Den
Nationale
Sårbarhedsudredning

Rapport fra underudvalget
vedrørende
el-, naturgas- og teleforsyning
samt it-forhold

25. august 2003

Indholdsfortegnelse

1. Indledning og sammenfatning

1.1. Baggrund og formål med udredningen

Udredningen er udarbejdet af underudvalget vedrørende el-, naturgas- og teleforsyning samt it-forhold. Underudvalget er nedsat af Udvalget for National Sårbarhedsudredning i regi af Indenrigs- og Sundhedsministeriet. Underudvalget består af repræsentanter fra IT- og Telestyrelsen, Energistyrelsen, Videnskabsministeriet, Elkraft System, Eltra og DONG Transmission.

Det følger af kommissoriet for underudvalget, at formålet med udredningen er en beskrivelse af sårbarheder vedrørende el-, naturgas- og teleforsyning samt it-forhold - herunder sårbarheder vedrørende den indbyrdes afhængighed mellem sektorerne - og en beskrivelse af beredskabsmæssige tiltag i relation hertil. Underudvalget er desuden efterfølgende anmodet om at give en oversigt over afhængigheder til øvrige sektorer omfattet af Den Nationale Sårbarhedsudredning - samt om en beskrivelse af internationale forhold af betydning for beredskabsplanlægningen nationalt.

1.2. Nærmere afgrænsning af opgaven

Elområdet er medtaget i udredningen for så vidt angår de virksomheder, som varetager produktion, transmission, distribution og det såkaldte *systemansvar*. Derimod er handelsvirksomhederne ikke medtaget, da deres funktioner ikke har betydning for sektorens sårbarhed og beredskab.

For så vidt angår *naturgasområdet* er bygas medtaget i dele af udredningen. Dette skyldes, at naturgassektoren traditionelt har et samarbejde med bygassektoren om beredskab, sikkerhed m.m. og at de to sektorer derfor i beredskabssammenhæng normalt behandles samlet, selvom naturgas klart er den vigtigste energiform af disse to. Hovedvægten er derfor lagt på naturgasforhold.

For så vidt angår *teleområdet* er kun *offentlige* telenet og teletjenester medtaget i udredningen. Herved forstås telenet eller teletjenester, som af teleudbyderne stilles til rådighed på kommercielt grundlag til en ikke på forhånd afgrænset

kreds af brugere. Visse private eller lukkede telenet anvendes også til beredskabsmæssige formål, men er ikke medtaget i udredningen. Disse net kan f.eks. være etableret af beredskabsmyndigheder med et særligt behov for telekommunikation i beredskabssituationer.

Videnskabsministeriets og IT- og Telestyrelsens indsats på teleberedskabsområdet som sektoransvarlige myndigheder har i det seneste årti været rettet mod *udbydere af offentlige telenet og teletjenester* (i det følgende teleudbyderne). Dette har været et naturligt fokusområde med liberaliseringsprocessen og tilkomsten af de mange nye teleudbydere. Det har været - og er stadig - en væsentlig opgave at sikre et beredskab hos disse teleudbydere. Fokus for dette udredningsarbejde er på den baggrund teleudbyderne.

Videnskabsministeriet og IT- og Telestyrelsen har dog også en bemyndigelse, jf. afsnit 5.4.2, i forhold til sikring af statslige myndigheders telekommunikationsbehov og eget beredskab i relation hertil. Det er ikke i forbindelse med denne udredning undersøgt, hvorledes den enkelte statslige myndighed eller private virksomhed med samfundsvigtige funktioner har planlagt sit interne beredskab vedrørende eget telekommunikationsbehov, eller hvilke sårbarheder der måtte være i den forbindelse. Problemstillingen, som dog må antages at have væsentlig betydning for en sårbarhedsvurdering, er nærmere belyst i afsnit 7 og 8.3.

I et *nationalt* beredskabs- og sårbarhedsperspektiv er *it-området* nyt i den forstand, at der ikke findes en tradition for at tænke foranstaltninger med henblik på at sikre samfundets adgang til it-infrastrukturen i en beredskabssituation. For at kunne udarbejde en egentlig sårbarhedsanalyse, er det en forudsætning, at it-området er defineret i et nationalt perspektiv, og at væsentlige aktiver heri er fastlagt. Ved aktiver forstås her f.eks. virksomheder, knudepunkter eller datasamlinger. Da dette ikke er tilfældet, er udgangspunktet for it-området et andet end for både el-, naturgas- og teleområdet. Organiseringen af et *nationalt* it-beredskab er ligeledes et nyt område, hvilket også medvirker til, at udgangspunktet for sårbarhedsanalysen på it-området er et andet.

I afsnit 3.4 gives en definition af it-området med afgrænsning til blandt andet teleområdet. Ud fra bestemmelsen af it-området identificeres en række aktiver og trusler. Sårbarhedsaspekter knyttet til de mere veletablerede it-sikkerhedsområder behandles i afsnit 4. Sårbarhedsaspekterne behandles her ud fra de trusler, som kendes på it-området. Med udgangspunkt i en beskrivelse af status på en række trusler, gives et billede af samfundets sårbarhed over for disse.

1.3. Processen i forbindelse med udredningsarbejdet

Udredningen er udarbejdet på grundlag af det kommissorium, der er givet af Udvalget for National Sårbarhedsudredning for Underudvalget vedrørende el-, naturgas- og teleforsyning samt it-forhold.

Det skal i den forbindelse bemærkes, at det ikke inden for den givne tidsramme har været muligt at udarbejde fuldstændige og udtømmende beskrivelser af sårbarheder og beredskab inden for sektorerne.

I forbindelse med udredningsarbejdet er der afholdt en række møder i underudvalget samt i udvalgsledelsen. Herudover er der af nogle sektorer afholdt en række møder med eksterne bidragsydere. I den forbindelse er der tidligt i udredningsarbejdet afholdt et fællesmøde for de repræsentanter for andre myndigheder og private virksomheder, som underudvalget har fundet ville kunne bidrage til sårbarhedsudredningen. Formålet med dette fællesmøde var - udover at præsentere udredningsarbejdet - at sætte bidragsyderne sammen på tværs af sektorerne med henblik på en indledende drøftelse af de indbyrdes afhængigheder og sårbarheder på tværs af sektorerne. Herefter er arbejdet fortsat inden for de enkelte sektorer i underudvalget.

For el- og naturgassektoren gælder, at der gennem mange år er lagt stor vægt på at opnå en stor grad af forsyningssikkerhed for samfundet. Virksomheder inden for disse sektorer har derfor traditionelt et betydeligt *driftsberedskab*, som ikke alene er rettet mod at kunne håndtere de almindeligt forekommende driftsforstyrrelser som følge af uheld m.m., men også er rettet mod mere alvorlige hændelser som følge af vejrforhold m.m. Dertil kommer, at den sek-

torlovgivning, som danner rammerne for virksomhed inden for disse sektorer, indeholder en række bestemmelser, som har til formål at sikre forsyningssikkerheden.

For disse to energisektorer betragtes den civile sektors beredskab derfor som en overbygning på det eksisterende driftsberedskab, som primært er rettet mod at sikre forsyningssikkerheden. Denne overbygning vil således skulle supplere driftsberedskabet for så vidt angår de meget alvorlige og kritiske hændelser, som nu indgår i det nye beredskabsbegreb. Men reelt er der tale om, at de to begreber - dels *den civile sektors beredskab*, dels *forsyningssikkerhed* - er udviklet ud fra forskellige behov og betragtninger og at de i dag i nogen grad overlapper hinanden.

Begge energisektorer har således et løbende arbejde vedrørende beredskab. Således har de to systemansvarlige virksomheder inden for elsektoren - Eltra i Vestdanmark og Elkraft System i Østdanmark - i slutningen af 2002 efter anmodning af Energistyrelsen udarbejdet såkaldte temarapporter om beredskabsforhold inden for elsektoren. Som følge heraf er udredningsarbejdet for disse energisektorer baseret på det hidtil udførte beredskabsarbejde, som foretages i samarbejde med sektorernes virksomheder, og der har ikke været behov for at gennemføre særskilte interviews, høringer o.lign. over for disse sektorer.

Teleberedskab i relation til sikring af samfundsvigtig telekommunikation kan næsten føres tilbage til opfindelsen af telefonen, om end beredskabet naturligvis har ændret karakter med udviklingen på området. Den lovmæssige regulering af rammerne for teleberedskabet er således senest tilpasset sideløbende med en liberalisering af telemarkedet. Udredningsarbejdet for så vidt angår telesektoren, er baseret på den viden om beredskabsforhold, der er opbygget i IT- og Telestyrelsen i samarbejde med Videnskabsministeriet om blandt andet de regulatoriske forhold.

Liberaliseringen og konkurrencesituationen som den er i dag med et relativt stort antal teleudbydere, har imidlertid skabt et behov for et overblik over det *driftsberedskab*, som teleudbyderne ud fra kommercielle interesser har etableret med henblik på at sikre driftsstabilitet og forsyningssikkerhed. Til brug for en

vurdering af sårbarheder på teleområdet samt et overblik over det samlede beredskab på teleområdet, er der på den baggrund afholdt møder med teleudbyderne TDC, Orange, SONOFON og Telia. Disse udbydere er valgt, da de alle er netoperatører, og tilsammen dækker størstedelen af markedet for taletelefoni. Der er desuden afholdt møder med Broadcast Service Danmark, som har ansvaret for de senderstationer, der blandt andet anvendes til at udsende beredskabsmeddelelser via TV og radio, samt med Telekommunikations Industrien, som er teleudbydernes brancheforening.

Til en kortlægning af it-infrastrukturen og en vurdering af sårbarheder på it-området, er der ligeledes afholdt møder med en række aktører på området. Følgende myndigheder og private virksomheder har bidraget til udredningsarbejdet: TDC, UNI-C, Kommunernes Landsforening, Amtsrådsforeningen, Forsvarsministeriet, Forsvarets Efterretningstjeneste, ITEK, Hewlett Packard, Infonova og Dk-Hostmaster.

1.4. Sammenfatning

Områderne el, naturgas, tele og it udgør tilsammen en meget væsentlig del af det moderne samfund, idet de tegner en stor del af den tekniske infrastruktur. Sektorerne har som forsyningsområder en del fællestræk, og de enkelte sektorer er desuden i betydelig omfang afhængige af hinanden. Dette er baggrunden for, at det er valgt at behandle disse sektorer samlet i forbindelse med en sårbarhedsudredning. Alene sektorernes betydning for samfundet gør, at det er væsentligt at få skabt et overblik over sårbarheder i sektorerne, sårbarheder relateret til de indbyrdes afhængigheder sektorerne imellem samt de beredskabsmæssige tiltag i relation hertil.

Vedrørende de indbyrdes afhængigheder sektorerne imellem, har det vist sig, at særligt elsektoren er af afgørende betydning for de øvrige sektorer. Længerevarende svigt i elsektoren kan få betydelige konsekvenser for forholdene i de øvrige sektorer. Særligt for telesektoren er der tale om en kritisk afhængighed, idet telesektorens beredskab i relation til denne afhængighed kun udgør et højt sikringsniveau for så vidt angår kortvarige svigt i elforsyningen i geografisk be-

grænsede områder. På baggrund af elsektorens driftsberedskab, er der dog ikke nødvendigvis tale om en kritisk sårbarhed.

