system er avhengig av IKT-systemer.

Risiko- og sårbarhetsanalyse (ROS): En systematisk fremgangsmåte for å utlede potensielt tap gjennom en kartlegging av mulige uønskede hendelser og skadeomfanget av disse. Her inngår anslag eller beregning av sannsynligheten for at en uønsket hendelse skal inntreffe, og beregning eller anslag av hva som blir konsekvensen av hendelsen[2].

1.4. Rapportens struktur

Den resterende delen av rapporten har følgende struktur:

I kapittel 2 beskrives den teknologiske utviklingen med hensyn til sårbarhet, utvikling innen ulike trusseltyper og en vurdering av den generelle risiko som resultat av denne utviklingen.

I kapittel 3 presenteres et utvalg samfunnssektorer, der det er gitt en kvalitativ beskrivelse av funksjonenes avhengighet av IKT og vurderinger av den sårbarhet og risiko dette medfører for den enkelte sektoren.

I kapittel 4 gis det en kort vurdering av hver enkelt samfunnssektors sårbarhet og risiko som følge av avhengighet til IKT, med en etterfølgende samlet vurdering.

[1] Dersom en skal ta med i betraktningen svært sjeldne eller usikre trusseltyper er det nødvendig å definere nærmere hva som menes med sannsynlighet.
[2] I de fleste tilfeller der begrepet *analyse* benyttes i denne rapporten er begrepet *vurdering* mer formelt korrekt. Siden ordet *analyse* likevel er i bred anvendelse i det norske samfunnet velges det likevel å bruke dette.

Som en følge av konklusjonene fra kapittel 2 og 4 beskrives det i kapittel 5 en nasjonal strategi med tilhørende tiltak for sikring av IKT-systemer.

I kapittel 6 behandles noen faktorer knyttet til denne strategien og nasjonal beredskap.

En kortversjon av rapporten er lagt inn som vedlegg.

1.5. Sammendrag

Under følger et kort punktvis sammendrag av de viktigste faktorene som er beskrevet i rapporten. Denne er inndelt i en *situasjonsbeskrivelse,* som er hentet fra rapportens kapittel 1 – 4, og *strategi og tiltak,* som er hentet fra rapportens kapittel 5.

Situasjonsbeskrivelse

- Samfunnet og økonomien er blitt svært avhengig av IKT-systemer for produksjon av viktige varer og tjenester.
- Telekommunikasjon og kraftforsyning utgjør infrastrukturer der IKT-systemer er viktig for intern tjenesteproduksjon, samtidig som at tjenestene de produserer er nødvendig for at alle andre IKT-systemer skal fungere. Infrastrukturene er sårbare overfor en rekke typer trusler.
- Trusselbildet er i endring – nye mulige aktører kan inneha nye typer virkemidler som er spesielt effektive mot IKT-systemer. Det hersker imidlertid stor usikkerhet rundt *mulige* fremtidige trusler mot samfunnet.
- Systemenes innebygde kompleksitet er i seg selv også blitt en økende trussel.
- Faktorer som på negativ eller positiv måte påvirker sårbarhet:
  – Liberalisering og privatisering av viktige samfunnsinfrastrukturer.
  – Rask teknologisk utvikling – funksjonalitet går ofte foran sikkerhet.
  – Viktige IKT-systemer er tilknyttet globale nettverk, og utsettes derigjennom for nye typer trusler fra mange flere aktører.
  – Sterk sentralisering av viktige IKT-systemkomponenter og nettverksknutepunkt.
  – Sentralisering og outsourcing[3] av driftsfunksjoner.
  – Monopoltendenser innen programvare.

Strategi og tiltak

- Forslag til målsetning for arbeid med IKT-sårbarhet:
  ”Å etablere robusthet IKT-infrastruktur på et nivå som gjør det lite sannsynlig at viktige samfunnsfunksjoner stanses i en normalsituasjon. I en krise- eller krigssituasjon skal robustheten være tilstrekkelig til å opprettholde kritiske funksjoner.”
- Forslag til strategi for å redusere samfunnets sårbarhet:
  – Partnerskap mellom private virksomheter og offentlige myndigheter.
  – Fremme informasjonsutveksling mellom ulike typer samfunnsaktører.
  – Øke varslingsevnen.
  – Utdanning og kompetanseutvikling.
  – Forskning og utvikling.
  – Tilpassing av lover og regler.

[3] Sette bort driften av deler av virksomheten til andre virksomheter (maskiner og tjenester). Disse virksomhetene er ofte spesialister innen sitt område.

  – Statlig ansvar for å sikre infrastrukturtjenester fra telekommunikasjon og kraftforsyning.
- Forslag til tiltak i henhold til strategien:
  – Opprettelse av et Senter for Informasjonssikring (SIS) med operative og analytiske oppgaver innen IKT-sikring.
  – Styrket innsats innen forskning og utvikling.
  – Styrking av utdanning og kompetanseutvikling.
  – Arbeide for økt anvendelse av og utvikling av egnede metoder for risiko og sårbarhetsanalyser innen IKT-infrastruktur.
  – Brukerrettede tiltak.
  – Harmonisering og tilpassing av lovverk innen kriminalitetsbekjempelse.
- Strategi og tiltak bygger på en forutsetning om at staten tar ansvar for sårbarhetsreduserende tiltak innen telekommunikasjon og kraftforsyning.

2. Utvikling innen trusler og teknologi

2.1. Teknologi og teknologianvendelse

IT-sikkerhet og sårbarhet har kommet sterkere i fokus som følge av blant annet økning i systemenes kompleksitet og i antallet mulige trusler mot systemene. Tilgangen til det verdensomspennende Internettet er en sentral faktor i dette bildet. Behovet for elektronisk informasjonsutveksling er sterkt økende og dermed også behovet for sammenknytting i store nettverk. Flere virksomheter har tilsynelatende egne lukkede nett for kritisk informasjonsbehandling, men ofte viser det seg likevel at disse også har en knytning til eksterne nett slik at inntrengere kan benytte bakveier inn til systemene. Internasjonal handel og behovet for kommunikasjon gjennom åpne nett vil fortsatt utvikle seg sterkt. Dagens Internett er sårbart.

En utvikling mot konvergens mellom kringkasting, tele, tradisjonell IT og elektronisk handel vil ytterligere øke anvendelsesområdet for tjenestene, og vil dermed igjen skape et økt behov for sikring av systemene og informasjonen som flyter i disse. Det er til en viss grad utviklet metoder og teknikker for å skape sikrere systemer, men teknologiutviklingen gir også nye muligheter for kriminelle og andre som vil gjøre skade. Med dagens teknologi er det et klart motsetningsforhold mellom den sikkerhet som kan oppnås i et system, og brukernes ønske og behov for funksjonalitet. Sikkerhet i programvare og systemer må derfor alltid avveies i forhold til kostnader og funksjonalitet. Kompetanse er en viktig faktor.

2.2. Utfordringer mot IT-samfunnet

Samfunnet står i dag overfor et helt annet trusselbilde enn for få år siden. Dette gjelder både på den sivile og den militære delen av arenaen.

På den sikkerhetspolitiske arena har muren mellom øst og vest falt, og det er *i dag* vanskelig å konstruere noen *sannsynlig* nasjonalstatlig fiende mot Norge. Det betyr imidlertid ikke at det i fremtiden ikke vil finnes *mulige* fiender. Derfor vil Norge også i årene fremover bruke store beløp på å utvikle det militære forsvaret, selv om dette antagelig vil få en annen innretning enn under den kalde krigen.

Samfunnet har gjennom de senere årene også gjennomgått store endringer på andre felt. Det er i stor utstrekning tatt i bruk ulike former for teknologi for å bygge opp om velferd og velstandsøkning. Informasjons- og kommunikasjonsteknologi (IKT) utgjør en sentral teknologi i dette bildet. Utviklingen er nå kommet så langt at samfunnet og økonomien er blitt avhengig av teknologien for å kunne fungere, en utvikling som synes å fortsette. Produksjonen av de fleste varer og tjenester er i dag på en eller annen måte avhengig av IKT-systemer. Dette kan enten være som del av selve produksjonsprosessen eller som del av et omkringliggende driftsapparat for å gjøre varen eller tjenesten tilgjengelig for brukeren. Dersom disse IKT-systemene blir utsatt for forstyrrende hendelser vil dette raskt kunne få konsekvenser for leveransen av varene eller tjenestene til forbrukerne. Dersom en snur denne problemstillingen, og ser det hele fra en mulig angripers side, er IKT-systemene også blitt en våpenplattform for angrep mot samfunnet!

Den klare avhengigheten av teknologi har gjort samfunnet mer sårbart fordi det er blitt mulig å ramme samfunnet med enklere virkemidler enn tidligere. Nå er det ikke lenger bare nasjonalstater og store ressursrike organisasjoner som kan inneha en slik kapasitet. Mulige aktører i dag og i fremtiden dekker et mye videre spenn enn tidligere, fra enkeltindividene til nasjonalstatene. En finner i dag en rekke eksempler der selv enkeltindivider har vært i stand til å trenge seg inn i vitale IKT-systemer for samfunnet. Ett eksempel på dette er en 14-åring som fra gutterommet var i stand til å ta kontroll med damluker i et kraftforsyningsanlegg i Canada[4]. En har imidlertid så langt ikke kunne påvise at terrororganisasjoner eller nasjonalstater har stått bak massive strukturerte angrep, selv om det blir hevdet at slike angrep til en viss utstrekning blant annet har vært benyttet i Kosovokonflikten i 1999[5]. Det er også kjent at enkelte terrororganisasjoner i begrenset omfang har benyttet trusler, og også gjennomført enkle former for informasjonsangrep mot stater. Det sårbare samfunnet gjør det også enklere for kriminelle enkeltindivider og organisasjoner å nå frem til sine mål i ren vinnings hensikt.

En finner også en økte anvendelse og avhengighet av IKT-systemer på militær side. Dette har ført til at såkalte informasjonsoperasjoner i økende grad kommer inn som viktig del av de fleste nasjoners forsvarskonsepter. Det innebærer at det bygges opp militær kapasitet for både angrep mot og forsvar av militære og sivile informasjonsinfrastrukturer.

Også IKT-systemenes økende innebygde kompleksitet utgjør i seg selv en betydelig trussel. Systemene er nå så sammensatt at det ofte vil være ”umulig” å holde oversikt over strukturene i disse. De vil dekke store geografiske områder – gjerne hele verden, og de vil kunne spenne over mange virksomhetsområder. Enkle tekniske feil eller ytre påvirkninger fra natur eller individer vil kunne sette igang kjedevirkninger som ikke er forutsett. Svikt som følge av selv enkle tekniske feil eller feiloperasjoner fra mennesker kan raskt bli omfattende og fatale. Dette kan bli enda mer alvorlig dersom den initierende hendelsen kommer fra en kalkulerende fiende. På den annen side kan denne kompleksiteten også gjøre det vanskeligere for en angriper å være sikker på å nå sitt mål. Usikkerhet som følge av denne kompleksiteten utgjør uansett et alvorlig problem nettopp fordi systemoversikt er en klar forutsetning for å oppnå sikre systemer.

2.3. Trusler og virkemidler mot samfunnets IKT-systemer

Hendelser som forårsaker svikt i et IKT-system kan ha utspring i ulike årsaker. En skiller gjerne mellom villede og tilfeldige ikke-villede hendelser. Eksempler på årsak til tilfeldige hendelser kan være tekniske feil eller ødeleggelser som følge av en naturlig hendelse, for eksempel fra et uvær. Også menneskers feiloperasjoner av IKT-systemer inngår i denne kategorien. Slike hendelser vil stadig skje. Normalt vil en i utviklingen av IKT-systemene ta høyde for de fleste av disse typene hendelser ut fra et risikosynspunkt.

Villede hendelser er derimot hendelser som har sin årsak i menneskers vilje til å forårsake problemer. Motivet og kapasiteten til de som står bak vil være forskjellig, og vil kunne befinne seg i et spenn fra rene guttestreker til velstrukturerte og omfattende angrep fra høyt kompetente grupper av individer. I den første delen av dette spennet vil en i hovedsak finne

[4] Hagen/Nystuen, Forsvarets forskningsinstitutt (2000): ”Beskyttelse av kritisk infrastruktur – Besøk ved private og offentlige virksomheter i Canada og USA 31 januar – 4 februar 2000, FFI/REISERAPPORT-2000/01096.
[5] Grunnan T, Forsvarets forskningsinstitutt (2000): ”Deltagelse på konferansen ”Information Warfare Post Y2k: A National Security Perspective” i Washington DC”, 11-12 mai 2000, FFI/REISERAPPORT-2000/03881.

angrep som rammer tilfeldig mot den enkelte infrastruktur, mens en mot den andre ytterligheten vil finne angrep som rammer et på forhånd bestemt mål med høy presisjon og sikkerhet.

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 ikke nødvendigvis var tilsiktet. En slik kjedereaksjon kan innbefatte ulike former for teknisk svikt og feiloperasjon.

Sikker funksjon i et IKT-system er avhengig av følgende tre basisegenskaper:
- *Integritet* – at systemet er sikret mot manipulering med systemets funksjon og datainnhold.
- *Tilgjengelighet* – at systemet er sikret mot avbrudd i sin forventede funksjon og at systemet har tilgang til nødvendig datainnhold.
- *Konfidensialitet* – at systemets funksjon og datainnhold er sikret mot innsyn.

Tilfeldig svikt eller et villet angrep mot informasjonen innen en infrastruktur vil bestå av et sett med virkemidler rettet mot en eller flere av disse egenskapene.

IKT-systemene som står bak den enkelte infrastrukturens vare- eller tjenesteproduksjon vil være svært følsom overfor angrep rettet mot informasjonens integritet. Gjennom et integritetsangrep vil en angriper kunne manipulere informasjon knyttet til styring og kontroll med produksjonsprosesser. Ett eksempel på dette er angrep mot styresystemene for overføringsnettet i kraftforsyningen, der manipulering med informasjon vil kunne føre til omfattende strømbrudd. Illegal styreinformasjon til prosesser kan i verste fall føre til fysisk ødeleggelse av utstyr. Feiloperasjoner og enkelte former for teknisk svikt kan også ha tilsvarende virkning.

At informasjonen til en hver tid er tilgjengelig er en annen viktig forutsetning for effektiv tjeneste- og vareproduksjon innen en infrastruktur. 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 infrastrukturen. Tilfeldige feiloperasjoner og ulike former for teknisk svikt er ofte en typisk årsak til tap av tilgjengelighet.

Konfidensialitetssikring er av mindre betydning i IKT-systemer knyttet til produksjon av infrastrukturtjenester. For den enkelte sluttbruker av IKT-infrastruktur er derimot konfidensialitetssikring viktig, for eksempel for å hindre at informasjon om personlige forhold, forretningsstrategier eller nasjonens sikkerhetspolitiske disposisjoner avsløres.

Virkemidler mot IKT-systemer vil i hovedsak inngå i følgende kategorier trusler:
- Fysiske trusler
- Elektroniske trusler
- Logiske trusler
- Sosiale trusler

Innen disse kategoriene finnes en rekke ulike former for virkemidler som enkeltvis eller i kombinasjon utgjør en trussel mot et gitt infrastruktursystem. I en normalsituasjon er det mest

sannsynlig at virkemidlene vil forekomme enkeltvis eller i enkle og logisk sammenhørende kombinasjoner. I mer omfattende situasjoner, der strukturerte villede handlinger ligger til grunn, vil trusselbildet derimot være mer komplekst og kunne omfatte en rekke ulike virkemidler i kombinasjon.

2.3.1. Fysiske trusler

Fysiske trusler er rettet mot å skade infrastruktur med mål å redusere tilgjengeligheten til IKT-systemene. Disse kan være rettet mot så vel den tekniske informasjonsinfrastrukturen som selve informasjonen som er nødvendig for systemenes funksjon. Målene for slike angrep vil være sentrale datamaskiner, lagringsmedia for informasjon, forbindelsesveier og knutepunkt i kommunikasjonsnett og driftssentraler som står for styring og kontroll av IKT-systemene. Fysiske trusler vil også kunne rettes mot infrastrukturer som IKT-systemene igjen er avhengig av. Kraftforsyning er ett eksempel på en slik infrastruktur.

Fysiske angrep på kritiske IKT-systemer kan variere i intensitet fra ren ustrukturert vandalisme, via mer omfattende kriminelle handlinger, til sabotasjehandlinger som del av terror- og krigshandlinger. For å realisere fysiske trusler vil det være nødvendig med fysisk tilstedeværelse eller bruk av avstandsleverte våpen. Typiske virkemidler er klipping av kabler eller avsetting av sprengladninger.

Også naturlige hendelser som uvær vil med ulik intensitet kunne påføre fysisk skade på IT-infrastruktur. Slike hendelser vil i utgangspunktet ramme tilfeldig, men dersom omfanget er stort vil også skaden kunne bli omfattende. Særlig telenettet er utsatt for denne typen hendelser. Mulige klimaendringer i Norden vil her kunne være en faktor.

2.3.2. 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*, hvorav den siste er den viktigste.

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 mest hatt anvendelse i militær sammenheng. Det finnes også eksempler på at teknikken har vært benyttet i fredstid. Jamming av kringkastingssendere i politisk øyemed har vært mye 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 militære sammenheng.

Elektromagnetiske strålingsvåpen er en type virkemiddel 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 følsom

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 har 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 vil ødelegges i stort omfang. 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[6] har det vært foretatt en viss grad sikring, for eksempel i systemer innen kraftforsyningen og i det tidligere Televerkets telenett.

"High power Microwave" (HPM) er en relativt ny type strålingsvåpen. Her benyttes moderne radarteknologi på en enkel måte 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 installasjon 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 i dag mulig å få kjøpt slikt utstyr over disk i enkelte land.

Det er utgitt retningslinjer for sikring av viktige IKT-installasjoner i Totalforsvaret mot elektromagnetiske strålingsvåpen, og det arbeides for tiden med forskrifter for det samme.

Elektroniske trusler har som for fysiske våpen primær innretning mot IKT-systemenes tilgjengelighet.

2.3.3. Logiske trusler

Logiske trusler dreier seg om et sett med virkemidler direkte rettet mot IKT-systemenes logiske funksjon. 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 aktuelt på grunn av datasystemenes tilknytning til det åpne globale Internettet.

2.3.3.1. Direkte systemangrep

Gjennom ulike metoder vil en angriper gjennom eksterne tilkoblinger i sann tid kunne sørge for at et IKT-system får en bestemt og på forhånd planlagt oppførsel. Eksempler på eksterne tilkoblinger er Internett eller direkte modemforbindelser gjennom det offentlige telefoninettet.

[6] Kombinasjonen av det militære forsvaret og Det sivile beredskap (se kapittel 6).

Ett eksempel på virkning av en slik inntrenging er strømbrudd over store områder etter at bryterstillinger i et overføringssystem for kraft er endret gjennom manipulering av styresystemene. På samme måte kan damluker i store damanlegg styres.

Angrepet kan også rettes mot 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, som kontrolleres fra det samme driftssystemet, vil virkningen kunne bli omfattende og langvarig.

For å trenge inn i et system utenfra benyttes en rekke teknikker. Det finnes i dag en rekke 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, med unntak av beskyttelse mot enklere former for misbruk. Den dyktige innsideren har derfor også ofte godt arbeidsrom.

2.3.3.2. Programvareangrep

Programvare for datamaskiner består av en samling av svært mange, men enkle logiske operasjoner i sekvens som styrer datamaskinens enkeltfunksjoner. Et vanlig program som vi kjenner fra 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 IKT-systemet bestemte logiske funksjoner som er uheldig for brukeren av programvaren. 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 dupliserer 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 milliarder kroner, ifølge Computer Economics Research. Av disse utgiftene kan anslagsvis 1 milliard føres tilbake til norske bedrifter og offentlig virksomhet. Et av de mest kjente virusangrepene de senere årene - ”Melissa-viruset” - ble kjent fordi det spredde seg svært fort. 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. I 1997 gjorde American Online sine brukere klar over at en trojansk hest sirkulerte på e-post. Når programmet med den trojanske hesten ble åpnet, sendte det fra seg brukerens brukernavn og passord til utsenderen av den trojanske hesten. Utsenderen ble tatt og innrømmet i rettssaken å ha tilegnet seg mer enn 500 brukernavn og passord gjennom dette ulovlig angrepet.

De som er med å 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.

Vi har i den senere tiden sett at 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 vil bryte sammen, som igjen fører til tap av tjenestetilgjengelighet. Angrepet på internettstedet Yahoo! den 8. februar 2000 er det mest kjente og største angrepet av denne typen i Internetts historie så langt. Millioner av brukere kan ha blitt omfattet av angrepet i det de ikke kunne bruke Yahoo! sine tjenester (søkemotorer). DDoS-angrep er en mer omfattende avart av enklere *"Denial of Service Attacks"* (DoS).

En annen form for DoS-angrep, som også bør nevnes i denne sammenhengen, er teknikker for å blokkere tilgjengelighet i kommunikasjonsnettverk. Dette kan gjennomføres ved å sørge for at det går mer trafikk i nettet enn hva dette har kapasitet til å formidle. 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. En annen teknikk for å hindre tilgjengelighet i et kommunikasjonsnettverk er å generere falsk trafikk i nettet. Dette kan blant annet gjennomføres ved logiske angrep mot de sentrale drifts- og tjenesteproduksjonssystemene innen det enkelte nettverk. Resultatet vil bli det samme som for fysiske angrep, den legitime trafikken vil blokkeres.

Disse teknikkene synes så langt mest å ha vært benyttet til å skape blind og tilfeldig forvirring og skade hos mange brukere. En lang rekke virus og DoS-angrep er eksempler på dette. 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. Dette gjelder så vel masseprodusert programvare som Microsoft Windows, som spesielle programvaresystemer som benyttes til å styre systemer innen for eksempel kraftforsyning og teleinfrastruktur. 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 mere raffinerte teknikker og kombinasjoner av slike.

2.3.4. Sosiale trusler

Ovenfor er det beskrevet en rekke ulike typer tekniske trusler, både villede og ikke-villede. Disse vil enkeltvis eller i kombinasjon effektivt kunne føre til alvorlige virkninger for IKT-systemene og de systemer og infrastrukturer disse betjener. Imidlertid inngår også mennesket som en viktig ressurs både i planlegging og i operativ drift av IKT-sytemer. Derfor er også den menneskelige faktor viktig med hensyn til sårbarhet i disse systemene. IKT-eksperter kan med eller uten eget vitende påvirkes til å gjøre gale ting, gjennom metoder som villedning, propaganda eller utpressing. Politiske motiv har også vist seg være en viktig faktor. Eksperter kan også gjøres utilgjengelig i forhold til sine arbeidsoppgaver.

Ved å gjennomføre angrep direkte mot systemeksperten kan utenforstående også få innsidetilgang til systemer som ellers er godt beskyttet av fysiske og logiske sikringstiltak. Eksperten har alle systemrettigheter i moderne systemer og det er svært vanskelig å beskytte seg mot denne. Denne typen angrep er viktig for at angriperen skal få inngående kjennskap til systemets svakheter. En systemekspert vil også kunne sørge for at sikkerhetsmekanismer settes ut av drift for en tidsperiode slik at direkte angrep utenfra kan finne sted med færre hindringer.

Ikke-villede feil fra egne ansatte står for en stor del av den daglige svikten i IKT-systemer. Dette er i hovedsak et kompetanseproblem, men kan også komme av for dårlige kvalitetssikringsrutiner. Mulige årsaker kan være høy rotasjonen av programvare, at de ansatte får for liten opplæring i å håndtere programmene eller at de ansatte ikke følger de retningslinjene som virksomheten har - eller burde ha - utarbeidet.

Den sosial trusselen utgjør dermed en viktig trusel mot systemenes konfidensialitet, integritet og tilgjengelighet, og må ses i nær sammenheng med de mer teknologiske virkemidlene.

2.4. Trusselvurdering

Frem til i dag har svikt i IKT-systemer i hovedsak hatt årsak i enten tilfeldige ikke-villede hendelser eller ustrukturerte angrep fra enkeltindivider. De mest strukturerte angrepene synes så langt å ha dreiet seg om ulike former for vinningsforbrytelser. Bevisst underrapportering har imidlertid ført til at det finnes liten kunnskap om dette. Det fremtidige trusselbildet er mer uklart. Dette gjør det vanskelig å definere et nivå som grunnlag for iverksettelse av tiltak på både nasjonalstrategisk- og virksomhetsnivå.

Som nevnt ovenfor er det et prinsipielt skille mellom villede og mer eller mindre tilfeldige ikke-villede hendelser mot et IKT-system. Dette skillet er sentralt også i den videre drøftingen av trusler og trusselnivå.

2.4.1. Tilfeldige hendelser

For tilfeldige hendelser kan det tradisjonelle målet for risiko benyttes:

*Risiko = Sannsynlighet for svikt * Konsekvensen av en eventuell svikt,*

der sannsynlighet for svikt er en kombinasjon av hvilke sviktsituasjoner som teoretisk vil kunne oppstå, kunnskap om tidligere hendelser og hvor utsatt og sårbart systemet som helhet er overfor disse situasjonene. For de fleste komplekse systemer vil det være mulig med

bakgrunn i erfaringer å anslå en repetisjonsrate eller sviktintensitet som grunnlag for et sannsynlighetsmål. Det finnes også tyngre teoretiske metoder som kan benyttes der den historiske sviktintensiteten er svært lav. Dette gjør det mulig gjennom tiltak kontinuerlig å avstemme et systems sårbarhet til den til enhver tids gjeldene trusselsituasjonen, gitt at en rår over tilstrekkelige gode metoder for risikoanalyse.

Et utviklingstrekk er at systemenes kompleksitet og omfang fører til at feil og operatørfeil blir mer kritiske enn tidligere. I utgangspunktet enkle hendelser vil kunne føre til kaskaderende følgefeil og ustabilitet i systemoppførselen, der systemet i verste fall kan bryte helt sammen og bli utilgjengelig i lengere tid. En typisk årsak til slike effekter er gjensidige avhengigheter mellom ulike systemer. Denne utviklingen vil kreve bedre metoder for risiko-arbeid.

Som følge av klimaendringer synes det også å være en trend mot at det i fremtiden vil oppstå flere og mer omfattende uværssituasjoner enn tidligere. Selv om slike hendelser fremdeles vil være sjeldne i forhold til andre former for tilfeldige hendelser, vil de likevel kunne utgjøre problemer for fysisk IKT-infrastruktur på grunn av sitt store omfang. I Sverige har en nå satt i gang forskning på dette feltet fordi man innser at denne usikkerheten representerer en betydelig utfordring for sikkerhets- og sårbarhetsarbeid innen de fleste samfunnsinfrastrukturene.

2.4.2. Villede angrep mot systemene

Villede angrep kan være utført av et vidt spekter med aktører fra enkeltpersoner til grupperinger, organisasjoner, virksomheter og stater. Det er imidlertid ikke lenger hensiktsmessig å snakke om *sannsynlighet for svikt* i tradisjonell forstand, ei heller kan en snakke om sannsynlighet for at en hendelse vil finne sted. Det finnes svært lite empiri på omfattende angrep mot IKT-systemer, særlig når det gjelder logiske virkemidler av nyere dato. Det er mer hensiktsmessig å se på hva som er *mulig* med bakgrunn i en teknisk vurdering. Mulighet for svikt som følge av en villet handling kan uttrykkes som:

*Mulighet for svikt = Angripers motiv og intensjon * Angripers kapasitet * Sårbarhet*

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. Dette er imidlertid ikke tilstrekkelig. En angriper med en gitt intensjon må også 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.

Med denne definisjonen kan en studere et spekter av mulige aktører og hvilke motiv og intensjon disse vil kunne ha for et eventuelt angrep. Dette kan så vurderes opp mot hvilken kapasitet disse vil kunne forventes å ha i dag og i fremtiden. Hvorvidt de virkelig noen gang vil gjennomføre et angrep er svært usikkert og vil være helt avhengig av den videre utviklingen. Det sentrale spørsmålet blir til slutt om vi kun skal sikre oss mot det som er sannsynlig, eller om vi også bør sikre oss mot det som er mindre sannsynlig, men likevel mulig.

I tabell 2.1 er det er vist en enkel sammenstilling med syv 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[7]. Dette må derfor kun betraktes som en første tilnærming til problemstillingen som et grunnlag for videre diskusjon. Kapasitet for fysiske og elektroniske virkemidler er i tabellen slått sammen og benevnt fysiske virkemidler.

Aktør	*Motiv/intensjon*	*Kapasitet*		
		-Fysisk-	*-Logisk-*	*-Sosial-*
1. Inkompetent	Tilfeldig rettet skadeverk	**-**	***L***	**-**
2. Underholdningshacker	Mer eller mindre tilfeldig rettet skadeverk	**-**	***L***	**-**
3. Forulempet ansatt	Skade for arbeidsgiver	***L***	***L***	**-**
4. Kjeltring	Egen økonomisk vinning	***L***	***L***	**-**
5. Organisert kriminalitet	Økonomisk vinning	***L***	***M***	***L***
6. Terroristgruppering	Promotere/skape oppmerksomhet om sak	***M***	***H/M***	***H/M***
7. Statlig	Skade på eller overtagelse av annen stats territorium	***H***	***H***	***H***

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

Tabell 2.1 Villede trusler mot IKT-systemer – mulighet for svikt.

Utviklingen innen de fem 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. På grunn av at systemene nå er knyttet sammen i globale kommunikasjonsnettverk må nå også den eksterne trussel legges til. Dermed blir også gruppen av mulige angripere dramatisk mye større. Registrerte dataangrep de senere årene har da også i hovedsak kommet utenfra.

Innen de to førstnevnte aktørgruppene 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 gruppene vil ofte ramme tilfeldig. De vil i enkelte angrep likevel kunne utøve stor skade dersom de løper linjen helt ut etter å ha trengt seg inn i et mer eller mindre tilfeldig valgt system. Så langt synes de imidlertid 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. Det er allerede i dag tegn som tyder på en viss profesjonalisering av slike miljøer. Ut av dette kan det med tiden vokse ut subkulturer med lavere moralgrenser, som selv om de ikke selv har noe annet motiv enn underholdning kan finne på å selge sine tjenester til de som måtte ha et motiv. En slik utvikling må karakteriseres som usikker, men vil være alvorlig for samfunnet dersom den blir en realitet.

De tre 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, men konsekvensene for samfunnet som helhet trenger nødvendigvis ikke å bli så store hvis deres målgruppe også i fremtiden holdes avgrenset.

[7] Cilluffo,/Berkowitz/Lanz, Global Organized Crime Project, Centre for Strategic International Studies (USA) (1999): " Cybercrime, Cyberterrorism, Cyberwarfare - Averting an Electronic Waterloo".

Virksomheter som er utsatt for vinningskriminalitet vil også i større grad enn andre typer virksomheter være bevisst over risikoen ved dette, og vil dermed også legge mer ressurser i å sikre seg mot disse aktørene. Ut fra et samfunnsperspektiv er derfor denne aktørgruppen antagelig ikke den farligste, men også disse kan med tiden utvikle seg til å bli svært farlige hvis de finner nye muligheter for hva deres kunnskap kan brukes til.

Statlige aktører må i dag – og særlig 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 stater er i ferd med å bygge opp kapasitet på området.

Når det gjelder terroristorganisasjoner og substatlige aktører hersker det mer tvil. Én vurdering er at eksisterende terrororganisasjoner i liten grad kan forventes å ta i bruk denne typen virkemidler, men i stedet velger å holde seg til velkjente teknikker. Tradisjonelt har slike organisasjoner primært rettet sine virkemidler inn mot mennesker og menneskeliv, og har kun i liten grad vært interessert i samfunnsinfrastrukturer som mål[8]. Det kan likevel ikke utelukkes at det kan oppstå nye typer grupperinger og organisasjoner som i større grad vil bruke logiske virkemidler mot infrastruktur. Angrep mot infrastruktur i det moderne samfunnet vil i mye sterkere grad enn tidligere kunne være et middel for å oppnå former for kaos med stor presisjon, også med tap av menneskeliv. Med bruk av logiske virkemidler trenger en heller ikke være tilstede for å forårsake skade. En annen vurdering som er mye fremme i den offentlige debatten på området er at også tradisjonelle organisasjoner med tiden vil ta i bruk hele spennet av virkemidler. Dersom en tradisjonell gruppering ikke selv innehar nødvendig kompetanse og kapasitet vil de likevel kunne hente den inn fra de førstnevnte aktørgruppene, som en betalt tjeneste.

I en vurdering av ulike trusler må det tas utgangspunkt i hele spekteret fra fred til krise og krig. Mangfoldet av potensielle aktører som kan representere en sikkerhetspolitisk risiko for Norge må sees i en global sammenheng. Dette fordi Norge er tilknyttet globale nettverk hvor geografi og avstander ikke lenger spiller noen rolle. Selv om en så langt ikke finner empiri på angrep mot IKT-systemer knyttet til kritisk infrastruktur er det ikke mulig å avskrive dette for fremtiden. Det er i denne sammenhengen verdt å merke seg at logiske angrep mot telenettet i Norge, både fra substatlige og statlige aktører, vurderes av sikkerhetsmyndighetene å være omfattet med høy risiko også i fredstid (se avsnitt 3.3).

Det at IKT-systemene i økende grad knyttes sammen med det verdensomspennende Internettet fører også til at det blir vanskeligere å identifisere angriperne. 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 forvirrere den som angripes. Derfor kan det være vanskelig for en virksomhet som blir angrepet å umiddelbart fastslå årsaken til angrepet. Man kan tillegge andre aktører intensjoner og handlinger de ikke har. Man kan endre identiteten til maskinen man bruker som plattform for angrepet slik at den angrepne part tror at det er en bestemt aktør som står bak. Dette kan igjen utløse påstander om bedriftsspionasje som ikke har rot i virkeligheten. Det samme gjelder for stater. Stater kan få store problemer med å identifisere angriperens geografiske utgangspunkt, da man kan rute

[8] Brynjar Lia, FFI: "Er sivil infrastruktur sannsynlige mål for terroristgrupper i fredstid?", FFI/RAPPORT-2000/01703.

angrepene via flere land og gjennom datamaskiner i nettet som anonymiserer angriperen. På denne måten er det svært vanskelig å bedømme om det er "guttestreker" eller et direkte angrep fra et annet land det er snakk om. Under Gulf-krigen 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.

I denne sammenhengen er det verdt å merke seg at det også innen FN-apparatet arbeides med problemstillingen, på initiativ fra Russland. Her blir spesielt kritisk IKT-infrastruktur som telekommunikasjon vurdert å være viktige mål i fremtidige konflikter. En ser at denne typen mål vil være så kritiske for nasjonene at dette kan føre til økt regional ustabilitet i verden. En vil kunne få nye fronter mellom de som behersker virkemidlene og de som ikke gjør det. For tiden behandles det nå et russisk forslag til prinsipper for oppførsel blant stater med hensyn til informasjonsoperasjoner, der formålet er å begrense staters rett til å utnytte blant annet angrep mot sivil IKT-infrastruktur som middel i ulike former for konflikt. Her foregår det imidlertid en fundamental debatt om hvorvidt dette er en problemstilling for FN, med USA og Russland som motpoler.

2.4.3. Samlet trusselvurdering

Hvilket trusselbilde vi i dag er stilt overfor kan være vanskelig å bedømme. Det rapporteres stadig i dagspressen om nye sikkerhetsbrudd i banker, sykehus og andre enkeltvirksomheter. Vi ser også stadige rapporter om at svikt i teleoperatørenes nett fører til svikt i viktige samfunnsfunksjoner som lufttrafikk, nødnummertjenestene osv. Enkelte store ulykker og naturødeleggelser de senere årene har også ført til svikt i IKT-systemer, primært som følge av fysisk svikt i telenettene. Vi vet videre at det i forbindelse med de olympiske vinterlekene på Lillehammer var rettet trusler mot IKT-systemene. Et omfattende sikkerhetsopplegg innen denne delen av arrangementet hindret imidlertid slike anslag, som klart ville gitt en angriper godt omdømme i sine kretser.

Det ser ut til at konsekvenser som følge av rene fysiske uhell og uværssituasjoner har vært av størst betydning frem til i dag. Det har så langt vært registrert begrenset med konsekvenser for samfunnet av villede angrep. Dette illustreres også i tabell 2.2 som viser utviklingen i anmeldte dataangrep mot norske virksomheter de senere årene. Tallene er relativt lave, men det er likevel en alminnelig oppfatning at det virkelige tallet på grunn av underrapportering er betydelig høyere.

Anmeldte lovbrudd – dataangrep	*1995*	*1996*	*1997*	*1998*	*1999*
Inntrenging i datasystem	12	19	20	27	31
Avlytting av datasystem	0	0	0	0	6
Ulovlig avlytting telefon/rom	0	0	5	26	22
Ødeleggelse av samfunnsnyttige installasjoner	0	0	0	0	4
Ødeleggelse av dataavhengige samfunnsnyttige installasjoner	0	0	1	0	0
Rettsstridig forføyning – datasystem	0	0	7	13	13
Skadeverk på lagringsmedier (alle)	0	0	6	9	18
Sum	***12***	***19***	***39***	***75***	***94***

Tabell 2.2 Anmeldte lovbrudd – dataangrep (Kilde: SSB).

I mange av de situasjonene som har oppstått med årsak i uhell og uværssituasjoner har det vist seg at samfunnets avhengighet til IKT-systemene er i ferd med å bli svært stor. Likeså har det vist seg at systemkompleksitet og sentralisering av systemer og kompetanse har ført til at den enkelte sviktsituasjonen har vart lengere enn hva man kunne forvente ut fra hendelsens art. Menneskers feilvurderinger av komplekse systemer har vært en årsak til dette.

Når det gjelder fremtiden må det, på grunn av IKT-systemenes og infrastrukturenes økende kompleksitet, forventes at situasjoner med svikt vil oppstå med økende hyppighet. Fysiske ødeleggelser i IKT-infrastruktur som følge av endringer i klimasituasjonen kan også bidra til et mer sammensatt trusselbilde enn tidligere. En må også forvente at den teknologiske utviklingen vil føre til et enda større mangfold av virkemidler for logiske angrep. Hvilke aktører som vil kunne finne på å anvende slike virkemidler er derimot mer usikkert. Det som synes sikkert er at kapasitet for slike angrep finnes allerede i dag. En god illustrasjon på det siste er et forsøk gjennomført av USAs myndigheter i 1997. Her gjennomførte 35 spesialister, med tilgang til Internett og under dekke av å være en utenlandsk fiende, i løpet av kort tid logiske angrep som kunne skadet både sivile og militære mål i USA. Blant annet var de i stand til å mørklegge store deler av USA[9].

Det er forbundet med stor usikkerhet å vurdere fremtidig trusselnivå mot IKT-systemer og infrastrukturer i samfunnet. En må vurdere det som er mulig opp mot hva man mener er sannsynlig når beslutninger om beskyttelsestiltak skal tas. Den omfattende krigen synes i dag å være langt unna, men nye aktører kan komme på banen raskere enn vi aner og med betydelig kapasitet, særlig når det gjelder nyere former for angrepsvirkemidler. For samfunnet er det viktig at beskyttelsen er noenlunde balansert opp mot den konsekvens en mulig trussel ville kunne få, både i forhold til enkeltvirksomheter og samfunnet som helhet. Det er derfor trolig nødvendig å differensiere beskyttelsesnivået etter den kritikalitet det enkelte IKT-systemet har for samfunnet. Dette synes i utgangspunktet å være enkelt, men utgjør i virkeligheten en svært sammensatt utfordring blant annet på grunn av gjensidig avhengighet mellom de ulike systemene.

2.5. Teknologi og sårbarhet

Det blir av enkelte hevdet at den teknologiske utviklingen går mot økt sårbarhet, mens andre igjen hevder at teknologiene som utvikles i seg selv er robuste og at systemene der disse teknologiene inngår derfor også er robuste. Det er imidlertid viktig å ha klart for seg at det ikke er noen automatisk sammenheng mellom egenskapene til et system og teknologien som er anvendt i systemet med hensyn til sårbarhet.

Ett eksempel på dette er internett-teknologien, som blant annet benyttes i Internett. Denne har isolert sett mange robuste egenskaper for framføring av informasjon i et nett. Ideelt sett vil informasjonen kunne finne frem selv om nettets struktur ødelegges betydelig. Dette er likevel til lite hjelp dersom nettet som knytter det hele sammen ikke er i stand til å håndtere alle mulige brukere og formidle den trafikken disse genererer. Nettet vil da i stedet kollapse. Selv om teknologien også har egenskaper som gjør at nettet vil bygge seg opp igjen, vil det likevel igjen kollapse hvis ingen gjør noe med det underliggende problemet. Forutsetningen for at teknologien skulle fungere i et robust system var da også opprinnelig at man skulle ha kontroll med hvem som skulle ha tilgang til nettet og hva det skulle brukes til. Ingen har i dag kontroll

[9] Cilluffo,/Berkowitz/Lanz, Global Organized Crime Project, Centre for Strategic International Studies (USA) (1999): " Cybercrime, Cyberterrorism, Cyberwarfare - Averting an Electronic Waterloo".

med hvem som bruker Internett eller hva det brukes til. På denne måten blir den i utgangspunktet robuste teknologien satt inn i en arkitektur og i et system som er svært sårbart.

Et annet eksempel på en teknologi med robuste egenskaper er den såkalte SDH-teknologien,[10] som benyttes i overføringsdelen av moderne telenett. Disse nettene kan formes som fysiske ringstrukturer der brudd i én del av ringen ikke får konsekvenser for noen av de tilknyttede brukerne. Når teleoperatørene ut fra kommersielle vurderinger velger å legge begge delene av ringen i samme fysiske grøft utnytter man ikke denne muligheten fullt ut. Dette har vi har sett en rekke konsekvenser av gjennom utallige kabelbrudd i telenettet de senere årene.

Hvordan den enkelte operatør av IKT-systemer setter sammen teknologiene i tekniske arkitekturer og systemer er derfor minst like viktig for sårbarheten som at teknologiene i seg selv er robuste. Med en utvikling mot mer og mer markedsstyrte løsninger tyder mye på at utviklingen går mot økt sårbarhet, til tross for at teknologien som utvikles parallelt ofte vil ha mange robuste elementer. En tydelig trend går på at markedsaktørene er opptatt av enkeltfeil, men i mindre grad er opptatt av samtidige feil og svikt.

Noen hovedtrender innenfor teknologi, teknologianvendelse og sårbarhet er:

Liberalisering og avmonopolisering av sentrale infrastrukturer som telekommunikasjon og kraftforsyning har ført til at en økende del av denne infrastrukturen drives etter rene kommersielle kriterier, i tillegg til at den også i økende grad er privat eid. Også innen andre infrastrukturområder går utviklingen mot mer rendyrking av kommersielle interesser og økt privat eierskap. Dette fører til at tradisjonelle virkemidler for offentlig kontroll og påvirkning blir mindre virkningsfulle. En positiv virkning av denne utviklingen er muligheten til et økt mangfold.

Liberalisering og markedsutsetting fører til et sterkere behov for *informasjonsutveksling* mellom kommersiell og teknisk del av virksomhetene – også mot omverdenen gjennom det globale Internettet. Dette fører igjen til behov for å knytte sammen IKT-systemer som tidligere var fysisk adskilt, noe som øker utsattheten og sårbarheten til blant annet vitale samfunnsinfrastrukturer og produksjonssystemer.

Teknologiutviklingen skjer i et tempo som gjør det vanskelig for myndighetene og andre beslutningstakere å ha tilstrekkelig og tidsriktig kompetanse og informasjon om utviklingen. Disse står følgelig i fare for å gjennomføre tiltak som er i utakt med den til enhver tid gjeldende trusselsituasjonen. Til og med aktørene selv har i dag problemer med oversikten. Samtidig øker kompleksiteten, ikke minst på grunn av at de gjensidige avhengighetene mellom ulike typer systemer øker sterkt i omfang. Det krever høy *kompetanse* å sikre IKT-systemer, en kompetanse som i dag er mangelvare.

Med utviklingen av Internett og systembrukernes ønske og behov for å være tilknyttet dette, er IKT-systemene blitt *globalt tilgjengelige* og de nasjonale grensene utgjør ikke lenger noen begrensning i informasjonsflyten – på godt og ondt. En mulig trussel fra hvor som helst i verden gjør det vanskeligere å finne ut av hvem som står bak et eventuelt angrep, samtidig som det også kan være vanskelig å avgjøre hvem angrepet egentlig er rettet mot. Gjennom

[10] Synkron Digital Hierarki (SDH).

åpne og sammenknyttede nettverk kan en person, organisasjon eller stat gjennomføre angrep fra nær sagt hvor som helst i verden.

Teknologien blir i økende grad *åpen*. Det vil si at kommunikasjon mellom systemer skjer i henhold til omforente standarder. Dette er positivt for brukerne fordi disse lettere kan samhandle, men det kan også være negativt fordi det kreves mindre kunnskap for å gjennomføre angrep mot systemene. Sterke og svake egenskaper ved systemene er mer kjent for allmennheten.

Antallet *datakyndige over hele verden øker raskt*. Andelen av disse som utvikler seg til hackere må forventes å være et voksende problem. Deres teknikker blir mer avanserte samtidig som en opplever rask spredningen av billige, avanserte og brukervennlige hacker-verktøy. Det meste av dette distribueres åpent over nettet.

Det er en trend mot økt *sentralisering* der viktige datamaskiner og nettverksknutepunkt legges til et fåtall geografiske steder. Dette fører til at operatøren av systemene kan bruke viktig spisskompetanse mer effektivt, men vil samtidig gjøre systemet mer sårbart overfor ulike former for trusler mot disse stedene. Alle eggene samles i en kurv. På den annen side blir disse punktene enklere å beskytte fysisk fordi de ligger på færre steder.

Det er også en sterk trend mot *sentralisert drift* av IKT-systemer. Telenett kan i dag godt kontrolleres elektronisk fra andre land, noe som allerede er en realitet hos enkelte teleoperatører. Det samme kan driftsfunksjoner i datasystemer. Det er også en trend mot at både *IKT-systemene og driften av disse settes bort (outsources)* til egne spesialiserte virksomheter, innenfor eller utenfor landet grenser. Dette gir i utgangspunktet større mulighet til både sikker og effektiv drift, men gir også sterk avhengighet til den som har det sentraliserte driftsansvaret og dennes sikkerhetskompetanse. Muligheten til selv å ha kontroll over sårbarheten i egen virksomhet reduseres.

Disse utviklingstrekkene har samlet sett både negativ og positiv virkning på sårbarheten i IKT-systemene. *Trenden vurderes å gå mot at systemene blir relativt driftssikre og robuste mot enkelthendelser med middels til høy intensitet.* Det vil si hendelser som en operatør ”forventer” vil skje, og som det vil utgjøre et konkurransefortinn i markedet å beskytte seg mot. *For flere samtidige hendelser synes utviklingen derimot å gå mot betydelig økt sårbarhet. Denne sårbarheten blir markert høyere dersom utfordringene i tillegg kommer fra villede trusseltyper, der mennesker eller organisasjoner har intensjon om å gjøre skade.*

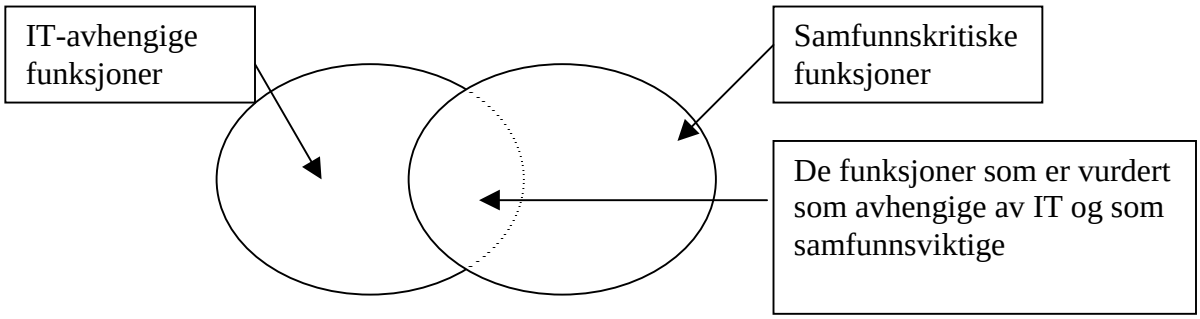
3. Samfunnets infrastruktur

3.1. Innledning

I dette kapitlet gjennomgås et utvalg samfunnssektorer med mål å si noe kvalitativt om sektorenes avhengighet av IKT-systemer, og hvor kritisk den ansvarlige sektormyndighet anser at denne avhengigheten er. Innspillene bygger i hovedsak på innspill hentet inn gjenom de ansvarlig fagdepartementene. Der det er gitt innspill fra andre etater eller institusjoner er dette nevnt spesielt.

Erfaringene fra år 2000-arbeidet er lagt til grunn for gjennomgangen. Dette omfattende arbeidet har gitt god erfaring om viktig infrastruktur og viktige samfunnsfunksjoner. Samtidig er det viktig å være klar over at år 2000 problemet var en kjent trussel og vi visste når den ville inntreffe. For IKT-sårbarhet generelt opererer vi med et vidt spekter av ulike trusler. Vi vet ikke når hendelser vil inntreffe eller hvem som vil rammes. Det kan også være vanskelig å vite hva som er årsaken til en hendelse, og eventuelt hvem som står bak. IT-sårbarhet er derfor et langt mer komplekst tema enn år 2000-problemet. Erfaringene fra år 2000-arbeidet er dermed heller ikke direkte overførbare, men gir likevel en pekepinn på veien.

Gjennomgangen nedenfor omfatter et utvalg av sektorer som vurderes å være IKT-avhengige og som samtidig innehar viktige samfunnsfunksjoner. Konklusjonene fra år 2000 arbeidet har dannet grunnlag for denne utvelgelsen.



Figur 3.1 De funksjonene som både er avhengige av IT og som er definert som samfunnskritiske kvalifiserer til vurdering. Det vil si de funksjonene som plasserer seg i fellesområdet for de to sirklene.

Basert på disse kriteriene er følgende samfunnssektorer valgt ut:

- Telekommunikasjon
- Kraftforsyning
- Transport
- Olje- og gass
- Bank og finans (betalingsformidling)
- Politi
- Redningstjenesten
- Sykehus
- Kommunehelsetjenesten
- Trygdesektoren

- Forsvaret
- Offentlig virksomhet/forvaltning
- Næringslivet

Telekommunikasjon og til dels kraftforsyning utgjør svært viktige samfunnssektorer for produksjon av tjenester for alle IKT-systemer. Disse to sektorene er derfor viet spesiell oppmerksomhet i den videre beskrivelsen. De tre sistnevnte sektorene, Forsvaret, offentlig virksomhet og næringslivet utgjør større virksomhetsstrukturer i samfunnet. I beskrivelsen har disse fått en mer begrenset behandling enn de øvrige sektorene, der kun enkelte viktige sider ved virksomhetene beskrives.

Vannforsyning og mediasektoren er ikke nevnt blant sektorene ovenfor. Dette begrunnes som følger:

Vannforsyning:
Vannverkene har i sin år 2000-planlegging vurdert egne beredskapsplaner og gjennomgått vannforsyningssystemets tekniske utforming og driftssituasjonen. I dette arbeidet er det spesielt forhold vedrørende leveringssikkerhet og desinfeksjon som det har vært fokusert på. Dette er grunnleggende funksjoner i enhver beredskapssituasjon.

2000-forberedelsene gir grunnlag for å anta at elektroniske komponenter ikke skaper nevneverdig risiko for svikt i leveringssikkerheten, da vannverkene har planer for manuell styring ved eventuell datasvikt. Slik sett er ikke vannforsyningen særlig sårbar for teknisk svikt. Mange av de små og mellomstore vannverkene har ikke elektroniske komponenter knyttet til teknisk utstyr. Som følge av dette vurderes IT-sårbarheten i sektoren å være liten.

Mediesektoren:
Prosjektet førte ikke opp mediesektoren som en kritisk sektor i forhold til avhengighet av IKT, noe som hadde sammenheng med de vurderinger som ble gjort i forbindelse med år 2000-arbeidet. I mediene opererer man med et mangfold av kanaler: Fjernsyn, radio, Internett og trykket presse. Flere kanaler som opererer på forskjellige nett i forskjellige systemer er en sårbarhetsreduserende faktor i seg selv. Faller fjernsynet i landet ut kan man fremdeles sende radiomeldinger over lokale nett. Utviklingen av innholdstjenester gjør også Internett til en alternativ kanal for rask informasjonsspredning.

Et forhold som er viktig å nevne i denne sammenhengen er en utvikling mot konvergens, både på eiersiden og på teknologisiden. Så godt som all informasjon er digitalisert og stadig større deler av informasjonen går i offentlige telenett. Dette gjelder både i produksjonen av informasjon og formidlingen av informasjon til sluttbruker. På formidlingssiden finner en nå for eksempel tilbud om Internett, fjernsyn, telefon og radio gjennom samme kabel-tv-tilknytning. Dette fører til at mangfoldet i mediekanaler ikke nødvendigvis er gjenspeilet i et tilsvarende mangfold i *tekniske* formidlingskanaler. Her kan det finnes strukturelle fellesnevnere som gjøre det hele mer sårbart enn vi tror.

Det har av praktiske årsaker ikke vært mulig å få tilgang til kvalifiserte vurderinger innen denne sektoren. At utviklingen fort kan gå i uønsket retning med hensyn til IT-sårbarhet er imidlertid noe vi bør være spesielt oppmerksomme på. Mediesektoren må betraktes som en svært viktig samfunnssektor også i fremtiden.

3.2. Innsamling av data og metode for risikovurdering

Kvaliteten på det innsamlede materialet gjenspeiler at prosjektet har operert innenfor svært korte frister. I tillegg kommer at IT-sikkerhetspersonell innen disse sektorene har vært en svært belastet gruppe fram til tusenårsskiftet. I praksis har svært mange av de underliggende etatene ikke vært i stand til å begynne arbeidet for IT-sårbarhetsprosjektet før i januar 2000. Materialets kvalitet er derfor i stor grad avhengig av om det innenfor de enkelte sektorene tidligere er gjennomført risiko- og sårbarhetsanalyser.

Hver bidragsyter ble i tillegg til å gi en kvalitativ beskrivelse av sin sektor med hensyn til IKT-avhengighet, også bedt om å anslå den IKT-relaterte risiko som de mener sin sektor er omfattet av. Dette skulle fylles inn i en tabell som vist i tabell 3.1, med en vurdering av sannsynlighet for svikt og en vurdering av konsekvens av svikt.

	Sannsynlighet for svikt			**Konsekvenser av svikt**		
Funksjon	Lav	Middels	Høy	Lav	Middels	Høy
IT-systemet til NN			X	X		
GPS-systemer i tange farvann hvor hurtigbåttrafikk er utbredt	X					X

Tabell 3.1 Eksempel på tabell for risikovurdering innen hver sektor.

De vurderinger som er gitt av det enkelte sektordepartement må i betydelig grad betraktes som subjektive, og det er derfor viktig å være klar over at det i materialet vil være til dels betydelige usikkerheter knyttet til risikovurderingene.

Vurderingen av sannsynlighet for svikt vil være avhengig av hvilket trusselbilde den enkelte har benyttet. Som nevnt i kapittel 2 er det også vanskelig å snakke om sannsynlighet for at noe skal skje dersom villede trusler tas med i betraktingen. Et annet problem knyttet til vurderingen av sannsynlighet er gjensidige avhengigheter, det vil si hvordan en som er avhengig av en annen tjeneste enn sin egen vurderer risikoen ved denne avhengigheten. Sannsynlighet for svikt i ulike typer teletjenester er en gjenganger i denne sammenhengen.

Vurderingen av konsekvens vil være avhengig av hvor langt ut i verdikjeden den enkelte har gått i sin vurdering. En ren teknisk svikt i en viktig samfunnsinfrastruktur vil ha langt mindre konsekvens for eieren av systemet enn hva den vil kunne være for enkeltmennesket og samfunnet. En totimers svikt i en teletjeneste vil isolert sett ha mindre konsekvens for produsenten av tjenesten enn for den som ikke får tilkalt akutt nødhjelp.

Tidsperspektivet vil også kunne være forskjellig. Noen vil være mer opptatt av fremtiden enn andre. Innenfor et område som er i så sterk utvikling som IKT og sårbarhet vil dette kunne ha vesentlig betydning for resultatet av den enkelte vurderingen.

Usikkerheten i de vurderingene som er gjort for hver sektor må derfor betraktes som betydelig. Det vil derfor også være vanskelig å gjøre gode sammenligninger innbyrdes mellom de ulike sektorene. Likevel vurderes det nyttig å ta med disse vurderingene fordi de uansett gir en viss pekepinn om hvilken IKT-relatert kritikalitet den enkelte sektor er omfattet av.

3.3. Telesektoren

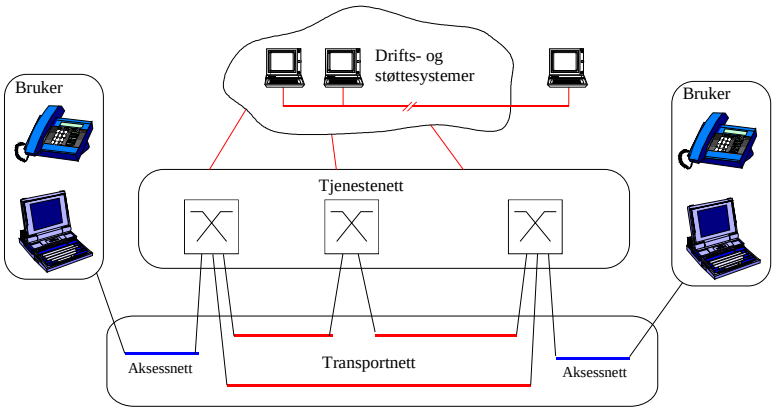
Telenettene er realisert gjennom en mengde funksjoner som sammen tilbyr overføring av informasjon gjennom en eller flere teletjenester. Disse funksjonene er igjen realisert i forskjellige systemer som står for alt fra fysisk overføring av informasjon til styrings- og kontrollfunksjoner ved bruk av avanserte datasystemer.

Telenettene i Norge er i dag så godt som heldigitalisert og dermed helt avhengig av IT for å kunne levere teletjenester. Alle teletjenester benytter i utstrakt grad IT for drift og vedlikehold, og de er dermed svært sårbare ved bortfall av IT-systemer. Alternative løsninger for teletjenestene uten bruk av IT-systemer er i dag ikke tilgjengelig.

3.3.1. Samfunnskritiske funksjoner

Grunnleggende elementer i telenettene er:

- Aksessnett
- Transportnett
- Tjenestenett
- Drifts- og støttesystemer



Figur 3.2 Telenettets prinsipielle oppbygning.

Transport- og aksessnett består av en fysisk infrastruktur som tar hånd om all transport av informasjon mellom geografise 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 nå i økende grad i bruk optiske fiberforbindelser i transportnettet. Fordelen med disse er at de har et svært høyt potensial for 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.

For å gi brukerne av teletjenester en tilstrekkelig grad av funksjonalitet er det opprettet såkalte tjenestenett som benytter transportnettet for å formidle informasjon mellom et antall tjenestenoder. Brukeren av en teletjeneste knyttes fysisk til tjenestenettet gjennom aksessnettet, og tjenestenettet sørger for at brukerens informasjon styres gjennom transportnettet frem til mottakeren. Drifts- og støttesystemer står for drift og administrasjon av

alle funksjoner i transport- og tjenestenettet. Disse systemene, som også er organisert som nettverk, er av svært stor betydning for sårbarheten innen moderne telekommunikasjon. 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.

Totalt sett vil telekommunikasjonsproblemer som følge av svikt innen hvert enkelt av disse 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
- vare- og drivstoffbeholdninger
- sentraliserte funksjoner, for eksempel innen kraftbransjen
- offentlige funksjoner, for eksempel innen utbetalinger, helsetjenester etc.
- trafikkavvikling innen samferdselssektoren

3.3.2. Årsakskjeder

Telenettene kan betraktes som et funksjonshierarki. Teletjenester er bygget opp med basis i et antall av enkeltfunksjoner og er derved avhengig av disse enkeltfunksjonene for å kunne fungere. En komplekst sammensatt teletjeneste vil kunne være et komplisert hierarki av nettfunksjoner. Dette vanskeliggjør oppgaven med å kvantifisere teletjenestenes sårbarhet og å sette opp årsakskjeder ut fra gjensidige avhengigheter.

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.

3.3.3. Sannsynlighet og konsekvens

Risiko mot norske telenett og teletjenester varierer med de ulike samfunnstilstandene fred (normaltilstand mellom stater og interesseorganisasjoner i et stabilt internasjonalt system), sikkerhetspolitisk krise (staten har problemer med å utøve sine primærfunksjoner som er å opprettholde nasjonal integritet og territorial suverenitet samt sikre befolkningens liv og helse) og krig (symmetrisk og/eller asymmetrisk aktør iverksetter planlagte og koordinerte operasjoner for å nekte statlig utøvelse av primærfunksjoner).

Begrepene ”krise” og ”krig” er i endring i innhold og mening. En fiende kan i dag bringe krise- og/eller krigstilstand til et land uten å være tilstede og heller ikke nødvendigvis røpe sin identitet. Det er lagt følgende definisjoner av aktører til grunn:
- Asymmetriske: Ikke-statlige grupper, organisasjoner etc.

- Symmetriske: Statsdannelser

Sannsynlige handlinger som er lagt til grunn er inndelt i fysiske angrep med ødeleggende virkninger for telenett og –tjenester, samt logiske angrep som er ulike former for ”software” som virkemiddel til å innhente etterretning samt å ødelegge eller degradere telenettene og deres tjenester. En trussel representerer en viss sannsynlighet for at uheldige hendelser kan inntreffe. Konsekvensene av slike hendelser definerer risiko for at:

- brukers informasjon skal bli endret, ødelagt, gå tapt eller bli gjort tilgjengelig for uvedkommende, eller at
- telenettene og –tjenestene ikke lenger er tilgjengelige for brukerne, eller ikke lenger har den avtalte kvalitet.

Med bakgrunn i de ovennevnte definisjoner har Forsvarets overkommando/ Etterretningsstaben på oppdrag fra TIFKOM-prosjektet (TIFKOM-prosjektet beskrives nærmere nedenfor) utarbeidet følgende risikovurdering vedrørende norske telenett og teletjenester:

Samfunnstilstand	**Aktører**	**Grov kategorisering av sannsynlige handlinger**	**Trussel → Risiko.**
Fred	Symmetrisk	Fysisk angrep	Liten
		Logiske angrep	Stor
	Asymmetrisk	Fysisk angrep	Middels
		Logiske angrep	Stor
Sikkerhetspolitisk krise	Symmetrisk	Fysisk angrep	Middels
		Logiske angrep	Stor
	Asymmetrisk	Fysisk angrep	Middels
		Logiske angrep	Stor
Krig	Symmetrisk	Fysisk angrep	Stor
		Logiske angrep	Stor
	Asymmetrisk	Fysisk angrep	Liten
		Logiske angrep	Liten

Tabell 3.2 Risikovurderinger innen telesektoren.

Sannsynligheten for alvorlig og langvarig svikt i teletjenester ut fra gjeldende trusselbilde vurderes å være liten overfor fysiske angrep, men derimot stor overfor logiske angrep dvs. forsøk på inntrenging i IT-systemer (*jf. tabellen ovenfor*). Konsekvensene ved slik svikt kan som nevnt foran vil være alvorlige for større eller mindre deler av samfunnet.

Dersom sikkerhetspolitiske kriser, økt terror etc. inntreffer, øker den menneskeskapte fysiske trusselen mot teletjenestene og dermed sannsynligheten for omfattende alvorlig og langvarig svikt. Konsekvensene for Totalforsvarets og samfunnets støtte til det militære forsvaret kan i så fall være svært alvorlige.

3.3.4. Oversikt over strategier og tiltak for å redusere sårbarheten i telenettene

De senere årene er det foretatt et omfattende utredningsarbeid mht. sårbarhet og sårbarhetsreduserende tiltak innen telekommunikasjon av Forsvaret, telemyndighetene og teleoperatørene i fellesskap.

Forsvarets forskningsinstitutt (FFI) gjennomførte i perioden september 1997 – februar 1999 en studie vedrørende sårbarhet og sårbarhetsreduserende tiltak innen området offentlig telekommunikasjon (BAS2). Studien var en oppfølging av BAS-prosjektet[11], og ble gjennomført etter oppdrag fra Justisdepartementet, Forsvarsdepartementet, Samferdselsdepartementet og Direktoratet for sivilt beredskap (DSB).

BAS2-prosjektet konkluderte 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 at 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 i tilstrekkelig grad. I studien er det også foreslått konkrete tiltak for å øke robustheten i de nasjonale telenett.

BAS2-studien peker bl.a. på det faktum at for å produsere teletjenester og drive disse mest mulig effektivt, tas det innen telekommunikasjon i bruk moderne informasjonssystemer i stort omfang. Informasjonssystemene bygger på såkalte åpne plattformer. Dette er en stor fordel ut fra et standardiserings- og funksjonssynspunkt, men en ulempe fordi dette generelt sett også gjør systemene mer åpne og sårbare overfor angrep mot integritet i funksjoner og data (hacking). Slike angrep vil, dersom de lykkes, kunne sette store deler av telenettene ut av funksjon for en periode. Programvaren som tilbys for bruk på disse systemene er heller ikke i særlig grad innrettet mot høy grad av sikkerhet overfor angrep, i alle fall ikke så langt. For flere systemer, som er vitale for tilgjengeligheten i telenettene, vil det kunne være et stort antall personer som har mulighet for tilgang til disse. Slike systemer gjør det samtidig også betydelig enklere enn tidligere for enkeltpersoner å utføre handlinger som kan få betydelige konsekvenser, enten på grunn av feilhandlinger eller bevisste handlinger. Den indre trusselen er derfor blitt betydelig mer alvorlig, og konsekvensene av slike handlinger vil kunne bli svært store.

For å redusere IT-sårbarheten i telenettene foreslår FFI at det kan det gjennomføres sårbarhetsanalyser og kontroll av teleoperatørenes mest kritiske informasjonssystemer, dvs. de drifts- og støttesystemene som direkte inngår i produksjonskjeden for teletjenester. Innføring av nye tjenester og funksjoner i telenettene (f.eks. nummerportabilitet) øker kompleksiteten og avhengigheten av slike IT-systemer ytterligere. Et annet tiltak for å redusere sårbarheten i telenettene er å opprettholde desentraliserte nasjonale data- og driftssentre slik at både regional (jf. Nord-Norge) og nasjonal driftskontroll av teleinfrastrukturen blir ivaretatt uten å være avhengig av IT-systemer utenfor landets grenser. Samarbeid og samøvelser mellom aktørene hvor rutiner og prosedyrer som anses viktige i en beredskapssituasjon blir prøvet ut

[11] I 1994 ble det besluttet å starte et samarbeidsprosjekt mellom FFI og DSB med utgangspunkt i at den sivile beredskapssektor i vid forstand trengte et mer helhetlig grunnlag for ressursallokering og et bedre system for den langsiktige planlegging. Prosjektet fikk benevnelsen BAS (Beskyttelse av samfunnet) og avleverte sin rapport i slutten av mars 1997.

er et annet tiltak for å redusere sårbarheten i telenettene. Omdisponering og omkonfigurering av ressurser i telenettet vil i stor grad være avhengig av operatørenes IT-systemer. For å gjennomføre ovennevnte tiltak påpeker FFI at det vil kunne være nødvendig med offentlig innsats ved at tiltakene følges opp av et statlig organ. Opprettelse av et slikt organ er nærmere utredet i TIFKOM-prosjektet, jf. nedenfor, og vil bli vurdert i forbindelse med Samferdselsdepartementets oppfølging av TIFKOM-rapporten.

Samferdselsdepartementet har hatt som målsetting å bruke FFIs utredning som utgangspunkt for en nasjonal strategi for telesikkerhet og –beredskap. 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 fritt konkurransemarked (forkortet til TIFKOM).

En prosjektgruppe bestående hovedsakelig av eksterne konsulenter 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. TIFKOM-rapporten gir innledningsvis en beskrivelse av samfunnets avhengighet av og behov for telekommunikasjon, samt sårbarhet og konsekvenser ved tap av telekommunikasjon. Videre gis det et bilde av hvilke trusler og utfordringer en kan stå overfor samt hvilket ambisjonsnivå en iht. prosjektgruppens anbefaling bør legge seg på for å sikre samfunnet den nødvendige robusthet i de samlede nasjonale telenett. I rapporten foreslås det også en rekke ulike tiltak for å redusere sårbarheten i telenettene. Den alminnelige etterspørselen etter teletjenester sikrer teletjenester med et visst sikkerhetsnivå. Markedsmekanismene alene vil imidlertid ikke sikre at samfunnets særlige behov for velfungerende telekommunikasjon f.eks. i krisesituasjoner tilfredsstilles. 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. I begge tilfeller fremheves behovet for ekstra telesikkerhet- og beredskap utover det som finnes i telenettene i dag. Det er foreslått tre sett av tiltakspakker som hver for seg gjenspeiler tre ulike ambisjonsnivåer. Prosjektet anbefaler at telesikkerhet og –beredskap bør komme opp på det valgte ambisjonsnivå i løpet av en 5-årsperiode og deretter vedlikeholdes. Prosjektgruppen foreslår bl.a. en ny organisering av arbeidet med telesikkerhet og –beredskap, og redegjør for ulike måter å finansiere et løft innen telesikkerhet og –beredskap. I TIFKOM-rapporten inngår det anbefalinger på organisatorisk, regulatorisk, økonomisk og teknisk plan.

Når det gjelder IT-sikkerhet, har TIFKOM-prosjektet bl.a. foreslått at teleoperatørene bør få krav om å sikre sine drifts-, vedlikeholds- og støttesystemer mot logiske trusler. Dette foreslåtte kravet vil innebære kartlegging av alle vitale informasjonssystemer, etablering og dokumentasjon av aksessrutiner og rettigheter (til systemer og fasiliteter) samt logisk/fysisk separasjon av nett for drifts-, vedlikeholds- og støttesystemer som har tilgang til Internett. I tillegg er det fremsatt forslag om at teleoperatørene skal la profesjonelle (red teams) prøve å finne svakheter i informasjonssystemene.

Samferdselsdepartementet mottok TIFKOM-prosjektets sluttrapport i slutten av mars og sendte denne på høring umiddelbart. Rapporten og de innkomne høringsuttalelsene vil danne

grunnlag for en nasjonal strategi for telesikkerhet og –beredskap i et telemarked med fri konkurranse.

3.3.5. Telenors vurdering

Som den ledende aktøren på det norske telemarkedet er Telenors arbeid med sårbarhet og sårbarhetsreduserende tiltak innen telekommunikasjon særdeles viktig, og Telenor arbeider kontinuerlig med sårbarhetsanalyser og tiltak for å redusere sårbarheten i sitt telenett. Nedenfor følger en kortfattet oversikt over hovedtrekkene i dette arbeidet.

Maskenett
Det faste transportnettet utgjør ryggraden for teletjenestene og er fra ende- og gruppesentralene og opp til fjernsentralene pålitelighetsdimensjonert, dvs. at det tas høyde kapasitetsmessig for at nettet også skal kunne avvikle trafikk i situasjoner med feil og overbelastning. Fjernsentralene er knyttet sammen i et landsdekkende maskenett med lastdeling mellom 2 eller 3 alternative veger, og Telenor har 2 utenlandssentraler som inngår i lastdelingen. I tillegg tilbys kunder med spesielt høye krav til sikkerhet/tilgjengelighet produkter som omfatter alternative lokale tilknyttinger til telenettet.

Gradvis degradering
De fleste teletjenester er statistisk dimensjonert ut fra en forutsetning om ressursdeling, og kan gjennom trafikkregulerende tiltak være bygget opp og dimensjonert på en måte som gir gradvis degradering i stedet for fullt sammenbrudd.

Fysisk sikkerhet
Telenor bygger i dag sin infrastruktur med strenge krav til fysisk sikring og adgangskontroll. Utstyr som er spesielt sårbart er til dels plassert i beskyttende anlegg; fjellanlegg og bunkere. Nødstrøm inngår i alle større tekniske anlegg. De senere år er det også lagt ned betydelige beløp i bedret sikring av abonnentnettet gjennom bedret avlåsing av fordelere etc.

Transportabelt utstyr
Transportabelt utstyr inngår i Telenors konsept for rask reetablering ved skade og ellers etter behov. Utstyret omfatter blant annet transmisjons- og sentralutstyr samt nødstrømsløsninger.

Prioritet
Viktige prioriterte telefoner (VPT) er en funksjon som i dag er implementert i endesentralene i Telenors tjenestenett for telefoni/ISDN. Prioritet som dekker telefoni og mobiltelefoni i hele tjenestenettet er i dag mulig dersom kundegrunnlaget er til stede.

Samtrafikkløsninger
Robuste samtrafikkløsninger mellom teleoperatørene utgjør en udiskutabel og fundamental forutsetning for å oppnå mest mulig robuste teletjenester. Det er her en utfordring at fleksible og gode løsninger for samtrafikk *kan* være motstridende til robuste løsninger. Samtidig vil en mer koordinert utnyttelse av de ulike aktørenes transportnett kunne være et betydelig bidrag til å redusere sårbarheten.

Logisk sikring
For å produsere teletjenester og drifte disse effektivt benyttes moderne informasjonssystemer i stort omfang. Sikring av drifts- og støttefunksjoner er herunder en prioritert aktivitet i det løpende sikkerhetsarbeidet hvor risiko- og sårbarhetsanalyser inngår som en viktig del.

Beredskap
Telenor har gjennomgående planer for beredskap og krisehåndtering. Arbeidet med beredskapsplanlegging som er utført under Program År-2000 innebærer en forsterket

kompetanse i Telenor når det gjelder planlegging og gjennomføring av beredskap, og det arbeides nå med videreføring og kontinuitet på dette området. I tillegg kommer at Telenor som en del av de spesielle samfunnspålagte oppgavene (SSO) viderefører sin totalforsvarsberedskap med samordning mellom militære og offentlige teleressurser. I tillegg har Telenor oppgaver iht. sivilt beredskapssystem (SBS).

3.3.6. Konklusjon

Samlet er konklusjoner for telekommunikasjon uttrykt i tabell 3.3 under.

	Sannsynlighet for svikt			**Konsekvenser av svikt**		
Funksjon	Lav	Middels	Høy	Lav	Middels	Høy
Aksessnettet	**X**			**x**		
Transportnett	**X**				**X**	
Tjenestenett		**x**			**X**	
Drifts- og støttessystemer		**x**				**X**

Tabell 3.3 Konklusjoner for telekommunikasjon.

Aksessnett og transportnett (stamnett) er fysiske infrastrukturer hvor svikt vil være begrenset til geografiske områder dvs. lokale eller regionale konsekvenser. Tjenestenett består av nettverksnoder som sentraler med tilhørende signaleringssystemer/databaser hvor svikt kan lamme tilgjengeligheten av bestemte teletjenester. Drifts- og støttesystemer er rene IT-systemer som i stigende grad sentraliseres til å håndtere hele nettet (dvs. landsdekkende) og har dermed stor potensiell sårbarhet. Aksess- og transportnett vil nok være mest sårbar for fysiske trusler. Tjenestenett (dvs. sentraler, noder) er i en mellomstilling med stort innslag av IT, mens drifts- og støttesystemer er rene IT-systemer og svært utsatt for logiske angrep. I fredstid vil det være størst sannsynlighet for logiske dvs. IT- angrep mot telenettet og i mindre grad fysiske angrep. Ved krise og krig øker derimot også risikoen for fysiske angrep.

3.4. Kraftsektoren

Informasjon om IT-sårbarhet i kraftsektoren er hentet fra det pågående BAS-prosjektet om kraftforsyningens sårbarhet (BAS 3), under ledelse av Forsvarets forskningsinstitutt (FFI)[12]. Prosjektet er ikke ferdigstilt, og flere problemstillinger knyttet til IT-sårbarhet og konsekvenser av kraftbortfall gjenstår. Likevel har FFI gjennom innhenting av informasjon om kraftsystemet, både innenlands og i andre land, fått betydelig innsikt i IT-avhengighet og –sårbarhet. Det er derfor mulig i det etterfølgende å si noe om de generelle utviklingstrekk innen dette feltet.

[12] Brev fra Forsvarets forskningsinstitutt - ref.: 2000/00449-5/FFISYS/JET/LLG/204.0, som svar på brev fra OED – ref.: OED/22 feb 00/3109/99/OG RS.

3.4.1. Kraftsektorens IT-systemer

IT-systemene som anvendes i dag er kommersielle systemer med en åpen arkitektur. Denne åpne arkitekturen er basert på internasjonale standarder fremfor proprietære standarder, og gjør systemene i seg selv mer sårbare både overfor angrep fra innsiden og angrep utenfra. IT-systemene består av et stort antall datamaskiner knyttet sammen i nett ved å benytte både offentlige teletjenester og kraftforsyningens eget telenett. Angrep utenfra er mulig fordi en i dagens kraftforsyning har behov for å knytte sine egne IT-systemer og nettverk sammen med andre aktørers IT-systemer, det vil si mer utstrakt bruk av åpne nett. Her benyttes også Internett som kommunikasjonsmedium. Dette innebærer i prinsippet at det er en sammenkobling av driftssystemene for kraftforsyningen og verden for øvrig.

Selv om det er mulig å foreta sikring av en tilknytning mot f eks Internett, gjør den åpne teknologien dette komplisert og vanskelig. Man blir ofte nødt til å inngå kompromisser mellom funksjonalitet og sikkerhet. Det finnes i dag få relevante krav til aktørene som sikrer et adekvat sikkerhetsnivå.