Sektorernes afhængighed af de offentlige telenet og teletjenester er også signifikant og for it-infrastrukturen helt grundlæggende. For elsektorens vedkommende vurderes der ikke at være en kritisk afhængighed af hverken tele-, it- eller naturgassektoren. Sammenbrud i en af disse sektorer vil påvirke elsektoren, men elforsyningen forventes at kunne opretholdes. Når der generelt ikke er tale om meget kritiske afhængigheder, skyldes det i vid udstrækning, at virksomheder inden for de enkelte sektorer i årenes løb har været bevidste om disse afhængigheder og har gennemført foranstaltninger for at reducere afhængighederne.

Udredningen omfatter også en vurdering af afhængighederne til de øvrige områder under Den Nationale Sårbarhedsudredning. På grund af tidsrammerne for udredningsarbejdet er disse afhængigheder først og fremmest beskrevet på en generel måde og i eksemplificeret form. Der er ikke umiddelbart tale om kritiske eller signifikante afhængigheder til andre områder eller sektorer.

På it-området har det ikke været muligt inden for tidsrammen for udredningsarbejdet at foretage en egentlig sårbarhedsanalyse. I et *nationalt* beredskabs- og sårbarhedsperspektiv er it-området nyt i den forstand, at der ikke findes en tradition for at tænke foranstaltninger med henblik på at sikre samfundets adgang til it-infrastrukturen i en beredskabssituation. For at kunne lave en egentlig sårbarhedsanalyse, er det en forudsætning, at it-området er defineret i et nationalt perspektiv, og at væsentlige aktiver heri er fastlagt. Bidraget på it-området indeholder på den baggrund en overordnet kortlægning af it-infrastrukturen som forsyningsområde ved identifikation af en række aktiver og trusler. Det er hensigten, at en egentlig sårbarhedsanalyse på it-området nu skal foretages i regi af IT- og Telestyrelsen i forbindelse med Videnskabsministeriets projekt it-beredskab.

Udredningen indeholder desuden et afsnit om sårbarhedsaspekter ud fra de trusler, som kendes på it-området generelt, f.eks. hacking og virus. Med ud-

gangspunkt i en beskrivelse af status på en række trusler, gives et billede af samfundets sårbarhed over for disse.

El-, naturgas- og telesektoren har forskellige udgangspunkter for beredskabet. Myndighedsstruktur, organisering og regulering på beredskabsområdet er forskelligt for sektorerne. Fælles for elsektoren og telesektoren er dog navnlig, at områderne er undergået en liberalisering. Også i naturgassektoren er der påbegyndt en liberaliseringsproces efter nogenlunde samme principper som for elsektoren.

De enkelte virksomheder er generelt meget bevidste om beredskabsforhold, de tekniske infrastrukturer i sektorerne vurderes at være robuste og driftsstabile over for uheld og andre tilsvarende hændelser, og de enkelte netværk er i høj grad sikret redundans ved ring- og maskestrukturer og dublerede systemer.

Sårbarhedsanalysen på områderne el, naturgas og tele har således vist, at der generelt er en høj grad af forsyningssikkerhed i forhold til hændelser, der er utilsigtede, tilfældige og hændelige som f.eks. tekniske eller menneskelige fejl, mindre kritiske vejrfænomener osv. Alle tre sektorer er imidlertid sårbare overfor direkte og bevidste angreb som terror- og krigshandlinger samt større naturkatastrofer som f.eks. orkaner.

Fælles for sektorerne er en forventning om, at liberaliseringens tendenser mod øget konkurrence og øget rationalisering hos de enkelte virksomheder vil kunne resultere i, at virksomhederne beslutter at prioritere beredskabsforhold lavere end hidtil. Afgørende herfor kan blandt andet blive, om kunderne efterspørger produkter med en højere grad af forsyningssikkerhed og dermed med et større beredskabsindhold. Det er derfor nødvendigt, at sektormyndighederne følger udviklingen i denne henseende. Det kan blive nødvendigt på visse områder at overveje at anvende lovgivning i større omfang end hidtil for at nå målsætninger om, at virksomheder skal have et minimumsniveau af beredskab.

Både el- og telesektoren har kunder, for hvem det er af afgørende betydning at være sikret mod forsyningssvigt, f.eks. beredskabsmyndighederne og hospitalerne. For elsektoren kan endvidere nævnes andre dele af sundhedsvæsnet, tra-

fiksektorerne og erhvervslivet. For både el- og telesektoren har det hidtil været et hovedprincip, at kunderne selv bør vurdere deres afhængigheder og deres behov for en højere grad af sikring, samt i den forbindelse selv sørge for foranstaltninger som f.eks. no break anlæg og nødstrømsanlæg. Princippet forudsætter dog, at den enkelte kunde har en rimelig mulighed for at vurdere risikoen for, at el- henholdsvis telesystemet afbrydes eller forstyrres. Det vil som regel være muligt at opnå bistand hertil hos de pågældende forsyningsselskaber eller gennem konsulentbistand. Alligevel kan der være risiko for, at udviklingen i sektorerne indebærer, at det i stigende grad bliver vanskeligt for en kunde at vurdere risikoen for afbrydelser/forstyrrelser i el- henholdsvis telesystemet. Det bør derfor overvejes, om der inden for de enkelte sektorer er behov for tiltag herom, f.eks. vejledning af særlige kundegrupper om deres sikringsbehov.

Der bør samtidig fortsat sikres en høj grad af forsyningssikkerhed. På nogle områder kan der være behov for en styrket dialog mellem myndighederne og branchevirksomhederne om beredskabsforhold, ligesom der som nævnt eventuelt kan blive behov for en lovgivningsindsatssindsats, der sikrer et minimumsniveau for beredskabet - set i lyset af disse forsyningsområders betydning for samfundet.

Det er således nødvendigt at sikre, at de enkelte virksomheder inden for sektorerne løbende tilpasser deres beredskab til det aktuelle trusselsbillede.

Det er i den forbindelse nødvendigt at revurdere sektorernes sårbarheder og beredskab, bl.a. over for terrorhandlinger, som ikke tidligere har indgået i overvejelserne om design, dimensionering og drift af forsyningssystemer. Terrorhandlinger vil således typisk indebære, at flere anlæg m.m. med stor sandsynlighed rammes samtidigt, og at de vigtigste anlæg har størst sandsynlighed for at blive ramt. Sårbarheden over for sådanne hændelser kan kun i begrænset omfang reduceres gennem dimensionering. Derimod kan forebyggende foranstaltninger (som adgangskontrol, monitorering m.m.) have en effekt, ligesom det er nødvendigt at have et retableringsberedskab, som kan udbedre skader hurtigt.

Det kan generelt overvejes at indføre økonomiske mekanismer, som indebærer incitamenter til at forbedre beredskabet. Som eksempel herpå kan nævnes, at der for elsektoren er overvejelser hos myndighederne om, at der for transmissions- og netvirksomheder skal indføres økonomiske konsekvenser af forsyningsafbrydelser som følge af netfejl, således at virksomhederne gives incitamenter til at forebygge sådanne forsyningsafbrydelser, bl.a. gennem bedre vedligeholdelse af nettene.

Det bør i øvrigt søges sikret, at beredskabshensyn fremover indgår i beslutningsgrundlaget for anlæg (design og dimensionering) og drift af forsyningssystemer som et af mange elementer på samme måde som funktionelle, økonomiske, personsikkerhedsmæssige, miljømæssige og æstetiske hensyn m.m. Beredskabshensyn bør derfor ikke udelukkende varetages af særskilte medarbejdere, men bør indgå som ét af mange hensyn i en integreret opgavevaretagelse.

Det er derfor væsentligt, at der inden for de enkelte sektorer arbejdes mod fastlæggelse af standardiserede metoder for udførelse af sikkerheds- og sårbarhedsvurderinger, som sikrer, at sådanne vurderinger foretages på en ensartet måde. Derved bliver det muligt at foretage sammenligninger mellem virksomheder inden for den samme sektor og mellem virksomheder i forskellige sektorer.

For virksomheder og myndigheder, som er centrale for det civile beredskab, kan det overvejes at fastlægge en regelmæssig turnus for gennemgange af disses beredskab.

2. Sårbarhedsområdet

I det følgende beskrives kort områdets betydning for samfundet og tilknytningen til de øvrige sektorer i samfundet. En overordnet beskrivelse af infrastrukturen i de enkelte sektorer findes i afsnit 3. En beskrivelse af de regulatoriske og organisatoriske rammer for sektorerne findes i afsnit 5.

2.1. Områdets betydning for samfundet

El, naturgas, tele og it udgør tilsammen en meget væsentlig del af det moderne samfund. Disse sektorer tegner navnlig en stor del af den tekniske infrastruktur i samfundet - en infrastruktur, som holder samfundet i gang: Maskiner, systemer, netværk, procedurer, produktion, handel - og mennesker.

Informations- og netværkssamfundet er fundamentalt afhængigt af anvendelse af it og telekommunikation. Samfundsvigtige funktioner afhænger heraf. Offentlig og privat virksomhed er i dag i et overvældende omfang baseret herpå. It- og teleinfrastrukturen kan ikke fungere uden el. Og uden el kan befolkningen i vidt omfang heller ikke anvende blandt andet it- og teletjenesterne. El er altafgørende for det moderne samfund.

De enkelte sektorer er i vidt omfang afhængige af hinanden. Særligt elsektoren er af vital betydning for de øvrige sektorer. Længerevarende svigt i elsektoren kan få betydelige konsekvenser for forholdene i de øvrige sektorer gennem en slags dominoeffekt. De indbyrdes afhængigheder på tværs af sektorer stiller på den baggrund udfordringer for beredskabet i den civile sektor.

2.2. Tilknytningen til andre sektorer

Som bilag til denne udredning er vedlagt en skematisk gengivelse af afhængighedsforholdene til de øvrige sektorer under Den Nationale Sårbarhedsudredning, som de vurderes at se ud år 2003. Underudvalget vedrørende el-, naturgas og teleforsyning samt it-forhold er anmodet om at fremkomme med en vurdering af afhængighedsforholdene til de øvrige sektorer dels som de ser nu, og dels som de forventes at se ud år 2010. Da der ikke umiddelbart er grund til

at tro, at afhængighedsforholdene vil se væsentligt anderledes i år 2010, er et skema herfor ikke udfyldt.

Nedenfor beskrives nærmere hvori afhængighederne består, for så vidt angår de afhængigheder, der er vurderet at være moderate, signifikante eller kritiske. Opmærksomheden skal henledes på, at der - grundet tidsrammerne for denne udredning - ikke er tale om en nærmere analyse af afhængighedsforholdene, men om en umiddelbar vurdering heraf blandt andet baseret på de interviews, der på tele- og it-området er foretaget af eksterne bidragsydere til udredningen, det vil sige private virksomheder m.fl. i de enkelte sektorer. En nærmere vurdering af afhængighedsforholdene mellem områderne el, naturgas, tele og it og beredskabet i relation hertil, findes i henholdsvis afsnit 3.5 og 5.5.

Elsektoren er ikke direkte afhængig af andre sektorer i en grad, som indebærer, at svigt i en anden sektor kan forventes at resultere i svigt i elforsyningen. For elsektoren vurderes afhængighederne – under en alt-andet-lige forudsætning om svigt alene inden for den pågældende sektor - således:

- Over for *telesektoren* vurderes afhængigheden at være *signifikant* for så vidt angår taletelefoni i offentlige telenet. Når afhængigheden ikke vurderes som kritisk, skyldes det bl.a. at dele af energisektoren har reduceret afhængigheden ved anvendelse af private telekommunikationsforbindelser og faste kredsløb. Ved totalt svigt af offentlig teleforsyning vil transmissionssystemets drift være relativt lidt berørt, mens distributionssystemets drift vil være mere berørt, idet flere fjernkontrolsystemer er afhængige heraf. Umiddelbart vil elsystemets drift fortsætte og ved vedvarende svigt i teleforsyningen, kan elanlæg bemandes, og talekommunikation kan foretages over private kommunikationsanlæg.