3.4.2. Produksjonssystemet

Nesten all produksjon av kraft i Norge er i dag basert på vannkraft. Vannkraft vil også i fremtiden utgjøre hovedtyngden av kraftproduksjonen, selv om en liten del av kraftproduksjonen i fremtiden kan komme fra gasskraft eller alternative energikilder.

Vannkraftverk er sammenlignet med f eks kjernekraftverk eller kullkraftverk – i seg selv enkle å drive og behovet for IT-systemer i selve produksjonsprosessen er begrenset. Tidligere var vannkraftverk bemannet og ble drevet lokalt. Funksjoner som start og stopp av aggregat ble formidlet ved driftstelefoni. Som en følge av effektiviseringen innen bransjen er det i dag vanlig at denne typen funksjoner ved de enkelte verkene fjernstyres fra driftssentraler. Kommunikasjon mellom systemansvarlig for nettet (Statnetts landssentral) og den enkelte produsents driftssentral foregår fremdeles over driftstelefon.

På produksjonssiden er det i dag én aktør av nasjonal betydning, som står for ca 30% av Norges kraftproduksjon. I tillegg kommer en rekke mindre aktører, men som i en regional sammenheng også har vesentlig betydning. I tillegg kommer en rekke industriverk og mindre aktører med verk av i hovedsak lokal betydning.

En IT-basert driftssentralløsning gjør det mulig gjennom et ”Denial-of-Service-angrep” å forhindre styring av kraftverkene ved å bryte sambandsforbindelsen mellom driftssentralen og kraftverket, eller nekte aktøren å bruke det fjernstyrte styringssystemet. Konsekvensen av dette er at en hindrer sekundærregulering av det samkjørte kraftsystemet. Dette går greit over et kortere tidsrom, men over lenger tid med større svingninger i forbruk vil en mangel på produksjonsstyring være fatalt. Dette avhenger imidlertid av at antallet kraftverk uten styring er av en viss størrelse. Angrep mot mindre aktørers systemer vil kun få lokale effekter, i hvert fall i et kortere tidsperspektiv. I slike situasjoner må verkene bemannes, noe som igjen er avhengig av tilstrekkelig kompetent personell. I dag synes dette å være mulig, mens det noe frem i tid vil kunne være vanskeligere. Det kan tillegges at en grunnforutsetning for alle typer drift av kraftforsyningen er at driftstelefonisystemene fungerer. Også her er det en fare for en utvikling mot mer sårbare løsninger på samme måte som innen offentlig telekommunikasjon.

Et vellykket integritetsangrep mot IT-systemer i kraftproduksjonssystemet vil kunne være fatalt, særlig dersom dette rammer de største aktørene. Gjennom et slikt angrep vil angriperen gjennom kontroll med aggregatstyring kunne oppnå å bryte ned den likevekt som må være mellom forbruk og produksjon i nettet. Dette kan føre til nettsammenbrudd. Her vil det også være nødvendig å bemanne kraftverkene og gjennomføre manuell styring. Med økende kompleksitet i IT-systemenes oppbygning og de funksjonene disse utfører, er det imidlertid en fare for at en slik overgang til manuell kontroll i fremtiden kan medføre betydelige problemer og tidsforsinkelser.

En trend mot færre og større aktører innen kraftproduksjonen vil kunne gjøre det enklere å ramme kraftforsyningen gjenom flere alternative mål for et angrep.

3.4.3. Overføringssystemet

Fra produksjonsverkene går den elektriske energien via et overføringsnett, og gjennom et distribusjonsnett ut til den enkelte abonnent. I takt med økende effektivisering er IT-avhengigheten i driften av overføringsnettene økende, og dermed også potensielt IT-sårbarheten. Dette gjør seg gjeldende på flere områder:

Alle komponenter i overføringssystemet er utstyrt med automatisk vern som kobler ut strømmen på linjer og andre komponenter etter gitte kriterier (kortslutning, spenningsfall, lynnedslag osv). Tradisjonelt har disse vernene vært enkle elektro-mekaniske komponenter. Disse komponentene inneholder nå i økende grad mikroprosessorer, som gjør tilknytting til datanett mulig. Dette muliggjør sentralisert konfigurasjon av disse, slik at kriteriene for utkobling av strømmen kan endres. Bryterne er under normal operasjon ikke avhengig av samband til en nettsentral, men hvis utenforstående skulle greie å skaffe seg tilgang til innstillingene av slike vern kan disse feilprogrammeres til å bryte strømmen selv under normale driftsforhold. En vellykket manipulasjon med slike komponenter kan i sin ytterste konsekvens føre til nettsammenbrudd.

IT-systemer benyttes nå i utstrakt grad i forbindelse med driftsmessig styring av nettene, og for beslutningsstøtte i forbindelse med nettdrift. I driftssentralene mottas fortløpende data fra en rekke målere i nettet, noe som bl a danner grunnlaget for å fordele belastningen av strøm i nettet ved hjelp av fjernstyring av brytere og andre komponenter. En trend i tiden er som nevnt at man av økonomiske grunner søker å utnytte det eksisterende nettet maksimalt, fremfor å bygge ut nye kraftlinjer. Spesielt i tidsrom med høyt strømforbruk og tilhørende høy belastning på nettet fører dette til meget stor avhengighet av driftsstyringssystemene for å sikre at nettet fungerer. Et angrep mot driftsstyringssystemene vil raskt kunne føre til ustabilitet i nettet, slik at store områder mister strømmen.

Også mot overføringsnettet er det et integritetsangrep som vil ha størst konsekvenser for forsyningen. Dersom en angriper får kontroll med f eks effektbrytere i hovednettet vil vedkommende raskt kunne oppnå et nettsammenbrudd. Etter et vellykket anslag mot driftssystemet kan en normal driftssituasjon relativt raskt gjenopprettes hvis det autoriserte driftspersonellet gjenvinner uforstyrret tilgang til driftssystemene. Hvis dette ikke skjer må drift av nettene skje manuelt og lokalt. I forbindelse med årtusenskiftet demonstrerte kraftbransjen evne til å drive både produksjon og distribusjon av kraft uten bruk av IT-systemer. Dette var imidlertid en godt planlagt operasjon som det uten tvil hadde tatt tid å improvisere. Et annet utviklingstrekk er at et stadig færre antall personer har kompetanse på

manuell drift av systemene, og at man derfor blir mer og mer avhengig av at de automatiserte systemene fungerer. Den økte anvendelse av IT-systemer og den kompleksitet dette medfører vil i fremtiden kunne medføre at en slik overgang til manuell drift vil kunne fortone seg betydelig mer vanskelig.

Det kan også nevnes at i 1997 demonstrerte et tredvetalls dataeksperter at det er mulig å bryte ned store deler av det Nord-Amerikanske kraftnettet gjennom eksterne angrep fra Internett med bruk av standard "hacker"-verktøy.

3.4.4. Konsekvenser av bortfall av kraftforsyning

Bortfall av elektrisk kraft vil påvirke hvert enkelt individ og nesten alle samfunnsfunksjoner på en negativ måte. For den enkelte innbygger vil tap av strømforsyning raskt oppleves meget ubehagelig. Om vinteren vil mangel på lys og oppvarming være problematisk, om sommeren vil oppbevaring av matvarer raskt bli problematisk. Mangel på kokemuligheter og varmt vann til vask og hygiene er andre konsekvenser. Radio/TV som er avhengig av strømtilkobling vil ikke virke – det samme gjelder PC-er i hjemmet. I dag er de færreste hjem kritisk avhengig av en fungerende PC, men dette kan endre seg i fremtidens samfunn der det forventes vekst i bruk av elektronisk handel, banktjenester, informasjon etc. Slike tjenester vil kunne fortrenge dagens systemer, og dermed øke IT-avhengigheten.

De fleste mennesker har etterhvert mobiltelefon, og denne vil virke så lenge det er strøm igjen på batteriet. Her er imidlertid situasjonen den at nødstrøm ikke har vært prioritert i forbindelse med de siste års raske utbyggingen av mobiltelefonnettet. Konsekvensen av dette er at store deler av mobiltelefonnettet vil falle ut umiddelbart ved strømbrudd. Dette kan igjen påvirke kraftselskapenes evne til å gjenopprette kraftforsyning, blant annet fordi man er avhengig av mobiltelefoni for å påkalle, og holde kontakt med f eks montører og driftspersonell.

Det er mange andre IT-systemer i samfunnet som også er avhengig av kraftforsyningen. Generelt vil brudd i kraftforsyningen føre til at samtlige IT-systemer som ikke er sikret med nødstrøm slutter å fungere. Dette gjør at anslag mot kraftforsyningen (ikke nødvendigvis bare anslag mot dens IT-systemer, men også fysiske angrep) er en potensielt meget effektiv måte å sette store deler av samfunnets IT-systemer ut av spill på. Mange samfunnsviktige funksjoner, som f eks sykehus, har tatt konsekvensen av dette, og har anskaffet nødaggregater. Imidlertid er dette systemer som sjelden benyttes, noe som øker faren for at ikke alt virker som det skal hvis behovet for nødstrøm plutselig oppstår. Høsten 1999 mistet f eks Drammens-området strømmen, noe som også rammet Sentralsykehuset i Buskerud. Her sviktet nødaggregatene, og dette førte til en svært prekær situasjon ved sykehuset. Et annet problem er at eldre nødaggregater ofte er underdimensjonerte fordi virksomheten har vokst og/eller gjort seg avhengig av flere elektrisk drevne systemer. På plussiden må det likevel noteres at mange virksomheter anskaffet eller oppgraderte nødstrømforsyningene sine som en del av år 2000-beredskapen.

BAS-prosjektet har pr i dag ikke oversikt over status når det gjelder sikring av kritiske samfunnssystemer ved hjelp av nødstrøm. Dette, og konsekvenser av bortfall av strømforsyning generelt, er forhold som prosjektet vil utrede nærmere fremover.

Konsekvensene av et strømbrudd vil generelt øke proporsjonalt med varigheten av strømbruddet. Strømbrudd av kortere varighet enn ca ett døgn vil neppe føre til utålelige

samfunnsmessige konsekvenser, men vil oppleves ubehagelig og frustrerende av de fleste og kan innebære betydelige økonomiske tap. Det er også verd å merke seg at det kan ta lang tid å reetablere normalsituasjonen etter bare et kortvarig strømbrudd. Dette blant annet fordi det tar tid å reetablere IT-systemer som har sviktet som følge av strømbruddet.

3.4.5. Trender innen anvendelse av IT i kraftforsyningen

Etter Energiloven av 1990 har kraftforsyningen gjennomgått en betydelig effektivisering. Ett ledd i denne effektiviseringen er en betydelig anvendelse av moderne informasjonsteknologi, som i samme periode også har gjennomgått en betydelig utvikling. IT benyttes i dag primært til å styre ulike funksjoner i kraftforsyningen og til å innhente ulike typer måledata fra systemene.

Til forskjell fra tidligere da mye personell var utplassert på installasjoner som transformatorstasjoner, kraftverk o l, utføres i dag i økende grad kontroll av systemet fra sentralt plasserte driftssentraler. (Tidligere foregikk kommunikasjon gjennom et enkelt driftstelefonisystem, som var bygget opp med tanke på høy robusthet.)

Nyere konsepter for driftssentralløsninger muliggjør at et selskap kan styre de fleste funksjonene i sine systemer fra en enkelt sentral, noe som muliggjøres av dagens IT-systemer. For ytterligere å gjøre driften av kraftforsyningen effektiv innføres det løsninger som gjør det mulig for driftspersonell å styre kraftverk fra hjemmekontor ved hjelp av hjemme-PC med modemtilknytning til driftssentralene.

Et annet forhold som følger av økt effektivisering av kraftsystemet og sterkere utnyttelse av ressurser, er mindre marginer og dermed økende avhengighet av effektiv beslutningsstøtte for blant annet å hindre kaskaderende utkoblinger. Enkeltfeil kan da i verste fall medføre større sammenbrudd i nettet. Slik beslutningsstøtte – og iverksettelse av tiltak – er igjen avhengig av fungerende informasjonssystemer med tilgjengelig kommunikasjon med enhetene ute i nettet.

Tilrettelegging for konkurranse i bransjen har også ført til et økt behov for informasjonsdeling mellom ulike aktører. Eksempler på aktører er operatører, markedsaktører, forsikringsselskap osv. I dette ligger det et sterkt behov for formidling av informasjon som er en del av de enkelte aktørenes IT-systemer.

Man ser også en utvikling mot verdiøkning av tjenester gjennom en bransjekonvergens. Dette vil si at man slår sammen tjenester som kraftleveranser, kabel-TV, telefoni og vannforsyning. Et slikt tjenestekonsept forutsetter en god IT-samordning, noe som dramatisk vil øke avhengigheten av IT.

3.4.6. FFIs vurdering av kraftsektorens IT-sårbarhet

Selv om det kan hevdes at avhengigheten av IT i dag fortsatt er moderat, antas det at avhengigheten vil øke betydelig i nær fremtid tilsvarende den generelle IT-avhengigheten i samfunnet for øvrig.

Kraftforsyningen synes å være relativt sårbar overfor målrettede anslag mot IT-systemene som inngår i denne, og i særlig grad dersom anslagene rettes mot systemene til de største aktørene innen overføringsnettet. Konsekvensene av strømbrudd vil kunne være omfattende

og betydelige. Anslag mot kraftforsyningen kunne være en potensielt meget effektiv måte å ramme samfunnsviktige IT-systemer på.

I dag anses det imidlertid mulig relativt raskt å reetablere normal systemdrift og kraftforsyning fordi systemene som sådan fremdeles er noenlunde oversiktlige, og også fordi det i dag finnes tilstrekkelig med kompetent personell til å reetablere manuell drift. Det er imidlertid mulig at slike manuelle løsninger i mindre grad vil være tilgjengelige i fremtiden. Faktorer som ytterligere effektivisering og bransjekonvergens med sammenknytting av ulike IT-baserte tjenesteplattformer fører til en betydelig høyere IT-avhengighet, og en betydelig økt kompleksitet i systemene. Dersom en slik utvikling får gå upåvirket, særlig med tanke på konsekvensene ved større alvorlige påkjenninger, vil dette føre til betydelig økt sårbarhet. Dette betyr ikke at enkeltaktører i norsk kraftforsyning i dag har en virksomhet som er utilfredstillende.

3.4.7. Konklusjon

Konklusjoner for kraftsektoren:

	Sannsynlighet for svikt			**Konsekvenser av svikt**		
Funksjon	Lav	Middels	Høy	Lav	Middels	Høy
Kraftproduksjon		**X**			**X**	
Overføringsnettet		**X**				**X**

Tabell 3.4 Konklusjoner for kraftsektoren.

3.5. Transportsektoren

Innenfor transportsektoren har en flere former for transport og flere ansvarlige aktører. For å forenkle fremstillingen vil vi dele transportsektoren opp i:

- Trafikk på vei
- Trafikk på bane
- Trafikk på sjø
- Trafikk i luften

Vi vil også se litt på logistikkproblemene som er knyttet til transport. Dette vil vi behandle under ett for alle typer transport.

På et overordnet plan vil ikke svikt i en av transporttypene automatisk være samfunnskritisk, da man i stor grad kan nytte de komplementære transportmidler. Dette kan medføre tap av tid, men ikke nødvendigvis tap av kapasitet. At de fleste aktører i transportsektoren opererer med svært lite overflødig transportutstyr gjør at det likevel vil bli et underskudd når en ser samfunnet som helhet, men ikke nødvendigvis til prioriterte samfunnsfunksjoner, geografiske områder eller viktige aktører.

All transport er styrt av regler, i hovedsak regler som er forankret i internasjonale avtaler eller ordninger. Det er ulik grad av kompleksitet i trafikkavviklingen avhengig av hvilke type

transportmiddel man snakker om, noe som også gjelder i hvilke grad IT er brukt i styringen og overvåkningen av trafikken.

3.5.1. Trafikk på vei

Ordinær veitrafikk er den typen transportmiddel som er minst avhengig av IT. I hovedsak er IT innenfor veitrafikken nyttet til styring av lyssignaler samt overvåkning av veier og tunneler. Ved bortfall av lyssignaler vil vanlige regler for trafikkavvikling gjelde, og trafikken vil gå tilnærmet som normalt, med noen forsinkelser på grunn av omstillingen fra et automatisk system til et system hvor hver enkelt sjåfør skal nytte de ordinære trafikkreglene. Ved bortfall av overvåkningsmuligheter for veier og tunneler vil muligheten til raskt å oppdage hendelser bortfalle eller bli kraftig redusert. Dette gjelder både kameraer/sensorer samt publikumsstyrte varslingsordninger (telefoner i tunneler osv.).

I sum kan man si at for trafikk på vei er det liten sannsynlighet for forstyrrelser som følge av IT-relaterte problemer, og konsekvensene ved bortfall vil i overveiende grad være begrensede.

3.5.2. Trafikk på bane

Organiseringen av jernbanen i Norge er, noe forenklet, delt i tre:
- *Jernbaneverket* er ansvarlig for infrastruktur på det statlige jernbanenettet,
- *NSB BA* er i dag ansvarlige for vognmateriell på alle områder, unntatt
- *Flytoget AS* som er et heleid datterselskap av NSB BA, men som har ansvar for sine egne vogner og infrastruktur og Malmtransport As som har ansvaret for malmtransporten på Ofotbanen.

Trafikk på bane blir stadig mer avhengig av digitale systemer. En rekke manuelle systemer har blitt erstattet eller supplert av digitale systemer i de senere årene, og denne utviklingen ser ut til å skyte fart. I tillegg blir systemene stadig mer integrerte med hverandre og utenforliggende systemer.

3.5.2.1. Jernbaneverket

For å foreta en vurdering av IT-sårbarhet på systemer i Jernbaneverket er det hensiktsmessig å dele inn i følgende funksjoner:
- Kjørestrøm (strøm for togframføring)
- Signalsystemer (signaler for kontroll og framføring av tog)
- Telesystemer
- Administrative systemer

Forutsetningen for at alle de nevnte funksjonene skal være operative er leveranse av ekstern elektrisk kraft. Denne kraften blir tilpasset Jernbaneverkets interne system i dertil egnede omformere. Uten tilførsel av ekstern kraft vil togframføringen bli redusert og måtte opphøre etter relativt kort tid på elektrifiserte banestrekninger dersom det ikke foreligger reserve dieselmateriell. En del viktige signal- og sikringssystemer har reservekraft for en begrenset periode.

Kjørestrøm

Med kjørestrøm menes den strømmen som skal til for å kunne kjøre tog på de elektrifiserte banestrekningene i Norge. For å kunne ha kontroll på kjørestrømmen må man ha en rekke brytere og vern. Dette overliggende anlegget er ikke IT- avhengig, og kan styres manuelt. For å kunne kontrollere og fjernstyre, samt å ha bedre oversikt over anlegget har man sentrale

kontrollsystemer for brytere og vern. Disse kontrollsystemene er databaserte, og lokalisert i 6 el-kraftsentraler i Norge. Avhengigheten til datateknikk er i stor utstrekning knyttet til kommunikasjonen mellom sentralene og anleggsdelene. Disse har redundans via eksterne teleoperatørers linjer. Det finnes dessuten mulighet for å benytte manuelle rutiner slik at forsyningen av kjørestrøm kan opprettholdes ved utfall av fjernstyringssystemene. Manuelle rutiner medfører bruk av personell ute i anleggene. Både omformere og lokale brytere kan betjenes av personell dersom el-kraftsentralene er falt ut. Tilgang på tilstrekkelig kvalifisert personell kan være et problem dersom fjernstyringen for store områder faller ut.

Signalsystemer
De fleste av Jernbaneverkets strekninger består av lokale signal- og sikringsanlegg på stasjonene som styres og overvåkes fra noen få fjernstyringssentraler.
Jernbaneverkets anlegg er av ulik alder og utførelse, men generelt kan man si at anlegg utenfor Oslo-området ikke er databaserte og følgelig ikke utsatt for den type feil vi her snakker om. I Oslo-området er det de siste årene foretatt store utskiftninger og oppgraderinger, og de nye systemene er i hovedsak databaserte.

De systemer som utfører sikkerhetskritiske funksjoner er konstruert for å feile til en restriktiv tilstand (for eksempel at signaler viser rødt). Dette er med på å redusere sårbarheten.

Nye systemer for fjernstyring av tog er i hovedsak databaserte. Disse består av en sentralenhet som kommuniserer med de lokale signalanleggene ute på strekningene via tele-/ datakommunikasjonsløsninger. Til denne kommunikasjonen benyttes det egne kabler. For å øke tilgjengeligheten benyttes ulike løsninger for omvegsforbindelse/rerute.
Dersom man mister forbindelsen med stasjonene finnes det imidlertid mulighet for å benytte manuelle rutiner slik at togframføringen kan opprettholdes. Disse manuelle rutinene medfører bemanning av en del stasjoner. Ved feil som rammer store eller trafikktette områder vil man ikke ha tilstrekkelig med mannskap for å bemanne det antall stasjoner som er nødvendig for å kunne kjøre med normal kapasitet.

Telesystemer
Telesystemer er i stor grad databaserte og representerer ofte forbindelselinjer mellom ulike datasystemer. Både data- og telesystemer har stor geografisk utstrekning noe som gjør dem sårbare for brudd. Utviklingen innenfor området går i retning av stadig større avhengighet til databasert utstyr. Systemer som er basert på elektronikk vil ha en del komponenter som vil være ute av funksjon fra tid til annen. Kravet til tilgjengelighet, det vil si at systemet fungerer, er høyt. Graden av redundans i systemene er derfor stor.

Enkeltstående kabelforbindelser for transmisjon er bare i noen grad dublert. Imidlertid er telesystemene som helhet bygget med redundans slik at enkeltstående feil ikke skal medføre brudd i forbindelsen mellom kritiske anleggsdeler. Dermed vil togtrafikken kunne holdes i gang selv om ett system svikter. Togframføringen vil kanskje måtte forsette med mindre kapasitet på grunn av redusert framføringshastighet, men den vil ikke måtte opphøre. Forutsetningen er at sikringssystemet fortsatt fungerer. Det er liten sannsynlighet for at svikt i telesystemene skal medføre stans i togframføringen.

Administrative systemer
Utfall av administrative systemer vil i de fleste tilfeller kun få begrenset omfang da Jernbaneverkets interne nett er bygd opp med distribuerte servere i hovedenhetene (geografisk spredt). En langvarig svikt eller stans i administrative systemer anses ikke som særlig

sannsynlig, men kan medføre store ulemper. Det vil likevel neppe forårsake stans i togtrafikken.

Tiltak og strategi
Behovet for videre analyser antas å være størst i forhold til "ikke-tekniske" scenarier slik som eksterne trusler og organisering. Det antas også å være behov for en overordnet analyse av de ulike systemenes avhengighet til hverandre og identifisering av svake ledd i forhold til Jernbaneverkets primære tjenesteytelse.

3.5.2.2. NSB BA
For den mest kritiske infrastrukturen finnes det en rekke beredskapstiltak som kan settes i verk ved IT-relaterte problemer som påvirker driften. Det finnes dessuten manuelle alternativer for alle de kritiske digitale systemer der dette er mulig.

For alle nyere systemer er det svært liten sannsynlighet for svikt. Sannsynligheten for svikt på noen av de eldre systemene er betydelig større, men disse blir kontinuerlig overvåket, slik at feil kan oppdages så raskt som mulig.

Konsekvensene ved bortfall av banetrafikk vil få størst konsekvenser for området rundt Oslo S, men dette er svært lite sannsynlig. Det er også slik at mellom 25-30 % av godstrafikken i Sør-Norge går på bane. Ved bortfall av denne må både personer og gods transporteres på vei, luft, og sjø. Dette ville bety en merbelastning på disse transportformene som ville medføre betydelige forsinkelser.

De mest sannsynlige truslene er en eller annen form for katastrofe – brann, sabotasje eller større ulykke- som rammer NSB-Datas lokaler. For det enkelte system er den mest sannsynlige truslen feil i programvare eller basis programvare.

Tiltak for å redusere sårbarheten kan være å øke kompetansen, forskning og utvikling, organisatoriske endringer, fysiske og personmessige tiltak samt innføringen av ulike tekniske løsninger/nye systemer.

3.5.3. Trafikk på sjø
Hovedformålet med Kystverkets virksomhet er å sørge for best mulig sikkerhet og fremkommelighet for de som ferdes, oppholder seg eller driver næringsvirksomhet i kystsonen, samt å legge alle forhold til rette for at disse kan drive sin virksomhet under best mulige konkurranseforhold og på den mest rasjonelle måte. Dette oppnås bl.a. gjennom å yte navigasjonsveiledning i form av fyrbelysning, elektronisk navigasjon, oppmerking, los- og trafikksentraltjenester samt å holde farledene åpne og fri for hindringer, tilstrekkelig dype og brede mv.

Etter en samlet vurdering av Kystverkets totale virksomhetsområde sett i lys av de kriterier som skal legges til grunn for at en funksjon skal anses som samfunnskritisk, har man imidlertid konkludert med at for de fleste av funksjoner vil en svikt i IT-systemene neppe få slike konsekvenser at det kan karakteriseres som samfunnskritisk. Dette har sammenheng med at IT-avhengigheten enten er liten, at få blir berørt eller at skadeomfanget vil være begrenset og i mindre grad påvirke vitale samfunnsmessige funksjoner.

Dog er det tre områder/funksjoner innenfor Kystverkets ansvarsområde som skiller seg ut og som må gjøres til gjenstand for nærmere vurdering. Dette er :

1. Meldings- og informasjonsfunksjonen (M&I) i kystforvaltningen.
2. Kystverkets DGPS nett.
3. Trafikksentraler (VTS).

3.5.3.1. Meldings- og informasjonsfunksjonen (M & I)
Dette er en ny funksjon som skal, slik det er bestemt av Stortinget, koordinere meldings- og informasjonsflyten i kystforvaltningen. Funksjonen ivaretar anløpsmeldinger for skip, farlig last rapportering, losformidling, radarinformasjon mv. M&I funksjonen skal rapportere data til blant annet politi, havner og tollmyndigheter. NAVCO-tjenesten (meldinger til de sjøfarende om avvik og farer) er en viktig del av M&I-funksjonen. M&I funksjonen skal være fullstendig elektronisk. Innenfor denne sektoren er ett av stikkordene effektiv meldingsflyt, noe som ikke er realiserbart uten digitale systemer. Det er lagt opp til at man har backup på meldinger og doble systemer der det er kritisk. Manuelle systemer er i bruk i dag, og vil inntil videre kunne ta unna til en viss grad. Man baserer seg da på at man har telefon- og faksforbindelse til de forskjellige parter.

Stans av en slik tjeneste når den er ferdig etablert vil medføre vanskelig tilgang på informasjon. Man kan tenke seg et scenario der et skip går på grunn, og det er umulig i løpet av kort tid å finne ut om skipet fører farlig eller forurensende last. Det mest sannsynlige scenario er brudd på teleforbindelsen eller korte serveravbrudd, der informasjonen vil være på lufta etter kort tid.

Herunder er det viktig at man dobler opp de mest kritiske delene av tjenesten som er servere og kommunikasjonsutstyr. Opprettelse av avbruddsfrie strømforsyninger er også viktig. I tillegg må det etableres en brannmur slik at ikke uvedkommende slippes inn i datasystemene.

3.5.3.2. Kystverkets DGPS nett.
Dette er en tjeneste som benyttes av flere og flere fartøy for nøyaktig navigering i norske farvann. Kystverkets tjeneste er i dag basert stort sett på single-dekning. Dette betyr at en stasjon dekker et vist geografisk område. Kystverket har 12 slike stasjoner langs kysten. Etter hvert som tjenesten blir mer og mer stabil, stoler flere på tjenesten. DGPS brukes i dag i stor utstrekning sammen med elektroniske sjøkart til navigering. Hvis DGPS benyttes har man en nøyaktighet på 5 meter, mens man med GPS alene har en posisjonsnøyaktighet på 100 meter. Dette betyr at hvis korreksjonssignalene blir borte mens man navigerer i trange farvann så vil sjansen for havari være betydelig større. Godt sjømannskap tilsier at man ikke skal stole på et system alene, men det viser seg at når et system blir stabilt så vil en båtfører sette sin lit til det, og gi det en uforutsett stor vekt.

Avhengighet av IT systemer
Kystverket benytter seg av IT-utstyr for utregning av korreksjonssignaler. Dette medfører at hvis IT-utstyret er nede, så vil det ikke gå korreksjoner ut på lufta. Det er installert backup-systemer på hver stasjon som tar over hvis hovedsystemet feiler, men usikker strømforsyning, usikre teleforbindelser og andre faktorer ute på fyrene gjør installasjonene sårbare. Ved bortfall av korreksjonssignalene vil fartøyførerne benytte andre navigasjonshjelpemidler. Sannsynligheten for driftsavbrudd er relativt høy. Stans i systemet vil føre til at navigasjon ved bruk av GPS blir vesentlig mer unøyaktig. Dette kan øke sannsynligheten for havari i trange farvann. Det mest sannsynlige scenariet er bortfall av strømforsyning på fyrene og programstopp. Lyn er også en faktor som kommer inn og som vil føre til lengre driftsstans.

Tiltak og strategi
Herunder er det viktig at man dobler opp de mest kritiske delene av tjenesten. Dette betyr at hvis man vil sikre kontinuerlig dekning så bør det etableres dobbelt så mange stasjoner slik at 2 stasjoner dekker samme område.

3.5.3.3. Trafikksentraler (VTS)
Trafikksentraler er utbygd i Brevik, Fedje og Oslofjorden. En trafikksentral på Kvitsøy er under utbygging. Hovedformålet til trafikksentralene er å ha døgnkontinuerlig oversikt over trafikken til sjøs i deres respektive geografiske områder. Trafikksentralene har radardekning over hele dekningsområdet, og har mye samme funksjon som et flyplass-kontrolltårn.

Avhengighet av IT systemer
Innenfor denne sektoren er et av stikkordene effektiv meldingsflyt, noe som ikke er realiserbart uten digitale systemer. Det er mulig å utføre en del av oppgavene manuelt. Man baserer seg da på at man har telefon og faks-forbindelse til de forskjellige fartøyene.

Stans av en slik tjeneste når den er ferdig etablert vil medføre vanskelig tilgang på informasjon. Av sikkerhetskritisk informasjon er rapportering av farlig last et sentralt element.

Tiltak og strategi
Herunder er det viktig at man dobler opp de mest kritiske delene av tjenesten som er servere og kommunikasjonsutstyr. Dette er gjort for de trafikksentralene som er etablert

3.5.4. Trafikk i luften

3.5.4.1. Luftfartstilsynet
Luftfartstilsynet forvalter en omfattende portefølje av ulike IT-systemer som er sentrale i myndighetsutøvelsen. De systemene som har størst betydning for tilsynet og dermed samfunnet direkte er Norges luftfartøyregister, Luftfartssystemet og Sertifikatregistret. Alle disse er basert på IT-systemer. Tilsynet vurderer at det vil få store konsekvenser for tilsynet dersom disse IT-systemene skulle bli utsatt for villede eller ikke-villede angrep. Tilsynet vil derfor sette i gang et prosjekt i løpet av høsten 2000 med målsetting å bedre IT-sikkerheten i systemene.

3.5.4.2. Luftfartsverket
Luftfartsverket forvalter en rekke administrative og operative systemer knyttet til operasjonen av norsk luftfart. Disse systemene er i stor grad basert på og avhengig av moderne IKT. For å drive operativ kontroll med aktiviteten i luften over hele landet er det også behov for å knytte IT-systemene sammen i landsomfattende nettverk. Ulike typer telekommunikasjonsløsninger utgjør dermed en svært viktig ressurs i Luftfartsverkets operative drift.

IKT-systemer inngår som helt vitale i blant annet følgende funksjoner:
- Etablering av grafisk luftromsbilde for å gi flygelederne ved kontrollsentraler og lufthavner oversikt over fly i luften eller under landing.
- Integrasjon av ulike radar- og identifikasjonssystemer som brukes som kildeinformasjon for etableringen av luftromsbilde.
- Radiosystemer for kommunikasjon med fly i luften og på bakken.
- Navigasjonshjelpemidler for fly i luften og under innflyging.
- Informasjonsutveksling med lufttrafikktjenestene i andre land.

I tillegg kommer en rekke IKT-systemer som er av noe mindre betydning, men som likevel kan skape forstyrrelser i trafikkavviklingen dersom de skulle svikte. Ett eksempel er IKT-basert bagasjehåndtering.

Luftfartstjenesten er dermed svært avhengig av velfungerende telekommunikasjon og IT-systemer for øvrig. Det vil likevel være mulig å drive trafikkavvikling selv om enkelte av funksjonene skulle svikte, blant annet ved å operere gjennom forhåndsplanlagte prosedyrer. Effektiviteten i trafikkavviklingen vil imidlertid kunne bli svært lav. Skjer en svikt på et uheldig tidspunkt i en pågående trafikkavvikling kan utfallet bli svært alvorlig. IKT-systemer er også helt nødvendig for moderne flys evne til å fungere som fly, flyets navigasjonsmuligheter og kommunikasjon med andre fly og luftromskontroll på bakken.

Luftfartsverket har i lengre tid arbeidet med sikkerhet og sårbarhetsanalyse. Som medlem av ICAO er Norge forpliktet til å følge internasjonale krav til sikkerhet, integritet og kontinuitet. For alle Luftfartsverkets operative og administrative IT-systemer blir det derfor gjennomført risiko- og sårbarhetsanalyser. Det er utarbeidet kvalitetssikringsmanualer for alle regioner og i hovedadministrasjon. Luftfartsverket arbeider også med å lage en håndbok og prosedyrer for sikkerhetsledelse.

I henhold til Luftfartsverkets skjema for registrering av risiko og sårbarhet vurderes ulike former for IT-relatert uønsket hendelse mot systemene å få konsekvens for mennesker og helse. Følgende hendelser er klassifisert med konsekvens *en viss fare* eller høyere:

- Telekommunikasjon inn til eller ut av lufthavnen feiler eller degraderes: Dette vurderes å kunne få kritisk betydning for både mennesker og helse. Sannsynligheten vurderes imidlertid som lav.
- Navigasjonssystemet for innflyging fungerer ikke: Dette vurderes å kunne få kritisk betydning for mennesker og helse. Sannsynligheten vurderes også her for å være lav.

3.5.5. Spesielle problemstillinger knyttet til godstrafikk

Situasjonen er en noe annen for godstrafikken enn for persontrafikken, det være seg på veg, bane, luft eller sjø. I tillegg til den sårbarheten som de forskjellige trafikkformene har i seg selv, har man innenfor godstrafikken en sårbarhet som er knyttet til IT-basert logistikkstyring (flåtestyring). Måling/veiing og scanning av gods, samt databaser som holder oversikt over hvor i systemet godset er, er alle sårbare for svikt i sine IT-systemer. Til en viss grad kan noe av godset bringes videre, men i tilfeller hvor transport og logistikkstyring er avhengig av IT, vil dette være svært vanskelig. Logistikksystemene er dessuten ofte koblet mot Internett, noe som er med på å gjøre systemene åpne for uautorisert inntrenging og manipulering.

3.5.6. Konklusjon

Konklusjoner for transportsektoren:

	Sannsynlighet for svikt			Konsekvenser av svikt		
Funksjon	Lav	Middels	Høy	Lav	Middels	Høy
Trafikk på vei[A]		X		X		
Trafikk i luft						
1. Samband	X			X		
2. Navigasjon	X				X	
3. Trafikkstyring	X					X
Trafikk på bane[B]						
1. Kjørestrøm		X		X		
2. Signalsystemer	X					X
3. Telesystemer	X					X
Trafikk på sjø						
1. Melding/informasjon		X			X	
2. DGPS nettet		X		X		
3. Trafikksentraler		X			X	
Godstrafikk[C]						
1. Logistikk/godsstyring		X			X	

Tabell 3.5 Konklusjoner for transportsektoren.

[A] Vegvesenet har "daglig" svikt i ulike system et eller annet sted i landet, men det har meget sjelden innflytelse på trafikken i vesentlig grad. Konsekvenser kan bli en noe redusert sikkerhet for trafikantene.

- Mørklagte tunneler øker sjansen for uhell.
- Svikt i nødtelefonsystem eller alarmanlegg reduserer varslingsmuligheter dersom uhell oppstår.
- Svikt i trafikksignalanlegg vil kunne føre til tregere trafikkavvikling i viktige kryss. Trafikkregler gjelder for slike situasjoner. Vikepliktskilt eller høyreregelen.

[B] Det er vurdert sannsynlighet for at ett enkelt system vil svikte. Sannsynligheten for at et system vil svikte er i stor grad avhengig av hvor mye redundans som er bygget inn i IT-systemene. Det er i størst grad bygget inn redundans i signal- og telesystemene. Konsekvensen av en feil vil være svært forskjellig avhengig av hvilket system som feiler og hvor dette er plassert.

For de IT-avhengige kjørestrømsystemene finnes det andre systemer og manuelle rutiner som kan benyttes og som begrenser konsekvensen av en feil. For signalsystemene er de IT-avhengige systemene stort sett å finne i Oslo-området og på strekninger med stor trafikk. Feil på ett av disse vil kunne føre til store konsekvenser dersom det skjer på et tidspunkt med stor trafikk. Telesystemene er en viktig del av både kjørestrøm- og signalsystemene. En feil i telesystemene kan få store konsekvenser dersom det skjer i en viktig forbindelse for en strekning med stor trafikk.

[C] Konsekvenser ved kortvarig svikt i logistikk/godsstyring som følge av svikt i IT-systemer vurderes til å være middels. Ved langvarig svikt vurderes konsekvensene for samfunnet til å bli høye.

3.6. Olje- og gassektoren

Kapittelet om IT-sårbarhet i petroleumssektoren er i hovedsak basert på Oljedirektoratets erfaringer i forbindelse med tilsynsvirksomheten på den norske kontinentalsokkelen. Oljedirektoratet har opparbeidet betydelig innsikt i aktuelle problemstillinger i forbindelse med IT-avhengighet og –sårbarhet, og i det etterfølgende gis en generell og overordnet fremstilling av saksfeltet og hvordan sektoren i stor grad har planlagt for hendelser hvor IT-utstyr kan svikte. Håndtering av denne type problematikk preger i stor grad hverdagen for operatørene. Det kan bl a nevnes at produksjonsregulariteten på årsbasis for feltene varierer mellom 90 – 98%. De nedstengninger som foretas omfatter både planlagte og ikke-planlagte produksjonsnedstengninger. Selv om en rekke funksjoner og fysiske innretninger er IT-avhengige, er altså sannsynligheten for at IT-feil får innvirkning på leveransene erfaringsmessig relativt liten.