- Over for *naturgassektoren* vurderes afhængigheden at være *signifikant*. Det skyldes dels en afhængighed på produktionssiden (ca. 25 % af elproduktionen er baseret på naturgas, som dog i nogen grad kan erstattes af andet brændsel), dels en sammenhæng på forbrugssiden.

Selvom de naturgasbaserede elproduktionsanlæg således vil udgå af drift ved totalt svigt af naturgas, forventes et sådant naturgassvigt ikke at opstå pludseligt og elsystemet kan derfor med en forholdsvis kort tidsfrist sikre elforsyningen på anden måde.

- Over for *it-sektoren* vurderes afhængigheden at være *moderat* for så vidt angår it-infrastrukturen, som den er defineret i afsnit 3.4. Ved totalt svigt af it-tjenester vil elmarkedsaktørerne og de systemansvarlige virksomheder således blive berørt, men for systemdriften forventes det ikke at resultere i problemer med elforsyningen.

- Over for *vejtransportsektoren* vurderes afhængigheden at være *moderat*. Det skyldes behovet for, at personale kan komme på arbejde samt behovet for at kunne foretage transport til elledninger, transformerstationer og andre anlæg som led i den løbende drift og vedligeholdelse.

- Over for *søtransportsektoren* vurderes afhængigheden at være *moderat*. Det skyldes behovet for skibstransport af kul og olieprodukter til de centrale kraftværker. Da kraftværkerne har store lagre, bl.a. af kul, vil afhængigheden først kunne mærkes ved længere tids afbrydelse af skibstransporten.

- Over for *olieprodukter* vurderes afhængigheden at være *moderat*. Det skyldes, at der anvendes olieprodukter i elproduktionen på de centrale kraftværker, men at dette olieforbrug dog er af mindre betydning i forhold til kul og naturgas.

For *naturgassektoren* vurderes afhængighederne - under en alt-andet-lige forudsætning om svigt alene inden for den pågældende sektor - således:

- Over for *elsektoren* vurderes afhængigheden at være *signifikant*. Det skyldes, at en række anlæg, bl.a. M/R-stationer, kræver el til opvarmning af gassen som følge af trykreduktionen. Styring af M/R stationerne og ventilstationerne er ligeledes afhængig af el. Ved svigt i elforsyningen skal stationerne opereres manuelt på hver lokalitet.

Kommunikationen med stationerne kan opretholdes i ca. 3-24 timer med stationernes nødstrømsforsyningsanlæg. Gasforsyningen vil kunne opretholdes med manuel overvågning og styring.

- Over for *telesektoren* vurderes afhængigheden at være *kritisk*. Det skyldes den store afhængighed af offentlige telenet og teletjenester til brug for kommunikation til alle anlæg og stationer. Alle fjernkontrolsystemer kommunikerer via TDC's tekniknet, som er et robust og selv kontrollerende netværk. Gasforsyningen kan opretholdes, men det kræver manuel overvågning på hver lokalitet hver 12. time.

- Over for *it-sektoren* vurderes afhængigheden at være *moderat* for så vidt angår it-infra-strukturen, som den er defineret i afsnit 3.4.Ved totalt svigt af it-tjenester vil gasmarkedsaktørerne og de systemansvarlige virksomheder således blive berørt, men for systemdriften forventes det ikke at resultere i gasforsyningsproblemer.

- Over for *vejtransportsektoren* vurderes afhængigheden at være *moderat*. Det skyldes behovet for, at personale kan komme på arbejde samt behovet for at kunne foretage transport til gasledninger, M/R-stationer og andre anlæg som led i den løbende drift og vedligeholdelse.

For *telesektoren* vurderes afhængighederne - under en alt-andet-lige forudsætning om svigt alene inden for den pågældende sektor - således:

- Over for *elsektoren* vurderes afhængigheden at være *kritisk*. Teleforsyningen er grundlæggende afhængig af elforsyningen. Allerede ved afbrydelser af elforsyningen på en varighed af mere end 4-6 timer, vil det kunne medføre betydelige afbrydelser af teleforsyningen – særligt hvor elforsyningen er afbrudt i et eller flere større geografiske områder.

- Over for *vejtransportsektoren* vurderes afhængigheden at være *moderat*. Det skyldes behovet for, at personale kan komme på arbejde og i den

forbindelse behovet for at kunne foretage transport til bygninger og installationer m.v. i telenettene som led i den løbende drift og vedligeholdelse.

- Over for *olieprodukter* vurderes afhængigheden at være *moderat*. Det skyldes primært behovet for olie til tankanlæg til nødstrømsanlæg.

For *it-sektoren* vurderes afhængighederne - under en alt-andet-lige forudsætning om svigt alene inden for den pågældende sektor - således:

- Over for *elsektoren* vurderes afhængigheden umiddelbart at være *kritisk*. It-området er grundlæggende afhængig af elforsyningen. Da eventuelle beredskabsforanstaltninger relateret til denne afhængighed ikke er undersøgt, jf. afsnit 5.5, kan afhængigheden ikke vurderes nærmere.

- Over for *telesektoren* vurderes afhængigheden at være *kritisk*. Denne afhængighed følger allerede af afgrænsningen af infrastrukturen på it-området. Den del af samfundets it-anvendelse, der er baseret på it-infrastrukturen, som den er defineret i afsnit 3.4, er grundlæggende baseret på bl.a. teletjenester hos teleudbyderne og dermed teleinfrastrukturen. Teleinfrastrukturen leverer de fysiske lag i it-infrastrukturen, dvs. kabler m.v.

- Over for *vejtransportsektoren* vurderes afhængigheden at være *moderat*. Det skyldes behovet for, at personale kan komme på arbejde og i den forbindelse behovet for at kunne foretage transport til lokationer som led i den løbende drift og vedligeholdelse af diverse udstyr.

- Over for *olieprodukter* vurderes afhængigheden umiddelbart at være *moderat*. Da dette forhold ikke er undersøgt nærmere, kan afhængigheden ikke beskrives nærmere.

3. Sårbarheder i infrastrukturen

Afsnit 3 omhandler sårbarheder i infrastrukturen på områderne el, naturgas, tele og it. For hvert område følger først en overordnet beskrivelse af infrastrukturen, og herefter en vurdering af sårbarheder. Sårbarheder skal i den forbindelse forstås bredt. Sårbarhederne kan udspringe af den tekniske infrastruktur (master, kabelføring etc.), organiseringen af området eller f.eks. lovgivningen på området. Sårbarheder vedrørende de indbyrdes afhængigheder mellem sektorerne er behandlet særskilt i afsnit 3.5.

3.1. Elområdet

I det følgende beskrives infrastrukturen på elområdet, hvorefter følger en vurdering af sårbarheder på området.

Beskrivelse af infrastruktur

Elsystemet

Elsystemet er af historiske årsager opdelt i to adskilte dele henholdsvis vest og øst for Storebælt:

- Elsystemet *vest for Storebælt* er en del af elsystemet på det europæiske kontinent og er direkte forbundet med dette gennem udlandsforbindelser til Tyskland. Derudover er systemet forbundet med Sverige og Norge gennem konvertering til jævnstrøm.

- Elsystemet *øst for Storebælt* er en del af det nordiske elsystem og er direkte forbundet med dette gennem udlandsforbindelser til Sverige. Derudover er systemet forbundet med Tyskland gennem konvertering til jævnstrøm.

Der er ingen direkte forbindelse mellem de to danske elsystemer, dvs. ingen Storebæltsforbindelse.

De to elsystemer beskrives nedenfor under ét på grund af de mange fællestræk.

Elsektoren er siden 1999 blevet liberaliseret, således at aktiviteterne *produktion af el* og *handel med el* i dag foretages på markedsvilkår af kommercielle virksomheder. Andre aktiviteter, der indgår som forudsætninger for produktion og handel, udføres fortsat af monopolvirksomheder. Dette gælder således:

- *Drift af transmissions- og distributionsnet* varetages af transmissions- og netvirksomhederne
- *Sikring af det samlede systems tekniske drift*, herunder forsyningssikkerheden for el, varetages af de systemansvarlige virksomheder

Elsystemet kan mere detaljeret beskrives således:

a. *Elproduktion* foretages teknisk af

   - *centrale kraftvarmeværker*, i alt 35 generatorer på 15 kraftværker med en samlet kapacitet på ca. 7.100 MW (heraf 3.100 MW i Vestdanmark og 4.000 MW i Østdanmark)
   - små og mellemstore *decentrale kraftvarmeværker*, i alt ca. 1.000 anlæg med en samlet kapacitet på ca. 2.250 MW (heraf 1.600 MW i Vestdanmark og 650 MW i Østdanmark)
   - *vindmøller*, i alt ca. 5.500 anlæg med en samlet kapacitet på knap 2.900 MW (heraf 2.320 MW i Vestdanmark og 570 MW i Østdanmark)

   Produktionsanlæggenes fordeling på forskellige anlægstyper er således ret forskellig for Vest- og Østdanmark.

b. *Transmissions- og distributionsnettene* transporterer el fra produktion til forbrugere og drives af

   - *transmissionsvirksomheder* (omfattende net og anlæg for spændinger på 100 kV og derover), hvoraf der er i alt 13 virksomheder
   - *netvirksomheder* (omfattende net og anlæg for spændinger under 100 kV), hvoraf der er i alt 129 virksomheder af meget forskellig størrelse

Omfanget af denne virksomhed fremgår tydeligere af følgende oversigt:

Tabel 3.1.

Ultimo 2001	**Luftledninger (km)**	**Kabler (km)**	**Stationer**
400 - 132 kV	5.391	773	145
60 - 30 kV	6.107	2.301	907
20 - 6 kV	14.068	45.422	68.048
0,4 kV	17.813	75.351	-
I alt	43.379	123.847	69.100

Også her er der betydelige forskelle mellem Vest- og Østdanmark.

c. *Udlandsforbindelserne*, som er forudsætning for eksport og import af el og som samtidig er væsentlige for elsystemets driftssikkerhed, indgår i transmissionsnettet og drives af transmissionsvirksomhederne.

d. *Systemansvarlig virksomhed* skal sikre den fysiske stabilitet (balancen) i det samlede elnet, elmarkedets funktionalitet samt forsyningssikkerheden for el på både kort og langt sigt. Denne systemdrift varetages af de systemansvarlige virksomheder - Eltra (i Vestdanmark) og Elkraft System (i Østdanmark) - der som et væsentligt virkemiddel har rådighed over transmissionsnettet.

e. *Elhandel* foretages af en række handelsselskaber, heraf 45 selskaber med forsyningspligt for et geografisk område og 22 selskaber uden forsyningspligt.

De systemansvarlige virksomheders systemdrift

El adskiller sig fundamentalt fra de fleste andre varer derved, at el i praksis ikke kan lagres. Det betyder, at der på ethvert tidspunkt skal være en præcis balance mellem produktion plus nettoimport på den ene side og forbrug på den anden side. Det er derfor nødvendigt, at der foretages en løbende overvågning af systemet og løbende korrektioner for at håndtere den kontinuerlige variation i forbrug, produktion og eksport/import, herunder de uundgåelige produktions- og netfejl af mindre konsekvens i det daglige. Endvidere er det nødvendigt at sikre et velfungerende elmarked, da en række forhold vedrørende elsystemets funktionalitet forudsættes varetaget af markedsmekanismerne.

Systemdrift varetages som nævnt af de to systemansvarlige virksomheder, som således er centrale for elsystemets funktionalitet, også i en krisesituation. De systemansvarlige virksomheder disponerer herved over dels produktionsreserver, dels det samlede transmissionssystem incl. udlandsforbindelserne. Systemets tilstand overvåges kontinuerligt ved hjælp af blandt andet online-målinger.

Driften af transmissionsnettet planlægges af de systemansvarlige virksomheder dels dagen før, dels løbende i driftsdøgnet på en sådan måde, at man på ethvert tidspunkt kan undvære en vilkårlig netkomponent og en vilkårlig central produktionsenhed, jf. afsnit 3.1.2 nedenfor. Systemdriften disponerer produktionsreserver og omkobler transmissionsnet ved hjælp af it-systemer og/eller ved telefonkontakt med de kontrolrum, som styrer de centrale produktionsanlæg og transmissionsnettet.

De systemansvarlige virksomheder skal som nævnt også sikre forsyningssikkerheden for el og har derfor indgået aftale med produktionsvirksomheder om, at produktionsanlæg holdes i reserve. Dette sikrer, at der på ethvert tidspunkt er dels tilstrækkelig produktionskapacitet, dels de driftsreserver der er nødvendige for håndteringen af den normale drift og for indsætning ved driftsforstyrrelser.

Elsystemets sammenhæng med udlandet

De systemansvarlige virksomheder indgår i et internationalt samarbejde gennem udlandsforbindelserne til Tyskland, Norge og Sverige. Gennem samarbejdsorganisationerne UCTE (Vesteuropa) og Nordel (de nordiske lande) indgår de systemansvarlige virksomheder i et integreret driftssamarbejde med nabolandene, som blandt andet indeholder fællesskab om visse driftsreserver.

Det danske elsystem er relativt lille i en europæisk sammenhæng og har samtidig meget store udlandsforbindelser. Kapaciteten på udlandsforbindelserne sat i forhold til det maksimale indenlandske forbrug er således ca. 84 % for Danmarks vedkommende, mens de sammenlignelige tal for de øvrige nordiske lande er 18 - 28 % og for Tyskland og Frankrig på 16 - 23 %.

De relativt kraftige udlandsforbindelser indebærer en stor robusthed for det danske elsystem, men har omvendt også den konsekvens, at forstyrrelser af elsystemet i nabolandene kan påvirke det danske elsystem. Samlet opnås der dog gennem udlandsforbindelserne en væsentlig robusthed.

Elproduktion

Produktionen i elsystemet omfatter dels *central*, dels *decentral* produktion.

De centrale værker - dvs. de store kraftværker som producerer ind på transmissionsnettet - leverer stort set alle systemtjenester, og er derfor afgørende for elsystemets drift.

Den decentrale produktion består af decentrale kraftvarmeanlæg og af vindkraftanlæg, hvor den enkelte enhed er relativt lille og derfor størrelsesmæssigt ikke er kritisk for elsystemet. Den decentrale produktion indebærer således lille sårbarhed for det enkelte anlæg, men samtidig giver den decentrale anlæg elsystemet en reduceret robusthed over for netfejl, idet de for at beskytte sig selv typisk foretager automatisk frakobling af nettet i fejlsituationer. Den decentrale produktion kan ikke afhjælpe bortfald af central produktion, dels fordi de decentrale kraftvarmeanlæg producerer efter varmebehovet, dels fordi vind-

kraftanlæggene producerer efter vindforholdene. I teknisk henseende forudsætter den decentrale produktion, at det overordnede elsystem fungerer, og derfor giver den decentrale produktion ingen hjælp i den situation, hvor elsystemet er nede (såkaldt *dødt net*), ligesom dens evne til at levere driftsreserver og andre systemydelser ofte er meget begrænset.

Transmissions- og distributionsnettene

Transmissionsnettene er overordnede sammenhængende net for henholdsvis Vest- og Østdanmark og er for en stor del sammenmasket, dvs. at der er mindst 2 forsyningsveje ind til et givet anlæg, f.eks. en transformerstation. Den videre fordeling til forbrugerne foretages så gennem distributionsnettene, der ikke i samme grad er maskeopdelt.

Transmissionsnettet består af to spændingsniveauer, dels 400 kV, dels 132/150 kV. I det åbne land består det især af luftledninger, mens det er kabellagt i større byområder og i særlige naturområder.

Transmissionsnettets dimensionering og driftsplanlægning er baseret på det såkaldte *n minus 1- princip*, dvs. at det skal kunne tåle udfald af en vilkårlig enkeltkomponent, jf. afsnit 3.1.2 herom.

Distributionsnettene hænger generelt ikke indbyrdes sammen, men kan ofte kobles sammen, hvis der er brug for det. Distributionsnettene er typisk delt i 3 spændingsniveauer på henholdsvis 50/60 kV, 10-20 kV og 0,4 kV (det er den spænding, der kommer ud til privatkunder som 230/400 V).

De to laveste spændingsniveauer drives normalt som radialer[1] ud fra en transformerstation, der hver dækker et lille antal forbrugere, hvorimod 50/60 kV-nettet - der i struktur ligner transmissionsnettet - normalt drives som ringe omkring en transformerstation. Derfor får en fejl i 50/60 kV-nettet ofte ikke betydning for forbrugerne, hvorimod en fejl på en radial i 10-20 kV og 0,4 kV-

[1] Et net, der drives som radialer (dvs. som eger i et hjul), har kun én forbindelse mellem to punkter og har derfor en større sårbarhed end hvis nettet er masket, således at der altid er flere forbindelser mellem to punkter.

nettene typisk vil føre til udkobling af dette net og dermed af de forbrugere, der er tilsluttet nettet. Normalt kan der dog i en sådan situation hurtigt etableres en reserveforsyning gennem netomlægninger.

Vurdering af sårbarheder

Elsystemet har, blandt andet som følge af de særlige karakteristika for el, en række sårbarheder, men hensyntagen til og imødegåelse af disse sårbarheder har til stadighed indgået i design og dimensionering af elsystemet. Tilsvarende er hensyntagen til sårbarhederne en væsentlig del af grundlaget for tilrettelæggelsen af den løbende drift, herunder planlægning af udbygnings- og vedligeholdelsesarbejder, og det vil i en krisesituation eller i en potentiel krisesituation være muligt at tilrettelægge driften, således at elsystemets eksponering over for disse sårbarheder formindskes..

n minus 1-princippet

Som nævnt er transmissionsnettet og udlandsforbindelserne afgørende for transport af el fra produktionsanlæg til forbrugerne, for udlandsforbindelserne, for opretholdelsen af et velfungerende elmarked og for elsystemets funktionalitet. Transmissionsnettet er baseret på det såkaldte *n minus 1- princip*, dvs. at systemet skal kunne tåle udfald af en vilkårlig enkeltkomponent. Dette princip er som hovedregel ikke anvendt i distributionsnettene, som er opbygget anderledes.

Princippet anvendes både ved dimensionering af elsystemer og ved den løbende drift. Anvendelse af princippet ved driften sikrer, at der i muligt omfang tages hensyn til, om dele af elsystemet i perioder er ude af drift på grund af udbygnings- og vedligeholdelsesarbejder.

I store elforsyningsområder (dvs. 100 MW eller derover) som f.eks. Hovedstadsområdet og Nordsjælland anvendes derfor i praksis et *n minus 2-princip* (også benævnt et *trebenet forsyningsprincip).* Hensigten hermed er at muliggøre, at der i perioder foretages udbygning eller vedligeholdelse af dele af elsystemet - med den konsekvens at den ene reservemulighed ikke er til rådighed - og sam-

tidig opretholde n minus 1-princippet intakt i driften. Omvendt kan udbygnings- og vedligeholdelsesarbejder i mindre forsyningsområder i perioder indebære, at det ikke er muligt at opretholde n minus 1-princippet intakt under drift.

Anvendelse af n minus 1-princippet til dimensionering og drift har til formål at sikre redundans i elsektoren og er udtryk for den betydning, som sektoren og myndighederne tillægger forsyningssikkerheden inden for elsektoren. Princippet rummer naturligvis problemstillinger i detaljerne:

a. Det kan ikke udelukkes, at enkelte større transformeranlæg eller transmissionslinietracéer efterhånden har fået en sådan betydning, at de reelt ikke vil kunne undværes uden større problemer.

b. I mange tilfælde er transmissionslinier og transformeranlæg ikke i væsentlig grad adskilt fra de reservesystemer, som skal fungere i tilfælde af udfald af de pågældende linier og anlæg.

   - Således er mange transmissionslinier dobbeltlinier med to sæt ledninger på den samme masterække, men ved brug af n minus 1-princippet anses disse dobbeltsystemer normalt som to uafhængige transmissionslinier. Årsagen til disse dobbeltlinier er økonomiske, politiske og miljømæssige, idet det gennem lang tid har været og fortsat er meget svært at få tilladelse til at bygge nye transmissionslinier gennem landskabet.

   - I enkelte tilfælde er to transmissionslinier på korte strækninger placeret med en sådan afstand, at skader på den ene transmissionslinie vil kunne forårsage skader på den anden linie.

   - Tilsvarende har transformeranlæg normalt flere linier ind i anlægget, og der kan være både 400, 132/150, 60/50 og 10 kV inden for det samme anlæg. Selv om alle linier, transformere m.m. således er samlet inden for det samme lille stationsområde, anses de for at være redundante systemer i overensstemmelse med n minus 1-princippet.

c. På den anden side har erfaringer fra konkrete situationer både i Danmark og i udlandet vist, at der kan være en større redundans end svarende til n minus 1-princippet, således at elsystemet i praksis (og afhængigt af situationen) kan tåle udfald af mere end en enkeltkomponent.

Transmissionsnettene incl. udlandsforbindelserne

Mere specifikt gælder om elsystemets sårbarhed på grund af *transmissionsnettene* blandt andet:

- Luftledninger er i sagens natur særligt udsatte og dermed sårbare, men kan til gengæld normalt repareres hurtigt.
- Nedgravede ledninger (kabler) er mindre sårbare, men til gengæld er reparation af kabelanlæg (såvel til vands som til lands) ofte en langvarig proces.
- Udlandsforbindelserne er både sårbare og har kritisk betydning, da det vil være problematisk at opretholde elsystemets drift uden disse.
- Transformeranlæg er generelt sårbare - især i stationer med kun en enkelt transformer - og reparation af dem kan tage lang tid.

Transformeranlæg er normalt ubemandede, men indhegnet og aflåst. I tilfælde af terrorvirksomhed kan adgang dog reelt ikke forhindres. For nogle anlæg er der etableret overvågnings- og alarmsystemer, som aktiveres ved utilladt adgang, men dette er ikke gennemført for hele elsystemet. Transmissionslinier er naturligvis hverken bemandede eller indhegnede.

Den tætte samkørsel mellem det danske elsystem og elsystemerne i Norge, Sverige og Tyskland indebærer, at det danske elsystem ikke kan betragtes som et system, der drives i såkaldt *ødrift*. Systemet kan derfor udsættes for driftsforstyrrelser fra nabolandene og kan omvendt også sende egne driftsforstyrrelser videre til nabolandene. Elsystemerne er imidlertid også dimensioneret til at kunne håndtere sådanne forstyrrelser i rimeligt omfang og samtidig giver sam-

driften med nabolandene en stor stabiliserende effekt, som reducerer systemets sårbarhed over for kritiske påvirkninger.