3.6.1. IT-sårbarhet i petroleumsvirksomheten

Krav til virksomheten er hjemlet i petroleumsloven med forskrifter og spesielt er prosess-/sikkerhetsrelatert IT regulert i forskrift om sikkerhets- og kommunikasjonssystemer på innretninger i petroleumsvirksomheten. Forskriften kommer til anvendelse ved planlegging, prosjektering, bygging og bruk av prosess-, sikkerhets- og kommunikasjonssystemer. Innretninger, systemer og operasjoner skal alltid planlegges, utformes og gjennomføres med sikte på at ingen enkeltfeil under bruk skal føre til en fare- eller ulykkessituasjon. Der dette ikke er praktisk gjennomførbart, skal tekniske, operasjonelle eller prosedyremessige tiltak iverksettes for å møte en slik fare- eller ulykkessituasjon.

Typisk for operatørenes IT-infrastruktur er skillet mellom de åpne administrative nettverkene og de lukkede prosessnettene. De administrative nettene har normalt ingen funksjoner knyttet direkte til drifts- og leveransesystemene. Her legges ordinære IT-sikkerhetsrutiner til grunn, som f eks passordbeskyttelse, branndører etc.

Det legges adskillig strengere sikkerhetsrutiner til grunn for prosessnettene. Prosessnettene er kritiske for drift og leveranser. Disse nettene, som i stor grad er adskilte og autonome IT-systemer designet for spesifikke anlegg, er nøye overvåket og preges generelt av meget høye kontroll- og sikkerhetsstandarder. Innretninger med prosessanlegg er alltid utstyrt med prosesskontrollsystemer som styrer og regulerer prosess- og hjelpesystemene på en sikker måte. Systemene har alltid høy pålitelighet. Komponenter og utstyr som inngår i systemet, skal være tilpasset de belastninger de kan utsettes for. Dette gjelder i første rekke mekaniske belastninger, men har også konsekvenser for de krav som stilles til robustheten til den informasjonsteknologi som til enhver tid benyttes. I tillegg til normal operasjon av prosessen (innretningen), er det også sikkerhetssystemer som skal kunne håndtere unormale prosessituasjoner, inkludert lekkasjer, brann og nødavstengning.

Nødavstengningssystemene omfatter det totale system, inkludert manuelle utløsningsstasjoner, ventiler, aktuatorer, rør, akkumulatorer, signaler o l som er nødvendig for hurtig og sikker stansing og seksjonering av prosessen, samt utstyr som er nødvendig for å eliminere tennkilder.

Videre baseres sikkerhetssystemene i stor grad på prinsippet om redundans. Dette betyr at to parallelle systemer må svikte før virksomheten stanser. Et tilsvarende prinsipp for å hindre ulykker er det s k ”fler-barriere-prinsippet”. I praksis vil det si at flere ledd må svikte før en

reell fare oppstår. I tillegg benyttes det s k ”fail-safe-prinsippet" hvor dette er praktisk mulig. Ett eksempel her er nødavstengningsventilene som automatisk går til en forhåndsdefinert sikkerhetsposisjon dersom det oppstår kabelbrudd eller strømutfall.

Innretningene har også nødvendig internt og eksternt kommunikasjonsutstyr. Utstyret og bruken av dette skal på en effektiv og sikker måte ivareta aktuelle kommunikasjonsoppgaver på innretningen og mellom innretningen og landorganisasjonen, så vel under normal drift som i beredskaps- og nødsituasjoner. Videre skal det tilfredsstille nasjonale og internasjonale anerkjente normer for den enkelte innretning, dersom ikke særlige forhold tilsier andre løsninger. For øvrig kommer konsesjonsvilkår i medhold av telegrafloven til anvendelse ved planlegging og anskaffelse av kommunikasjonssystemer om bord i enhver norsk innretning, jf petroleumslovens § 1-5.

3.6.2. Sårbarheten til IT-systemene som anvendes i petroleumsvirksomheten

Den enkelte operatør utarbeider akseptkriterier for å uttrykke et akseptabelt risikonivå i virksomheten. Akseptkriteriene utformes med hensyn til så vel sannsynlighet for som konsekvens av identifiserte ulykkeshendelser. På grunnlag av akseptkriteriene velges det en dimensjonerende ulykkeshendelse. Med dette menes en ulykkeshendelse som i henhold til de definerte akseptkriteriene representerer en uakseptabel risiko, og som derfor legges til grunn for utforming og bruk av innretninger og gjennomføring av virksomheten for øvrig. Sikkerhetssystemene skal alltid utformes/beskyttes slik at funksjonsdyktigheten opprettholdes i nødvendig tid ved en dimensjonerende ulykkeshendelse. De vurderinger som legges til grunn for akseptkriteriene må alltid dokumenteres gjennom risikoanalyser i h t Oljedirektoratets forskrift for gjennomføring og bruk av risikoanalyser i petroleumsvirksomheten (analyseforskriften).

Identifiserte ulykkeshendelser,sammenholdt med operatørens akseptkriterier, vil således kunne klarlegge hva som er tilstrekkelige sikkerhetssystemer for den enkelte innretning. Dette vil kunne variere noe avhengig av hvilken type innretning det er snakk om, f eks om det dreier seg om en produksjonsinnretning, flyttbar boreinnretning, ubemannet innretning eller undervannsinnretning osv.

Prosessystemene testes og kvalitetssikres meget grundig før anleggene settes i drift. Dette gjelder både for menneske-maskin-kommunikasjon og mot ev. feil som introduseres i forbindelse med systemendringer i driftsfasen. Behovet for endringer i driftsfasen varierer fra operatør til operatør. Utfordringen ligger i å beholde systemenes integritet i forbindelse med slike endringer. Operatørene og IT-leverandørene har utviklet gode kvalitetssikringsrutiner på dette området. Menneske-maskin-kommunikasjon er for øvrig et sentralt område i Oljedirektoratets tilsynsvirksomhet.

Dersom uønsket nedstengning av utstyr kan medføre risiko i seg selv, kan utstyret unntas automatisk nedstengning. Eksempel på slikt utstyr kan være dynamisk posisjoneringsutsyr og utstyr i forbindelse med brønnaktiviteter mv. Denne type utstyr er i så fall utstyrt med egne manuelle nedstegningssystemer, og det skal være utarbeidet prosedyrer for slike situasjoner.

Av de opplysninger som foreligger om IT-svikt i petroleumsvirksomheten, fremgår det at dette oftest skyldes kortslutning, dårlig kontakt, disc-feil eller prosessor-feil. Slike feil oppstår enkeltvis, og kan ramme ett system, men vil neppe komme samtidig i flere systemer. Som

regel kan denne type feil rettes opp raskt ved hjelp av service-personell og reservedeler (alternative back-up systemer). Tiden som medgår før problemet er løst vil som regel være relativt kort, og fører normalt ikke til produksjons- og leveranseproblemer.

Et annet årsaksforhold kan være dårlig kontraksjon av IT-systemet, enten av utstyret eller programvaren, eller det er programmert med bristende logikk slik at en uheldig kombinasjon av uforutsette omstendigheter kan forårsake feil håndtering av informasjonen. Slike feil vil som oftest opptre isolert, men kan under visse omstendigheter (for eksempel ved skuddår) være gjengangere i mange systemer samtidig. En diversifisering av systemleveradører, ulik teknologigenerasjon og ulike teknologikombinasjoner for å unngå spredning av slike feil, vil redusere sannsynligheten for denne type feil. Erfaringen fra overgangen til år 2000 viste dessuten at leveransene av olje og gass var upåvirket av enkeltproblemer som oppstod. (De feil som ble registrert ble for øvrig i tillegg korrigert før selve tusenårsskiftet inntraff.)

En annen årsakskategori for IT-feil er bevisst sabotasje. Det kan ikke utelukkes at utro tjenere har interesse av å påføre IT-systemene feil som kan føre til produksjonstap, selv om sannsynligheten her er liten. Oljeselskapenes sikkerhetsrutiner knyttet til adgangskontroll og passordbeskyttelse, samt andre kontrollrutiner, er imidlertid laget for å minimalisere mulighetene for så vel intern som ekstern sabotasje (virus og hackere).

Imidlertid har selskapene (og Oljedirektoratet) back-up-rutiner som gjør at ethvert datagrunnlag i stor grad kan gjenopprettes dersom IT-feil oppstår. IT-feil vil i all overveiende grad oppdages umiddelbart. Beslutninger og handlinger utsettes til feilen er rettet opp. Produksjonen kan imidlertid påvirkes dersom logistikken svikter mht. å ha tilstrekkelig reservedeler og personell tilgjengelig for å unngå lange nedstengninger. Denne problemstillingen er imidlertid under kontinuerlig evaluering hos operatørselskapene for å sikre at den optimale balanse av reservedelsbeholdninger, back-up-systemer og personell offshore/onshore opprettholdes.

3.6.3. IT-sårbarhet i forhold til leveranseregularitet av olje og gass

Olje- og gassinstallasjoner er spredt over et stort område på den norske kontinentalsokkelen, med bl.a. et undersjøisk transportnett som består av tusenvis av kilometer med rørledninger fra Norge til terminaler på kontinentet og i Storbritannia. Produksjonssystemet omfatter et komplisert samspill mellom plattformer, ilandføringsrør og landingsterminaler i Norge og i andre land. Dette sikrer høy utnyttelse av produksjonssystemet, med høy utvinningsgrad og kostnadseffektivitet som resultat. Det sikrer i tillegg fleksibilitet og handelfrihet i fremføringen av leveransene dersom noe uforutsett skulle oppstå, som f eks svikt i IT-systemer.

Hovedsakelig eksporteres all olje og gass som produseres på norsk kontinentalsokkel. Kun 5-10 % av samlet oljeproduksjon går til de norske raffineriene. Et forsyningsmessig avbrekk vil få minimale konsekvenser for det norske samfunn på kort sikt.

Det er visse forskjeller mellom henholdsvis olje- og gassleveransene som bør nevnes i en slik sammenheng. Oljen dekker en mye større andel av den totale energietterspørselen enn gass. Oljeindustrien er en global industri med et meget godt utbygd distribusjonsnett med flere alternative transportmåter, hovedsakelig skip.

Distribusjon av gass skiller seg vesentlig fra salg av olje. Gass omsettes typisk på langsiktige kontrakter, og transporteres i rørledninger. Dette innebærer at distribusjonsnettet både fra selger- og til kjøperland og videre til enkeltkonsumenter er fastlagt. Selv om transportnettet er statisk, er det imidlertid en viss fleksibilitet for omruting dersom svikt eller feil skulle oppstår i deler av transportsystemet. Fleksibiliteten vil ytterligere bedres etterhvert som nye gassfelt bygges ut, nye rørledninger legges og transportnettverk i ulike regioner kobles sammen. Fleksibiliteten og omrutingsmulighetene i distribusjonssystemene alene, kan være tilstrekkelig for å opprettholde leveranseregularitet i en rekke tenkelige situasjoner, også ved IT-svikt i delsystemer.

Rent IT-messig, er det konsekvente skillet mellom de mer åpne administrative nettverkene og de lukkede prosessnettene - som styrer produksjons- og leveransesystemene - med på å forsterke robustheten og minske sårbarheten i petroleumsvirksomheten. Det er i praksis små muligheter for at IT-svikt ett sted i kjeden kan få avgjørende konsekvenser for totalleveransene fra norsk kontinentalsokkel. Imidlertid vil IT-svikt ved spesielle transport- og leveransekoordineringssentre på fastlandet kunne medføre at formidlingen av leveranseoppdrag hemmes og at transportsystemene utnyttes dårligere i den perioden svikten varer.

Videre finnes det sentrale knutepunkter i transportsystemet som må anses å være mer kritiske enn andre. Flere systemer vil her ikke kunne erstattes på kort sikt av andre systemer. Til en viss grad kan man kompensere med prosedyrer, men ikke på en slik måte at man opprettholder full kapasitet i reparasjonsfasen dersom et slikt knutepunkt rammes av IT-svikt.

3.6.4. Trender innen anvendelse av IT i petroleumsvirksomheten

Utviklingen av både teknologi og arbeidsprosesser fører til at driften av anleggene blir mer effektiv. Nye fiberkabler som knytter innretningen sammen til landorganisasjonen gjør at stadig flere oppgaver som tidligere ble gjort på plattformene, nå kan utføres på land. Dette kan føre til at også de rent operative oppgavene (selve prosesstyringen og -overvåkningen) utføres fra land. Totalt sett kan vi derfor si at næringen er mer IT-sårbar enn tidligere. Imidlertid må det her fortsatt skilles mellom de administrative nettverkene og prosessnettene. Det er prosessnettene som har umiddelbar betydning for drift og leveranser, og disse vil fortsatt i høy grad være lukkede systemer som det normalt ikke er mulig å koble seg på utenfra.

De elektroniske kommunikasjons- og sambandsløsningene gjennom Internett og bransjenett, som i økende grad utvikles mellom oljeselskap og leverandør for å skape kosteffektive løsninger for kompetanseutnyttelse og optimalisering av systemutnyttelsen, kan imidlertid øke sannsynligheten for at et problem kan forflytte seg fra selskap til selskap. Det blir imidlertid fokusert meget sterkt på tiltak for å motvirke dette når slike løsninger tas i bruk.

I tilknytning til utvikling og anvendelse av IT innen petroleumsvirksomheten, er det et vesentlig poeng for oljeselskapene å øke tilgangen på dybdekompetanse for vurdering av spesielle problemer og feil. Systemleverandørene spiller normalt en vesentlig rolle i livsløpet til et IT-system, spesielt ved systemendringer og driftsoptimalisering (best mulig utnyttelse av allerede eksisterende IT-systemer). Samarbeidet mellom leverandørene og industrien er derfor her vesentlig og utvikles i stadig større grad, f eks gjennom online-kommunikasjon. I tillegg

utvikler operatører som benytter samme systemleverandører et kostnadseffektivt samarbeid på tvers av selskapsstrukturer med hensyn til reservedeler og driftsstøtte (dybdekompetanse).

Det er også viktig å skape og vedlikeholde fora for erfaringsutveksling. Markedet i Norge er volummessig lite, og preges av få leverandører. Dette gir relativt god oversikt over generelle problemstillinger relatert til IT-systemene. Aktørene innen petroleumssektoren, inkludert operatører, leverandører, forskningsinstanser og Oljedirektoratet har f eks i en årrekke samarbeidet gjennom PDS-prosjektet (Pålitelighet i Datamaskinbaserte Sikringssystemer) i regi av SINTEF. Dette prosjektet ble startet mot slutten av 1980-årene og videreføres i dag som en bruker-/interessegruppe. Hensikten med prosjektet var å utvikle en modell for pålitelighetsvurdering av IT-baserte sikkerhetssystemer. I dag er det primært et forum for erfaringsutveksling i IT-sikkerhetsspørsmål.

Videre er det en viktig oppgave å skape formelle sikkerhetsstandarder. Her er ikke minst IEC 61508 Functional safety of electrical/electronic/programmable electronic safety related systems, sentral. Fokuset i standarden er rettet mot sikkerhetssystemer. Implementering av standarden er i ferd med å gjennomføres både nasjonalt og internasjonalt. Den er f eks benyttet som anerkjent standard i forslaget til nye forskrifter for petroleumsvirksomheten. Standarden vil ventelig kunne gi en mer enhetlig tilnærming til alle faser i livsløpet til et IT-system.

3.6.5. OEDs vurdering av petroleumsvirksomhetens IT sårbarhet

Petroleumsvirksomheten reguleres gjennom petroleumsloven og et meget omfattende, systematisk og tverrsektorielt regelverk, hvor sikkerhet og beredskap er høyt prioritert. Den innebygde driftssikkerheten er meget høy. Man har tatt høyde for et vidt spekter av potensielle fare- og ulykkessituasjoner. Den enkelte innretning og de driftssystemer som anvendes er således i utgangspunktet meget robuste.

I sikkerhetsforskriften ligger det videre krav til at driftstilgjengelighet skal inngå i grunnlaget for definering av petroleumsvirksomhetens krav til beredskap. Dette innebærer blant annet at leveranseavtaler er av betydning for hvilke beredskapskrav som defineres for virksomheten. Driftstilgjengeligheten og beredskapsspesifikasjonene til en innretning som inngår i et større produksjons- og transportsystem utformes alltid med tanke på øvrige deltakere i dette systemet. Det legges derfor store ressurser i bl a å utvikle pålitelige IT-systemer som sikrer høy grad av fleksibilitet og handlefrihet i produksjons- og transportsystemene og dermed også høy grad av leveranseregularitet. Anvendelsen av lukkede, autonome prossesnettverk for den enkelte innretning er her med på å sikre den samlede driftssikkerheten ved at IT-svikt ett sted ikke får alvorlige konsekvenser for systemet som helhet.

Systemer for kompetansesikring, organisert erfaringsutveksling i IT-sikkerhetsspørsmål og utvikling av formaliserte sikkerhetsnormer og -standarder er vesentlige strategier for å motvirke IT-sårbarhet i petroleumsvirksomheten.

3.6.6. Konklusjon

Konklusjoner for petroleumssektoren:

	Sannsynlighet for svikt			Konsekvenser av svikt		
Funksjon	Lav	Middels	Høy	Lav	Middels	Høy
Produksjonsfunksjon: Boring, seperasjon	**X**				**X**	
Prosessfunksjon: Landanlegg	**X**					**X**
Transportfunksjon: Rør, kompresjon	**X**			**X**		
Transportfunksjon: Knutepunkter	**X**				**X**	
Mottak: Måling	**X**			**X**		
Mottak: Fleksibilitet, omruting	**X**					**X**
Leveranseregularitet, Olje	**X**			**X**		
Levaranseregularitet, Gass	**X**				**X**	

Tabell 3.6 Konklusjoner for petroleumssektoren.

3.7. Bank- og finanssektoren

Betalingssystemet i Norge kan deles i tre hovednivåer,

(i) betalingstjenester for overføring av kontanter og kontopenger mellom privatpersoner, bedrifter og offentlige organer,

(ii) avregningssystemer for interbanktransaksjoner, verdipapirhandler og derivathandler og

(iii) betalingsoppgjør mellom bankene.

Disse tre hovednivåene utgjør en hierarkisk struktur der alle betalingstransaksjoner, som ikke gjøres opp ved bruk av kontante betalingsmidler, til sist gjøres opp enkeltvis eller som avregnede nettoposisjoner ved overføringer/oppgjør mellom bankenes konti i en oppgjørsbank, hovedsakelig Norges Bank.

Deltakerne i betalingssystemet er bankene, datasentraler og Norges Bank. Bankene og datasentralene er selvstendige selskaper med ansvar for egen virksomhet, herunder driften av egne datasystemer. I denne sammenheng har Verdipapirsentralen og Norsk Oppgjørssentral bl.a. en funksjon som datasentraler i verdipapirsektoren.

Norges Banks virksomhet er regulert i lov om Norges Bank og pengevesenet der det bl.a. fremgår at sentralbanken skal fremme et effektivt betalingssystem innenlands og overfor utlandet. Betalingsoppgjøret i Norges Bank skjer gjennom sentralbankens oppgjørssystem på grunnlag av nærmere regler og avtaler. I Norges Banks oppgjørssystem gjøres det daglig opp transaksjoner til en samlet verdi i størrelsesordenen 150 – 200 milliarder kroner.

Kredittilsynet skal se til at institusjonene i sektoren virker på hensiktsmessig og betryggende måte. Tilsynet skal bidra til betryggende soliditet, risikobevissthet, styring og kontroll i institusjonene. Videre skal det avdekke forhold som truer stabiliteten i det finansielle system og ha beredskap for håndtering av problemer i finanssektoren.

Lov om betalingssystemer m.v. ble vedtatt 17.12.1999, men er ennå ikke trådt i kraft. Loven beskriver ansvarsfordelingen slik at Norges Bank godkjenner interbanksystemer, Kredittilsynet godkjenner verdipapiroppgjørssystemer og fører tilsyn med systemer for betalingstjenester. Oppgavefordelingen mellom Norges Bank og Kredittilsynet i forhold til IT-sårbarhet og beredskap er i ferd med å bli sortert i henhold til de overordnete prinsippene.

3.7.1. Hovedutfordringer

Den sentrale utfordringen i utviklingen av betalingssystemet er avveining mellom hensynene til effektivitet og sikkerhet. Et moderne betalingssystem skal kunne behandle store transaksjonsmengder på kort tid og med høy grad av sikkerhet for betalere, betalingsmottakere og banker.

Effektiviteten i det norske betalingssystemet har økt med utviklingen av datateknologiske løsninger som har ført til større grad av automatisering i betalingsformidlingen. Samtidig har innføring av kostnadsorientert prising av betalingstjenester også bidratt til større effektivitet. Denne utviklingen kommer til uttrykk ved at bruk av elektroniske og kundebetjente betalingstjenester øker sterkt og bruk av papirbaserte betalingsinstrumenter avtar. Tilsvarende øker bruk av minibanker til uttak av kontanter, mens uttak over skranke i bankene avtar.

På den andre siden fører denne utviklingen til at bank- og finanssektoren er svært avhengig av IT-systemer som igjen er basert på tilgang til telekommunikasjon og strømforsyning. Betalingsoppdrag og finansielle transaksjoner passerer gjennom systemene til flere aktører i finansiell sektor. Funksjonsdyktigheten til et moderne betalingssystem er således avhengig av at den finansielle infrastrukturen fungerer, og at deltakerne i systemet utfører sine oppgaver og innfrir sine forpliktelser som forutsatt.

I tillegg til utfordringene innenfor dagens betalingssystemer, stilles det nye krav til sikkerhet og sårbarhet som følge av utbredelsen av Internett og elektronisk handel. Sårbarheten kan være større og sikkerheten svakere i den kommersielle delen av elektronisk handel enn i den finansielle delen. Økt anvendelse av betalingsmåter i åpne nett, stiller nye utfordringer og krav til tillit og sikkerhet.

3.7.2. Gjennomførte tiltak

I lys av utviklingen i moderne betalingsformidling har myndigheter og aktører lagt større vekt på å gjennomføre tiltak for å redusere sårbarheten i systemene for formidling, avregning og oppgjør av betalingstransaksjoner. Hver enkelt aktør har et selvstendig ansvar for egen drift, herunder beredskap for å håndtere avvikssituasjoner. Dette kan innebære etablering av

reserveløsninger ved eventuelle driftsavbrudd, alternativ strømforsyning, alternative telekommunikasjonslinjer og lignende. Videre har hver enkelt aktør et ansvar for å håndtere egen operasjonell risiko i betalingsoppgjøret knyttet til kreditt-, likviditets- og markedsrisiko.

For å bidra til kontinuerlig drift i betalingssystemet er det, i et samarbeid mellom myndigheter og finansnæringen, utredet mulige tiltak for å redusere sårbarheten i de felles systemene i finansiell infrastruktur. En arbeidsgruppe som ble oppnevnt av koordineringsorganet for finansiell beredskap, og som hadde ledelse fra Norges Bank og deltakere fra banknæringen og Posten Norge BA, la i januar 1998 frem en rapport med følgende fem forslag til sårbarhetsreduserende tiltak i prioritert rekkefølge:

i) Etablere et sentralt beredskapsråd for betalingsformidlingen
ii) Etablere beredskapsplaner for alternative betalingsmåter
iii) Utrede betalingsformidlingens prioritet til telekommunikasjon og elektrisk kraft
iv) Økt vekt på informasjon og beredskapstiltak for NBO[13] og NICS[14]
v) Plan for disponering og koordinering av nøkkelkompetanse

Forslag i) er fulgt opp ved at det i juni 1999, i samråd med Finansdepartementet og sentrale aktører i finansiell infrastruktur, ble etablert et sentralt beredskapsorgan for kontinuitet i den finansielle infrastruktur. Dette kontinuitetsorganet, som har ledelse og sekretariat fra Norges Bank og medlemmer fra aktørene i betalingssystemet og Kredittilsynet, har ansvaret for å komme frem til og koordinere tiltak for å løse krisesituasjoner og andre situasjoner som kan resultere i store forstyrrelser i den finansielle infrastruktur. I en krisesituasjon skal organet varsle og informere berørte aktører og myndigheter om hvilke problemer som har oppstått og hvilke tiltak som settes i verk for å løse problemene.

Kontinuitetsorganet skulle i første omgang være forberedt på å håndtere eventuelle problemer i forbindelse med overgangen til år 2000. Etter årsskiftet arbeides det med sikte på å videreføre kontinuitetsorganet med utvidet mandatet og endret sammensetning. Videre er det foreslått at kontinuitetsorganet endrer navn til "Beredskapsutvalg for finansiell infrastruktur". Siktemålet er at beredskapsutvalget vil erstatte eksisterende beredskapsorganer i finansiell sektor.

Som oppfølging av forslag ii) oppnevnte sentralt koordineringsorgan for finansiell beredskap/bank- og pengevesen i august 1998 en arbeidsgruppe for alternative betalingsmåter med oppgave å utarbeide forslag til beredskapsplaner for å gjennomføre betalingsformidlingen dersom krisesituasjoner rammer de ordinære betalingssystemene. Arbeidsgruppen har hatt ledelse og sekretariat fra Norges Bank og har for øvrig bestått av medlemmer fra banknæringen, Posten Norge BA og Norges Bank. Arbeidet i denne gruppen ble midlertidig innstilt i april 1999 på grunn av prioriteringen av arbeidet med år 2000 beredskap.

Forslag iii) er fulgt opp ved at kontaktpersoner fra Norges vassdrags- og energidirektorat og Telenor er knyttet til kontinuitetsorganet. I forbindelse med utarbeidelsen av beredskapsplaner for overgangen til år 2000 kom det frem at Telenor i sine beredskapsplaner

[13] NBO: Norges Banks oppgjørssystem.
[14] NICS: "Norwegian Interbank Clearing System" er bankenes felles avregningssystem som drives av Bankenes Betalingssentral.

behandler betalingsformidlingen som en viktig samfunnsfunksjon som skal gis prioritet ved retting av eventuelle feil. Norges Bank vil være kontaktpunkt mellom aktørene i finansiell infrastruktur og Telenor dersom det oppstår problemer med telekommunikasjon i finansiell infrastruktur av en slik karakter at de kan få samfunnsmessige skadevirkninger.

Beredskap innen strømforsyning blir i første rekke ivaretatt ved at de sentrale aktørene har egne aggregater for nødstrøm. Dersom det oppstår ubalanser i kraftmarkedet som varer i flere timer, har Statnett fullmakt til å gi direktiver om prioriteringer av kraftleveransene. Ved mer langvarige problemer i kraftmarkedet fastsettes prioriteringen gjennom beredskapsplaner fra Olje- og energidepartementet der håndhevelsen er overlatt de lokale nettselskapene. I slike tilfelle ligger samfunnsmessige hensyn til grunn for prioriteringene av kraftleveransene, bl.a. hensyn til liv og helse, telekommunikasjon, vannforsyning og andre vitale samfunnsfunksjoner. For øvrig har de lokale nettselskapene ansvaret for feilretting i den lokale strømforsyningen.

For øvrig ivaretas hensynene til informasjon og beredskapstiltak for NBO og NBO/NICS gjennom det løpende arbeidet med å videreutvikle disse systemene, herunder utarbeidelse av beredskapsplaner og reserveløsninger, jf forslag iv**)**.

Risiko- og sårbarhetsanalysen fra januar 1998 dekket de sentrale elementene i den finansielle infrastruktur. Kredittilsynet har ut fra sitt ansvar i begynnelsen av år 2000 startet prosjektet ”Risiko- og sårbarhetsanalyse av finansnæringens IT-infrastruktur”. Dette prosjektet ser på bredden av infrastruktur som også omfatter de ulike systemer for betalingstjenester.

Et mandat foreligger for prosjektet hvor de enkelte avdelinger i Kredittilsynet skal delta. Prosjektet består av to deler, først en kartleggingsdel av IT-infrastrukturen, videre skal det på bakgrunn av denne utføres en risiko- og sårbarhetsanalyse. Kartleggingen skal være ferdig 01.10.2000 august og sårbarhetsanalysen skal avsluttes innen 01.12.2000.

Finansnæringens IT-infrastruktur vil omfatte de datasystemer og nettverk, samt administrasjon, utvikling, drift, vedlikehold og sikring av de systemer som institusjonene under tilsyn besitter. Arbeidet skal danne grunnlag for utvikling av regelverk og tilsynsprogrammer. En ny IT-forskrift er planlagt ferdig i 2001.

Risiko- og sårbarhetsanalysen omfatter spesielt nye teknologier og produkter som Internett, EDI, Web-applikasjon servere, sertifikater og smartkort etc.

Rapporten skal konkludere med en oversikt og beskrivelse av de ca. 15 mest kritiske risiki- og sårbarhetsområdene i infrastrukturen sett i forhold til sikkerhet. Rapporten skal også beskrive hvordan resultatene kan påvirke Kredittilsynets fremtidige tilsynsarbeide.

Utfordringene er store for finansnæringen og for Kredittilsynet i forhold de mange endringer som nå skjer i samfunnet. Internettanvendelsene ser ut til å gi varig skifte i måten å utføre forretningsvirksomhet på. Det utvikles nye typer on-line tjenester i bank og finansnæringen, og det etableres nye strukturer for e-handel, e-penger og sertifikater.

3.8. Politisektoren

3.8.1. Politiets hovedoppgaver

Politiets hovedoppgaver er:
1. Opprettholde ro, orden og offentlig sikkerhet
2. Beskytte person, eiendom og fellesgoder
3. Forebygge, avdekke og forfølge kriminell virksomhet
4. Iverksette og organisere redningsinnsats der menneskers liv eller helse er truet
5. Iverksette tiltak for å avverge fare og begrense skade i ulykkes- og katastrofesituasjoner

Politioppgavene er definert i Politiloven §§ 2 og 27, jfr. Politiinstruksen § 2-2. Skulle Politiet miste evnen i vesentlig grad til å være operativ på en eller flere av disse områdene, måtte det anses som kritisk svikt.

Under år 2000-arbeidet ble Politiets hovedoppgaver definert som ikke-kritisk i forhold til IT-avhengighet. Denne vurderingen opprettholdes.

3.8.2. IT-avhengighet i forhold til å opprettholde politiets viktigste funksjoner

Hovedoppgavene til politiet slik de er listet ovenfor i kap. 3, vil i det vesentlige ikke bli berørt av at IT-systemene faller bort. De oppgaver som er nevnt under punktene 1, 2, 4 og 5 er i liten grad avhengig av IT for å kunne opprettholdes.

Å fore*bygge, avdekke og forfølge* kriminell virksomhet vil imidlertid kunne berøres til en viss grad. De to første elementene, forebygge og avdekke kriminell virksomhet er dog foreløpig i relativt liten grad avhengig av IT.

Til oppgaven å *forfølge kriminell virksomhet* brukes IT i forhold til oppsamling av opplysninger, registerbehandling, samt oppfølging og produksjon av dokumenter i straffesaksbehandlingen.

Svikt i IT-systemer vil innebære interne administrative problemer, økte restanser og vanskeligere tilgang til saksopplysninger.

Politiet kan likevel forfølge kriminell virksomhet med tradisjonelle midler. Den såkalte «saksbehandlingsløken» er fortsatt gjeldende i straffesaks-behandlingen, og slike dokumenter kan lages ved hjelp av frittstående PCer.

Den høyere påtalemyndighet vil få noen av de samme problemer i forhold til produksjon av dokumenter innenfor dette området. Avhengigheten til IT-systemer, registre og datanettverk er imidlertid i øyeblikket en god del mindre enn hos politiet, slik at konsekvensen blir enda mindre for påtalemyndigheten. Problemer kan avhjelpes på samme måte som i Politiet.

3.8.3. Nærmere om det å forfølge kriminell virksomhet

Det er således først og fremst registerbehandling, samordning og oppfølging av tilknyttede saker i straffesaksbehandlingen, altså de administrative deler av etterforskningen som i noen grad vil bli berørt av en svikt i relaterte IT-systemer. Totalt sett berører dette relativt få mennesker.

Kvaliteten på tjenesten *forfølge* kriminell virksomhet påregnes altså å kunne bli berørt i negativ retning etter noen tid. Bortfall av noen administrative deler av etterforskningen kan nok likevel rettes opp med et etterslep på to til tre uker. Det er derfor liten grunn til å tro at en svikt i IT-tjenesten vil føre til alvorlig skade/tap i forbindelse med denne funksjonen, hverken for samfunnet, egen virksomhet eller andre.

3.8.4. Sannsynlighet for svikt

Politiet har vurdert de trusler som IT-sårbarhetsprosjektet legger til grunn som sannsynlige. Det synes vanskelig å si noe konkret om risikoen for at slike trusler skal realisere seg. Sagt på en annen måte, er det liten grunn til å tro at Politiet vil være mindre utsatt for slike trusler enn andre.

En vurdering av sårbarheten er hovedgrunnen til at politiet ikke ønsker å kople sitt datanettverk mot eksterne nett på det nåværende tidspunkt.

3.8.5. Særlig om politiets kommunikasjonssystemer

Radio: Politiet benytter seg i dag av to systemer.

a) Konvensjonelt system: Det er et lukket analogt radiosystem som dekker et og et distrikt. Distriktene benytter basestasjoner som er utplassert i Telenors anlegg, Forsvaret, bedrifter og hos private eiere. Basestasjonene er styrt av linjer leid hos Telenor, radiolink eller styrt direkte av radioer for aktivisering. Alle områdene kan kommunisere med nabodistriktene. Kraftforsyningen er det vanlige strømnettet, men de aller fleste har også batteribackup ved strømstans eller tilgang til egen strømgenerator. Systemet er gradvis oppbygd siden midten på 70-tallet og består i dag av ca. 400 basestasjoner, som dekker mesteparten av landet.

b) Edacs er et trunket radiosystem, digitalt og 100% kryptert, som består av siter (opptil 6 basestasjoner på samme sted) styrt av linjer i Telenors nett fra en sentral enhet i systemet. Systemet er utplassert sør i Østlandsområdet (Østfold, Follo, Oslo, Romerike og Asker & Bærum). Systemet kan tillate at alle hører alle, men av hensyn til kapasitet og operative årsaker er dette regulert slik at man benytter egne talegrupper for å kommunisere med andre enheter. Kraftforsyningsmessig er den enkelte basestasjon drevet av det vanlige strømnettet og har backup batterier ved strømstans.

Det fremtidige system TETRA er på mange måter identisk med EDACS og har etter alt å dømme muligens enda mindre sårbarhet enn EDACS.

Telefon: Telefonsystemet er bygd opp med at hver ”selvstendige” lokasjon har egen sentral, egen betjening og egne systemer for backupdrift (4-24 t) ved strømstans. Linjenettet som benyttes er Telenors nett, leide linjer fra andre leverandører etc.

Hvilken betydning har systemene for politietaten?
Radio benyttes til den operative daglige virksomhet mellom mobile enheter og vakta i det enkelte politidistrikt. Telefonsystemet benyttes også i den daglige operative virksomhet, men dekker primært det administrative behovet for kommunikasjon.

Av disse systemene er radiosystemet minst sårbart for det operative behov ved linjebrudd og strømstans. Eksempel: Ved kabelbruddet i Kristiansand, kort tid tilbake, hvor store deler av telefonnettet var ute av drift, virket radiosystemet 100% i hele politidistriktet.

Politiet er helt avhengig av egne kommunikasjonssystemer for å drive sin virksomhet. Systemene må være minst mulig grad være avhengig av andre leverandører/tjenester.

Avhengighet av andre leverandører
Det konvensjonelle radionettet er konstruert slik at om basestasjoner feiler finnes det overlapping, i de fleste områder, som dekker opp det området som mistet dekning i 80 til 90 % av tilfellene. Selv om politiet er avhengig av leverandører som foretar service på slikt materiell er sårbarheten middels til minimal. Det finnes også mobile reservebaser i alle distrikt som kan settes inn i nødstilfeller og ved spesielle anledninger for å dekke opp det operative behov.

Edacs er et komplekst "datasystem" som er avhengig av Telenors linjenett for å fungere optimalt. Linjebrudd vil redusere funksjonaliteten, men sitene lever sitt eget liv og kan kommunisere på vanlig måte og gir radiokommunikasjon innenfor sitt dekningsområde. Større feil på den enkelte base må settes bort til egne serviceleverandører, men de øvrige baser på siten fungerer tilfredsstillende. Linjebrudd fra hjernen (hoveddatamaskinen) i systemet vil alltid redusere den operative virksomhet i stor grad, selv om de andre baser fungerer tilfredsstillende. Her må vi ha hjelp av Telenor. Det er vurdert å bruke radiolinje istedenfor fast linje som reduserer avhengigheten av andre leverandører. Så langt er det ikke budsjetterte midler til dette, men det er klart mer økonomisk på sikt enn nåværende situasjon med leide linjer.

Telefonsystemet trenger service både fra leverandøren av telefonsentralene og Telenors linjepersonell når feil oppstår. Enkle serviceoppdrag og daglig oppdatering gjøres av personell fra Politiets materielltjeneste (PMT).

Sårbarhet
Radio: Konvensjonelt radiosystem vurderes til liten opp mot middels sårbarhet ved feil. Edacs vurderes opp mot middels sårbarhet ved feil. Backup av konvensjonelle baser reduserer dette noe.

Telefonsystemet: Feil i systemet gir middels sårbarhet for politiet, som kan benytte radio og i enkelte tilfeller mobiltelefon som erstatning. For samfunnet gir dette en større sårbarhet.

Vurdering av risiko
Det er vanskelig å gi klare estimater for dette. Siden deler av systemene er avhengige av Telenors nett, må det for dette vises til Telesektors vurderinger i rapporten.
Feilprosenten på eget materiell er svært lav, men ytre faktorer vil kunne påvirke dette.

3.9. Redningstjenesten

3.9.1. Generelt

Med redningstjenesten forstås den offentlig organiserte virksomhet som utøves i forbindelse med øyeblikkelig innsats for å redde mennesker fra død eller skade som følge av akutte

ulykkes eller faresituasjoner, og som ikke blir ivaretatt av særskilt opprettede organer eller ved særlige tiltak.

Den grunnleggende ide er at alle ressurser, statlige, fylkeskommunale, kommunale, private og frivillige, som er egnet for akuttinnsats for å redde liv, skal kunne mobiliseres for innsats i den offentlige redningstjenesten. Redningstjenesten er derfor organisert som et samvirke mellom en rekke offentlige etater, private og frivillige organisasjoner. Redningstjenesten er således ikke en organisasjon, men mer en funksjon.

Hovedredningssentralene i Nord- og Sør-Norge mottar og distribuerer nødmeldinger. Videre står de for samordningen av redningstjenesten i Norge.

Systemene som brukes til å motta og distribuere nødmeldinger er vurdert som følger ;

3.9.1.1. Nærmere om systemene
Telefonsentral Nord/Sør
Begge Hovedredningssentralene (HRS ene) har installert nye Ericsson telefonsentraler i forbindelse med årtusenskiftet. Ericsson-sentralene har vist at de er meget stabile, både eldre og nye installasjoner, og ”sannsynligheten for svikt ” er derfor satt lavt. I større grad enn tidligere kommer nødmeldinger fra sjøfarende på mobiltelefoner. HRS ene er også avhengig av Ericsson-sentralen i mottak av nød- meldinger fra lufttrafikktjenesten og kystradioene, derfor er ” konsekvenser av svikt ” satt høyt.

For øvrig vises det til avsnittet om sårbarhet i Telesektoren generelt.

Mottakerutstyr, Inmarsat
Inmarsat er et satellittbasert kommunikasjons- og alarmeringssystem, og er en viktig element av GMDSS (Global Maritime Distress Safety System). HRS Sør-Norge mottar nødmeldinger fra de områder som Inmarsat dekker ved sin nedleserstasjon på Eik. Mange elementer i Inmarsat systemet som fører fram til HRS Sør-Norge gjør at sannsynligheten for svikt er satt til middels. Ved bortfall av systemet kan nødalarmer ikke bli registrert og konsekvensen vil være høy.

Samarbeidspartnere, avhengige systemer, strøm, tele
Redningstjenesten er et samvirke av offentlige og private organisasjoner. Hovedredningssentralene er avhengig av et telesamband og strømforsyning som fungerer. Sentralene har egne nødaggregater som kan forsyne de vitale enhetene over korte perioder. Telelinjer er levert og operert av hovedsakelig Telenor og all kommunikasjon med samarbeidspartnere foregår for det meste gjennom telenettet. HRSene vurderer mulighetene for svikt som middels basert på erfaring. Konsekvensene ved eventuell svikt vil være høy da viktig nødtrafikk, både alarmering og informering, vil bortfalle.

Skipsradioregister og Operativ PC nettverksstruktur
HRS ene er tilsluttet Skipsradioregisteret som opereres av Telenor Nett. Tilslutningen er basert på gammel teknologi til HRSene, i motsetning til ny teknologi opp mot kystradioene. På den bakgrunn settes sannsynligheten for svikt til middels. Konsekvensen settes til middels på grunn av at informasjonen kan hentes ut via Kystradioene. Operativt IT-system skal være et hjelpemiddel til å drive bedre og mer effektiv redningstjeneste. I og med at systemet er i innkjøringsfasen er sannsynligheten for svikt satt til middels. Konsekvensen er satt til

middels, basert på at det er fullt mulig å drive redningstjeneste over kortere perioder ved hjelp av papir og blyant og et godt planverk.

Nytt operativt IT-system er i ferd med å utarbeides og installeres ved HRS ene.

Opptak av nødsamtaler
Det er nylig installert nytt opptaksutstyr, kort- og langtidslagring, ved HRS ene. Basert på lite erfaring er sannsynligheten for svikt satt til middels, og konsekvensen satt til middels. Dette er basert på at det er kun i etterretningsøyemed at opptakerne har en viktig funksjon.

Mottakerutstyr Cospas/Sarsat
Cospas/Sarsat er et satelittbasert alarmeringssystem, som også posisjonerer aktive nødpeilesendere. Alle verdens skip over en viss størrelse har i en årrekke vært utstyrt med nødpeilesendere som automatisk aktiviseres ved havarier. Det samme gjelder delvis for fly. Systemet er i dag satelittstyrt. Cospas / Sarsat baserer seg på sovjetiske og amerikanske lavbanesatelitter i polare baner som brukes til å detektere og posisjonsbestemme aktiviserte nødpeilesendere.

Norge er tilsluttet Cospas/Sarsat og det er etablert en nedleserstasjon i Tromsø som sammen med HRS Nord Norge leverer varslinger til de nordiske og baltiske land. Det er mange elementer i systemet og det er på det grunnlag satt middels sannsynlighet for svikt. Konsekvensene vil være høye i og med at nødsignaler fra nødpeilesendere (sjø, luft og landmobile) ikke kan bli oppfanget.

3.9.1.2.Mulige årsaker til svikt i HRSenes funksjoner
Mulige årsaker til svikt er:
- Svakhet i programvare
- Svakhet i ”embedded systems”
- Svikt i avhengige systemer, som strøm og alminnelig telekom.
- Svikt hos samarbeidspartnere
- Svikt hos leverandører

3.9.1.3. Særlig om samarbeidspartnere
Samarbeidspartnere er viktige for HRSenes vitale funksjoner. Svikter systemene hos viktige samarbeidspartnere vil HRSene kunne få store problemer med å gjennomføre sine funksjoner.

Oversikt over noen viktige samarbeidspartnere;
HRSene samrbeider med 55 lokale redningssentraler (LRS) representert ved landets politidistrikter og Sysselmannen på Svalbard. I tillegg samarbeider HRSene med en lang rekke instanser som Luftforsvaret, Luftambulansen, Sjøforsvaret, Redningsselskapet, Kystradioen, Trafikksentralen, Værtjenesten, telenor, Netcom, Inmarsat, Cospas / Sarsat, Oljeindustrien, Helse- og brannvesen, samt AMK-sentralene etc. I tillegg kommer de frivillige sentralene som Røde Kors, Norsk Folkehjelp med fler.

3.9.2. Tiltak

Som det går frem benytter redningstjenesten i dag en rekke ulike IKT-systemer for å kunne utføre sine oppgaver. For en rekke av disse er det ikke mulig å finne umiddelbare erstatninger. Dette selv om et bortfall må anses som dramatisk. Imidlertid finnes det i dag en rekke

kommunikasjonsmidler som kan brukes alternativt innen Redningstjenesten. Dette er utvilsomt en styrke.

Det vil i fremtiden vektlegges å videreutvikle operative kriseplaner til bruk ved bortfall av et eller flere systemer som Redningstjenesten benytter.

I tillegg må en nøye følge prosedyrer for oppfølgning og kontroll av vitale systemer for å unngå svikt.

3.9.3. Konklusjon

Konklusjoner for redningstjenesten:

	Sannsynlighet for svikt			**Konsekvenser av svikt**		
Funksjon	Lav	Middels	Høy	Lav	Middels	Høy
Telefonsentral, sør og nord	**x**					**x**
Mottakerutsyr, Inmarsat		**x**				**x**
Samarbeidspartnere Avhengige systemer, strøm, tele		**x**				**x**
Skipsradioregister Operativ PC-nettverksstruktur		**x**			**x**	
Opptak av nødsamtaler		**x**			**x**	
Mottakerutstyr Cospas /Sarsat.		**x**				**x**

Tabell 3.7 Redningssektoren.

3.10. Sykehussektoren[15]

I sykehus benyttes IT i økende grad både i kjerne- og støttefunksjoner samtidig som eksterne virksomhetskritiske leveranser til sykehus blir mer teknologistyrt. Parallelt med den bedring av kvalitet og effektivitet som anvendelse av IT medfører utvikles en økende avhengighet til IT-systemer. I den grad virksomhetskritiske funksjoner baseres på teknologi er det nødvendig å utvikle sikkerhetssystemer teknisk og organisatorisk for å redusere enhver mulighet for svikt. I denne sammenheng er det tre hovedgrupper av interesser en må ivareta:

1. Sikre opprettholdelse av kritiske funksjoner som er helt eller delvis avhengig av IT.
2. Sikre tilgangen til IT-basert data.
3. Forhindre urettmessig tilgang til, bruk, endring osv. av IT-basert data.

[15] Omtalen av sykehussektoren er basert på en rapport fra Guide Consulting AS utført på oppdrag fra SHD. Materialet er basert på informasjon fra et utvalg av seks sykehus.

Sykehusene er avhengige av at samfunnets infrastruktur opprettholdes, først og fremst med tanke på kommunikasjon (tele- og radio), vann- og strømforsyning samt transporttjenester. Uteblir disse funksjonene over tid, reduseres sykehusene raskt og drastisk til begrenset virksomhet av type øyeblikkelig hjelp (ØHJ) der effektiv virksomhet ikke kan opprettholdes. Man kan klare seg ved kortere avbrudd mht vann- og strømforsyning, men brutt telekommunikasjon gir umiddelbare konsekvenser for akuttmottakene. Langvarige avbrudd anses fra sykehushold som svært usannsynlig.

Nedenfor følger en gjennomgang av en rekke funksjoner ved sykehusene for å identifisere hva som er kritisk og hvor kritiske disse er.

3.10.1. Akuttmottakene

Akuttmottakene er sårbare fordi de er svært avhengig av både telekommunikasjon og IT. De er blant annet avhengig av å se relevant informasjon om pasienten umiddelbart og i det minste identifisere ved fødselsnummer. Det skrives ut etiketter med unik pasient identifikasjon for merking av blodprøver ol. og ved svikt i denne funksjonen må en ta i bruk en midlertidig identifikasjon som må korrigeres på et senere tidspunkt. Feil kan oppstå og i beste fall medfører det stress og ekstra arbeid med gjenstående ajourføring i IT-systemet. Akuttfunksjoner er mer utsatt enn andre fordi avbrudd gir umiddelbare konsekvenser. Sannsynlighet for korte avbrudd er stor og erfart flere ganger både innen tele og IT.

3.10.2. Kommunikasjonstjenester

Kommunikasjonstjenester generelt medfører sårbarhet fordi det ikke finnes erstatning i gode nok alternative systemer og manuelle rutiner. Erfaringen på noen sykehus er at ekstern telefoni har vært mer utsatt enn interne tilkallingssystemer. Et sykehus har opplevd tilfeller av brudd på kabel og feil på kort med omfattende konsekvenser og ikke fungerende backupsystemer (alternativ routing og mobiltelefoni). Et annet sykehus påpeker sårbarhet i forbindelse med plassering av intern sentral. Forøvrig ser det ut til at det er gjort mye mht utskifting og modernisering av interne sentraler.

3.10.3. Formidling av lab.svar (analyseresultater)

Analyseresultater er svært avhengig av IT. Om systemet svikter og stopper opp vurderes det som virksomhetskritisk. Systemet kan imidlertid være i drift og i bruk og fomidle korrupte data på grunn av systemfeil og databaseproblematikk. Dette kan i enkelte tilfeller vurderes som livskritisk. Korrumpering av data på denne måten kan skje og har skjedd ved flere anledninger. Laboratoriene har lang tradisjon for bruk av IT og har innarbeidet gode sikkerhetsrutiner mht å kontrollere, fange opp og korrigere data. Det hender imidlertid at feil svar formidles inn i pasientinformasjonssystemet, direkte til intern eller til ekstern rekvirent. Liknende problemstillinger er aktuelle innen andre områder, men likevel ikke så kritisk som her, selv om kontrollrutinene innen andre områder er dårligere. Når systemet stanser, er det svært ressurskrevende å følge opp driften av den virksomhetskritiske delen ved manuelle rutiner.

3.10.4. Journalskriving

Journalskriving er sårbar og gir en type kjedereaksjon som vokser i alvorlighetsgrad og omfang avhengig av tidsaspektet for systemsvikt. Skrivetjenesten er i utgangspunktet sårbar på de fleste sykehus og en strever for å være ajour med journalskriving. Som regel er det et etterslep. Ved forskjellig type svikt kan det oppstå feil som innebærer en del etterfølgende opprydding. Ved stans inntreffer raskt store opphopninger som gir uoversiktlige forhold og utilgjengelig journal. Konsekvenser kan være utsatt behandling. Kostnaden er høy. Det er mye overtidsarbeid og innleie av ekstra ressurser innen skrivetjenesten for å ta igjen det tapte. Langvarig svikt kan medføre virkelig store problemer med å ajourføre den elektroniske journal. Så lenge det er et "hull" i den elektronisk journal må en dobbelt sjekke med papirjournalen og det er selvfølgelig tidkrevende og ubekvemt.

3.10.5. Overvåking, terapi, diagnostikk og analyse

Dette er funksjoner som i hovedsak er støttet av medisinsk teknisk utstyr som sykehusene i overveiende grad har bedre kontroll på ved god dokumentasjon, opplæring, support og reservelager. Utstyret er dessuten mindre komplekst og frittstående. Funksjoner innen disse områdene blir gradvis mer sårbare ved overgang til mer avansert elektronikk og IT-avhengighet. Det stilles større krav til opplæring av både brukere og teknisk personell. Om utstyr svikter er det ikke like enkelt å skifte det ut og en distanserer seg etterhvert i mange sammenhenger fra å kunne gå tilbake til manuelle rutiner. Radiologi er svært aktuelt i den sammenheng ved satsing på PACS[16] og samspill med RIS[17]. Et av sykehusene melder at tilbud om strålebehandling stopper helt opp dersom IT-svikter.

3.10.6. Administrasjon av pasientflyt og polikliniske konsultasjoner

Administrasjon av pasientflyt er også sårbar og virksomhetskritisk. IT-avhengigheten er ikke absolutt fordi det er rimelig god beredskap i manuelle rutiner. Alvorlige og omfattende problemer kan imidlertid oppstå. Det ligger så mange rutiner innebygd i systemet vedr. planlegging, innkalling, brev til flere instanser, inn- og utskriving m.m. at det i beste fall blir uoversiktlig og mye etterfølgende ajourhold. Det kan også innebære færre behandlede pasienter, tapte inntekter og lengre ventelister.

3.10.7. Situasjonen ved sykehusene

Sannsynligheten for at nevnte områder og funksjoner kan rammes som beskrevet vurderes som relativt stor. Direkte trusler som kan forårsake IT-svikt er i hovedsak tekniske feil, systemfeil og sågar menneskelig svikt. Kritiske faser og situasjoner mht systemsvikt er ved endring, oppgradering og innføring av nye systemer. Spesielt kritisk i den sammenheng er integrasjon av flere databaser og senere endringer relatet til det.

Beredskap i form av manuelle systemer er rimelig god, men også noe varierende. I de fleste sykehusene er det delegert ansvar til avdelingsledere for vedlikehold og opprettholdelse av manuelle systemer. Toppledelsen kan i denne sammenheng ikke svare for hvorvidt det utføres i tilstrekkelig grad. Det innrømmes en viss fare for at det kan dabbe litt av etter at beredskapen var på topp ved årtusen-skiftet. Et par av sykehusene har vektlagt samordnet og aktiv videreføring av beredskapssystemer.

[16] Picture Archive Communication System.
[17] Radiology Information System.

Enkelte sykehus mener manuelle beredskapsrutiner i stor grad kan erstattes ved større investering i grunnleggende tekniske sikkerhetsløsninger (som f.eks. duplisering). Man er svært skeptiske til hensiktsmessigheten og muligheten av å opprettholde manuelle rutiner i en utvikling der IT-avhengigheten øker. Foreløpig er mangel på penger en hindring for å realisere dette.

Katastrofeplaner omfatter i liten grad IT-basert virksomhet da IT-svikt ikke vurderes truende for liv og helse. Sykehusenes katastrofeplaner omfatter uforutsette hendelser internt og eksternt som utgjør en trussel for liv og helse og nødvendig beredskap for håndtering av henholdsvis evakuering eller mottak av et større antall pasienter. Det er tradisjon for et seriøst vedlikehold av disse. De områder som i forbindelse med år 2000-arbeidet ble vurdert som de mest kritiske (lengre avbrudd i vann- og strømforsyning samt telekommunikasjon) er i overveiende grad lagt inn i disse planene.

Underliggende trusler kan gjøre seg gjeldende i forhold knyttet til teknisk sikkerhet, organisatorisk sikkerhet, ressurssituasjon, dokumentasjon og brukere.

Teknisk sikkerhet er noe varierende. Noen sykehus sliter fremdeles med mer eller mindre gammelt utstyr og gammel teknologi som innebærer risiko for svikt og sammenbrudd. Flere påpeker sårbarhet mht svikt i kjølesystem samt serverhavari . De fleste sykehusene har kommet langt i teknisk fornyelse og dermed den tekniske sikkerhet nytt utstyr og teknologi tilfører. Det gjenstår likevel et sårbart område felles for alle sykehusene og det er sikring av servere, spesielt mht å redusere den tid det tar å gjenopprette systemtilgang etter et ev. havari. Flere sykehus understreker i den sammenheng behov for en gjennomført duplisering; - dvs speiling av alle kritiske servere mot et fysisk adskilt rom i annet bygg. Mangel på penger oppgis som grunn til at sykehusene ikke har installert en slik eller liknende løsninger. Det er jevnt over kostbare løsninger.

Uansett hva som måtte gjenstå har sykehusene et klart tyngre fokus på tekniske sikkerhetsløsninger framfor organisatoriske.

Organisatorisk sikkerhet samt forankring av og holdning til sårbarhets- og sikkerhetsarbeid varierer, men er overveiende mangelfull. Sykehusene vedkjenner at det er mye ugjort.

Av seks sykehus har to i løpet av 1999 utført en metodisk og dokumentert sårbarhetsanalyse av IT-relatert virksomhet. Analysene er gjennomført ved ekstern bistand. Den ene anses å være overfladisk og generell og lite anvendelig med tanke på oppfølgende tiltak for å redusere sårbarheten. De øvrige sykehusene har i forbindelse med år 2000-arbeidet utført interne mer eller mindre dokumenterte vurderinger av hva som i den sammenheng var kritiske IT-systemer og hvilke tiltak som skulle prioriteres. Utredning og vurdering av sannsynlighet for IT-svikt og mulige konsekvenser er av den grunn ikke spesielt fremtredende. Innenfor funksjoner basert på teknisk og rent medisinsk teknisk utstyr er det i større grad utført metodiske og dokumenterte sårbarhetsanalyser, inklusive sannsynlighets- og konsekvensvurdering.

De fleste sykehusene mener å ha sikkerhet på dagsorden, men av forskjellige grunner hatt problemer med å realisere et samordnet, metodisk og dokumentert arbeid.

Sikkerhetsarbeid er forankret hos direktøren med uklarhet om hva det reelt innebærer på enkelte av sykehusene. Forankring i linjen er forøvrig i overveiende grad fraværende. Det er lite praktisering av systemeierskap eller at funksjoner utenom IT-avdelingen har spesielt ansvar for en applikasjon og de data som behandles der. Sjeflege har formelt sett medisinsk registeransvar, men på enkelte sykehus har det liten praktisk betydning. Utenom laboratoriene er det sjelden å se rutiner og avklarte ansvarsforhold mht å sjekke datakonsistens, fange opp og rette feil.

Det skal også nevnes at to av sykehusene har startet og er til dels godt på vei i prosesser med sterkt organisatorisk grep for å samordne, systematisere og dokumentere sikkerhetsarbeid. Arbeidet er forankret i toppledelsen og det skal forankres i linjeledelsen helt ned til brukernivå. På det sykehuset som er kommet lengst innrømmes det at en av de viktigste utfordringene er opplæring og ansvarliggjøring av enhver bruker mht sikker informasjonsbehandling. Begge sykehusene er i dialog med Datatilsynet med sikte på å få godkjenning derfra etterhvert. De øvrige sykehuse har planer om det samme og har til dels påbegynt prosesser i den forbindelse.

Mangel på ressurser innen IT er blitt et kritisk sårbart område. Den økonomiske situasjon har gitt marginale muligheter for å sikre stabil opprettholdelse av nødvendig kapasitet og kompetanse. Større sykehus har i perioder vært rammet hardt, men har jevnt over flere ressurser å spille på samt en mulighet for å opprettholde et attraktivt faglig miljø, hvilket er en vesentlig faktor for å kunne holde på og rekruttere nye ressurser. Små og til dels mellomstore sykehus er spesielt utsatt. Flere er i en situasjon der de har 1 – 3 nøkkelpersoner som de er helt avhengige av og når som helst kan miste i en tid der det konkurreres nådeløst om IT-kompetense.

Dokumentasjon av nettverk/systemer henger sammen med ressursforhold. Nettverk er bygget opp og system er implementert med mange og fortløpende tilpasninger uten særlig tradisjon for å dokumentere dette. Behovet for dokumentasjon har etterhvert blitt påtrengende ikke minst for å løse opp avhengigheten til spesielle nøkkelpersoner og gi mulighet for nye ressurser til å sette seg inn i driftsmiljøet. Uansett de skippertak som gjøres for å dokumentere driftsmiljøet vedkjenner sykehusene at de sliter tungt med nødvendig oppdatering.

Kombinasjonen av avhengighet til få nøkkelpersoner og mangelfull nettverks- og systemdokumentasjon er meget bekymringsfull. Det forsterkes ytterligere ved å se det i sammenheng med linjeorganisasjonens svake eierskap til (ansvar for) de systemer man benytter til å forvalte informasjonen vedr. eget virksomhetsområde.

Brukere har lenge vært en underprioritert gruppe både mht opplæring, oppfølging og ansvarlig delaktighet. Med denne bakgrunn utgjør de en uoversiktlig og uberegnelig faktor i sikker informasjonsforvaltning. Enkelte sykehus påpeker et sårbarhetsproblem i ”utro tjenere”. Det er ikke meldt om hendelser, men mer at de er oppmerksom på at bevisst utroskap kan forekomme og at man vanskelig kan gardere seg fullt ut mot dette. Det erkjennes imidlertid at sårbarheten i denne sammenheng er primært knyttet til manglende informasjon og oppfølging mht å gi brukerne et grunnlag for ansvarlig anvendelse av IT.

Eksterne leveranser vedrørende telekommunikasjon, strømforsyning, vann og avløp er fra sykehusene vurdert som mest kritisk ved svikt og sammenbrudd. Det var også disse områder som hadde størst fokus under år2000-arbeidet. Sårbarheten vurderes likevel ikke til å være

tilsvarende stor. Konsekvensene er riktignok ved lengre avbrudd svært alvorlig og omfattende, men sannsynligheten vurderes til å være gjennomgående liten. Beredskapen er gjennomgående god med noe varierende forutsetninger og resultater. Enkelte sykehus har f.eks. mulighet til raskt å koble seg til alternativ vannforsyning, mens andre ikke har det. Enkelte sykehus har tilgang til aggregatkapasitet og drivstofflagre som kan supportere all kritisk virksomhet inntil 2-3 uker. Andre sykehus har en mer redusert dekning, som f.eks. i et tilfelle der røntgenvirksomheten ikke dekkes, og der drivstoffkapasiteten heller ikke kan holde reserveaggregatene i gang over like lang tid.

Ekstern IT-kommunikasjon er foreløpig begrenset og sykehusene har ikke påpekt sårbarhet knyttet til eksisterende løsninger og praksis. E-post via internett foregår isolert fra sykehusenes produksjonsnett.

3.10.8. Konklusjon

Konklusjoner for sykehussektoren:

	Sannsynlighet for svikt			**Konsekvenser av svikt**		
Funksjon	Lav	Middels	Høy	Lav	Middels	Høy
Tele/elektronisk kommunikasjon		**X**				**X**
Pasientbehandling		**X**			**X**	
Administrasjon		**X**		**X**		

Tabell 3.8 Sykehussektoren.

3.11. Kommunehelsesektoren

I dag er bruken av IT i kommunehelsetjenesten beskjeden. Det er svært lite bruk av IT i pleie- og omsorgssektoren, mens ca 90% av allmennlegene og en for oss ukjent andel av helsestasjons- og skolehelsetjenesten bruker IT, særlig i form av pasientadministrative systemer/journalprogrammer. Manglende elektronisk samhandling mellom tjenestefelt og med spesialisthelsetjenesten gjør den dagsaktuelle sårbarheten beskjeden. Farene for driftsproblemer antas imidlertid å være betydelig, pga lav teknisk kompetanse. Dette vil trolig først og fremst resultere i merarbeid og forsinkelser, og takket være papirbaserte reservesystemer ikke i alvorlig fare for brukernes liv og helse.

Sårbarheten vil øke betydelig i kommende år, fordi nettbasert informasjonsutveksling mellom tjenestefelt og mellom kommunehelsetjeneste, spesialisthelsetjeneste og trygdeetat vil vokse eksplosivt. Mange av de forhold som er omtalt som problematiske for sykehus kan ramme kommunehelsetjenesten. Virus og korrumpert informasjon kan tenkes spredd til kommunene via epikriser mv. Driftsstans ved sykehusets tjenester kan føre til forsinkelser for kommunehelsetjenesten (for eksempel prøvesvar og gjennomføring av telemedisinske konsultasjoner).

3.12. Trygdesektoren

Trygdeetaten vil utbetale nesten 200 milliarder kroner over statsbudsjettet i 2000. Om lag 1,05 millioner nordmenn har sin hovedinntektskilde fra folketrygden (til livsopphold). Dette

inkluderer pensjon, uførepensjon, attførings- og rehabiliteringspenger og sykepenger og ytelser til enslige forsørgere. Dersom vi også inkluderer andre brukere er vi totalt oppe i 1,6-1,7 millioner nordmenn som mottar vesentlige ytelser via trygdekontoret. Trygdeetaten mottar og behandler store mengder persondata, herunder sensitive personopplysninger om helseforhold, ved behandling av søknader fra medlemmene av folketrygden og oppgjør med behandlere, leverandører og tjenesteytere. Etatens tjenester vurderes til å være samfunnskritiske og det vil få store konsekvenser dersom disse tjenester delvis eller helt ikke skulle fungere i en krisesituasjon, f.eks ved bortfall av utbetalingskjeden i et lengre tidsrom. Etaten er meget avhengig av telekommunikasjon, "bankenes utbetalingskjede", interne IT-systemer og leverandører for å opprettholde sin drift herunder fatte vedtak og foreta utbetalinger.

Etaten har en omfattende IT-infrastruktur med ca 460 lokale nettverk og sentralisert stormaskindrift. Det arbeides kontinuerlig med å holde seg oppdatert for å unngå skadevirkninger som følge av tap eller ødeleggelse av data, samt forsinket eller uautorisert behandling av informasjon. Informasjonssikkerhet skal inngå som en naturlig del av etatens daglige virksomhet. Etaten skal løpende vurdere og gjennomføre sikkerhetstiltak som trygger etatens evne til å fremstå som en ledende etat, og som ikke bryter den tillit våre medlemmer, samarbeidspartnere og oppdragsgivere har til Trygdeetaten.

Ved valg av teknologi som skal håndtere opplysningene på en sikker måte, vil bl. a personopplysningsloven, økonomireglementet for staten, arkivloven, taushetspliktsbestemmelsene i folketrygdloven og forvaltningsloven stille krav til hvordan opplysningene kan sendes, oppbevares og benyttes.

Trygdeetaten har en viktig samfunnsmessig funksjon. Det er mange som er avhengige av ytelser som tilstås og utbetales gjennom trygdeetaten. Det er viktig at det er utarbeidet et system for å håndtere eventuelle beredskapssituasjoner, slik at saksbehandlingstiden ikke øker drastisk og at stønadsmottakerne får sine ytelser uten unødig opphold.

I St.meld. nr. 24 (1992-93) om den fremtidige sivile beredskap vektlegges det at beredskapsorganisasjonen i en eventuell beredskapssituasjoner bør være mest mulig lik organiseringen i fredstid. Utøvelse av myndighet bør skje gjennom de samme ledd som i fredstid.

Etaten har i de senere år arbeidet systematisk med kartlegging av sårbarhet innen de IT-systemer som er kritiske for å opprettholde etatens funksjoner, og med å gjennomføre nødvendige forbedring tiltak. Etaten har innført metoder og verktøy for å sikre kontroll med egen sårbarhet og gjennomfører løpende risiko- og sårbarhetsanalyser. Kartlegging av IT-sårbarhet i etaten er også sett i sammenheng med etatens gjennomgang og oppdatering av planverk for *"kriser i fred og kriser i krig"*.

3.13. Forsvaret

Det er mange og til dels kompliserte sammenhenger mellom Forsvarets oppgaver, struktur og virksomhet. Forsvarets ulike enheter og sektorer bidrar til å løse dels forskjellige oppgaver og dels forskjellige deler av samme oppgave. Forsvarets informasjonssystemer må også understøtte disse prosessene.

Forsvarets oppgaver kan deles inn i to hovedkategorier:

- *Fredstidsoppgaver* som Forsvaret utfører som en del av sin ordinære virksomhet i fredstid, det vil si suverenitetshevdelse og myndighetsutøvelse, etterretningstjeneste, sikkerhetstjeneste, internasjonalt militært engasjement, redningstjeneste og annen samfunnsnyttig bruk av Forsvaret
- *Krigsoppgaver* som Forsvaret utfører i krise og krig basert på mobiliseringstiltak. Krigsoppgavene har størst betydning for Forsvarets struktur og virksomhet, men utføres bare etter mobilisering.

Fredsoppgavene innbefatter rednings-, kystvakt-, etterretnings- og sikkerhetstjeneste og støtte til det sivile samfunn. Svikt i sambands - og informasjonssystemene som understøtter disse virksomhetsområdene medfører umiddelbare konsekvenser. Samtidig håndterer systemene informasjon som kan bli utnyttet, enten for å oppnå kortsiktige militære eller politiske mål, eller for å oppnå strategisk informasjonsoverlegenhet. Sistnevnte aspekt representerer en undergraving av nasjonens interesser og berører bl. a forhold og tillit til andre nasjoner.

Forsvarets sentrale mål er produksjon og forvaltning av militær makt iht politiske krav. Det er et paradoks at man bruker betydelige beløp for å skape en ressurs som man håper det aldri blir behov for. Dersom Forsvarets sambands- og informasjonssystemer svikter, får ikke dette nødvendigvis umiddelbare og synlige konsekvenser fordi produktene ikke er direkte etterspurt før krise - krig. Bryter en aktør seg inn og henter informasjon om krigsorganisasjonen vil han kunne tilegne seg inngående kjennskap til militære konsepter og planer, og han kan påvirke informasjonen til ledelsen. Dette behøver nødvendigvis ikke å få nasjonale konsekvenser på kort og lang sikt, men kan svekke Forsvarets troverdighet.

Den tekniske driftssikkerheten til de systemer som understøtter virksomheten er generelt sett god. Det er liten sannsynlighet for at flere systemer i fredstid skal svikte samtidig. Det finnes i tillegg alternative løsninger som kan benyttes ved teknisk svikt, noe som er gjenspeilet i beredskapsplanene.

Forsvarets virksomhet er avhengig av en stor andel sivil tjenesteproduksjon i fred, krise og krig. Eksempler på dette er strømforsyning, vannforsyning, logistikk og sivil sambandsinfrastruktur. En svikt i disse systemene vil få konsekvenser for Forsvarets IT-sårbarhet. Dette selv om Forsvaret disponerer betydeligere ressurser innenfor alle disse områdene og kan derfor redusere konsekvensene av svikt.

Det leveres også elektroniske tjenester fra institusjoner i det sivile samfunn som vil kunne få vesentlig betydning for Forsvarets virksomhet dersom de svikter. Krigsavlønning er et eksempel på dette. 230.000 personer skal få utbetalt hjemmelønn ved bruk av elektronisk betalingsformidling. Hvis lønn ikke utbetales kan dette få innvirkning på moral og kampevne, og illustrerer noe av den sårbarhet Forsvarets står overfor i en situasjon. Utvikling av informasjonssystemer bør derfor settes inn i et helhetlig fred, krise og krigsperspektiv.

3.13.1. Informasjonssystemer - Forsvarets perspektiv

Det totale informasjonssystem er helheten av organisasjon, personell, kompetanse, teknologi, prosedyrer og data som er nødvendig for planlegging, gjennomføring, ledelse og kontroll. De deler av det totale informasjonssystem i Forsvaret hvor informasjonsteknologi (IT) benyttes eller planlegges benyttet, utgjør Forsvarets informasjonssystern (FIS).

FIS skal sikre effektiv utveksling og behandling av informasjon mellom politiske og militære myndigheter samt med relevante ledd i totalforsvaret og NATO, i fred, krise og krig.

Forsvarssjefen (FSJ) har vektlagt denne vide definisjonen av FIS bl a for å synliggjøre at FIS er en endringsagent. Risiko- og sårbarhetsutviklingen er på denne bakgrunn ikke å anse som et teknisk problem, men et problem som eies og styres av virksomhetens ledelse.

Forsvaret har en stor utfordring i å anvende og bruke informasjonsteknologi for a oppnå gevinster i virksomheten. Derfor må virksomhets- og omstillingsstrategien være koordinert med IT-strategien. Måloppnåelse ift organisasjonens utnyttelse av teknologi betinger imidlertid strategi for systemutvikling, styringskonsepter og ressursstyring tilpasset organisasjonens kompetanse, kultur, omstillingsevne/vilje og dynamikk.

Forsvarets investeringsstrategi vektlegger bruk av hyllevarer der nasjonal kontroll ikke anses nødvendig. Konsekvensen er at Forsvaret bruker det andre organisasjoner har skapt i sin teknologiutvikling og omstilling. Dette bør spesielt vektlegges i et NATO og totalforsvarsperspektiv. Forsvaret har en mulighet til å demonstrere hurtigere omstillinger og mer effektiv organisering ved a ta i bruk nye løsninger for utnyttelse av teknologi. Forsvaret vil derfor sette fokus på teknologiutnyttelse og ikke utvikling av teknologi.

3.13.2. Forsvarets strategi for utvikling av FIS - systemutvikling

FSJ har på bakgrunn av definisjonen av FIS og politiske pålegg besluttet at utviklingen av FIS skal styres sentralt. Denne rollen innebærer overordnet koordinering av omstillingen av Forsvarets virksomhet og kompetanseutvikling gjennom utnyttelse av tilgjengelig teknologi med et helhetlig fokus. Helhetlig og overordnet styring av omstillingen og kompetanseutviklingen skal ivaretas av fellesnivået i FO. NATO-alliansen og totalforsvarskonseptet er sentrale elementer i den strategiske styringen.

Koordineringsrollen betinger:
- Kompetanse som ser virksomhetens strategi sammen med utviklingen av FIS
- Kompetanse til a koordinere innføringen av teknologi med utviklingen av organisasjonen

Aspektene innebærer en kontinuerlig samhandling og koordinering med brukeren og materiellforvaltning iht informatikkfaglige prinsipper i et Personell, System og Organisasjons (PSO) - perspektiv. Forsvarets informatikkfaglige fellesbetegnelse på dette er systemutvikling. Systemutviklingsstrategien i Forsvaret omfatter bl a:
- ledelse - ledelsesutøvelse
- virksomhetsprosesser
- organisasjonsstruktur - dynamikk
- kompetansestruktur
- organisasjonspsykologi
- maktstruktur
- teknologi

Systemutvikling kan ikke sees uavhengig av risikostyring. Risiko og sårbarhet er integrerte aktiviteter i systemutviklingsprosessen fordi virksomhetens aksepterte sarbarhet har en nytte og en kostnad. Sårbarheten er en størrelse som virksomhetens ledelse har et ansvar for å styre og kontrollere, og ikke minst akseptere i et kost - nytte - risiko perspektiv. Dette bør

kombineres med utvikling av gode beredskapsplaner som kan bidra til reduksjon av sårbarhet, og reduksjon av organisatoriske eller teknologiske kostnader i fredstid. Beredskapsplanlegging må derfor håndteres som en integrert del av systemutviklingen. Fokus må settes på å styre risiko og sårbarhetsutviklingen iht virksomhetens mål og ambisjoner.

Forsvaret erkjenner at det ikke er mulig å redusere virksomhetens sårbarhet til tilnærmet lik null. En slik målsetting er ikke forenlig med de økonomiske rammer. Den kan også være til direkte hinder for Forsvarets åpenhet mot det sivile samfunn og samarbeidet med andre institusjoner.

Utstrakt sikring av systemer/virksomhet kombinert med utvikling av proprietære systemer, kan være til hinder og skade for innovasjon, nytenkning og omstilling. Samtidig vil virksomheten alene måtte bære kostnadene forbundet med kompetanseutvikling på bruk, utvikling, drift og vedlikehold av egne systemer. En virksomhet som ikke lykkes i utnyttelse av teknologi som andre bruker, vil derfor bruke betydelig mer ressurser på kompetanseutvikling enn andre. Begge forhold vil kunne redusere organisasjonens evne til utnyttelse av et kommunikasjonsmedium og en endringsagent. Samtidig vil det pga den sikkerhetspolitiske situasjonen og trusselutviklingen, være nødvendig a sikre virksomheten innenfor en akseptert risiko.

Samtidig som teknologien gir nye muligheter, ser man også konturene av et trusselbilde med aktører med varierende intensjoner. Teknologien er middelet som gir aktørene mulighetene til å ramme virksomheten.

Utfordringen for Forsvaret er derfor å balansere åpenhet og teknologiutnyttelse, opp mot egen sårbarhet og kostnadene. Denne utfordringen kan i hovedtrekk uttrykkes iht følgende prinsipper:
- Virksomhetens leder er ansvarlig for styring av virksomhetens risikoutvikling
- Virksomhetens leder er ansvarlig for sikkerheten i virksomhetens informasjonssystemer
- Ledelsen er ansvarlig for å styre IT-sikkerhet slik at tiltakene er i samsvar med behovene.

3.13.3. Internasjonalisering og globalisering - nye trekk i utviklingen

Den teknologiske utviklingen binder enkeltmennesker, organisasjoner og nasjoner og sammen. Man må derfor forvente at det dukker opp kompetente aktører med destruktive målsettinger. Den trussel man selv er utsatt for, kan imidlertid utnyttes til egen fordel ved at andres sårbarhet og avhengighet til teknologi kan utnyttes til egen fordel der det er aksept for det.

Dette offensive aspektet, som betinger samordnet utnyttelse av kompetanse og ressurser som en integrert del av virksomhetens strategier og planer, går under navnet informasjonsoperasjoner (INFO OPS). Media kan i en slik sammenheng ha en sentral rolle. Media er imidlertid i sin natur en fri og uavhengig "ressurs" som ikke vil la seg styre og kontrollere. Media skiller seg derfor ut i forhold til andre ressurser som er under styring og kontroll.

3.13.4. Strategisk trusselutvikling

Aktører som kan representere en sikkerhetspolitisk risiko for Norge, må ses i en global sammenheng fordi vår infrastruktur er knyttet opp til et globalt nettverk. Mangfoldet av ulike

aktører som på sikt kan representere en sikkerhetsrisiko, gjør utfordringene større. Dette gjelder ikke minst med tanke på hvilke aktører virker dimensjonerende for våre trusselvurderinger og beredskapstiltak.

Siden det er forskjellige aktører med potensiale til å skade den nasjonal integritet, kan det være hensiktsmessig å foreta en kategorisering av hvilke aktører vi kan risikere å stå overfor når trusselen mot samfunnets virksomhet skal analyseres.

Symmetriske aktører. Denne kategorien defineres som andre stater eller allianser av stater med tilstrekkelig kapasitet til å undergrave vår nasjonale integritet ved hjelp av strategiske informasjonsoperasjoner (INFO OPS). Aktører på dette nivået drives primært av sikkerhetspolitiske målsettinger og intensjoner som kjennetegner suverene stater (nasjonal sikkerhet, integritet, suverenitet, velferd, tilgang på ressurser, innflytelse over egene valg etc).

Handlingsmønsteret kjennetegnes av rasjonalitet der anslag mot informasjonssystemer iverksettes på bakgrunn av rene kost-nytte vurderinger.

Asymmetriske aktører. Denne kategorien defineres som ikke- statlige aktører. Kategorien omfatter bade enkeltindivider og grupperinger av ulike avskygninger. Aktører på dette nivået drives av en rekke incentiver:

- politiske (ønske om internasjonal anerkjennelse og/eller oppmerksomhet, politiske innrømmelser overfor en stat)
- religiøse (ønske om endret religiøst innhold og/eller retning)
- økonomiske (ønske om tilgang på nasjonale ressurser eller penger til eget eller andres forbruk)
- sosiale - spenning (tidsfordriv, ønske om utforske sensitiv informasjon)
- hevn/revansje eller utfordring (ønske om å klare å bryte gjennom lukkede nettverk).