Elproduktionen

Om elsystemets sårbarhed på grund af *elproduktionen* gælder blandt andet:

- De centrale værker har samlet set stor betydning, da disse produktionsanlæg sikrer stabiliteten i elsystemet. Elsystemet drives normalt med tilgængelig reserveproduktionskapacitet, så der ikke er stor sårbarhed over for udfald af et enkelt centralt kraftværk. Samtidig har ingen af kraftværkerne en sådan betydning, at de ikke kan undværes på kort sigt. Derimod har elsystemet sårbarhed ved samtidige udfald af flere centrale kraftværker eller ved udfald af et enkelt centralt kraftværk kombineret med hændelser for transmissionsnettene.

- De decentrale kraftvarmeanlæg og vindmølleanlæg øger elsystemets sårbarhed ved netfejl. De har neutral virkning over for bortfald af øvrig produktionskapacitet,. Biomassefyret decentral kraftvarme og vindmølleanlæg ikke er sårbare overfor forsyningsafbrydelser for brændstoffer.

De centrale værker er altid bemandede. Det er forskelligt, i hvilket omfang der er etableret indhegning, adgangskontrol o.lign. I tilfælde af terrorvirksomhed kan adgang ikke forhindres, også fordi de alle har havneanlæg, hvor adgang fra søsiden vanskeligt kan forhindres. For nogle anlæg kan der være etableret overvågnings- og alarmsystemer, men dette er ikke tilfældet for alle anlæg.

I tilfælde af knaphed på el i det danske elsystem som følge af en ubalance mellem produktion og forbrug, der ikke kan modsvares af en elimport, er det et komplicerende element, at elforsyningen til den enkelte forbruger ikke kan begrænses og at elforsyningen ikke kan prioriteres til bestemte forbrugere. Endvidere vil de prisforhøjelser, som i en sådan situation typisk vil indtræde på elmarkedet, vanskeligt få effekt over for hovedparten af forbrugerne på grund af fastprissystemer og andre afregningsforhold. I praksis kan man i en sådan situ-

ation formentlig reducere elforbruget en del ved indsats over for bestemte forbrugskategorier samt ved hjælp af generelle mediekampagner.

Andre sårbarheder

For alle dele af elsystemet gælder, at det er sårbart over for, at personer uberettiget får adgang til at foretage udkobling af anlæg fra de kritiske kontrolrum enten direkte eller ved at true personalet.

En særlig problemstilling vedrører den såkaldte *start fra dødt net*, dvs. den situation hvor elsystemet som følge af helt usædvanlige hændelser er brudt sammen og altså uden spænding for hele Vest- eller Østdanmark. Problemstillingen er her, at en række af de centrale elinstallationer - store elværker, decentrale produktionsanlæg, udlandsforbindelser - forudsætter, at der er spænding på nettet for at kunne komme i gang.

Problemstillingen *start fra dødt net* har høj prioritet i elsystemets design, udbygning og drift og i takt med, at elsystemet ændres, revurderes det løbende, hvorledes det sikres, at opstart af et spændingsløst elsystem kan foretages under alle forhold.

Elsystemet er i nogen grad sårbart over for sammenbrud eller svigt af itsystemer, idet it indgår i alle dele af den løbende drift og monitering. De vitale systemer er normalt dublerede og dermed ikke sårbare over for enkeltfejl.

En særskilt sårbarhed kan ligge i det forhold, at transmissions- og netvirksomhederne af økonomiske årsager kan have vanskeligheder med at opretholde en høj standard af nettene og dermed en robusthed. Disse virksomheder, som ikke er konkurrenceudsatte, er omfattet af den såkaldte indtægtsrammeregulering, hvorefter deres indtægts- og dermed også udgiftsrammer løbende fastsættes af myndighederne. For virksomheder, som har vanskeligheder med at holde sig inden for indtægtsrammen, kan der være risiko for, at virksomhederne ser sig nødsaget til at reducere deres indsats vedrørende nettenes vedligeholdelse og udbygning samt beredskab i øvrigt.

Dette må ses i sammenhæng med, at der p.t. ikke er økonomiske konsekvenser for danske transmissions- og netvirksomheder knyttet til situationer med forsyningsafbrydelser som følge af netfejl. Det er dog under overvejelse hos myndighederne at etablere mekanismer, som giver virksomhederne incitament til at forebygge forsyningsafbrydelser som følge af netfejl.

Sårbarhed i relation til forskellige typer hændelser

I sin grundfilosofi er n minus 1-princippet orienteret mod tilfældige hændelser i form af driftsuheld og komponentfejl, som indtræffer uafhængigt af hinanden, og er baseret på, at risikoen herfor er nogenlunde lige stor for alle anlæg eller komponenter, således at der ikke er grund til markant større forebyggende foranstaltninger for nogle anlæg m.m. end for andre.

Disse forudsætninger kan ikke forventes opfyldt for hændelser som

a. naturskabte krisesituationer som f.eks. orkaner, lynstorme, oversvømmelser, skovbrande og naturkatastrofer i øvrigt, og

b. hærværk, sabotage, terrorvirksomhed o.lign.

I disse tilfælde vil de forhold, som forårsager udfald af et anlæg m.m., med stor sandsynlighed også forårsage udfald af et eller flere andre anlæg. Dertil kommer for så vidt angår terrorvirksomhed, at de mest kritiske anlæg må antages at have den største sandsynlighed for at blive mål for en aktion. Derfor kan n minus 1-princippet ikke give samme grad af forebyggelse over for sådanne hændelser.

Sammenfattende kan elsystemets sårbarhed over for forskellige typer hændelser beskrives således:

a. *Driftsuheld, uheld o.lign., som typisk indtræffer tilfældigt og som rammer anlæg m.m. uafhængigt af hinanden.* For transmissionsnettet giver n minus 1-princippet god redundans over for hændelser af denne karakter. Der kan dog være sårbarhed knyttet til perioder med udbygning eller vedligeholdelse af dele af elsystemet, hvor princippet ikke kan opretholdes fuldt ud, men hvor

der til gengæld i nogen grad kompenseres herfor gennem systemdriftens tilrettelæggelse i en sådan sårbar periode. For distributionsnettene, som ikke alle er baseret på n minus 1-princippet, er sårbarheden større, men til gengæld er konsekvenserne af udfald begrænset til forholdsvis små områder og udbedring vil normalt kunne ske hurtigt. De to nets dimensioneringskriterier er også forskellige, således udføres luftledninger ved hjælp af stålmaster i transmissionsnettet og i distributionsnettet typisk ved hjælp af træmaster (dog er kabellægning nu det normale).

b. *Naturskabte krisesituationer som f.eks. orkaner o.lign., hvor hændelsen nok indtræffer tilfældigt, men således at flere anlæg m.m. rammes på én gang.* For hændelser af denne karakter kan n minus 1-princippet ikke give samme grad af forebyggelse, men den redundans, som princippet indebærer, er stadig af stor værdi. Over for denne situation skal der være et retableringsberedskab, som kan udbedre skader hurtigt.

c. *Terrorvirksomhed, hvor hændelserne indtræffer planlagt og bevidst, således at flere anlæg m.m. med stor sandsynlighed rammes og således at de vigtigste anlæg har størst sandsynlighed for at blive ramt.* For sådanne hændelser giver n minus 1-princippet kun begrænset forebyggelse, idet sårbarheden kun i begrænset omfang kan reduceres gennem dimensionering. Derimod kan foranstaltninger som adgangskontrol, monitering m.m. have en forebyggende effekt, ligesom et retableringsberedskab, som kan udbedre skader hurtigt, er nødvendigt.

3.2. Naturgasområdet

Naturgassektoren samarbejder som nævnt i afsnit 1.2 med bygassektoren om beredskab, sikkerhed m.m. De indgår derfor begge i beskrivelserne nedenfor, dog med hovedvægt på naturgassektoren.

Beskrivelse af infrastruktur

Naturgassystemet kan opdeles i en række enkeltdele, som i det følgende gennemgås enkeltvis:

a. Naturgasforsyningen fra Nordsøen

b. Gasbehandlingsanlægget i Nybro

c. Transmissionssystemet

d. Naturgaslagrene ved Ll. Torup og Stenlille

e. De regionale fordelingsnet og distributionsnet

Naturgasforsyningen fra Nordsøen

Naturgasforsyningen fra Nordsøen omfatter dels en primær forsyning fra Dansk Undergrunds Consortiums (DUC) produktionsplatforme i Nordsøen, dels forsyning fra Syd Arne-feltet:

a. Den primære forsyning er fra DUC, hvor naturgas føres fra produktionsfelterne til Tyra Øst-platformen og derfra gennem rørledning til land. Denne rørledning står for ca. 90 % af forsyningen. Rørledningens kapacitet er ca. 26 mill. m^3/døgn, som om vinteren er fuldt udnyttet.

b. Naturgas fra Syd Arne-feltet føres i en separat rørledning til land. Rørledningen har en kapacitet er ca. 13 mill. m^3/døgn, som ikke er fuldt udnyttet.

DONG er operatør på begge rørledninger. De drives begge ved et driftstryk på op til 135 bar og er sammenkoblet ved DUC's Harald-felt. Hvis transporten i ledningen fra DUC-felterne må indstilles, kan en del af naturgastransporten derfor omlægges til Syd Arne-ledningen. På denne måde vil man kunne opretholde ca. 50 % af naturgasforsyningen.

Gasbehandlingsanlægget i Nybro

Gasbehandlingsanlægget i Nybro modtager og behandler naturgassen efter ilandføringen fra Nordsøen, dog kan naturgassen under normale driftsforhold sendes direkte ud i transmissionssystemet.

Gasbehandlingsanlægget er døgnbemandet.

Transmissionssystemet for naturgas

Transmissionssystemet er et 80 bars system. Det går fra Nybro-anlægget til Dragør og fra Ålborg til den dansk/tyske grænse. Derudover er der enkelte strækninger til større elværker. For hver ca. 10-15 km er der etableret linieventiler, således systemet kan sektioneres. Derudover er der ca. 40 M/R-stationer, som er grænseflade mellem transmissionssystemet og de regionale fordelingsnet.

En M/R-station er en måle- og regulatorstation, hvor gastrykket reduceres. Trykket reduceres fra 80 bar i transmissionssystemet til 40 og 19 bar i fordelingssystemet (40 bar i Jylland og 19 bar på Fyn og Sjælland), og fra 40 bar eller 19 bar til 4 bar, som er trykket i distributionsnettet. Reguleringssystemet sikrer, at distributionsnettets tryk ikke kan overstige 4 bar og dermed kan beskadige rørledningsnettet og de tilkoblede installationer.

Transmissionssystemet er et enstrenget system, dog med en dublering af ledningerne over Lillebælt og Storebælt samt en enkelt landstrækning (Nybro - Egtved). Hver af de to bæltkrydsninger har fuld transportkapacitet. Der er ca. 800 km transmissionsledning. Systemet er direkte forbundet med de tilsvarende systemer i Tyskland og Sverige. Ca. 40 % af naturgassen eksporteres.

Transmissionssystemet, herunder M/R-stationerne, er ubemandet, men overvåges og styres fra DONG's døgnbemandede kontrolcenter i Vejen.

Naturgaslagre

Naturgaslagre er etableret dels i Ll. Torup nord for Viborg og dels i Stenlille midt på Sjælland. Gaslageret i Ll. Torup er placeret direkte på transmissionssy-

stemet, mens Stenlille er forbundet med transmissionssystemet gennem en 40 km lang transmissionsledning, koblet på hovednettet.