Handlingsmønsteret skille seg fra statsnivået ved at operasjonene bærer preg av (tilsynelatende', irrasjonelle handlinger (for eksempel i form av religiøs og/ eller politisk ideologisk karakter) som ikke konvergerer med vestlige rasjonelle trusselvurderinger. Handlingsmønsteret kan også kjennetegnes av uforutsigbarhet som følge av fravær av en enhetlig og sentralisert ledelse, eller en klar og samlende politisk eller religiøs målsetting. En slik struktur åpner også opp for store variasjoner hva angår personlige initiativ og intensjon. Kategorien inneholder et utall av mulige motiver og intensjoner. En uttømmende inndeling blir således vanskelig.

"Semi-statlige aktører". Kategorien defineres som asymmetriske motstandere som nyter godt av statlig beskyttelse. Aktørene opererer mellom det statlige og det ikke-statlige nivået og fremstår som en mer ressurssterk og sofistikert aktørgruppe i forhold til den foregående gruppen. Deres intensjoner er ikke vesensforskjellig fra de øvrige kategoriene, men organiseringen og ressurstilgangen tilsier et mer systematisk og effektivt handlingsmønster fordi organisasjonsstrukturen er flatere og mer dynamisk. De har et bredere og mer innflytelsesrike kontakt nettverk. Det operasjonelle nedslagsfeltet blir følgelig preget av større valgfrihet. Deres virksomhet er i motsetning til de asymmetriske grupperingene mer politisk, religiøst og ideologisk motivert, snarere enn økonomisk orientert.

Vårt tradisjonelle trusselbilde utfordres ved at kompetent utnyttelse av egen eller andres sårbarhet (INFO OPS) kan utføres ved hjelp av enkle, billige og lett tilgjengelige virkemidler. Ettersom inngangsverdien er relativt lav og sannsynligheten for å bli avslørt eller oppdage et

angrep er liten, øker antallet potensielle aktører. Den tradisjonelle fienden/aktør var representert ved nasjonalstater med militærmakt. INFO OPS krever relativt få ressurser og øker følgelig spennet av potensielle fiender. Bildet kompliseres ytterligere ved at motiver og mål bak en trussel kan variere sterkt. Aktørenes størrelse star ikke nødvendigvis i forhold til den trusselen de potensiell sett kan utgjøre.

3.13.5. Forsvarets sårbarhetsutvikling

Forsvarets virksomhet og kompetanseinfrastruktur har vært preget av den kalde krigen, og man har brukt betydelige ressurser på å sikre virksomheten og dens informasjonssystemer mot en identifiserbar og statisk militær fiende. Konseptet har vært drevet frem av en målsetning om å kunne operere militære styrker når størstedelen av den sivile infrastrukturen ligger nede. Dette har medført at Forsvarets virksomhet for en stor del er understøttet av sambands- og informasjonssystemer med relativt sett sterke sikkerhetsmekanismer for å håndtere bortfall av sivil infrastruktur. Konseptet inkluderer flere parallelle systemer for bl. a understøttelse av Kommando - Kontrollprosessen (KK-Ledelsesprosessen). De økonomiske og sikkerhetspolitiske forutsetninger har imidlertid endret seg for så vel Forsvaret som NATO, som har vært økonomisk hovedsponsor.

Samtidig som de økonomiske og sikkerhetspolitiske forutsetninger har endret seg, har en sterk militært dreven teknologiutvikling måttet gi delvis tapt for en teknologiutvikling drevet frem av kommersielle interesser. Utviklingen kjennetegnes ved at de kommersielle interessene har store ressurser og svært korte ledetider fra ide til ferdig utviklet produkt. Det må påpekes at de kommersielt økonomisk drevne interesser ikke alltid er sammenfallende med militære behov og nasjonale sikkerhetsinteresser. Man må derfor søke kosteffektive og rasjonelle løsninger som støtter offentlige interesser og løsninger der kommersielle krefter ikke har interesser.

Norge baserer seg på et totalforsvarskonsept som primært skal kunne sikre logistikk og helhetlig styring av sivile og militære ledelses- informasjonssystemer til støtte for militære operasjoner i krig. Styringen av nasjonens samlede ressurser under slike forhold stiller strenge, og fordyrende, krav til sambands- og informasjonssystemene. Interoperabilitet, overlevelsesevne, tilgjengelighet og sårbarhet er sentrale områder. I prinsippet hjelper det lite om Forsvaret har utviklet motstandsdyktig infrastruktur og informasjonssystemer dersom det sivile samfunn baserer seg på sårbare systemer. Forsvaret som eneste finansielle kilde har heller ikke lenger råd til å utvikle motstandsdyktig infrastruktur kun til eget bruk. En aktør vil mest sannsynlig søke etter sårbare områder hvor effekten og ringvirkningene ved å sette inn ressurser blir størst mulig med minst mulig risiko for aktøren selv. En virksomhets samlede sårbarhet blir derfor ikke bedre enn det svakeste ledd.

3.13.6. Konklusjon

Globaliseringsprosessen bør resultere i internasjonalt forpliktende samarbeid og felles nasjonal tilnærming. Nasjonens sårbarhet som følge av økende avhengighet til informasjonsteknologi betinger nasjonal og helhetlig organisering og styring. Sårbarheten blir ikke bedre enn det svakeste ledd.

Sårbarhet bør behandles som en integrert del av systemutviklingen i et kost- nytte perspektiv. Forsvaret vil bruke systemutvikling som endringsagent i organisasjonen, og det er en sentral utfordring å balansere sårbarhet mot profesjonell utnyttelse av tilgjengelig teknologi.

Det er vesentlig å søke mot interesser, på tvers av privat- og offentlig sektor som støtter fellesskapet, for å oppnå kosteffektive og rasjonelle løsninger der de kommersielle krefter ikke har interesser.

3.14. Offentlig virksomhet

Tjenestetilbudet fra visse store offentlige etater er meget IT-intensive og vil derfor kunne få betydning for IT-sårbarheten i samfunnet. Spesielt gjelder det på områder hvor det forventes høy regularitet i tjenestene, eksempelvis ved trygdeutbetalinger, dagpenger fra arbeidsmarkedsetaten, tilgjengelighet til visse registereiere (Brønnøysundregistrene) osv. Spesielt trygdesektoren er trukket fram som samfunnskritisk sektor. I tillegg til den betydning som noen store tjenestesektorer har, er offentlig forvaltning generelt nødvendig for ledelse og informasjon i samfunnet. Kontinuitet i offentlig tjenestetilbud og myndighetsutøvelse vil være avhengig av en rekke interne støttefunksjoner og samordningstiltak mellom offentlige virksomheter som i økende grad forutsetter utstrakt bruk av IT. Nedenfor skal vi gi en kort oversikt over situasjonen for den sentrale statsforvaltningen med departementene og etatene, regional forvaltning med fylkesmannsembedene, samt knytte kommentarer til kommunal forvaltning. Synspunktene er basert på informasjon innhentet ved intervjuer og en enkel spørreundersøkelse.

Når vi har tatt for oss situasjonen med IT-sårbarhet i intern offentlig forvaltning, har vi begrenset oss til å få fram et bilde av hvilke kritiske prosesser og funksjoner som er avhengig av IT, og i hvor stor grad denne avhengigheten kan påvirke offentlige virksomheters funksjonsdyktighet. Vi har altså ikke gått nøyere inn på hvordan denne IT-sårbarheten i sin tur kan få konsekvenser overfor samfunnet, men stoppet ved den egenvurdering som de aktuelle virksomheter selv har gitt.

Det er særlig arbeidet med år 2000 problemet i statlig, regional og kommunal virksomhet som ligger til grunn når virksomhetene har gitt innspill/vurderinger om avhengighet av interne fagsystemer og databaser, felles økonomisk-/administrative systemer, kontorstøttesystem, lokalnett o.s.v. Det foreligger egne rapporter med vurderinger av IT- sårbarhet og beredskap i denne sammenheng (jf. rapport fra Asplan Analyse, *Evaluering av Y2K-arbeidet*).

3.14.1. Felles infrastruktur fra Statens forvaltningstjeneste

Den sentrale statsforvaltningen har gått sammen om *felles støttefunksjoner innen data- og teleområdet.* Disse administreres av Statens forvaltningstjeneste (Ft). Som hovedregel forestår Ft også daglig drift i samarbeid med valgte teleoperatører. De viktigste funksjonene som kan påvirke sentralforvaltningens virkemåte er:

- Statens tverrsektorielle nett (STN) som knytter sammen ca 17000 personer i et internt datanett, som foruten departementene også inkluderer tilknytning til en rekke etater og regional forvaltning med fylkesmannsembedene.
- Hussentralen for departementene med ca 8000 tilknytninger.

Ft sørger for at STN er skjermet med brannmurteknologi mot det åpne Internettet. Trafikkavvikling og eventuelle unormale hendelser blir logget og overvåket på flere måter. Man har til nå ikke funnet det praktisk å filtrere e-post. Men erfaringen har imidlertid vist at man kan bli meget sårbar for virusangrep på grunn av vedlegg til e-post når man benytter samme programvare fra Microsoft. I andre sammenhenger har det vært mulig å avverge ”spamming”-liknende forsøk utenfra. Videre har Ft i samarbeid med ekstern leverandør

kommet fram til en sikker måte for å knytte hjemmekontor (evt. mobilt kontor) opp til STN, slik at brukeren kan logge seg direkte inn på sitt lokale nett på sin faste arbeidsplass med forsvarlig autentisering og slik at overføring av informasjon foregår kryptert. Dette setter detaljerte krav til organisering av sikkerhetsfunksjonen i brukervirksomhetene. Fordi STN knytter sammen så vidt mange personer fra forskjellige virksomheter, må STN i praksis betraktes som et åpent nett. De tilknyttede virksomhetene må derfor selv avgjøre om de i sin tur trenger å skjerme seg ytterligere mot STN. Det vil typisk avhenge av om de lokalt har beskyttelsesverdig informasjon, personsensitiv informasjon el.l. Retningslinjer for tilknytninger til STN og sikkerhetsforanstaltninger er dokumentert i særskilte sikkerhetshåndbøker.

Det er gjennom den siste tiden lagt økende vekt på driftssikkerheten i STN bl.a. med reserveløsninger på alle kritiske punkter. Teknisk sett er sannsynligheten høy for at deler av nettverket kan falle ut i kortere tid, men pga reserveløsninger og redundans blir sannsynligheten for dobbeltfeil liten og de totale skadevirkningene derfor kortvarige og små. En ekstra fordel med reserveløsninger er at de også kan utnyttes i normalperioder til deling av belastningen.

Dagens organisering av STN gir god oversikt over sikkerhetssiden og mulighet for overvåkning av servicekvalitet. Eksempelvis gir STN ett kontrollerbart tilknytningspunkt til et lukket stamnettet som er under utbygging for informasjonsutveksling mellom EU-institusjonene og forvaltningene i EU/EØS-landene. Utfordringen fremover vil imidlertid være å kunne utbygge nettet med tilstrekkelig kapasitet for å møte sektorvise behov i konkurranse med nisjetilbud i markedet og i tråd med utviklingen/tilbudet av ny teknologi og krav til driftskompetanse.

Når det gjelder hussentralen på telefoni har den lav sannsynlighet for å falle ut, men dersom den likevel skulle falle ut vurderes dette å kunne gi store konsekvenser. Aktuell strategi er derfor å satse videre på alternative løsninger (mobiltelefon, IP-telefoni). Utfordringen fremover ligger i konvergens mellom tele og data slik at også teledelen kan bli en del av datanettet. Det vil i så fall gjøre det nødvendig med grundig vurdering av sikkerhetsspørsmålene og sårbarheten.

3.14.2. Sentrale statsforvaltning og større etater

IT-avhengigheten i departementene er typisk knyttet til kontorstøtte (inkl. tekstbehandling, kalender, epost, osv.) og arkivfunksjon, økonomisystem, lønn/personalsystem, samt felles servermaskiner og lokalnett. Sannsynligheter for feil og konsekvenser blir vurdert noe ulikt, men helhetsbildet viser at risikoen knyttet til disse støttesystemene er liten. (Spesielt sikrede og lukkede løsninger som er isolert til den politiske ledelse, er ikke vurdert i denne oversikten.)

Noen virksomheter er kritisk avhengige av etatsspesifikke databaser, til dels med døgndrift. Gjennomgående synes imidlertid alle å ha foretatt grep slik at risikoen knyttet til systemene forblir liten. I praksis er det noe sprik med hensyn til om man registrerer unormale hendelser, om man har reserveløsninger, om man har utpekt sikkerhetsansvarlig. Eventuelle ROS-analyser har vært gjort i forbindelse med år 2000 arbeidet.

Enkelte tjenesteytende etater og registereiere (eksempelvis A-etaten og Brønnøysundregisterne) har gått profesjonelt til verks, i alminnelighet utført ROS-analyser og

og etablert en sikkerhetsorganisasjon for å ta seg av utfordringene knyttet til sårbarhet. Slike virksomheter vil ha bygget opp en driftskompetanse og en infrastruktur som er nødvendig for å ha kontroll og kunne styre utviklingen mot nye tjenester på nett, enten det er i tjenesteyting utad eller for offentlig innrapportering. Disse offentlige registerne inngår i en rekke verdikjeder som man ikke har god nok oversikt over for å kunne analysere sårbarheten og gjøre forbedringer. Etter hvert som offentlige innkjøp legges om etter nye prinsipper for e-handel, vil sikkerhet og sårbarhet også måtte kalkuleres inn.

For all offentlig virksomhet er det en målsetning at elektronisk saksbehandling skal bli en normal arbeidsform (jf. AADs handlingsplan 1999-2001 for elektronisk forvaltning). Dette vil over tid kunne føre til økt IT-sårbarhet fordi viktig informasjon lettere kan gå tapt. Saksbehandlere blir vevd sammen med hverandre i saksbehandlingsprosessen og kan bli gjensidig avhengige av hverandre gjennom de felles verktøy de utnytter. I sitt program for innføring av elektronisk saksbehandling, som drives av Statskonsult på vegne av AAD, kan Statskonsult peke på en rekke kompensatoriske tiltak som vil kunne redusere IT-sårbarheten.

3.14.3. Regional statsforvaltning

Regional statsforvaltning med fylkesmannsembedene har en nøkkelrolle når det gjelder å koordinere det sivile beredsskapsarbeidet. Gjennom ROS-analyser og tilsyn følger de også opp at kommunene tar beredsskapsmessige hensyn i sin planlegging. Med hensyn til utpeking av kritiske prosesser som er avhengig av IT og der svikt i IT-systemene kan ha konsekvenser for omverdenen har år 2000 arbeidet gitt en viss oversikt. De mest kritiske prosessene knytter seg til behandling og betaling av tilskudd til enkeltpersoner, men risikoen er meget lav. IT-systemene kan være fraværende og bli erstattet med manuelle rutiner opptil en ukes tid uten for stor skadevirkninger. Derimot møter embedene større utfordringer når det gjelder å skjerme beskyttelsesverdig informasjon, herunder personsensitiv informasjon i sine lokale nettverk. Det er her startet et arbeid for å oppnå tilstrekkelig informasjonssikkerhet basert på retningslinjer fra Datatilsynet. Kjernen i tiltakene er systematiske, periodiske egenkontroller med vurdering av trusselbildet og kontroll av at retningslinjene etterleves.

3.14.4. Kommunal forvaltning

År 2000 gjennomgangen har gitt kommunene bedre oversikt over avhengigheten av IT og beredskapsplaner slik at kommunene står bedre rustet til å håndtere kriser eller uforutsette situasjoner. Mye av beredskapen vil imidlertid være knyttet til vanlige forsyningstjenester (vann/avløp o.a.), som er behandlet samlet andre steder i denne rapporten. IT er en forutsetning for kommunal tjenesteyting på en rekke felter. Uregelmessigheter i disse tjenestene vil være alvorlig nok for dem som rammes, men skadevirkningene anses likevel å være veldig avgrenset. De fleste kommuner drifter egne nett med interne ressurser og vil derfor være atskilt fra slike ytre trusler som formidles via Internett. Ca halvparten av kommunene hevder at de har mulighet for å knytte seg til eksterne nett. Fordi kommunene behandler mye data av personsensitiv art, må de sørge for Datatilsynets godkjenning dersom de kobler seg opp på eksterne nett.

Utover dette er det ikke fremkommet anvendelser av IT i kommunene som har samfunnskritiske konsekvenser. I fremtiden vil det ventelig knytte seg usikkerhet til økt bruk av IKT og Internett som altså kan gi større eksponering for trusler utenfra. Omlegging til elektronisk saksbehandling og omfattende bruk av infrastruktur vil ventelig bli som for

statsforvaltningen. Det er pekt på at denne økte risiko må møtes med holdningskampanjer, mer opplæring og innarbeiding av trygge rutiner.

3.14.5. Utviklingsretning

Mer utstrakt dataflyt og bruk av elektronisk kommunikasjon og rapportering på tvers av forvaltningsnivåene, inkl. kommunal sektor, betyr at flere virksomheter på disse nivåene i økende grad vil være eksponert i sårbarhetssammenheng. Disse virksomhetene samarbeider i det såkalte Forvaltningsnettsamarbeidet (FNS) for å komme fram til felles spesifikasjoner for anskaffelser og avtaler på området IT- og kommunikasjonsutstyr, inkl. visse sikkerhets-produkter og infrastruktur bl.a. digital signatur. FNS-avtalene sikrer at utstyr og tjenester kan spille sammen og utnytter konkurransen i markedet. Men utover dette kommer FNS ikke inn i bildet når det gjelder forhold knyttet til IT-sårbarhet. Ansvaret for sikkerhet ligger på den enkelte virksomhet som må velge adekvate løsninger i forhold til sine behov/krav.

Lokal forvaltning vil i stor grad være henvist til det nettilbud de kan få gjennom det kommersielle tilbud om Internettilgang. Det vil derfor ha stor betydning i fremtiden hvordan utviklingen av Internett blir med hensyn til sårbarhet og kvalitet. Generelt vil det være viktig også av hensyn til resten av forvaltningen og samhandlingen med publikum og næringsliv å få en reell og oppdatert oversikt over den eksisterende Internett-infrastrukturen i Norge og hvordan den vil utvikle seg (jf. svensk undersøkelse om Internett og sårbarhet ”Svenska delen av Internett”.) En slik utredning bør også ta opp hvilken rolle det offentlige skal ha i utviklingen av den norske delen av nettet.

3.14.6. Konklusjon

Konklusjoner for intern offentlig forvaltning:

	Sannsynlighet for svikt			**Konsekvenser av svikt**		
Funksjon	Lav	Middels	Høy	Lav	Middels	Høy
Statsforvaltningens infrastruktur	**X**				**X**	
Forvaltningens interne støttesystemer	**X**			**X**		
Fremtidige systemer med elektronisk saksbehandling	**X**				**X**	

Tabell 3.9 Offentlig forvaltning.

3.15. Næringslivet

Næringslivet spiller en viktig rolle både som operatør av kritisk infrastruktur, og som leverandør av de fleste andre varer og tjenester i samfunnet. Norske virksomheter opptrer i ulike sammenhenger som eier eller operatør av systemer som inngår i kritisk infrastruktur. Datasentraler, kraftverk og telekommunikasjonsselskaper er eksempler på slike virksomheter. Avhengig av hvilken sektor en opererer innenfor vil det kunne eksistere formelle krav, for eksempel konsesjonskrav. Næringslivets rolle som operatør og eier av kritisk infrastruktur er omtalt og tatt med i betraktning i forbindelse med gjennomgangen av de enkelte sektorene

ovenfor. Det foreligger trolig ingen samlet oversikt over slike operatører og i hvilken grad disse er gjenstand for formelle krav.

Det øvrige næringslivet spiller også en helt vesentlig rolle i økonomien og i samfunnet. Næringslivets avhengighet til IKT-systemer, og den sårbarhet som ligger innebygd i disse IKT-systemene, kan medføre økonomisk skade for hele samfunnet og bør derfor ikke undervurderes.

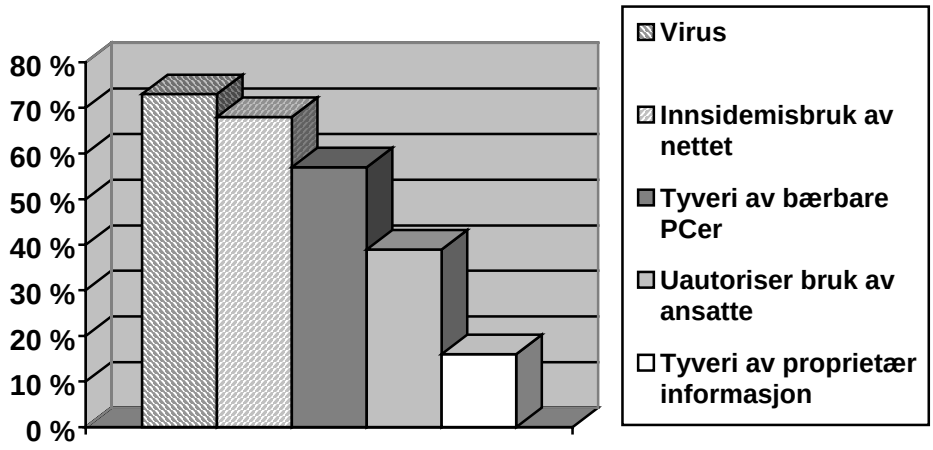
Betydelige forskjeller mellom norske bedrifter gjør det vanskelig å gi en felles beskrivelse av IT-sårbarheten i norsk næringsliv. For mange bedrifter vil opplysninger om inntrengningsforsøk være sensitiv informasjon, blant annet fordi markedet kan reagere negativt. Mørketallene antas å være store, og de få rapportene som eksisterer har klare metodiske svakheter. Behovet for økt kunnskap om situasjonen er betydelig.

IT-sårbarheten innen næringslivet antas generelt å være økende. I tabell 2.2 (s. 25) er det vist utviklingen i anmeldte lovbrudd som en indikator. Spesielt er økningen stor i 1998 og 1999 i forhold til foregående år. Dette bekreftes også av en undersøkelse fra Ernst & Young som gjengis nedenfor. Undersøkelsen er fra 1998 og er basert på en spørreundersøkelse der 188 virksomheter i Norge ga svar. Noen hovedpunkter er:

Risiko: 43 % av virksomhetene mener at deres informasjonssikkerhetsrisiko har økt det siste året.
Trusselbilde: Vel 40 % av virksomhetene sier de frykter datakriminelle mest.
Økonomiske tap: 60 % har hatt økonomiske tap på grunn av feil som skyldes uaktsomhet. Dette er en økning på 33 % fra året før. En fjerdedel av de som hadde økonomiske tap foretok seg ingen ting i etterkant. 57 % har hatt tap som følge av manglende tilgjengelighet, mot 28 % året før.
Policy: Seks av ti bedrifter har ingen sikkerhetspolicy eller –retningslinjer. Under 10 % har dokumenterte prosedyrer for å håndtere inntrengere.
Katastrofeplanlegging: Bare 27 % har en katastrofeplan. En tredjedel har aldri testet den.
Sikringstiltak: Risikovurderinger og vurdering av teknisk sårbarhet er blant de mest populære tiltakene, iverksatt av vel 40 %.
Internett: Bare 14 % bruker kryptering for å beskytte data som blir overført via internett.

Tilsvarende undersøkelser er utført i en rekke andre land. Ernst & Young konkluderer med at det synes å være en tendens til at man i Norge oppfatter det generelle trusselbildet som mindre truende enn man gjør i Sverige, Europa og i USA.

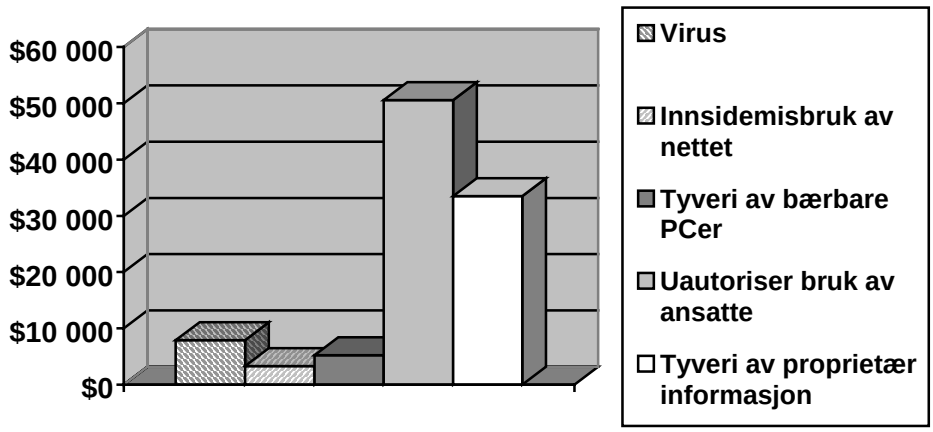
Når det gjelder frekvens av ulike typer hendelser er datagrunnlaget for Norge svært mangelfullt. I stedet gjengis tallmateriale fra USA. Vi ser ingen grunn til at tallene skal være svært forskjellige fra Norge, med unntak av at utviklingen kan ligge noe foran i USA i forhold til i Norge. Undersøkelsen vi refererer til er utført av Computer Security Institute (CSI) og FBI. Den omhandler 520 virksomheter. 64 prosent av disse svarte at de hadde blitt angrepet i løpet av det siste året. Denne prosentandelen har økt de tre siste årene som er referert (1996-1998).



Figur 3.3 Prosentandel av virksomheter som har blitt utsatt for ulike trusler i USA.

Virus er den mest vanlige trusselen, fulgt av misbruk av ansatte. Det er nesten seks ganger så vanlig å bli angrepet av virus som å bli utsatt for tyveri av proprietær informasjon. Vi ser også at misbruk fra ansatte er en svært vanlig angrepsmåte. Dette i motsetning til det som ofte er hovedantakelsen: At det i overveiende grad er utenforstående som gjennomfører angrepene. Samtidig ser vi at over 60 prosent av virksomhetene har vært utsatt for tyveri av bærbare PCer. I den grad tyveriet er foretatt for å skaffe seg en bærbar PC er hendelsen ikke alvorlig. Er derimot tyveriet foretatt for å få tilgang til sensitiv bedriftsinformasjon er det alvorlig. Tyveri av bærbare PCer er noen ganger ledd i industrispionasje.

Skaden av angrep kan vurderes i forhold til de økonomiske tapene som disse angrepene har påført den som ble angrepet. Det er meget vanskelig å anslå tap når man snakker om IKT-relaterte forbrytelser. Dette gjelder eksempelvis anslag av indirekte kostnader, slik som tap av ry, goodwill og fremtidige kunder. Er det tale om industrispionasje vil virksomhetens konkurransesituasjon kunne påvirkes. Økonomiske tap vil her være meget vanskelig å anslå.



Figur 3.4 Kostnader knyttet til trusler angitt i figur 3.3.

To kategorier peker seg ut i negativ retning i figur 3.4. Det er uautorisert bruk ved ansatte og tyveri av beskyttet informasjon. Dette er ikke overraskende. Selv om tyveri av beskyttet informasjon skjer sjelden, kan kostnadene være store fordi det kan gi betydelige konkurransefordeler for den som stjeler informasjonen. Slike angrep vil sannsynligvis være

målrettede mot en spesifikk type sensitiv informasjon, mens virus har en større tendens til å ramme "blindt".

Et økende problem både for næringslivet og samfunnet for øvrig knytter seg til tap av tjenestetilgjengelighet. I avsnitt 2.3.3.2 – Programvareangrep, omtales det som kalles Denial of Service Attacks (DoS), og de betydelig mer slagkraftige distribuerte DoS-angrepene. For ett år siden var distribuerte DoS-angrep et ukjent begrep i amerikanske sikkerhetsmiljøer. I februar 2000 ble en rekke slike angrep rettet mot ledende virksomheter som benytter Internett som kanal for handel. I løpet av en tre dagers periode ble Yahoo, Amazon, eBay, CNN.com, ZDNet, E*Trade og Excite.com gjenstand for total eller regional driftsstans i mange timer. En rekke andre firma og privatpersoner ble også rammet på grunn av trafikkork i nettet. De samlede tap anslås til å ligge i størrelsesorden ti milliarder kroner[18].

Distribuert DoS angrep er eksempel på en type angrep som utgjøre en økende trussel mot virksomheter som legger mye av sin forretningsdrift og kommunikasjon ut på Internett. Et vel forberedt distribuert DoS-angrep vil kunne ramme mange og skadene kan bli svært store. Problemet forsterkes ved at det i dag ikke finnes gode beskyttelsestiltak mot slike angrep. Bedrifter som planlegger å gjøre bruk av Internett i forretningsdrift og kommunikasjon må derfor nøye vurdere konsekvensene dersom tilgang til kommunikasjonsnettverk og -tjenester faller bort.

[18] Foredrag av advokat William Cook, Winston & Strawn, ved Telecommunications and Information Security Workshop, 27-29 september i Tulsa, Oklahoma. (Primærkilde er Yankee Group.)

4. Vurdering av infrastrukturenes sårbarhet

4.1. Vurdering av hver enkelt infrastruktur

Under følger en kort gjennomgang av enkelte av kjerneinfrastrukturenes sårbarhet i forhold til svikt i IKT-systemer. Denne bygger i hovedsak på funksjonsgjennomgangen i kapittel 3.

Telesektoren
Alle former for infrastruktur i telenettene vil være sårbare overfor fysiske trusler. Aksess- og transportnettinfrastrukturen vil være desidert mest utsatt fordi denne er vanskelig å beskytte. All tjenesteproduksjon og drift av nettstruktur og tjenester bygger på IKT-løsninger. Dermed vil disse delene av teleinfrastrukturen være mest utsatt for logiske og sosiale trusler. Konsekvensene av både logiske og fysiske angrep vil kunne bli langvarig svikt i tilgangen til teletjenester for brukerene. Særlig vil en kombinasjon av fysiske og logiske angrep være alvorlig.

I fredstid vil det være størst sannsynlighet for logiske angrep og i mindre grad fysiske angrep. Likevel har det vist seg at fysisk svikt som følge av graveuhell og lignende har vært den viktigste årsaken til svikt i teletjenester så langt.

Svikt i teletjenester som følge av svikt innen hvert enkelt av infrastrukturelementene vil kunne medføre alvorlige konsekvenser for samfunnet, selv under ellers normale forhold. Eksempler på generelle samfunnskonsekvenser som følge av svikt i telekommunikasjon kan være svikt i informasjon til befolkningen, svikt i alarm- og nødtelefoner, svikt i elektronisk betalingsformidling, svikt i vareforsyningen, svikt i sentraliserte funksjoner (for eksempel innen kraftbransjen), svikt i offentlige funksjoner som for eksempel helsetjenester, utbetaling av trygd og problemer med trafikkavvikling eksempelvis innen luftfart.

Kraftsektoren
Kraftsektoren er sårbar overfor svikt i IKT-systemer, både som følge av tilfeldig svikt og logiske/sosiale angrep. Dette er en sårbarhet som forventes å øke i fremtiden i takt med økt effektivisering og nedbemanning innen bransjen.

Et vellykket integritetsangrep mot IKT-systemene i produksjonssystemene og overføringssystemene for elektrisk kraft, vil kunne være alvorlig dersom det rammer de største aktørene. Gjennom slike angrep vil angriperen få kontroll med aggregatstyring ved kraftverkene og nettforbindelser i overføringsnettet, og vil dermed kunne bryte ned kraftforsyningen til forbruker. En trend mot færre og større aktører innen kraftproduksjonen vil kunne gjøre det enklere å ramme kraftforsyningen.

Et forhold som følger av økt effektivisering og sterkere utnyttelse av ressurser i bransjen, er mindre marginer og økende avhengighet av effektiv beslutningsstøtte for å hindre kaskaderende svikt. Det vil si at svikt på ett sted river med seg resten av systemet i en domino-effekt. Slik beslutningsstøtte er avhengig av fungerende IKT-systemer med tilgjengelig kommunikasjon med enhetene ute i nettet. Over tid vil dette øke avhengigheten til robuste IKT-systemer.

Kraftsektoren er svært avhengig av telekommunikasjon. Selv om sektoren i dag i hovedsak benytter egen teleinfrastruktur, som har særskilte krav til sikkerhet og robusthet, forventes sektoren i fremtiden i betydelige grad å bli avhengig av offentlige teletjenester.

Transportsektoren
Transportsektoren har i økende grad tatt i bruk og gjort seg avhengig av vel fungerende IKT-systemer. Mest karakteristisk er den økende avhengigheten av IKT-baserte flåtestyringssystemer for effektivisert godstransport. Disse er helt avhengig av en fungerende teleinfrastruktur. Ved svikt i disse systemene vil effektiviteten innen alle former for godstransport kunne reduseres dramatisk.

For den enkelte transportsektor er bildet forskjellig. Det rapporteres fra Vegvesenet at svikt i IKT-systemene for vegtrafikk kun i liten grad vil medføre konsekvenser for samfunnet, mens svikt i telesystemene for jernbanen derimot kan medføre betydelige konsekvenser for samfunnet. Luftransport utgjør imidlertid en sektor som er svært avhengig av IKT-systemer, og telekommunikasjon i særdeleshet. Dette er i den senere tid demonstrert gjennom en rekke sviktsituasjoner der lufttransport har stoppet opp som følge av at teletjenester har sviktet.

Olje- og gassektoren
Det konsekvente skillet mellom de mer åpne administrative nettverkene og de lukkede prosessnettene, som styrer produksjons- og leveransesystemene, er med på å forsterke robustheten i petroleumsvirksomheten. Det er i praksis små muligheter for at IKT-svikt ett sted i kjeden kan få avgjørende konsekvenser for totalleveransene fra norsk kontinental-sokkel. Imidlertid vil IKT-svikt ved spesielle transport- og leveransekoordineringssentre på fastlandet kunne medføre at formidlingen av leveranseoppdrag hemmes, og at transportsystemene utnyttes dårligere i den perioden svikten varer.

Videre finnes det sentrale knutepunkter i transportsystemet som må anses å være mer kritiske enn andre. Flere systemer vil på kort sikt ikke kunne erstattes av andre systemer. Til en viss grad kan man kompensere med prosedyrer, men ikke på en slik måte at man opprettholder full kapasitet i en reparasjonsfase.

Utviklingen av både teknologi og arbeidsprosesser fører til at driften av anleggene blir mer effektiv. Nye fiberkabler som knytter plattformene på sjøen sammen til landorganisasjonen gjør at stadig flere oppgaver som tidligere ble gjort på plattformene nå kan utføres på land. Dette kan føre til at også de rent operative oppgavene utføres fra land. Totalt sett kan vi derfor si at næringen kan gå mot å bli mer IKT-sårbar enn tidligere. Imidlertid må det her fortsatt skilles mellom de administrative nettverkene og prosessnettene.

Bank- og finanssektoren
Den sentrale utfordringen i utviklingen av betalingssystemene er avveiningen mellom hensynene til effektivitet og sikkerhet. Et moderne betalingssystem skal kunne behandle store transaksjonsmengder på kort tid og med høy grad av sikkerhet for betalerne, betalingsmottakerne og bankene.

Effektiviteten i det norske betalingssystemet har økt med utviklingen av datateknologiske løsninger, som har ført til større grad av automatisering i betalingsformidlingen. Samtidig har innføring av kostnadsorientert prising av betalingstjenester også bidratt til større effektivitet. Denne utviklingen kommer til uttrykk ved at banktjenester på Internett øker sterkt, mens bruk av papirbaserte betalingsinstrumenter avtar. På samme måte øker uttaket av kontanter fra

minibankautomater, mens uttak over skranke i bankene minker.

Denne utviklingen gjør at bank- og finanssektoren er svært avhengig av IKT-systemer. Betalingsoppdrag og finansielle transaksjoner passerer gjennom systemene til flere aktører. Funksjonsdyktigheten til et moderne betalingssystem er derfor avhengig av at den finansielle infrastrukturen virker.

I tillegg til utfordringene innenfor dagens betalingssystemer, stilles det nye krav til sikkerhet som følge av utbredelsen av Internett og elektronisk handel (e-handel). Økt anvendelse av betalingsmåter i åpne nett gir nye utfordringer og stiller økte krav til tillit og sikkerhet i fremtiden.

Politiet og redningstjenesten
Både politiet og redningstjenesten er avhengig av ulike former for kommunikasjonstjenester, både radiosamband og offentlige teletjenester. Den IKT-relaterte sårbarheten innen disse sektorene vurderes i hovedsak å være knyttet til tilgjengeligheten til disse tjenestene og IKT-basert brukerutstyr i tilknytting til anvendelsen av tjenestene. Sårbarheten er mer fremtredende i Redningstjenesten enn i Politiet.

Sykehussektoren
I sykehussektoren benyttes IKT i økende grad både i kjerne- og støttefunksjoner samtidig som at eksterne virksomhetskritiske leveranser til sykehus blir mer teknologistyrt. Parallelt med den bedring av kvalitet og effektivitet som anvendelse av IKT medfører utvikles en økende avhengighet til IKT-systemer.

Generelt vurderes sannsynligheten for sammenbrudd eller vesentlig reduksjon i virksomhetskritiske funksjoner som forholdsvis lav. Skulle det likevel inntreffe et sammenbrudd kan det imidlertid få svært store konsekvenser i alvorlighetsgrad og omfang. Muligheten for svikt i IKT-løsninger er absolutt til stede i forhold til flere aktuelle trusler, men sykehusene har beredskap i form a manuelle systemer som langt på vei kan kontrollere situasjonen og effekten.

Sykehusene er helt avhengig av tilgjengelige kommunikasjonstjenester, både gjenom radionett og offentlige teletjenester. Brudd i telekommunikasjon vurderes å gi umiddelbare konsekvenser for akuttmottakene.

Trygdesektoren
Etaten er meget avhengig av telekommunikasjon, bankenes utbetalingskjede, interne IKT-systemer og leverandører for å utøve drift og foreta utbetalinger. Trygdeetaten vil utbetale nesten 200 milliarder kroner over statsbudsjettet i 2000. Det vil få store konsekvenser dersom IKT-tjenester helt eller delvis skulle svikte i en krisesituasjon.

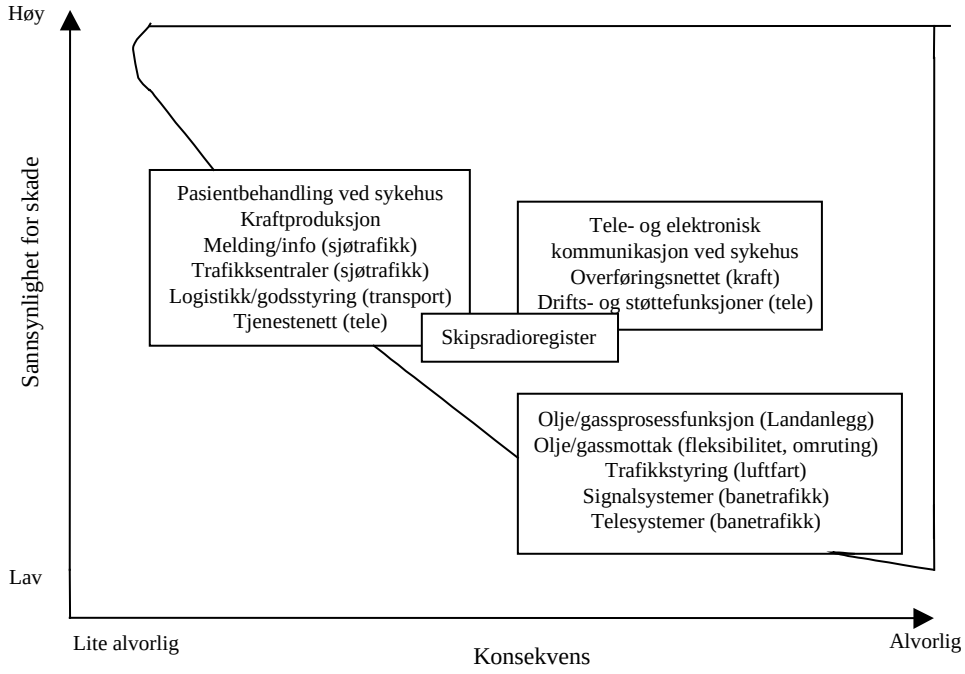
4.2. Sammenstilling av funnene

Et gjennomgående trekk ved alle funksjonene er en til dels betydelig avhengighet av IKT-systemer, både i form av den enkelte virksomhetens avhengighet av egne IKT-brukersystemer og i form av avhengighet av offentlige teletjenester. Robust tilgang til telekommunikasjon viser seg å være svært viktig for IKT-sårbarheten innen de fleste sektorene. Teletjenestene er igjen avhengig av IKT-systemer for å fungere. Robust kraftforsyning er også viktig for at all IKT-infrastruktur skal fungere. Fordi kraftforsyningen også er sterkt avhengig av IKT-systemer forsterkes også bildet av samfunnets avhengighet av IKT.

Forholdet mellom IKT-systemer generelt, telekommunikasjonssystemer og kraftforsyningen illustrerer også en utvikling mot økt gjensidig avhengighet på tvers av virksomheter og bransjer, der alle egentlig er avhengig av hverandre sine IKT-systemer.

Det er vanskeligere å få et klart bilde av hvor sårbar den enkelte funksjonen egentlig er. Særlig gjelder dette de enkelte vurderingene av sannsynlighet for svikt, der det fremkommer ulike oppfatninger for de enkelte virksomhetene. Det som er mer tydelig er at dersom det først skulle gå galt, selv om dette blir vurdert som usannsynlig, vil konsekvensene kunne bli betydelige allerede i dag. For mange av sektorene tyder innspillene på at avhengigheten til IKT-systemer og dermed konsekvensene av svikt vil øke i tiden fremover.

I figur 4.1 er hovedfunn fra de forskjellige sektorene forsøkt plassert inn i en grafisk modell, for å synliggjøre og identifisere de forskjellige funksjonenes IKT-sårbarhet. Dette er ikke en uttømmende oversikt. Det er en rekke problemer med å sammenstille funksjonene i en slik modell, og den kan lett feiltolkes hvis dens innhold ikke ses i sammenheng med de skriftlige vurderingene av sektorene. Plasseringen i en slik modell er ikke absolutt, men basert på fagpersoners ulike vurderinger. De ulike funksjonene har heller ikke fått en eksakt plassering, men er plassert innenfor et område. Modellen omfatter ikke alle funksjoner eller sektorer, og må ikke oppfattes som fullstendig. Jo høyere sannsynlighet for svikt kombinert med hvor alvorlig konsekvensen av en svikt er, jo mer sårbar er funksjonen. I henhold til de innspill som er innhentet for de enkelte funksjonene er det ikke identifisert funksjoner der sannsynligheten for svikt er høy samtidig som at konsekvensen av en eventuell svikt også anses å være svært alvorlig.



Figur 4.1 Sammenstilling av risiko på noen utvalgte områder.

Det er imidlertid viktig å understreke at innspillene i stor grad bygger på dagens situasjon. Med en utvikling der økonomien og samfunnet i økende grad integreres i det verdensomspennende informasjonsnettverket, der vi ikke en gang har full nasjonal

kontroll over den delen av nettverket som dekker eget landområde, er situasjonen bekymringsfull. Enkeltindividene, næringslivet og forvaltningen knytter seg nå nærmest ukritisk opp mot denne informasjonsinfrastrukturen, og blir dermed også helt avhengig av den. Samtidig ser vi at informasjonsinfrastrukturen og de kommunikasjonsløsningene som velges innehar betydelige svakheter. Enkelte hevder til og med at store deler av denne infrastrukturen vil kunne kollapse om få år. Selv om det kan argumenteres for at sannsynligheten for at dette vil oppstå er relativt lav, er likevel spørsmålet om vi som samfunn kan akseptere å utsette oss for slik risiko. Som beskrevet i avsnitt 3.15 har man i USA allerede sett at angrep mot e-handels bedrifter har fått store konsekvenser både for bedriftene som er rammet og kundene. Mye tyder på at vi nå er i ferd med å legge alle eggene i en kurv, der vi både som samfunn og enkeltindivider vil kunne oppleve alvorlige problemer dersom kurven skulle vise seg å briste.

Kunnskap om problemet er en sentral faktor. Vi tror mer enn vi vet. Det er mye usikkerhet om både trussel og virkning, særlig når vi ser litt frem i tid. Likevel tar vi i bruk de nye mulighetene - ofte uten kritisk å tenke på sikkerhet og sårbarhet.

Det er derfor av stor betydning at vi, samtidig som at vi utvikler insentiv for å fremme økonomisk vekst og velstand gjennom å ta i bruk de elektroniske mulighetene, også tenker på sikkerhet. Dette er to sider ved utviklingen som må utvikles i nært samspill.

Til tross for at det kan påvises at samfunnets sårbarhet øker betydelig som følge av den økte anvendelsen og avhengigheten til IKT, bruker vi i dag svært lite ressurser på å sikre oss mot dette. I kapittel 5 foreslås det derfor en strategi og et sett med tiltak som en første tilnærming til problemet.

5. Strategi og tiltak for sikring av IKT-systemer

5.1. Generelt om behovet for sikring av IKT-systemer

Utviklingen innen teknologi, teknologiavhengighet og trusler gjør det nødvendig for det moderne samfunnet å treffe tiltak for å redusere samfunnets sårbarhet. Dette gjelder uavhengig av om samfunnet befinner seg i fred, krise eller krig. Det foreslås derfor en overordnet målsetning for det videre arbeidet med IKT-sårbarhet og kritisk infrastruktur:

Å etablere robusthet i IKT-infrastruktur på et nivå som gjør det lite sannsynlig at viktige samfunnsfunksjoner stanses i en normalsituasjon. I en krise- eller krigssituasjon skal robustheten være tilstrekkelig til å opprettholde kritiske funksjoner.

For å realisere dette målet er det nødvendig med en helhetlig strategi, der det legges avgjørende vekt på de spesielle utfordringene IKT-sårbarhet stiller til samarbeid, informasjonsutveksling og fleksibilitet. Strategien må inneholde tiltak som har innebygd en høy grad av dynamikk og som gjenspeiler områdets raske utvikling.

Tiltak for sikring av IKT-infrastruktur vil fundamentalt bestå av en kombinasjon av *tekniske og organisatoriske tiltak*. De rent tekniske tiltakene benyttes for å redusere sårbarhet i enkeltfunksjoner og komponenter i det sammenknyttede systemet. Organisatoriske strukturelle tiltak brukes for å minimere betydningen av tekniske sårbarheter og imperfeksjoner gjennom blant annet å utnytte systemet som helhet best mulig. Dette kan være fordi det er teknisk umulig å redusere de tekniske sårbarhetene i tilstrekkelig grad eller fordi dette ikke er kosteffektivt.

Disse to typene tiltak har på mange områder så langt vært skjøttet av den enkelte infrastruktureier og har i overveiende grad vært tilstrekkelige i karakter og omfang. Telesektorens infrastruktur reguleres imidlertid av telelovens bestemmelser om sikring av det offentlige telenett på en rekke områder. Imidlertid utgjør infrastrukturene som er nevnt innledningsvis et mangfold både i struktur og når det gjelder kritikalitet for samfunnet. Tiltakene som kreves for å sikre disse infrastrukturene i fremtiden vil også være mangeartede. Systemer innen noen infrastrukturer krever sterkere former for tiltak enn andre, både med hensyn til organisatoriske og rent tekniske tiltak. For eksempel har Forsvaret i dag svært strenge regler for tilknytting av sine nettverk mot eksterne nettverk. Slike strenge regler vil imidlertid ofte være funksjonshemmende. Private leverandører av vitale infrastrukturtjenester vil også ofte anse at slike regler vil virke konkurransehemmende i et fritt marked, og vil til en viss grad kunne søke å unngå å etterleve disse.

Med bakgrunn i utviklingen som er skissert ovenfor er det et økende behov for en tredje type tiltak, som kan kalles *informative tiltak*. Dette dreier seg om et sett med overordnede tiltak som har som primært mål å bygge opp om og gjøre de to førstnevnte tiltaksgruppene mest mulig effektive. I korthet dreier dette seg om tiltak som øker kunnskapsoverføring både mellom ulike typer virksomheter og mellom

ulike kompetansekategorier i samfunnet. I den strategien som foreslås er denne typen tiltak dominerende.

5.2. Markedets evne til egenregulering av sårbarhet

Formålet med nasjonale strategier og tiltak for sikring av IKT-systemer er å sørge for sikringsmekanismer som oppfyller den overordnede målsettingen for IKT-sikring. Her inngår tiltak som den enkelte virksomhet som står for drift av IKT-systemer normalt selv ikke finner det hensiktsmessig å stå for. Dette kan være fordi den enkelte virksomheten i sitt eget perspektiv ikke finner dette økonomisk regningssvarende, eller at dette praktisk sett ikke er mulig å gjennomføre for den enkelte. To forhold er sentrale som forutsetning for den videre drøftingen av tiltak og strategier:

- Trusler
- Systemenes evne til egenregulering av sårbarhetsnivå ut fra markedskriterier

I dette bildet hører selvfølgelig også den statlige reguleringen som er bestemt gjennom den til enhver tid gjeldende lovgivningen, for eksempel teleloven.

Som beskrevet i kapittel 2 er trusselbildet i ferd med å bli bredere og mer sammensatt enn tidligere. Ikke minst vurderes logiske trusler mot åpne IKT-systemer i dag å utgjøre en betydelig trussel mot viktige infrastrukturer i samfunnet. Også aktørsiden går mot å bli mer mangeartet enn tidligere. Omfattende svikt som følge av i utgangspunktet enkle tilfeldige tekniske feil eller feiloperasjoner, er også i økende grad sannsynlig på grunn av systemenes kompleksitet. Hva som til enhver tid er det rette trusselnivået er imidlertid vanskelig å definere. Det er derfor en viktig samfunnsoppgave å sørge for at tidsriktig trusselinformasjon tilflyter alle aktørene i markedet, noe som er gjenspeilet i strategien som foreslås.

Leverandører av kritiske infrastrukturtjenester driver i økende grad sin virksomhet etter bedriftsøkonomiske prinsipper. Tidligere ble sikkerhet og beredskap hos mange av disse leverandørene bestemt av føringer gitt av sterke beredskapsorganisasjoner innen de enkelte virksomhetene, noe som har utgjort fundamentet for sikkerhet og beredskap frem til i dag. I dag er det i stedet markedet og kundenes daglige behov som er styrende for det sikkerhetsnivået den enkelte virksomheten har på sin vare- og tjenesteproduksjon. Nivået vil styres av forhold som skade på driftsutstyr, tapt fortjeneste som følge av driftsstans eller tapt omdømme i markedet. Virksomheter som leverer strøm, vann og telefoni, kan ønske å profilere at de tar sikkerhet på alvor, og gjennom dette gi virksomheten et kvalitetsstempel og en konkurransefordel. Denne typen regulering vil imidlertid i hovedsak være rettet mot hendelser som opptrer hyppig eller som medfører svært stor konsekvens. Denne reguleringsmekanismen vil i mange tilfelle sørge for et godt nivå, men vil ikke kunne dekke opp mot større og alvorlige trusler mot samfunnet.

En annen driver som i økende grad er viktig å ta med er forholdet til forsikringsmarkedet. Leverandører av infrastrukturtjenester, som tidligere i stor grad var selvassurandører, vil søke å minimere økonomisk risiko gjennom forsikringsordninger. Dette gjelder både skade på egne driftsmidler og leveringsavbrudd i forhold til kunde. Et eksempel på dette finner en innen kraftforsyningen der aktørene nå tar i bruk private forsikringsordninger. Dette

innebærer at forsikringsselskapene må opparbeide en betydelig kompetanse knyttet til risikovurdering for hver type forsikringsobjekt. Denne typen profesjonell risikokompetanse vil med tiden også utvikles til å dekke IKT-området og vurderes å bli en betydelig driver til å redusere samfunnets IKT-sårbarhet.

Selv om utviklingen som helhet går mot større IKT-sårbarhet finnes det dermed også i denne utviklingen drivere som til en viss grad balanserer ut denne sårbarheten gjennom en egenregulering. Disse driverne legges til grunn for utformingen og gjennomføringen av strategi og tiltak.

Fordi det er aktørene i markedet som til enhver tid har best forutsetninger for å kjenne teknologien og systemene, er det viktig å understreke at det er en fundamental forutsetning at strategien skal være et supplement til kreftene i et åpent fungerende konkurransemarked.

5.3. Strategi for å redusere samfunnets IKT-sårbarhet

Offentlig og privat sektor har felles utfordringer og et gjensidig avhengighetsforhold innen IKT-sårbarhet. Staten har ansvar for stabilitet, trygghet og et velordnet samfunn. Privat sektor er ikke bare en viktig leverandør av infrastrukturtjenester hvor det stilles krav om stabile leveranser, men er også avhengig av et effektivt økonomisk system for å operere i det nasjonale og det globale markedet. Det kan få store økonomiske konsekvenser for enkeltpersoner, virksomheter og offentlige etater hvis IKT-systemene deres er utilgjengelige eller ikke virker som forutsatt. Det er også nødvendig å vite at informasjonen ikke har blitt manipulert. Behovet for å beskytte elektronisk informasjon som lagres, behandles og formidles på nettet har økt sterkt. I det følgende beskrives elementer som foreslås å inngå i en strategi for å redusere samfunnets IKT-sårbarhet.

Partnerskap mellom private og offentlige myndigheter
Det bør etableres et partnerskap mellom myndighetene og virksomheter, som enten står for drift eller som er avhengig av IKT-infrastruktur. Dette er et overordnet prinsipp for flere av de tiltak som foreslås, og setter fokus på nødvendigheten av samarbeid, gjensidig tillit og utveksling av informasjon. Ikke minst er dette viktig i en utvikling der flere og flere operatører av vital samfunnsinfrastruktur går over fra å være offentlige forvaltninger til å bli private virksomheter. Her finnes det også en gråsone med virksomheter som helt eller delvis er eid av det offentlige, men som er pålagt å drive sin virksomhet etter rene kommersielle kriterier.

Vi ser at man også i andre land har valgt samarbeidsløsninger mellom det private og offentlige for å redusere samfunnets IKT-sårbarhet. Ideen om partnerskap er hentet fra USA, hvor dette er et hovedforslag i "Critical Foundations, The Report of the President's Commission on Critical Infrastructure Protection, 1997". I USA har en gjennom lang tid hatt et betydelig mer markert skille mellom privat og offentlig sektor enn i Norge. Utviklingen i Norge går imidlertid nå raskt i samme retning, særlig innenfor sektorer som telekommunikasjon og kraftforsyning. Med de nye utfordringene mot informasjonssamfunnet vurderes et slikt partnerskap av myndighetene i USA å være svært viktig. Også i Sveits arbeider en nå etter tilsvarende prinsipper.

Informasjonsutveksling
I tillegg til et behov for informasjonsutveksling gjennom et partnerskap, er det også et stort behov for å utvikle fleksible og dynamiske mekanismer for innbyrdes informasjonsutveksling mellom ulike typer virksomheter innenfor IKT-infrastruktur, både private og offentlige. Én viktig årsak til dette er at de gjensidige avhengighetene mellom de ulike virksomhetenes infrastruktur øker betydelig. Det vil si at virksomhetene i økende grad er avhengig av hverandre. Kompetanse og kunnskap er en annen viktig årsak. Kompleksiteten som ligger i systemer og infrastruktur er etter hvert blitt så stor at ingen kan ha full oversikt. I en slik situasjon vil et forum for informasjonsutveksling og samarbeide være svært viktig. Dette gjelder både mellom virksomheter innen samme bransje og mellom ulike typer bransjer.

En sentral problemstilling er at en slik informasjonsutveksling vil kreve en høy grad av tillit mellom aktørene fordi disse ofte vil være redde for å blottstille sikkerhetshull i egen virksomhet.

Øke varslingsevnen
Internett er nå i bruk innen alle deler av det norske samfunnslivet. Vesentlige deler av det norske samfunnsmaskineriet er i dag også en del av det globale nettverk, selv innenfor drift og produksjon av vitale infrastrukturtjenester. Dersom systemene ikke er godt nok beskyttet vil disse være enkle å trenge inn i og angripe. Mange operatører av kritisk infrastruktur har i dag ikke tilstrekkelig informasjon om verken sårbarhet eller trusler til å reagere raskt i en kritisk situasjon.

Det vurderes derfor å være behov for gjennom tiltak å tilrettelegge for teknisk overvåking, varsling og håndtering av sikkerhetshendelser mellom virksomheter. Viktige typer informasjon som må utveksles som del av et samarbeide dreier seg om inntrufne hendelser, om nye trusler og om alvorlige tilfeller av svikt i systemer. I kritiske situasjoner er det viktig for aktørene med rask varsling og informasjonsutveksling med andre aktører. Dette er nødvendig for at den enkelte aktør skal kunne respondere raskt med tidsriktige virkemidler i takt med at nye trusler kommer opp. Ikke minst vil et partnerskap med myndighetene gi mulighet for at det løpende blir utviklet gode og tidsriktige trusselvurderinger.

For å lykkes med strategielementene privat og offentlig partnerskap, informasjonsutveksling og økt varsling må noen forutsetninger oppfylles. Følgende faktorer er identifisert som viktige:
- *Økonomisk eller annen nytte av deltakelse.* Dersom deltakelse kan forhindre fremtidige tap eller gi virksomhetene et konkurransefortrinn øker sannsynligheten for at de vil delta.
- *Konfidensiell informasjonsbehandling.* Den informasjonen som den enkelte virksomhet avgir i form av hendelsesrapportering eller informasjon om konkrete mottiltak må behandles på en måte som skaper tillit. Anonymisering av informasjon før videre fordeling er en sentral utfordring.
- *Regi og opplegg for samarbeidet.* Forutsetningene for et samarbeid må være klare. Dette innebærer at det er tydeliggjort hvor mye samarbeidet koster, hvem som er initiativtaker, hvem som deltar, hvilket ansvar og oppgaver det enkelte medlem har, hva samarbeidet omfatter og hvilken informasjon som skal deles.

- *Likeverd.* Deltakerne i et samarbeid må oppfattes som likeverdige og alle bør bidra. Samarbeidet skal ikke føre til pålegg og deltakerne må enes om en felles plattform. Det er viktig at aktørene ikke bare gir fra seg informasjon, men at de også får informasjon tilbake.
- *Frivillighet.* Det er lite trolig at et pålagt samarbeid vil gi den fortrolighet og likeverd som skal til for å etablere et samarbeid for utveksling av sikkerhetsinformasjon.

Utdanning og kompetanseutvikling
Bevisstheten og kunnskapen om IKT-sårbarhet og sikkerhet er generelt for lav i mange organisasjoner og virksomheter. Personer som arbeider med IKT-sikkerhet blir ofte enslige svaler innen virksomhetene. Det er derfor behov for å etablere nettverk til andre som arbeider med det samme for å beholde motivasjon og få faglige oppdateringer, for dermed å kunne gjøre en enda bedre jobb. Det har oppstått et kompetansegap i forhold til hvor komplekse IKT-systemene er blitt, og i forhold til utfordringene som det nye trusselbildet gir. Det landsomfattende utdanningstilbudet innen IKT-sikkerhet bør styrkes, og det bør bygges opp mer spissede utdanningstilbud ved enkelte av institusjonene.

Forskning og utvikling
I dag finner vi ingen koordinert sivil analysevirksomhet eller statistikkinnhenting i Norge. Med unntak av hva som foregår innen enkelte bedrifter og i enkelte rene teknologiske miljøer, skjer det lite forskning på området. Mye av det som foregår er også lite tilgjengelig fordi det foregår i lukkede kommersielle miljøer. Det norske fagmiljøet på området er relativt svakt, selv om det er under oppbygging. Det er derfor behov for å iverksette tiltak for styrket forskningsaktivitet.

Sikring av infrastrukturer som er av vital betydning for samfunnets øvrige IKT-systemer
De bedriftsøkonomiske motivene for å forebygge skade begrunner ikke alltid like stor satsing på sikkerhet som de samfunnsmessige hensyn krever. Skade på infrastruktur vil i noen tilfeller påføre andre enn eierne uforholdsmessig mye større tap enn eierne selv. Enkelte infrastrukturer er av helt vital betydning for samfunnets øvrige IKT-systemer og bør derfor tillegges ekstra stor betydning. Dette gjelder i første rekke *offentlig telekommunikasjon*, som inkluderer så vel tradisjonelle teletjenester som anvendelsen av Internett som kommunikasjonstjeneste. Også en vel fungerende *kraftforsyning* er en fundamental forutsetning for at IKT-systemene i samfunnet skal kunne fungere.

Det meste av denne infrastrukturen er i sin natur vanskelig å beskytte. Imidlertid er vitale komponenter og delsystemer i disse infrastruktursystemene gitt en viss sikring, selv om det også kan rettes spørsmål mot denne med bakgrunn i den våpenteknologiske utviklingen. Nye private aktører i det konkurranseutsatte markedet har heller ikke gjennom arv tilgang til samme mulighet for fysisk sikring.

Begge typene infrastrukturer er også karakterisert gjennom omfattende anvendelse av IKT-systemer både i tilknytning til driftsoppgaver og tjenesteproduksjon. Sikring mot elektroniske og særlig logiske trusler mot infrastrukturene har det imidlertid så langt vært lagt lite fokus på.

Dette gjør det nødvendig for de respektive fagmyndighetene å stille krav til sikkerheten innen disse infrastrukturene som går lenger enn hva de enkelte infrastruktureierne finner bedriftsøkonomisk lønnsomt, og å kontrollere at kravene blir oppfylt. Disse kravene må innbefatte ulike former for tiltak rettet mot fysiske og elektroniske, så vel som logiske trusler. Det tidligere omtalte TIFKOM-prosjektet legger gjennom sine anbefalinger til rette for en ytterligere sikring innen telesektoren. Sårbarhetsutvalget foreslår i denne forbindelse at retningslinjene for sikring av kraftforsyningen tas opp til snarlig revisjon for også å innbefatte nye typer trusler.

Tilpasning av lover og regler
For myndighetene vil det være en utfordring å utvikle et juridisk rammeverk som fremstår som relevant og slagkraftig i forhold til den dynamikk i samfunnsutviklingen som informasjons- og kommunikasjonsteknologien skaper. Mange lover og regler er i dag ikke tilpasset utviklingen og de nye mekanismene som informasjonssamfunnet har ført med seg. En sentral utfordring på dette området er avveiningen mellom enkeltindividets frihet og behovet for kollektiv beskyttelse.

Telemyndigheten henviser for øvrig til en kommende gjennomgang av telelovgivningen med formål å oppdatere denne i forhold til åpningen av telemarkedet og den gradvise integrasjonen mellom media-, tele- og IT-sektorene.

5.4. Tiltak for å realisere strategien

Tiltak i en nasjonal strategi for sikring av vitale informasjonsressurser kan deles inn i tre hovedinnretninger, som innbyrdes er komplementære:
- *Grunnleggende tiltak* – tiltak som må gjennomføres på nasjonalt nivå for å utvikle folket, organisasjonene, lov- og regelverk og øvrige tradisjoner på en måte som gjør nasjonen som helhet bedre i stand til å møte angrep eller annen svikt i kritiske informasjonsnettverk.
- *Forebyggende tiltak* – tiltak som minimerer muligheten for at ulike former for angrep mot eller annen form for svikt i IKT-systemer skal få omfattende konsekvenser for anvendelsen av systemet. Herunder kommer også tiltak som virker avskrekkende for en eventuell angriper.
- *Tiltak for deteksjon og respons* (skadebøtende)– tiltak som sørger for identifikasjon og klassifisering av angrep og annen svikt, og som sørger for gjenoppbygging og reetablering av systemene til normal driftstilstand så raskt som mulig etter en svikt.

Innenfor disse hovedinnretningene foreslås det følgende tiltak som del av den strategien som ble presentert i avsnitt 5.3:
1. Etablering av Senter for informasjonssikring (SIS).
2. Program for forskning og utvikling.
3. Styrket utdanning og kompetanseutvikling.
4. Risiko- og sårbarhetsanalyser.
5. Brukerrettede tiltak.
6. Gjennomgang av behov for tilpasning av lover og regler.

Det første tiltaket – Senter for informasjonssikring – vil være innrettet mot alle hovedinnretningene som er nevnt ovenfor. De fire øvrige tiltakene vil i hovedsak være av grunnleggende karakter. Det ligger til grunn at forebyggende tiltak og tiltak for deteksjon og respons normalt bør ligge hos den enkelte aktør, fordi det er denne som har best forutsetninger for å planlegge og gjennomføre disse. Gjennom de foreslåtte grunnleggende tiltakene sørger imidlertid samfunnet for at aktørenes egne tiltak får en best mulig profil i forhold til brede samfunnsmessige hensyn.

5.4.1. Senter for informasjonssikring (SIS)

Som et av hovedtiltakene for å realisere strategien foreslås det etablert et Senter for informasjonssikring (SIS). Et grunnprinsipp for tiltaket er partnerskapet mellom myndighetene og ulike offentlige og private virksomheter. Senteret bør ha som overordnet målsetting å koordinere deler av innsatsen for å styrke IKT-sikkerheten og bidra til en mer robust IKT-infrastruktur. Senteret bør være et ressurs- og kompetansesenter for offentlige og private aktører. Det foreslås at senteret også blir tillagt operative oppgaver.

Det foreslås at SIS tillegges følgende hovedoppgaver, som i utstrakt grad vil være overlappende og innbyrdes avhengige:

- Gjennomføring av trusselanalyser og utarbeidelse av kortsiktig og langsiktig varsling til deltagerene.
- Operativt meldings- og håndteringssenter for sikkerhetsbrudd, som gir deltagerne mulighet til å respondere raskt med tidsriktige virkemidler.
- Utvikle kompetansenettverk og forestå informasjonsspredning og annet holdningsskapende arbeid overfor deltagerne.
- Bidra til generell informasjonsspredning med mål å styrke generell IKT-sikkerhetskompetanse og holdningsskapende arbeid i samfunnet som helhet.
- Forestå en aktiv dialog med institusjoner innenfor forskning og utvikling.
- Forestå kontakt og samarbeid med tilsvarende organisasjoner i andre land.

5.4.1.1. Oppgaver

Trusselanalyser

SIS foreslås å forestå en løpende innhenting av analyser om kortsiktige og langsiktige utviklingstrender i IKT-trusselbildet. En løpende innsamling av anonymisert statistikk om sikkerhetsbrudd i IKT-systemer, både innen offentlig forvaltning og næringsliv, inngår som en viktig del av denne oppgaven.

Formålet med dette er å sikre brukerne av senteret en god kunnskapsbase for både dagens og fremtidens trusler. Den bearbeidede informasjonen utgjør et viktig grunnlag for å kunne gi løpende trusselvurderinger og tidlig varslingsinformasjon til brukerne av SIS. Dette er kunnskap som er svært viktig for at den enkelte bruker skal kunne etablere et sikkerhetsnivå på systemer innen sin egen virksomhet som er best mulig balansert. Dette vil også være et viktig instrument for myndighetene i deres beslutningsprosess. Informasjonen vil også på et generelt nivå brukes for å øke bevisstheten om trusselbildet hos senterets kunder og ellers i samfunnet.
Trusselanalyse og varsling er en funksjon som vil ha en sterkt økende betydning i takt med at både IKT-systemer og trusler utvikles mot til å bli mer og mer sammensatte.

En sentral utfordring for SIS blir å håndtere informasjon som samles inn for analyse på en slik måte at de ulike kildene for informasjonen ikke kan spores og kompromitteres. Dette dreier seg i stor grad om sensitiv informasjon som må komme fra virksomheter innen næringsliv og offentlig forvaltning. Her må både krav til sikring etter beskyttelses- og sikkerhetsinstruksen og næringslivets krav til beskyttelse tilfredsstilles. Informasjonen må etter behandling presenteres på et aggregert nivå avhengig av hva den skal brukes til, og kildene må anonymiseres. Rutiner for dette vil kunne vise seg å bli en betydelig utfordring, noe man også har erfart i USA.

Hvor stor del av analysekapasiteten som skal ligge innenfor et SIS, og hva som bør ligge innenfor de tilknyttede organisasjonenes egen virksomhet må imidlertid utredes. Brede trusselanalyser krever bred kompetanse fra flere myndighetsmiljøer – både sivile og militære, og informasjonsgrunnlaget vil til dels være av svært sensitiv art. Det vil derfor være behov for en grenseoppgang. Selv om det må forutsettes at disse myndighetsmiljøene må ha en tilknytting til senteret, vil utveksling av sensitiv kildeinformasjon alltid være problematisk. Å finne mekanismer som tar hånd om dette på en tilfredsstillende måte er et klart suksesskriterium for gjennomføringen av senterets oppgaver.

Operativt meldings- og håndteringssenter
Det foreslås at det i SIS inngår et meldings- og håndteringssenter for sikkerhetsbrudd (MHS). Dette senteret foreslås å få en koordinerende og operativ rolle i forhold til aktører innen:

- Statlig, fylkeskommunal og kommunal forvaltning
- Forsvaret (Totalforsvaret)
- Private og offentlig eide operatører av vital infrastruktur
- Næringslivet for øvrig
- Institusjoner innen forskning og utvikling

Selv store organisasjoner med tung anvendelse av IKT-systemer opplever i dag at de er isolert og uten et egnet kontaktnett når det oppstår angrep eller større svikt i IKT-systemer. Mangel på krisehåndteringskompetanse fører ofte til lite effektiv situasjonshåndtering. Ofte vil eneste mulighet være å kontakte selskaper som kun har rene kommersielle interesser. Dette er blant annet en erfaring fra senere tids virus-angrep, gjennom ”I Love You”-viruset og etterfølgende varianter.

Den primære oppgaven for MHS vil være løpende innhenting og registrering av informasjon om angrep og annen svikt fra brukerne av senteret etter hvert som disse skjer. Med bakgrunn i tilgjengelig trusselinformasjon og tilknyttet krisehåndteringskompetanse, skal MHS bidra til at sikkerhetsbrudd håndteres effektivt på tvers av sektorer og organisatoriske skiller. Dette dreier seg om både kortsiktig og mer langsiktig bistand til den enkelte brukeren som er rammet. En viktig rolle for MHS vil være å bistå med å etablere og videreforedle nettverk med krisehåndteringskompetanse innen IKT-systemer.

Et forhold som må avklares er forholdet til Forsvaret og deres oppgaver i fred, krise og krig, både som bidragsyter og som eventuell bruker av et MHS. Selv om Forsvaret gjennom sine krigsoppgaver har klare særinteresser og krav, utgjør også Forsvaret en viktig funksjon i fred og krise som i mange sammenhenger yter tjenester til det sivile

samfunn. Forsvaret er også gjennom Totalforsvarskonseptet helt avhengig av både sivil offentlig forvaltning og næringslivet for å kunne fungere effektivt i en krigssituasjon.

Kompetansenettverk og informasjon
SIS bør forestå kompetansespredning til deltagere i næringsliv og offentlig sektor med mål å forebygge hendelser. Teknisk kunnskap om ulike sikkerhetstiltak er én faktor, men like viktig er det å utvikle de ansattes generelle kompetanse for blant annet å unngå feller som virus og dårlige passord. Det sistnevnte vurderes i dag å være et betydelig problem også innen virksomheter som står for drift av samfunnsviktig infrastruktur. Det er også behov for å spre informasjon om retningslinjer, standarder, lover og regler på området. Det bør vurderes å utarbeide ulike former for veiledning for hva som kan gjøres når sikkerhetsbrudd først har oppstått.

En sentral del av denne oppgaven vil bestå i å utvikle og vedlikeholde kompetansenettverk innen spesielle fagområder av felles interesse for deltagerne. Disse områdene vil endres over tid i takt med utviklingen. Dette kan for eksempel gjennomføres gjennom opprettelse av ulike typer fora der spesielle problemstillinger kan drøftes blant deltagerne. Et annet eksempel er å påvirke og bistå bransjeorganisasjoner og tilsvarende organisasjoner i at det tas opp IKT-sårbarhetsrelatert stoff i kursopplegg, seminarer og andre sammenhenger. SIS bør også kunne stå som arrangør for seminarer og konferanser der spesielle problemstillinger tas opp.

Et annet konkret eksempel på kompetanseutvikling og informasjonspredning er utvikling av en veileder for sikring av IKT-systemer. Målsettingen med et slikt dokument vil i første rekke være å sette i gang en prosess med å utvikle sunne prinsipper for sikring av IKT-systemer, men som i neste omgang kan anvendes av deltagerne ved planlegging av egne IKT-systemløsninger. Veilederen må være levende i den forstand at de ulike kompetansemiljøene innen SIS gjennom løpende diskusjon og andre bidrag sørger for at den er oppdatert etter gjeldene trussel- og teknologiutvikling. Et eksempel på informasjon som kan finnes i en slik veileder er tilgjengelighet til ulike typer sikkerhetssystemer i et IKT-system, for eksempel sikkerhets-scannere for nettverket eller brannmurer. En slik veileder vil også kunne utvikles til å inneholde anbefalinger med hensyn til valg a ulike produkter og hvordan disse best bør konfigureres, der det også kan inngå en løpende oppdatert oversikt over kjente svakheter ved disse produktene. Critical Infrastructur Assurance Office i USA har stått for utarbeidelsen av en første versjon av et lignende dokument ”Best Practices for Securing Critical Information Assets”, som nå i første omgang benyttes som grunnlag for diskusjon.

En slik veileder vil, i tillegg til den direkte nytten den har for de deltagende virksomhetene, også være et viktig informasjonsunderlag når myndighetene skal utarbeide krav og retningslinjer til sikring av IKT-systemer innen vitale infrastrukturer, som for eksempel telekommunikasjon. Dette vil blant annet kunne bidra til at kravene som stilles raskere blir realistiske og forenlig med hva som er kostnadseffektivt målt opp mot akseptert risiko.

Generell informasjonsspredning
SIS vil som foreslått utvikles til å bli et kompetansesenter for IKT-sårbarhet. SIS bør derfor også medvirke til generell kompetansespredning i samfunnet som helhet.

Forskning og utredninger
Forskningsmiljøene bør ha en sterk kompetansemessig tilknytning til SIS. SIS bør også ha som oppgave å opprette og videreutvikle en aktiv dialog mot utdannings- og forskningsmiljøene for å øke fokuset om IKT-sikkerhet. Ikke minst gjelder dette idéer og forslag til igangsetting av forskningsprosjekt innen IKT-sikkerhet.

Internasjonale kontakter
Flere nasjoner i den vestlige verden er nå i ferd med å etablere organisasjoner med lignende innretning som det her foreslås for SIS. Fordi IKT-sårbarhet er et grenseløst problem er internasjonalt samarbeid på flere nivå svært viktig. SIS bør være det nasjonale kontaktpunktet mot internasjonale søsterorganisasjoner slik at tillitsforhold også opprettes og vedlikeholdes overfor disse. Utvikling av kompetansenettverk på tvers av nasjonsgrensene er av sentral betydning.

Det er imidlertid viktig å understreke at dette må komme som et komplement til og samordnes med annen internasjonal kontakt på området innen justis- og forsvarssektoren.

5.4.1.2. Deltagelse
Deltagelsen i SIS bør være så bred som mulig. Det er også viktig å sørge for en balansert deltagelse uten at enkelte sektorer eller bransjer blir for tunge. Det er videre viktig å sørge for at senteret gjenom deltagende virksomheter blir tilført den nødvendige kompetansen, samtidig som at senteret ikke dupliserer eksisterende aktiviteter i andre organ. Det må derfor forventes at for enkelte samfunnssektorer og virksomhetsområder, som allerede har etablert en omfattende aktivitet på området, vil senteret ha en mer koordinerende og analyserende rolle.

Virksomheter som inngår som deltagere eller ressurser i et SIS vil være:
- Spesielle myndighetsorgan
  – Etterretnings, overvåkings- og sikkerhetstjenestene (EOS)
  – Politiet
  – Sektormyndigheter for vital infrastruktur
- Øvrig statlig, fylkeskommunal og kommunal forvaltning
- Private og offentlige infrastruktureiere og deres bransjeorganisasjoner
- IKT-næringen
- Næringslivet for øvrig
- Bransjeorganisasjoner
- Institusjoner innen forskning og utvikling

Fra offentlige myndigheter inngår justismyndighetene og nasjonale sikkerhetsmyndigheter som sentrale aktører, ikke minst når det gjelder bidrag til trusselanalyser og varsling. Også myndighetsorgan med ansvar for sektorvis beredskap bør ha en tilknytting til senteret. De sistnevnte har blant annet et ansvar i å bestemme ambisjonsnivået på sikring av vital samfunnsinfrastruktur.

I gruppen infrastruktureiere inngår alle som eier og opererer IKT-systemer som del av sin produksjon av varer og tjenester. Forholdet mellom disse aktørene og næringslivet

for øvrig vil ofte kunne være et kunde-leverandørforhold og dels være et konkurranseforhold. Dette utgjør også en av de store utfordringene for et senter, fordi en innen den enkelte virksomheten vil kunne finne mye informasjon om foretningsstrategier gjennom informasjon om IKT-systemer. Det vil også kunne oppstå spenninger mellom store leverandører av tjenester og brukerne av tjenestene. Erfaring fra andre land har vist at bransjeorganisasjonen kan ha en viktig rolle i en slik sammenheng.

I gruppen forskning og utvikling finner en først og fremst offentlige og private forsknings- og utdanningsinstitusjoner fordi disse vil ha en sentral rolle med hensyn til både kortsiktig og langsiktig kompetanseutvikling. I denne sammenhengen er det også av interesse å nevne forsikringsbransjen og enkelte konsulentselskaper med kjernekompetanse. Disse vil gjennom sin kommersielle virksomhet blant annet opparbeide sentral metodekunnskap knyttet til IKT-sårbarhet.