Gaslagrene indeholder op til 1,7 mia. m³ naturgas, hvoraf ca. 700 mill. m³ er arbejdsgas, dvs. gas der kan trækkes ud i løbet af ca. 4 vintermåneder. Udtrækskapacitet en er ca. 20 mill. m³ pr. døgn.

Gaslagrene anvendes dels til belastningsudjævning om vinteren, hvor produktionen fra Nordsøen ikke er tilstrækkelig, dels som nødforsyningslager i tilfælde af havari på ledningsnettet. Endvidere anvendes gaslagrene for en mindre dels vedkommende til systemdrift og til kommercielle formål.

Gaslagrene kan være døgnbemandede, men kan også overvåges fra kontrolcentret i Vejen. Gaslageret i Ll. Torup kan opereres direkte fra Vejen.

De regionale fordelingsnet og distributionsnet

De regionale fordelingsnet og distributionsnet omfatter:

a. De regionale fordelingsnet, hvor naturgassen fordeles fra DONG's M/R-stationer over i de regionale fordelingsnet, dvs. Naturgas Fyn (NGF), Naturgas Midt-Nord (NGMN), Hovedstadens Naturgas (HNG) og DONG.

b. Distributionsnettene, som er vidt forgrenet og når ud til ca. 300.000 private husstande samt hovedparten af erhvervskunderne. Distributionsnettene opererer mellem 4 bar og 0,1 bar og er af plastrør. Fra distributionsnettene går naturgassen ind til den enkelte forbrugerinstallation.

Mange erhvervskunder er *afbrydelige*, dvs. har aftalt levering med en afbrydelighedsklausul. De kan således afbrydes med det aftalte varsel og overgå til anden energiform. Dermed øges forsyningssikkerheden for den resterende del af naturgasmarkedet, dvs. det *uafbrydelige* marked.

Bygas

Bygassektoren omfatter bygassystemerne i Københavns, Frederiksberg og Ålborg kommuner samt Svendborg og Kolding. Bygasforsyningen i Svendborg og Kolding er dog under afvikling.

I København og Frederiksberg spaltes naturgas til bygas på Sundby Gasværk. Alternativt kan benzin anvendes til produktion af bygas, der således ikke er sårbar over for en afbrydelse af naturgasforsyningen. Distributionsnettet, som overvåges fra Sundby Gasværk, forsyner ca. 175.000 kunder med gas til husholdning og industriformål samt i begrænset omfang til opvarmning.

I de øvrige kommuner anvendes en blanding af naturgas/luft, der udsendes til forbrugerne. Der er tale om mindre anlæg med fra 600 til 25.000 forbrugere.

Vurdering af sårbarheder

Naturgassektoren er ikke umiddelbart en kritisk sektor for samfundet. Naturgas kan imidlertid have betydning for elsektoren, dels fordi elproduktionen er noget afhængig af naturgas, dels fordi elforbruget vil blive kraftigt påvirket opad i tilfælde af afbrydelser af naturgasforsyningen, jf. afsnit 3.5.

I naturgassystemet er de mest sårbare elementer dels søledningerne, dels bæltkrydsningerne. Uheld på disse dele af systemet vil have store konsekvenser for naturgasforsyningen for hele landet eller dele af landet. Reparationstiden for disse ledninger er på op til ca. 60 dage.

På land er rørledningerne nedgravet med ca. 1-2 m jorddækning og dermed ikke direkte synlige. Reparationstiden for skader er fra 1/2 døgn op til 1-2 uger, afhængigt af ledningstryk og dimension.

Alle M/R-stationer og ventilstationer/grupper ligger over jorden og derfor synlige og dermed mere udsat for skader. Større stationer er indhegnet og aflåst, mindre stationer er delvis indhegnet, men aflåst, alene som forebyggelse af almindeligt hærværk. Reparationstiden er fra 1 døgn op til 2 uger.

En skade på Nybro-anlægget kan medføre, at gassen ikke kan behandles og dermed ikke opfylder kvalitetskravene, samt at gassen ikke forvarmes. Naturgasforsyning vil dog fortsat være mulig.

En skade på et gaslager om vinteren, hvor gasforbruget er størst, kan gøre det nødvendigt at afbryde dele af det *afbrydelige gasmarked* for at opretholde gasforsyningen til resten af markedet. Ved dimensioneringen er det forudsat, at kun ét af lagrene rammes af uheld.

It-problemer, f.eks. som følge af større virus- eller hackerangreb, vil indebære betydelige problemer for naturgassystemet. Da næsten al kommunikation er afhængig af it-systemer, vil den interne og eksterne kommunikation i værste fald kunne ophøre. Endvidere vil kontrolcentrene kunne miste kommunikationen med de ubemandede anlæg og stationer og dermed mulighederne for overvågning og styring. Ligeledes vil databaser kunne blive ødelagt og vitale data kunne gå tabt.

Bygasanlæggene er afhængig af naturgas, idet bygas fremstilles af naturgas blandet med luft. Dog er rørledningsnettet ringforbundet med et nødproduktionsanlæg placeret langt fra det primære produktionsanlæg. Københavns Energi kan som alternativ fremstille bygas på grundlag af benzin.

3.3. Teleområdet

I det følgende beskrives telemarkedet og teleinfrastrukturen, hvorefter følger en vurdering af sårbarheder på teleområdet.

Fokus for de følgende afsnit er sikring af *taletelefoni* i beredskabssituationer. For så vidt angår *internet- og datatjenester*, hører disse delvist til it-området, som det er defineret i denne udredning, jf. afsnit 3.4. Teleinfrastrukturen leverer de fysiske lag i it-infrastrukturen, dvs. kabler m.v. De teleudbydere, der har egen infrastruktur - f.eks. TDC - også kaldet netoperatører, kan samtidig være ISP'ere (Internet Service Providere). Disse udbydere vil høre til såvel tele som it-området. Den del af samfundets it-anvendelse, der er baseret på it-infrastrukturen er med andre ord grundlæggende baseret på blandt andet tele-

tjenester hos teleudbyderne og dermed teleinfrastrukturen. Herved vil de følgende afsnit i vid udstrækning også omfatte internet- og datatjenesterne.

Beskrivelsen af infrastrukturen for så vidt angår udsendelse af beredskabsmeddelelser til befolkningen samt vurderingen af sårbarheder på området, er baseret på oplysninger modtaget fra teleudbyderen Broadcast Service Danmark. Selskabet, som ejes af DR og TV2, har blandt andet til opgave at stå for driften af de senderstationer, der anvendes til spredning af DR's og TV2's lyd- og billedprogrammer - herunder programmer til opfyldelse af de beredskabsmæssige forpligtelser, der påhviler selskaberne efter lov om radio- og fjernsynsvirksomhed. Der består navnlig en pligt til at udsende meddelelser til befolkningen i beredskabssituationer.

Beskrivelse af infrastruktur

Telemarkedet og teletjenesterne

Telesektoren er kendetegnet ved at være meget dynamisk. Den teknologiske udvikling og markedsudviklingen går stærkt. Udbuddet af tjenester og antallet af teleudbydere ændrer sig til stadighed. Med liberaliseringen af telemarkedet op gennem 1990'erne har telemarkedet været præget af vækst - en vækst, der er baseret på en massiv vækst i befolkningens anvendelse af telekommunikationstjenester, herunder særligt internet- og mobiltjenester. Den samlede vækst i perioden har været på omkring 67 procent svarende til en årlig vækstrate på 11 procent. Fra år 2000 indtraf dog en opbremsning i denne udvikling. Den samlede omsætning på telemarkedet udgør fortsat mere end 30 milliarder kr. årligt. Men konkurrencen er hård og telemarkedet har i lighed med flere andre markeder i samfundet været præget af en afmatningsperiode i de seneste år. Teleudbyderne har af forskellige årsager været i en økonomisk krise, der blandt andet har betydet masseafskedigelser i branchen og større fokus på rentabiliteten i tjenesteudbuddet.

Væksten i antallet af teleudbydere med liberaliseringen af det danske telemarkedet har også betydet en øget vækst i engroshandlen udbyderne imellem.

Samtrafikområdet er f.eks. vokset betydeligt. Valgmulighederne for befolkningen er på den baggrund øget - tjenesteudbuddet er blevet bredere.

De mest udbredte teletjenester kan fortsat opdeles i fastnet, mobil- og internetjenester. Denne traditionelle opdeling vil dog på grund af de forskellige former for konvergens blive stadig mere vanskelig at opretholde.

Teleudbyderne er i dag i vidt omfang udenlandsk ejet selskaber. Teleselskaberne er i vid udstrækning fortsat styret fra Danmark som selvstændige selskaber under større udenlandske koncerner. Infrastrukturen er i vidt omfang fortsat også beliggende inden for landets grænser.

Udviklingen på telemarkedet - konkurrencesituationen, teleudbydernes økonomi, den stigende konvergens, globaliseringstendensen etc. - har stor betydning for samfundets sårbarhed og for den måde, hvorpå et nationalt teleberedskab bør indrettes. Fremtidige udfordringer afledt af blandt andet udviklingstendenserne på telemarkedet er belyst i afsnit 7.3.

Telenettene

Det er ikke hensigten inden for rammerne af denne udredning at udarbejde en oversigt over den samlede danske teleinfrastruktur. Ved *teleinfrastrukturen* skal her forstås den samlede mængde af udstyr og kabler, som benyttes til at producere de offentlige teleydelser. En sådan - meget omfattende - beskrivelse ville desuden kun give et øjebliksbillede af infrastrukturen, som ikke er statisk, men ændrer sig hastigt i takt med den teknologiske udvikling og udviklingen på telemarkedet.

Nogle teleudbydere er netoperatører, det vil sige de ejer - og udbyder normalt også - egne net, mens andre teleudbydere omvendt lejer netkapacitet hos en netoperatør. Andre teleudbydere formidler eller sælger kun teletjenester. I teleinfrastrukturen anvendes desuden *forskellige teknologier* til fremføring af teletrafikken. Den anvendte teknologi varierer teleudbyderne imellem og afhænger desuden normalt af typen af teletjeneste eller net. De forskellige typer af teknologier - f.eks. radiokæder, lyslederkabler og kobberpar, der anvendes i teleinfrastrukturen, vil ikke blive belyst nærmere i forbindelse med denne udredning.

I det følgende beskrives kort de *typer af net*, som traditionelt indgår i teleinfrastrukturen, og hvortil er knyttet forskellige sårbarheder, som beskrevet i afsnit 3.3.2 nedenfor.

Accessnettet forbinder den enkelte telekunde med nærmeste knudepunkt i teleudbyderens tekniske infrastruktur (central, switching eller routningsudstyr). Accessnettet er normalt et såkaldt "stjernenet". Helt karakteristisk for accessnettet er nemlig, at det kun er den enkelte telekunde, der anvender den pågældende del af teleinfrastrukturen. Teleudbydernes accessnet vil på den baggrund typisk være mindre kritisk i forhold til en beredskabssituation, men dette vil naturligvis afhænge af hændelsens omfang og karakter.

I *transportnettet* transporteres teletrafikken rundt mellem knudepunkterne i nettet. Teleudbydernes transportnet kan på den baggrund udgøre en meget kritisk del af infrastrukturen. Transportnettet er dog normalt et "maskenet", hvilket betyder, at der er *redundans* i nettet, således at teletrafikken kan ledes andre veje gennem nettet, hvis der skulle opstå et brud.

Selvom teletjenester udadtil er forskellige - f.eks. fastnetstelefoni og mobiltelefoni - udnytter de typisk delvist de samme ressourcer i telenettene. Mobiltelefoni fremføres således delvist også gennem den samme teleinfrastruktur som fastnetstelefonien.