Den enkelte virksomhetens tilknytningsform til SIS og hva dette vil innebære må konkretiseres i det videre arbeidet.

5.4.1.3. Organisering

SIS foreslås organisert på en ikke-profitt og ikke-kommersiell basis, der aktiviteten finansieres med bidrag fra medlemmene og Staten. Ett eksempel på en mulig organisasjonsform er en stiftelse. Organisasjonen må tilføres styringsmekanismer som gjør at medlemmene og Staten i fellesskap løpende kan sørge for at virksomheten får en formålstjenlig utvikling.

Et sentralt tema er om den overveiende delen av aktiviteten i senteret skal samles til en tung sentral enhet, eller om det i stedet skal etableres en sentral koordinerende enhet, som kun står for en begrenset kjernevirksomhet, og som knyttes sammen med flere bransjevise enheter. De ulike land velger ulike løsninger for dette, og erfaringene så langt viser at det neppe eksisterer en optimal løsning. En mulighet er at det legges opp til at de enkelte bransjene og sektorene selv velger den løsning de ser som mest tjenlig for seg selv. I et lite land som Norge er det i praksis begrenset hvor mange enheter man kan etablere. Selv i USA har det vært tungt å etablere bransjevise varslingssentra, og foreløpig er det kun innen finans- og energisektoren en har lykkes. Innen kraftforsyningssektoren i USA har det for øvrig vist seg at en sterk bransjeorganisasjon har vært et suksesskriterium. Her er det igangsatt et pilotprogram i samarbeid mellom en bransjeorganisasjon og myndighetene.

Det tidligere omtalte TIFKOM-prosjektet har foreslått at det i Norge etableres et beredskapsorgan for telekommunikasjonssektoren. Et slikt organ må ha en tett tilknytting til SIS først og fremst fordi en innen telesektoren er svært avhengig av IKT i forbindelse med tjenesteproduksjon og driftsoppgaver. NTSB vil i tillegg også kunne utgjøre en viktig kompetansebase for SIS i telekommunikasjonsspørsmål.

For offentlig virksomhet bør det antagelig organiseres en egen enhet. Det er en viktig oppgave å mobilisere og informere statsforvaltningen, kommunale og fylkeskommunale virksomheter. I dag rapporterer disse i liten grad om aktuelle hendelser, og det er god grunn til å tro at det skjer en omfattende underrapportering fra det offentliges side.

Det bør unngås å etablere tjenester innen områder hvor det allerede er et godt tjenestetilbud. En mulighet er å bygge videre på den kompetanse og de ordningene som allerede eksisterer i Norge, og å legge senteret til en eksisterende institusjon. Det er behov for å foreta en nærmere vurdering av hva som er aktuelle alternativer og den beste løsningen.

Et annet sentralt spørsmål er forholdet mellom SIS og myndighetene i en beredskapssituasjon. SIS kan da ha en viktig rolle som rådgiver for myndighetene når det gjelder trusler og mulige virkemidler. Det er imidlertid nødvendig å avklare hvilken formell rolle senteret skal ha i forhold til beredskapslovgivningen i krise og krig. Det er viktig at det ikke legges inn føringer som påvirker senterets mulighet til å fungere i fred.

For å komme raskt i gang foreslås det igangsatt et forprosjekt i regi av Nærings- og handelsdepartementet. En viktig del av forprosjektet vil være å kartlegge næringslivets interesse for deltagelse i og bidrag til SIS.

5.4.2. Styrket innsats for forskning og utvikling

IKT-sårbarhet og -sikkerhet er et relativt nytt fagområde i Norge hvor det innen sivil sektor finnes liten forskningsinnsats. Følgelig er det en mangel på kompetanse. Det vurderes å være et betydelig behov for samordnet innsats på flere felt innen området. Det foreslås derfor etablert et strategisk forskningsprogram innen IKT-sårbarhet og sikkerhet. Et slikt strategisk program bør også følges opp i de brukerstyrte forskningsprogrammene med bevilgninger til prosjekter innen IKT-sårbarhet og sikkerhet. Det er viktig at privat næringsliv deltar i denne forskningsinnsatsen, i tråd med partnerskapstankegangen.

Forskningsinnsatsen innen IKT-sårbarhet bør lede til følgende:
- Grunnleggende kompetanseoppbygging i samfunnet innen IKT-sårbarhet og sikkerhet.
- Øke kunnskapsnivået innen offentlig forvaltning for å styrke beslutningsgrunnlaget i spørsmål som gjelder IKT-sårbarhet og sikkerhet.
- Øke bevissthets- og kompetansenivået i virksomheter som i sin produksjon av varer og tjenester er avhengig av sikre IKT-systemer.
- Sørge for at det utvikles ulike former for sikkerhetsmekanismer på ulike organisatoriske og tekniske nivå som på sikt vil kunne bidra til å styrke sikkerheten i IKT-systemer.

Innen hvilke områder det er behov for spesiell forskningsinnsats vil måtte være gjenstand for en løpende vurdering. En vil til en viss grad oppleve en kobling mellom det som kan kalles forskning og det som mer vil fortone seg som utredning. Imidlertid er det viktig - særlig innledningsvis - å se dette i nær sammenheng fordi det er et stort behov for å etablere et egnet metodeunderlag, som også kan benyttes i en videre utredningssammenheng. Noen hovedområder der det vurderes å være behov for IKT-sårbarhetsrelatert forskning er:
- Samfunnsmessige og kulturelle aspekter.
- Sårbarhetsanalyser og systemanalyse – metoder.
- Trussel og trusselvurderinger.

- Teknologiske problemstillinger – IKT-sikkerhet.

Samfunnsmessige og kulturelle aspekter
IKT-systemer vil i økende grad påvirke og bli påvirket av sosiale og kulturelle forhold i samfunnet. Samfunnet vil bli mer og mer avhengig av IKT-systemer for å være i likevekt. En kan anta at det med økende avhengighet til IKT også blir større risiko for at svikt i enkelte vitale IKT-systemer vil kunne forstyrre denne likevekten alvorlig. Innsikt om hvordan et samfunn eventuelt vil kunne rammes av svikt i IKT-systemer vil være en viktig del av et helhetlig arbeide med å sikre systemene og samfunnet.

Arbeid innen dette området bør også kunne samordnes med brukerstyrte forskningsprosjekter. Ett eksempel kan være forskning innen IKT-anvendelse i varetransportsektoren, der en også legger innsats i å studere de konsekvenser ulike former for IKT-relatert svikt vil få for sektoren og samfunnet som helhet.

Sårbarhetsanalyse og systemanalyse
Risiko- og sårbarhetsanalyser er en viktig type verktøy ved håndtering av sårbarhets- og sikkerhetsspørsmål i store og små systemer. Denne analyseformen danner et viktig grunnlag for beslutningsstøtte fordi en beslutningstaker gjennom denne kan opparbeide forståelse om komplekse system på en strukturert måte. Analysen kan gjennomføres på et overordnet plan der målsettingen mer går på bevisstgjøring og holdningsskapende arbeid i forhold til sikkerhets- og beredskapsansvarlige, eller som mer detaljerte analyser der målsettingen er å fortelle en konstruktør hvilke konkrete sårbarheter systemet innehar. Begge typer analyser har i lang tid vært gjennomført med bruk av hevdvunne metoder.

Dagens IKT-infrastruktur bygger ofte på svært komplekse systemer, der mennesker og teknologi er tett integrert. Disse sosio-tekniske systemene trenger nødvendigvis ikke å være så komplekse teknologisk, men de vil likevel i sin struktur kunne være svært komplekse og dermed vanskelige å forstå. Ofte vil disse strukturene gå på tvers av ulike sektorer. En vil kunne finne at deler av strukturene er under kontroll av konkurrerende virksomheter. Gjennom internetteknologien er det mulig å bygge sammen ulike systemer, som også kan være basert på flere grunnteknologier, til store verdensomspennende nettverkssystem. Denne sammenbyggingen kan gjennomføres desentralisert uten noen helhetlig overordnet arkitektur eller sentral kontroll. Dette innebærer stor fleksibilitet i utbyggingen av strukturene i systemet, men gjør det i ettertid vanskelig å forstå hva som skjer hvis deler av systemet utsettes for svikt, enten denne kommer som følge av en tilfeldig hendelse eller skjer med ond vilje. Det har i slike systemer ofte vist seg at en ikke har hatt oversikt over hvilke ressurser systemet som helhet har vært avhengig av. Det har derfor heller ikke vært mulig å gjennomføre tilstrekkelig gode sårbarhetsanalyser.

Ett eksempel på en slik systemanalyse er modellering av gjensidige avhengigheter innen nettverkssystem. I USA er man i ferd med å utvikle en metode for slik analyse, der de for tiden også er i gang med å gjennomføre analyse av vitale systemer innen de føderale sektorene. På lengere sikt ser en for seg at dette metodeapparatet også skal tas i bruk innen privat sektor. Så langt har en funnet oppsiktsvekkende resultater, der en blant annet har funnet ut at systemressurser som befinner seg på USAs vestkyst har

vært kritisk for systemer som de i utgangspunktet trodde var begrenset geografisk til Washington DC[19].

Det vurderes derfor å være behov for å videreutvikle risikoanalysen til å håndtere mer dynamiske og komplekse fenomener, og til å inkludere menneskelige og organisatoriske aspekter på en bedre måte enn i dag. Her kan det pekes på at vi i Norge som følge av oljevirksomheten i Nordsjøen er langt fremme når det gjelder risikoforskning. Selv om mange problemområder er forskjellige bør det likevel være mulig å dra betydelige synergieffekter innen dette området.

Trussel og trusselvurdringer
En viktig forutsetning for sårbarhets- og sikkerhetsarbeid er kunnskap om hvilke utfordringer som legges til grunn for arbeidet. Trusselvurderinger utgjør et viktig element i enhver risiko- og sårbarhetsanalyse. Fordi systemene frem til i dag har vært bygget på lukket teknologi og har vært enkle i sin struktur, har en i hovedsak vært opptatt av pålitelighetsaspektet. Dagens IKT-systemers åpne arkitektur gjør at disse også er utsatt for ulike former for angrep. At disse systemene i økende grad tilknyttes det globale Internettet øker denne utsattheten betydelig.

Dagens sikkerhetspolitiske bilde er mer nyansert enn før, noe som også kan sies om ulike former for kriminell aktivitet. Forebyggelse av kriminalitet, ulykker og andre trusselkilder krever spesifikk samfunnsvitenskapelig kunnskap for å kunne identifisere og prioritere problemer og tiltak. Det er ikke åpenbart hva som er de mest effektive og samtidig de mest akseptable mottrekkene. Det vurderes derfor å være behov for økt innsikt innen dette området for løpende å kunne håndtere denne delen av utviklingen i en stadig skiftende verden. Analyse av trusselutvikling og varsling utgjør for øvrig også en sentral funksjon i Senter for informasjonssikring.

Teknologiske problemstillinger
Under teknologiske problemstillinger finnes en rekke delproblemstillinger knyttet både til grunnteknologi og arkitekturer i IKT-systemer. Dette gjelder både programvare-, maskinvare- og infrastrukturrelaterte problemstillinger, der det vurderes å være behov for utvikling av teknikker for beskyttelse, respons og skadereduksjon og reetablering av systemfunksjonalitet etter svikt. Også pålitelighet i programvarebaserte systemer med høy kompleksitet inngår som en naturlig del av dette området.

Noen eksempler på mulige forskningsområder er:
- Utvikle teknologier, arkitekturer og organisatoriske løsninger som gir beskyttelse mot både tilfeldig svikt og angrep.
- Utvikle automatiske mekanismer for sikkerhetsmonitorering (sårbarhets-scanning) for å kontrollere at IKT-systemer ikke brukes av de legitime brukerne på en måte som ikke er forenlig med gjeldene sikkerhetspolicy og prinsipper.
- Utvikle mekanismer for inntrengningsmonitorering og deteksjon av mulige angrep mot nettverk (anomalideteksjon).
- Utvikle mekanismer for å inngå i tiltak som reduserer skaden av en teknisk svikt eller angrep. Eksempler på slike mekanismer er teknikker for avskjerming av

[19] Hagen/Nystuen, Forsvarets forskningsinstitutt (2000): "Beskyttelse av kritisk infrastruktur – Besøk ved private og offentlige virksomheter i Canada og USA 31 januar – 4 februar 2000, FFI/REISERAPPORT-2000/01096.

nettressurser (deler av nettet), teknikker for avskjerming av aksess til systemene og lignende.
- Teknikker for å finne ondartet kode og annen programvareanomali både med hensyn til standardisert programkode (operativsystemer) og applikasjonsprogramvare. Dette vil blant annet være et nyttig tiltak for styrke integritetsvernet i programvare til kontroll- og driftssystem innen vital infrastruktur, såkalte SCADA-system (Supervisory Control and Data Aqusition), der såkalte trojanske hester utgjør en betydelig trussel (se avsnitt 2.3.3).
- Forståelse av den menneskelige faktor i sammenheng med IKT-sikkerhet.

Det foreslås at en styrket innsats innen forskning og utvikling organiseres gjennom NFR. Det er derfor allerede foreslått et forprosjekt under NFR som har som mål å utarbeide et forslag til forskningsstrategi innen området. Det er viktig at denne strategien relateres til andre relevante pågående og fremtidige forskingsprogram innen IKT-området. Sentrale problemstillinger i dette forprosjektet vil være å kartlegge hva som i dag foregår av relevant IKT-sårbarhets- og sikkerhetsforskning og hvilke miljøer som står for denne.

5.4.3. Utdanning og økt kompetanse

Et av hovedproblemene innen IKT-sikkerhet i dag vurderes å være manglende bevissthet og kompetanse innen mange virksomheter. Kompetent personell innen fagområdet er en mangelvare, og det er følgelig behov for å styrke IKT-utdanningen med fokus på sikkerhet på alle nivåer, fra videregående skole til universitet. Det foreslås en modell hvor sikkerhet integreres i IKT-utdanningen, og blir en større del av denne enn det en finner i dag. Dette vil bidra til å styrke kompetansenivået innen IKT-sikkerhet i det brede. I tillegg er det behov for spesialkompetanse ved at IKT-sikkerhet etableres som eget fag ved enkelte universiteter og høyskoler.

Mange av de som i dag er engasjert i drift av IKT-systemer har enten ingen formell bakgrunn for dette eller har en utdanningsbakgrunn som er foreldet. Det er derfor også viktig at det legges opp til videre- og etterutdanning innen området. Dette kan skje på en generell IKT-plattform eller innenfor en bransjeutdanning.

Det foreslås at dette hovedtiltaket også inngår som et av aktivitetsområdene til Senter for informasjonssikring, som kan stå for en faglig pådriverrolle.

5.4.4. Risiko- og sårbarhetsanalyser

Risiko- og sårbarhetsanalyser blir i stadig økende grad viktige instrumenter for å ta hånd om sårbarhets- og sikkerhetsspørsmål i samfunnet. Slike analyser brukes i dag blant annet i prosessindustrien, der virksomhetene i Nordsjøen har gått foran. Også i norske kommuner har en tatt i bruk slike analyser, men på et høyere virksomhetsnivå.

Risiko- og sårbarhetsanalyser kan foregå på et overordnet virksomhetsnivå med et høyt abstraksjonsnivå, eller de kan være detaljerte og dreie seg om for eksempel en teknisk prosess. Hensikten med den første typen analyse vil først og fremst være å identifisere kritiske funksjoner og finne ut hva som skjer hvis disse svikter, men uten at en går inn i detaljer i disse funksjonene. Slike analyser er ofte kvalitative der det overordnede målet er å fremme kunnskap om system og organisasjon. Den andre

typen, som representerer en motsatt ytterlighet er ofte rent kvantitative og beskriver i detalj både sannsynlighet for svikt i systemet og konsekvensen av eventuell svikt. Konsekvens beskrives ofte i monetære verdier eller tap av liv. Begge typer analyser – og spennet mellom dem – er viktige verktøy for beslutningsstøtte.

Det bør derfor arbeides for at risiko- og sårbarhetsanalyser blir tatt i bruk av virksomheter som er avhengig av IKT-systemer, både innenfor næringsliv og forvaltning. Risiko- og sårbarhetsanalyser bør gjennomføres som en integrert og rutinemessig del av den enkelte virksomheten. Slike analyser kan også anvendes av myndighetsorganer med overordnet fag- og tilsynsansvar som et fundament for kontakt med næringslivet. I visse sammenheng kan de også danne grunnlag for kravspesifikasjoner og iverksettingen av tiltak innen viktige samfunnsviktige systemer.

Det må imidlertid utvikles hensiktsmessige metoder og verktøy for dette (se avsnitt 5.4.2). Analyseverktøyet bør blant annet bli mer enhetlig slik at analysene også kan nyttes i tverrsektorielle vurderinger. Oppfølging av risiko- og sårbarhetsanalysene med tiltak er et ansvar som må forankres i ledelsen i hver virksomhet.

5.4.5. Brukerrettede tiltak

Selv om det innen de enkelte infrastrukturene settes i verk ulike tiltak for å redusere sårbarhet, vil disse aldri kunne bli tilstrekkelig robuste stilt overfor enhver mulig utfordring. Derfor er det viktig også å rette tiltak direkte mot sluttbrukerne, som befinner seg i enden av verdikjeden. Målgruppen sluttbruker dreier seg om alt fra privatpersoner til virksomheter i næringsliv og offentlig forvaltning.

Det er viktig å sørge for at sluttbrukeren til en hver tid er klar over hvor sårbar vedkommende er på områder denne vanskelig selv kan ha full kunnskap om eller kan ha mulighet til påvirke. Sluttbrukerne bør også på en egnet måte få informasjon om tilgjengelige teknikker for å redusere egen sårbarhet. Dette kan gjøres gjennom utvikling av ulike typer veiledere. Det bør fra samfunnets side også legges til rette for at sluttbrukeren skal kunne ta i bruk tiltak, for eksempel slike som tilbys i infrastrukturer for bruk av elektroniske signaturer.

5.4.6. Lovverk og kriminalitetsbekjempelse

Det er en hovedutfordring å skape et mer dynamisk lovverk som reflekterer den raske teknologiutviklingen. Dette er viktig av to årsaker. For det første er lovverket sentralt i forhold til kriminalitetsbekjempelse der det brukes som et instrument for å avskrekke mot handlinger som er uheldige for samfunnet. Lover og regler har også tradisjonelt vært benyttet som et instrument til holde samfunnets sårbarhet på et akseptabelt nivå i forhold til aktører som eier eller står for drift av kritiske samfunnssystemer. Dette er nærmere behandlet i avsnitt 5.6.

Det er vanlig å betegne ett Internett-år som sju vanlige år med hensyn til hastighet i utviklingen. Lovforberedelse er imidlertid en grundig prosess som kan ta flere år. Lovutformingen står i fare for å bli akterutseilt i forhold til det samfunnet lovene skal regulere. Det vurderes derfor å være et behov for å innføre mekanismer som gjør at lovforberedelse på dette feltet kan skje raskere.

Det er videre et behov for å gjennomgå den øvre strafferammen for datainnbrudd, som nå er inntil seks måneder. Ved straffeskjerpende omstendigheter kan straffelovens § 145, tredje ledd, lede til fengsel i inntil to år for datainnbrudd. Sårbarhetsutvalget vurderer dette som lavt i forhold til hvor alvorlige konsekvenser datainnbrudd kan ha, og i forhold til allmennpreventive hensyn. Den ordinære strafferammen for ordinære innbrudd er fengsel i inntil ett år, jf. straffelovens § 147, med mulighet for å gå opp til fire år ved straffeskjerpende omstendigheter.

En annen hovedutfordring er at lovverket er nasjonalt, mens systemene rekker over landegrensene. For Internett-angrep eksisterer ikke landegrenser, noe som kompliserer politiarbeidet, og stiller krav til internasjonalt samarbeid og etterforskning. En hacker kan være fra et land Norge ikke har utleveringsavtale med. Dette reiser også spørsmål om informasjon på Internett kan lovreguleres eller om nettet er et anarki. Hvis man ønsker å publisere noe på Internett som er ulovlig i ett land, kan man benytte seg av tjenestetilbydere (ISPer - Internett Service Providers) i et annet land hvor dette er lovlig. FBI i USA har tatt konsekvensen av dette og har gjennom de senere årene utvidet sin rolle i det internasjonale politisamarbeidet med opprettelse av en rekke nye regionale kontorer, blant annet ett i København for Skandinavia.

Enda en hovedutfordring er personvernet og hvordan forholdet mellom teknologi og individ bør reguleres. Dagens utstrakte bruk av kort og mobiltelefon gjør at vi legger igjen stadig flere elektroniske spor. Av mange grunner kan det være ønskelig å koordinere og koble informasjon om enkeltmennesker for å bedre informasjonskvaliteten, og for å fremskaffe mer kunnskap om den enkelte borger. Men dette medfører også vanskelige dilemmaer i forhold til personvernhensynet.

Beredskaps- og sårbarhetsarbeidet fokuserer ofte på nødvendig tilgang til opplysninger. Enten opplysninger som er nødvendige i en beredskapssituasjon, eller for et effektivt kriminalarbeid. Det pågår for tiden en diskusjon vedrørende politiets tilgang til trafikkdata (loggene). Politiet er avhengig av tilgang til trafikkdata (logger) for å spore opp gjerningspersoner på Internett, for eksempel etter et dataangrep. I dag er ikke tjenestetilbyderne pliktige til å føre logger, og personvernet blir brukt som argument mot at tjenestetilbyderne foretar logging utover det som er nødvendig av faktureringshensyn og kontroll med sikkerheten i systemene.

For å få til en mer effektiv kriminalitetsbekjempelse vurderes det å være behov for blant annet følgende tiltak:

- Tjenestetilbyderne pålegges å føre logger for en begrenset tidsperiode.
- Dersom politiet retter anmodning forlenges oppbevaringstiden av loggene. Hver sak behandles som enkelttilfelle for å redusere de dilemmaer som hensynet til personvernet gir. Forlenget oppbevaringstid er spesielt aktuelt i påvente av formell begjæring fra utenlandsk politi.
- Norske myndigheter bør arbeide aktivt for at oppkoblingsinformasjon kan innhentes og utveksles effektivt mellom ulike lands politi. Herunder kommer også arbeid for å unngå at det i deler av verden opprettes såkalte ”Internet havens” som tilbyr anonymitet for brukerne.

Sårbarhetsutvalget ser i sin vurdering behov for å vurdere om det bør innføres plikt for tjenestetilbyderne å rapportere om kjent misbruk av deres tjenester til politiet. Dette er blant annet aktuelt i saker om hvitvasking av penger.

Det bør også nevnes at det nylig er utarbeidet forskrifter til Lov om forebyggende sikkerhetstjeneste (Sikkerhetsloven), som for tiden er ute til høring. I samlingen av forskriftene til Sikkerhetsloven, vil det blant annet finnes en forskrift for monitorering av informasjonssystemer, samt en forskrift om inntregningstesting i informasjonssystemer.

5.5. Sikring av vitale infrastrukturer

I nær all vare- og tjenesteproduksjon i samfunnet er IKT blitt en sentral ressurs. Tidligere var det et strengt skille mellom den prosessorienterte delen av virksomheten, som står for selve produksjonen og driftsoppgaver knyttet til produksjonen, og den administrative og merkantile delen av virksomheten. Den teknologiske plattformen innen disse to virksomhetsdelene var ofte forskjellig og det var heller ingen bred tilgang på teknologiske løsninger for å knytte disse sammen. I dag finner en derimot samme type teknologiske plattformer på begge sider, samtidig som at det er enkel tilgang til fleksible nettverksløsninger som bygger på åpne og omforente standarder. Mange av virksomhetene blir mer og mer konkurranseutsatt og med strengere krav til avkastning fra eierne, både private og offentlige. Behovet for samarbeid både innenfor og utenfor den enkelte virksomheten har også økt, noe som igjen har ført til behov for å ta i bruk de nye mulighetene til å knytte seg sammen i felles nettverk. Eksempler på informasjonsflyt er:

- Kontinuerlig flyt av produksjonsdata mellom prosessdel og merkantil del av virksomheten.
- Avregningsinformasjon mellom merkantil del og eksterne kunder, som også kan være konkurrenter.
- Teknisk status, diagnoseinformasjon eller versjonsoppdateringer mellom systemer i prosessdelen av virksomheten og eksterne leverandører/produsenter av utstyret, i inn- eller utland.
- Drift av prosessanlegg fra hjemmevakt.

Dette gjør at prosessystemene blir mer sårbare overfor angrep utenfra, og det vil derfor være behov for ulike typer organisatoriske og tekniske tiltak for sikring. Her inngår tiltak som:

- Sårbarhetsanalyse - gjennomgang og analyse av kritiske ressurser i systemet, som kommunikasjonsveier, filtjenere og lignende.
- Tiltak for beskyttelse av kritiske deler som sentrale filtjenere og lignende mot fysiske våpenvirkninger, sabotasje og tyveri. Sikring av bygningsmasse, overvåkingssystemer og adgangskontroll inngår som sentrale virkemidler.
- Etablere fysisk redundans i kritiske kommunikasjonsveier.
- Sikring mot elektroniske og logiske angrep gjennom organisatoriske og tekniske tiltak.

Disse tiltakene må det i utgangspunktet forventes at den enkelte virksomheten selv står for ut fra bedriftsøkonomiske kriterier. For virksomheter som står for viktige samfunnsoppgaver vil det i tillegg være behov for å treffe tiltak som gir et økt

sikkerhetsnivå utfra overordnede samfunnsinteresser. Disse tiltakene må primært funderes i krav til tilgjengelighet av varer og tjenester i fred, krise og krig. Slike krav må stilles av den enkelte sektormyndighet med et nivå som gjenspeiler det enkelte systemets kritikalitet for samfunnet.

For de enkle fysiske tiltakene vil kontroll av krav være enkelt å gjennomføre. Når det gjelder sikring mot sofistikerte logiske angrep, både fra en insider eller utenfra, vil kontroll av sikringsnivå derimot kunne være svært vanskelig. I hovedsak finnes det to typer virkemidler for kontroll av tiltak, som også kan kombineres:

- Strukturert gjennomgang og analyse av kritiske IKT-systemer.
- Aktive penetrasjonsforsøk der en autorisert utenforstående forsøker å bryte seg inn i IKT-systemer som er identifisert som kritiske.

Begge virkemidlene må karakteriseres som svært kompetansekrevende, både i forhold til kravformulering og prosessen med verifikasjon av kravet. Selv om det enkelte myndighetsorgan ikke selv skal stå for den detaljerte prosessen vil det likevel være behov for betydelig grunnforståelse. Det er også viktig med et godt samarbeid og samforståelse mellom myndighetene og den enkelte virksomhet for at denne typen virkemidler skal fungere.

For å oppnå et godt sikringsnivå mot IKT-trusler er det nødvendig med tiltak som går på tvers av alle sektorene. Selv om det isolert sett vil være mulig å oppnå et noenlunde godt sikringsnivå innen hver enkelt samfunnssektor, vil dette kreve store ressurser. Strategien og tiltakene som er beskrevet i denne rapporten vil bidra til at sektorene ses i sammenheng med hensyn til IKT-sårbarhet, og vil understøtte de sektorspesifikke tiltakene som er nevnt ovenfor. Dette vil gi synergieffekter som vil være klare suksesskriterier for sikring av alle viktige IKT-systemer og infrastrukturer i samfunnet.

5.6. Statens rolle og ansvar for tiltak innen vital IKT-infrastruktur

En problemstilling dreier seg om Statens rolle og ansvar for IKT-sårbarhet og sikkerhet, og hvordan dette ansvaret best skal forvaltes. Tidligere er det uttrykt et stort behov for at spesielle tiltak må iverksettes innenfor områder av vital betydning for samfunnet som helhet, og hvor naturlige reguleringsmekanismer ikke forventes å være tilstrekkelig (avsnitt 5.2). Innen slike områder vil statlig påvirkning kunne skje på ulike måter gjennom:

- lover, forskrifter og spesielle regler som beskriver krav til virksomheten, og de varer og tjenester som virksomheten produserer.
- insentiver til tiltak innenfor den enkelte virksomhetens virkeområde.
- kjøp av spesielle tiltak, som enten kan finansieres over statsbudsjettet eller gjennom avgifter.

Det vil være behov for å definere sikkerhetskrav på ulike områder innen IKT-sektoren for ulike program- og maskinvareprodukter, for kommunikasjonsinfrastruktur som telenettet og Internett og for annen infrastruktur der IKT er kritisk ressurs. Dette vil i hovedsak dreie seg om overordnede krav til en tjeneste eller vares kvalitet eller tilgjengelighet. I visse sammenhenger kan en også tenke seg mer detaljerte krav, for eksempel der overordnede krav blir for vanskelig å utvikle eller kontrollere. Kravene

må være kontrollerbare, noe som ofte kan være vanskelig fordi tjenestene og varene bli mer og mer komplekse i sin oppbygging. Kontroll vil kreve kompetanse, men denne vil ofte være spesialisert og dermed vanskelig å få tilgang til utenfor det miljøet som skal kontrolleres. At krav ikke skal være konkurransevridende er en annen viktig forutsetning for at krav skal kunne fungere som virkemiddel.

Deler av dette arbeidet kan skje gjennom sertifiseringsordninger. I Norge er det under etablering to ordninger for sertifisering av IKT-sikkerhet: En ordning for sertifisering av IT-sikkerhet i organisasjoner hvor Norsk Akkreditering er operatør, og en ordning for sertifisering av IT-sikkerhet i produkter og systemer hvor Forsvarets sikkerhetstjeneste er operatør. Begge ordningene legger til grunn evalueringskriterier og avtaleordninger som er internasjonale. Dette er viktig fordi produkter og tjenester flyter over landegrensene. For myndighetene vil sertifiseringsordningene blant annet gjøre det enklere å stille krav om sertifiserte produkter eller tjenester med et bestemt sikkerhetsnivå. Norge har nylig gått med i en internasjonal ordning for produktevaluering, basert på evalueringskriteriene Common Criteria. Deltagelse i sertifiseringsordninger vil også kunne virke som frivillige insentiv fordi deltagelsen vil kunne være med på å kvalitetsmessig fremme tjenesten eller varen i markedet. En problemstilling er imidlertid om denne typen ordninger i dag er tilstrekkelig fleksible til å kunne møte utfordringene i den raske utviklingen.

For å sikre at enkelte vitale tjenester i samfunnet får en tilfredsstillende kvalitet og sikkerhet vil det også være behov for å gjøre dette ved at Staten tar ansvaret gjennom oppkjøp av konkrete tiltak. Dette vil typisk være tilfelle der en finner komplekse markedsmessige forhold i kombinasjon med høy teknisk systemkompleksitet som ligger til grunn for en tjenesteproduksjon. I slike tilfeller vil krav kunne bli vanskelige å formulere, og en vil også måtte forvente stor motstand fra aktørene dersom de ikke blir stilt overfor krav av en tilstrekkelig kvalitet.

For teleområdet har det tidligere TIFKOM-prosjektet foreslått å etablere organisasjonen Nasjonal telesikkerhet og –beredskap (NTSB), som blant annet skal stå for utvikling av sikkerhetskrav innen telesektoren. Slike krav må formuleres gjennom en løpende prosess på grunnlag av risiko- og sårbarhetsanalyser. Det må forventes at denne organisasjonen også må forestå statlige innkjøp av spesielle beredskapstiltak for at de overordnede kravene skal bli tilfredsstilt, noe som i stor utsrekning gjøres av en tilsvarende organisasjon i Sverige. Det vurderes å være et behov for å forankre et tilsvarende ansvar som for telesektoren også for andre vitale sektorer, og å få vurdert organisatoriske løsninger for dette.

Et problem i dag er at en innen Staten ikke innehar en tilstrekkelig kompetanse eller kapasitet med hensyn til tilsyn av IKT-sikkerhet innenfor all samfunnskritisk virksomhet. Innenfor organisasjoner som Post- og teletilsynet og Forsvarets sikkerhetstjeneste (Nasjonal sikkerhets-myndighet) finnes det likevel en viss kompetanse på deler på området, men heller ikke her finner en noen helhetlig samfunnsinnretning. Gjennom opprettelsen av organisasjoner som NTSB og tilsvarende for andre sektorer vil behovet for kompetanse øke. Det bør foretas en nærmere vurdering av hvordan en best skal kunne bygge opp og beholde et kompetansenivå på området innen Staten. Her vil det også være nødvendig å foreta en

avgrensing av de ulike statlige organisasjonenes innbyrdes ansvar. Forholdet til det foreslåtte SIS utgjør en sentral faktor.

6. Nasjonal beredskap og totalforsvaret

Forsvaret av Norge bygger på Totalforsvarskonseptet. Totalforsvaret består av det militære forsvar og Det sivile beredskap, og bygger på prinsippet om at samfunnets samlede ressurser om nødvendig skal kunne mobiliseres for forsvaret av Norge. Dette innebærer at alle deler av samfunnslivet er forpliktet til å ta del i forsvaret av landet, og at de sivile og militære enhetene er forutsatt å skulle forsterke og utfylle hverandre på sentralt, regionalt og lokalt nivå. Hensikten er på best mulig måte å beskytte folk og samfunn mot ekstraordinære påkjenninger under sikkerhetspolitiske kriser og i krig.

Totalforsvarskonseptet innebærer videre at en rekke oppgaver som i mange andre land ivaretas av den militære sektor i Norge dekkes av det sivile samfunn. Dette gjelder spesielt forsyninger og transport. Ved krig kan Forsvaret rekvirere sivile fly, skip, kjøretøy og lignende.

Forsvaret er i ferd med å gjennomgå omfattende strukturelle endringer. Endringer i Forsvarets strukturer og operasjonsmønstre medfører økende behov for å være mobil og flyttbar, både innenfor og utenfor landets grenser. Tilgangen til sikker informasjon og informasjonsutveksling blir stadig viktigere både for Forsvaret og virksomhetene som inngår i Det sivile beredskap. I tillegg til at informasjon er viktig for å organisere en militær operasjon, benyttes informasjon også i økende grad til å effektivisere gjennomføringen av operasjoner på slagmarken. Under Kosovo-konflikten ble for eksempel våpnenes målsøkerbilder direkte overført til stridsledelsens operasjonsrom. Denne informasjonen ga stridsledelsen nye muligheter til raskt og dynamisk å påvirke operasjonenes videre gang. I tillegg til å anvende informasjon til å øke egen effektivitet er det også et mål å sørge for å hindre motstanderens informasjonsanvendelse.

Dette har blant annet ført til at det er satt i gang en studie av fremtidens kommunikasjonsinfrastruktur for Forsvaret – MILKOM. I studien legges det vekt både på brukerbehov og tekniske løsninger, og en arbeider med et tidsperspektiv fram til 2020. Det legges vekt på også å inkludere de viktigste aktørene innen Det sivile beredskap som tjenestebrukere, samtidig som at det også vurderes å benytte deler av sivil teleinfrastruktur som del av Forsvarets informasjonsinfrastruktur. Størst mulig ressursutnyttelse er et viktig mål - en trend som også gjør seg gjeldende i andre land. En tenkelig modell, som også den tidligere omtalte TIFKOM-studien peker på, er at en skal tilby robuste teletjenester til viktige samfunnsaktører som *et påbygg* til offentlige teletjenester med lavere robusthetsnivå (se avsnitt 3.3).

Forsvaret blir dermed også mer avhengig av sivile informasjonsinfrastrukturer for sin egen kjernevirksomhet. Ett eksempel som illustrerer viktigheten av dette er at Forsvarsdepartementet i USA for tiden gjennomfører dyptgående risikoanalyser knyttet til mulige fremtidige militære operasjoner og avhengigheten av sivil infrastruktur[20]. Økt militær anvendelse av sivile infrastrukturer fører også til at disse i økende grad vil være utsatt som mål i en militær konflikt.

[20] Critical Infrastructure Protection (CIP) Staff, US Department of Defense.

Fremtidens trusselbilde vil være mangfoldig og sammensatt. Dagens og morgendagens samfunn vil være sårbart på en annen måte enn tidligere, og trusselbildet vil endres deretter. Dette setter krav til utformingen av landets fremtidige forsvar, der det ikke minst vil kreves økt samspill mellom det vi i dag ser som separate sivile og militære ansvarsområder. Morgendagens digitale samfunnsøkonomi kan for en angriper være et like verdifullt mål som overtakelse av landområder.

I andre land som tradisjonelt ikke har hatt et totalforsvar i vår betydning er man nå også i ferd med å ta i bruk begrepet. Her bruker man imidlertid begrepet totalforsvar om nasjonens forsvar mot et vidt spekter av trusler fra ulike typer aktører i fred, krise og krig. Fokuset på nasjonens forsvar blir dermed utvidet til i større grad også å inkludere ikke-militære aktører. Dette har blant annet årsak i at mange av morgendagens trusler mot samfunnet inneholder til dels kraftige virkemidler som også kan anvendes av andre enn nasjonalstater - virkemidler som kan ramme nasjoner hardt.

Mange lands militærvesen er nå i ferd med å planlegge for bruk av såkalte defensive informasjonsoperasjoner (IO-D), som del av sitt virkemiddelapparat. Dette innebærer primært å utnytte informasjon og IKT-ressurser for å oppnå overlegenhet i egen militære kapasitet, med bruk av et antall metoder og virkemidler. IKT-infrastruktur inngår som et viktig middel i slike operasjoner. Den samme infrastrukturen vil dermed også være et viktig mål for militære operasjoner sett fra en angriper. Tiltak for å beskytte både sivil og militær infrastruktur inngår derfor også som sentrale element i å beskytte seg mot motpartens informasjonsoperasjoner. Det må imidlertid understrekes at informasjonsoperasjoner er et vidt og sammensatt område som går langt utenfor denne beskrivelsen.

I dette bildet har imidlertid beskyttelse av infrastruktur på mange måter vist seg mest vanskelig å håndtere. Ikke på grunn av teknologisk kompleksitet, men på grunn av strukturell kompleksitet. Det militære forsvarets behov for samvirke med det sivile samfunnet utgjør en klar utfordring i dette. Konseptet med defensive informasjonsoperasjoner knyttes nå i andre land nært sammen med blant annet program for beskyttelse av sivil informasjonsinfrastruktur. Siden informasjonsoperasjoner også dreier seg om beskyttelse av sivil samfunnsinfrastruktur er dette en like viktig sivil oppgave som en militær oppgave, og som derfor også må ledes fra politisk hold.

Selv om det i ulike sammenhenger også i Norge er pekt på flere av disse faktorene, er den praktiske oppfølgingen på overordnet nivå så langt av begrenset karakter. Den filosofi som den foreslåtte strategien i kapittel 5 bygger på vurderes imidlertid *i utgangspunktet å være uavhengig* av totalforsvarets videre utvikling. Denne er enkelt basert på å oppnå størst praktisk mulig sikring av samfunnets informasjonsinfrastrukturer i fred, krise og krig. Det er likevel klart at *totalforsvarets fremtidige virksomhet og behov må ses i nær sammenheng med og samordnes med de tiltak som inngår strategien*.

Vedlegg 1 - Kortversjon av hovedrapporten