Et *backbonenet* er et nets "ryggrad", det vil sige den del af nettet, som binder de vigtigste led i nettet sammen. Det kan være centraler, kabler m.v. Betegnelsen "corenet" anvendes undertiden om samme funktion. Backbonenettet udgør den vigtigste del af transportnettet. Teleudbydernes backbonenet udgør den mest kritiske del af teleinfrastrukturen, da det er her, konsekvenserne vil være størst, hvis et eller flere netelementer sættes ud af funktion. Her vil flest teleforbindelser kunne blive afbrudt i en beredskabssituation. Backbonenettet er dog normalt ligeledes et "maskenet" og centralt udstyr er ofte dubleret. Den redundans, der herved er i nettet, betyder, at teletrafikken - afhængigt af hændelsens omfang og karakter - vil kunne ledes andre veje gennem nettet, hvis der skulle opstå et brud.

Udsendelse af beredskabsmeddelelser via radio og TV

Udsendelse af, beredskabsmeddelser til befolkningen fra DR og TV2 sker via disse selskabers *sendenet*. Sendenet er betegnelsen for net bestående af et antal sendere, der til sammen giver den ønskede dækning af et geografisk område. Et sendenet består således af en række *sendestationer* strategisk placeret for rundsendelse af signaler. Signalerne fremføres til sendestationerne i et *transmissionssystem* kaldet *distribution*.

Sendestationens centrale funktion er *masten*, hvorpå der er monteret en rundspredende *sendeantenne* i en passende højde på 200 eller 300 meter over terrænet. Højden spiller sammen med en række andre faktorer en afgørende rolle for senderens dækningsområde. Sendeantenner for rundspredning er placeret øverst i masten. Sendeantenner er meget forskellige i udformning afhængig af frekvensområde og tjeneste. I nogle tilfælde benyttes samme antenne til udsendelse af flere programmer samtidigt. På sendemasterne er typisk også placeret antenner til brug for andre teletjenester, f.eks. mobiltelefoni.

Senderudstyr - herunder nødstrømsgeneratorer er placeret i bygninger tæt ved sendemasterne. Bygningerne indeholder typisk også udstyr for andre teletjenester, hvis funktion er knyttet til antenner i masten. Bygningerne er ikke bemandede. Broadcastsystemerne overvåges 24 timer i døgnet fra en centralt placeret overvågningscentral.

Sendenettene for henholdsvis lyd- og billedprogrammer er forskellige, og DR og TV2 anvender desuden forskellige teknologier i forbindelse med programfremføringen (distributionen).

- DR TV

Sendenettet består af 11 hovedsendere - sendestationer - fordelt over hele landet og ca. 20 hjælpesendere i områder, hvor der er dårlig dækning fra hovedsenderne. Programmerne fremføres - distribueres - til sendestationerne hovedsagelig via satellit direkte fra DR. Sendestationerne er forsynet med et såkaldt "ballempfang" og automatisk omskiftning, hvis hovedforsyningen via satellit

skulle svigte. Ballempfanget udgør således en alternativ fremføringsmulighed[2]. Sendestationerne er desuden forsynet med nødstrømsgeneratorer.

- TV2

Sendenettet består af 16 hovedsendere - sendestationer - fordelt over hele landet. Programmerne distribueres til sendestationerne via TV2's eget radiokædenet suppleret på enkelte strækninger med fiberkabler. I sendenettet kan distribution af landsprogrammet fra Odense omlægges til distribution af programmer fra TV2's 8 regionale studier. TV2's sendenet er kun i mindre omfang forsynet med ballempfang. Senderne er i øvrigt udublerede og indeholder ingen redundans. TV2 nettet er ikke forsynet med nødstrøm.

- FM-nettet

Der er i dag 4 FM programmer, der udsendes via 4 FM-sendere plus reserve sender på hver sendestation. Samtlige sendestationer er tilkoblet nødstrømsforsyning med diesel, og hovedsenderne har ballempfang med automatisk omskiftning ved udfald. Distribution af programmer fra DR til sendestationerne sker via fast lejede 2 Mbits kredsløb hos TDC.

- AM-nettet

AM-udsendelser på mellembølge og langbølge er indrettet på sendestationen Kalundborg Radio. Programmerne distribueres fra DR på digitale linier lejet hos TDC.

Vurdering af sårbarheder

I det følgende beskrives de sårbarheder, der er identificeret på teleområdet. Som nævnt indledningsvis til afsnit 3.3 ovenfor, er fokus for vurderingen sikring af *taletelefoni* i beredskabssituationer. Herudover er der et særligt afsnit om sårbarheder relateret til udsendelse af beredskabsmeddelelser via radio og tv.

[2] Systemet er et transportsystem for broadcast-signaler, der benyttes som reservesystem for normal distribution via radiokæde, satellit eller kabel af signaler til sendestationer.

Beredskabsplanlægning

Teleudbyderne har en høj bevidsthed og viden om beredskabsforhold. De har i vidt omfang udarbejdet beredskabsplaner og foretager risiko- og konsekvensanalyser i forhold til trusler mod driftsstabiliteten. Generelt er beredskabet dog rettet mod vejrfænomener og utilsigtede hændelser som f.eks. lynnedslag og menneskelige og tekniske fejl. Der er desuden relativ stor forskel på sikringsniveauet hos de teleudbydere, der har medvirket i forbindelse med denne udredning. Det skal i den forbindelse understreges, at et tilsyn har vist, at de alle lever op til lovgivningens krav på området, jf. afsnit 5.4.3.

Bag valget af sikringsniveau ligger typisk en bevidst prioritering - en balance i forhold til henholdsvis sikring af driftsstabilitet og økonomi. I forhold til teleudbydernes beredskabsplanlægning udgør det en vis sårbarhed. Det er en sårbarhed, der må overvejes, dels i forhold til det politisk ønskede sikringsniveau på teleområdet, og dels i forhold til finansieringen af sikringsforanstaltninger. Konkurrencesituationen på telemarkedet, som den ser ud i dag, gør, at også sikringsniveauet udgør et konkurrenceparameter teleudbyderne imellem. Overlades valget af sikringsniveau og finansieringen af konkrete sikringsforanstaltninger til teleudbyderne selv, er der dog risiko for en nedprioritering af teleberedskabet med en høj sårbarhed til følge - en sårbarhed hvis udvikling også vil være svær at følge over tid.

Organisation og personale

Ved personale til brug for teleberedskabet, sondrer teleudbyderne typisk mellem et beredskab - en sikkerhedsorganisation - i dagligdagen, der skal håndtere mindre forstyrrelser i driften, og et udvidet beredskab, som typisk består af en form for krisestab, der kaldes sammen i ekstraordinære, kritiske beredskabssituationer. Der er dog stor forskel teleudbyderne imellem. Kun en af teleudbyderne har et decideret virksomhedshjemmeværn, jf. afsnit 5.3.1.

Det må antages at udgøre en vis sårbarhed, såfremt der ikke er tilstrækkeligt personale til rådighed til at håndtere en mere kritisk beredskabssituation. Sårbarheden kan dog ikke umiddelbart opgøres eller beskrives nærmere, idet den

blandt andet vil afhænge af den konkrete hændelse, det vil sige beredskabssituationens karakter og omfang. Generelt har teleudbyderne også en god kontaktflade til andre teleudbydere, diverse serviceaftaler med andre virksomheder osv. Så afhængigt af situationen, vil der kunne indgås aftale om ekstra personale. Problemstillingen er også behandlet nedenfor i afsnittet om regulatoriske forhold.

Bygninger og installationer

Teleudbyderne har i vidt omfang sikret bygninger og installationer i teleinfrastrukturen i forhold til vejrfænomener og utilsigtede hændelser etc. Dette er særligt tilfældet for så vidt angår backbone- og transportnettene. Bygninger, som indeholder udstyr, der udgør vigtige knudepunkter i teleinfrastrukturen, er desuden i vidt omfang sikret mod uvedkommendes indtrængen i form af fysisk og eller logisk adgangskontrol, videoovervågning og skalsikring. Accessnettene er ikke sikret i samme omfang, men skader på disse net vil til gengæld typisk kun betyde eventuelle driftsforstyrrelser eller nedbrud i et begrænset geografisk område.

På grund af strukturen i backbone- og transportnettene, jf. afsnit 3.3.1 ovenfor, er der desuden i meget høj grad tale om redundans i disse net. Det betyder, at hvis f.eks. et hovedkabel eller en sendermast sættes ud af funktion, vil trafikken kunne dirigeres en anden vej i nettet.

Bygninger og installationer er kun i mindre omfang sikret mod fysiske angreb som terror- og krigshandlinger. Bygninger med driftsudstyr, udearealer, master, kabler m.v. er meget sårbare mod disse tilsigtede handlinger. Da der i vidt omfang er redundans i telenettene vil et angreb - med mindre det er alt ødelæggende eller strategisk rettet mod flere lokationer - dog typisk kun medføre driftsforstyrrelser eller nedbrud i et begrænset geografisk område. Hertil kommer, at borgerne i dag har flere muligheder med hensyn til valg af teletjenester. En myndighed eller en virksomhed med et særligt kommunikationsbehov - herunder i en beredskabssituation - kan f.eks. sikre sig ved at købe alternativ

fremføring i faste telenet eller ved at have forskellige typer teletjenester til rådighed.

Netsikkerhed

For så vidt angår selve nettene - netsikkerheden - er der generelt tale om et højt sikringsniveau og teleudbyderne har en høj bevidsthed omkring it-sikkerhed i forhold til driften. Telenettene er i vidt omfang sikret såvel fysisk som logisk mod uautoriseret adgang til nettene, mod vandskader, brand, menneskelige fejl etc. Nettene vurderes generelt at være robuste i forhold til utilsigtede eller hændelige hændelser etc. Nettene er dog sårbare i forhold til direkte angreb ved terror- eller krigshandlinger.

På nogle områder er der foretaget en - bevidst - nedprioritering af sikkerheden af økonomiske årsager. Dels i forhold til de tilsigtede direkte angreb som terror- og krigshandlinger, men dels også i et vist omfang på enkelte områder vedrørende it-sikkerheden generelt, f.eks. hvor en teleudbyder har placeret dubleret, vitalt teleudstyr i samme bygning. Da de enkelte sikringsforanstaltninger varierer noget teleudbyderne imellem, bør det overvejes at indføre minimumskrav til netsikkerheden.

Forhold vedrørende lovgivningen

Den gældende lovgivning om teleberedskabet er beskrevet nærmere i afsnit 5.3.1. Den teknologiske udvikling og udviklingen på telemarkedet i navnlig det seneste årti har medført et behov for at revurdere teleberedskabet og i den forbindelse også lovgivningen på området.

a. Bekendtgørelse om teleberedskabet

Bekendtgørelsen indeholder regler om organisatoriske forhold, herunder regler vedrørende IT- og Telestyrelsens beføjelser og forvaltningsorganet NALLAs beføjelser, når NALLA aktiveres[3]. Herudover indeholder bekendtgørelsen

[3] NALLA er et forvaltningsorgan, oprettet til at varetage beredskabsmyndighedernes behov for udnyttelse af telekommunikationsnet i beredskabssituationer, jf. afsnit 5.3.2.

særligt regler om, hvilke vilkår for udbud af telenet og teletjenester IT- og Telestyrelsen kan fastsætte.

Bekendtgørelsen indeholder blandt andet regler om teleudbydernes beredskabspligt. Teleudbyderne skal planlægge og sikre, at det nødvendige personale er til rådighed ved gennemførelse af teleberedskabet. Herved forudsættes det, at teleudbyderne har et internt teleberedskab, men der er ikke fastsat nærmere krav til karakteren og omfanget af et sådant teleberedskab. Der er samtidig hjemmel til, at personale, der varetager nøglefunktioner hos teleudbyderen, ved ansøgning herom kan fritages for mødepligt i forsvaret i forbindelse med krise eller krig, også benævnt designeringsordningen. Personale, der ønsker at deltage i det frivillige hjemmeværnsarbejde, vil indgå i virksomhedshjemmeværnet. Det er hensigten, at personalet herved skal kunne passe deres arbejde under krise og krig indtil det tidspunkt, hvor hjemmeværnet/Forsvaret eventuelt overtager ansvaret for bevogtning og beskyttelse af det pågældende tjenestested.

Problemstillingen er også behandlet ovenfor i afsnittet om sårbarheder vedrørende teleudbydernes organisatoriske - og personalemæssige forhold. Det må antages at udgøre en vis sårbarhed, såfremt der ikke er tilstrækkeligt personale til rådighed til at håndtere en mere kritisk beredskabssituation. Sårbarheden kan dog ikke umiddelbart opgøres eller beskrives nærmere, idet den blandt andet vil afhænge af beredskabssituationens karakter og omfang.

For så vidt angår IT- og Telestyrelsens (og NALLAs) kompetence til i en beredskabssituation at afgøre hvilke forbindelser hos teleudbyderne der skal dækkes af telenettenes fremføringsmuligheder, når disse ikke kan tilgodese alle behov, til at give de fornødne direktiver til teleudbyderne vedrørende prioritering af reetablering af ødelagte teleanlæg samt til at beordre en generel begrænsning af trafikken i telenet og teletjenester, jf. afsnit 5.3.2, kan et manglende overblik over de enkelte udbyderes udbud af telenet og teletjenester udgøre en vis sårbarhed. Der er et behov for at styrke det operative samarbejde med teleudbyderne, således at der i en beredskabssituation hurtigt og effektivt kan

indhentes oplysninger fra teleudbyderne om det aktuelle udbud af telenet og teletjenester, om kontaktpunkter, om eventuelle driftsmæssige problemer etc.

b. Bekendtgørelse om sikring af offentlige telenet og teletjenester

Bekendtgørelsen har til formål at tilvejebringe en sikring af offentlige taletelefonitjenester i faste telenet, der opfylder beredskabsmyndighedernes[4] behov for anvendelse af sådanne tjenester i beredskabssituationer. Sikringen giver abonnenter, der er udpeget af beredskabsmyndighederne, en fortrinsstilling ved adgangen til at benytte offentlige taletelefonitjenester i faste telenet.

Ved sikring af offentlige taletelefonitjenester i faste telenet forstås to særlige foranstaltninger: Sikret fortrinsret og sikret adgang. Ved sikret fortrinsret forstås en fast etableret mulighed for adgang til at benytte offentlige taletelefonitjenester i faste telenet til at gennemføre opkald forud for ikke udpegede abonnenter. Ved sikret adgang forstås en særlig foranstaltning, der indebærer, at ikke udpegede abonnenter midlertidigt udelukkes fra at foretage opkald i offentlige taletelefonitjenester i faste telenet.

Denne sikringsordning gælder kun taletelefoni i faste telenet, og således ikke taletelefoni i mobilnettene. Sikringsordningen omhandler desuden kun fortrinsret til opkaldsmulighed. Der er ingen krav om eller garanti for, at opkaldet kan gennemføres. Opkaldet er således ikke sikret en fortrinsret frem til modtager af opkaldet - herunder en fortrinsstilling gennem flere udbyderes net.

Sikringsordningen er på den baggrund meget sårbar. For det første er man ved anvendelse af mobiltelefoner i en beredskabssituation ikke sikret en fortrinsstilling i telenettene. Omvendt vil der i det tilfælde, hvor sikringsforanstaltningen sikret adgang er etableret, og hvor abonnenter, der ikke er omfattet af ordningen, er afskåret fra at foretage opkald via fastnetstelefonen, kunne ske det, at disse abonnenter vil forsøge at anvende mobiltelefonen. Det vil i praksis kunne medføre, at telenettene overbelastes og - afhængigt af situationen - at trafikken blokeres. Det skyldes, at opkald via mobiltelefoner i et vist omfang

[4] Ved beredskabsmyndighederne forstås det militære forsvar, redningsberedskabet, politiet og øvrige civile myndigheder.

afsluttes i samme centraler som fastnetsopkald. IT- og Telestyrelsen (eller NALLA) kan dog i forbindelse med en beredskabssitation give direktiv om lukning af teletjenester, således at primært taletelefoni i faste net kan anvende den grundlæggende infrastruktur til afvikling af samfundsvigtig telekommunikation.

Sikringsordningen gælder desuden p.t. kun for enkelttilslutninger, og ikke for forbindelser tilsluttet digitale PABC'ere (omstillingsanlæg). Også opkald herfra vil kunne hindre opkald fra abonnenter med fortrinsstilling i at gennemføre opkaldene i en beredskabssituation. Og omvendt er opkald fra PABC'ere ikke sikret en fortrinsstilling. Det skal i den forbindelse bemærkes, at beredskabsmyndigheder som f.eks. Forsvaret anvender PABC'ere.

c. Bekendtgørelse om faste kredsløb til beredskabsmæssige formål

Bekendtgørelsen har til formål at sikre retningslinier for tilvejebringelse og opretholdelse af samfundsvigtig telekommunikation til brug for beredskabsmyndighederne. Bekendtgørelsen omhandler i den forbindelse beredskabsmyndighedernes mulighed for at leje faste kredsløb[5] hos teleudbyderne. Bekendtgørelsen omfatter en række krav til de teleudbydere, der udbyder faste kredsløb til beredskabsmæssige formål, vedrørende proceduren for etablering, ændring, nedkobling samt fejlretning af faste kredsløb.

Faste kredsløb til beredskabsmæssige formål registreres løbende i NALLA, jf. afsnit 5.3.2, og vil indgå i forbindelse med IT- og Telestyrelsens- eller NALLAs prioritering af telenet og teletjenester i en beredskabssituation. Her vil kredsløbene kunne prioriteres højere end andre teletjenester.

Der er ikke identificeret sårbarheder i forbindelse med selve bekendtgørelsen. Det skal dog bemærkes, at sårbarheden i praksis vil afhænge af sikringsniveauet i de faste telenet, da kredsløbene er en del af teleinfrastrukturen. Kredsløbene vil som faste kredsløb være fremført på en måde, der gør, at de ikke i samme

[5] Ved faste kredsløb forstås telekommunikationsfaciliteter, hvorved der enten stilles analog eller digital transmissionskapacitet til rådighed til slutbrugere eller andre.

grad som andre teletjenester vil være berørt i en situation, hvor telenettene er overbelastede, hvilket er en styrke. Sårbarheden vil dog normalt være den samme som ved andre teletjenester, hvad angår f.eks. naturkatastrofer, fysiske angreb ved terrorhandlinger etc.

En sårbarhed relateret til ordningen er muligvis, at visse myndigheder m.fl. ikke er bekendt med ordningen. Problemstillingen indgår i afsnit 8.3 under punktet om en vejlednings indsats i forhold til myndighedernes planlægning af eget kommunikationsbehov og beredskab.

Udsendelse af beredskabsmeddelelser via radio og tv

Sendenettene til udsendelse af DR's og TV2's lyd- og billedprogrammer er generelt meget robuste, og der er i et vist omfang redundans i nettene. DR's og dele af TV2's sendenet er forsynet med såkaldte "ballempfang", jf. afsnit 3.3.1 ovenfor, der udgør en alternativ fremføringsmulighed.

Herudover er det en styrke, at DR's og TV2's sendenet er to næsten helt adskilte net, og herved udgør to alternative udsendelsesmuligheder for beredskabsmeddelelserne. Lydprogrammerne på FM udsendes via samme sendemaster som DR's billedprogrammer, men medmindre der er tale om sabotage mod sendestationerne og masterne, vil man således også kunne vælge mellem disse to udsendelsesmuligheder. Lydprogrammer på AM udsendes fra én landsdækkende sendestation, Kalundborg Radio, som således også udgør en udsendelsesmulighed.

Sendenettene er robuste over for naturkatastrofer, tekniske og menneskelige fejl og andre hændelige eller utilsigtede hændelser. De enkelte sendestationer er dog meget sårbare over for fysiske angreb som terror eller krigshandlinger. Masterne ligger åbent i landskabet og kan rammes af granater, raketter etc. fra stor afstand. Selv lette håndvåben kan ødelægge fødekablerne til antennerne og dermed stoppe udsendelserne. Et sendestop vil i givet fald være længerevarende, da antenner og fødekabler ikke er lagervare hos producenten. Fremstilling og levering må formodes at vare mindst 5-6 måneder. Hvor kritisk en sårbarhed der vil være tale om afhænger af hvor mange og hvilke sendestationer, der

sættes ud af drift. Alle seere og lyttere i Danmark kan modtage lyd og billedprogrammer fra mere end én sender, og mere end 1 million danskere er forsynet med radio og tv via kabel. Derudover findes et stort antal private parabol modtagere.

Lyd og billedsignalerne kan "jammes"[6], men det vil kræve en ganske kraftig sendestyrke at "jamme" DR's og TV2's hovedsendere. "Jammes" en enkelt sender, vil det desuden kun stoppe udsendelserne i det område af landet, senderen dækker. Forebyggende foranstaltninger er ikke mulige, men IT- og Telestyrelsens mobile pejlevogne vil kunne identificere, hvorfra de signaler, der "jammer" en sender, udsendes.

Det forhold, at sendemasterne også benyttes af flere mobiloperatører, udgør også en vis sårbarhed. Ved et angreb mod en sendestation, kan man herved sabotere flere tjenester samtidig. Det udgør i den forbindelse også en sårbarhed, at der i en del af masterne er fælles udnyttelse af antennerne mellem DR og TV2.

Den største sårbarhed vurderes dog at kunne være der, hvor beredskabsmeddelelser produceres og udsendes fra. Hvorvidt der reelt er tale om en sårbarhed - herunder hvorvidt der på disse lokationer er etableret sikringsforanstaltninger til at imødegå trusler som f.eks. fysiske angreb, uvedkommendes indtrængen, naturkatastrofer etc. - er imidlertid ikke undersøgt i forbindelse med dette udredningsarbejde. Dette forhold hører under Kulturministeriet.

Sammenfatning af sårbarheder

De mest kritiske sårbarheder er sammenfattet i det følgende:

- Generelt udgør det en sårbarhed, at teleudbydernes *beredskabsplanlægning* i vidt omfang er styret af økonomiske hensyn. Der er herved en høj risiko for nedprioritering af beredskabet. Det gør det desuden vanskeligt at følge udviklingen i sårbarheden.

[6] Udsendelse af støj på frekvensen

- *Bygninger og installationer* i telenettene er meget sårbare over for fysiske angreb som terror- og krigshandlinger. Da der i vidt omfang er redundans i telenettene, vil et angreb dog typisk kun medføre nedbrud i et begrænset geografisk område - med mindre et angreb er altødelæggende eller strategisk rettet mod flere lokationer.

- *Nettene* er ligeledes sårbare over for tilsigtede handlinger.

- Sårbarheder relateret til *lovgivning* på teleberedskabsområdet er:

a. Et manglende overblik over de enkelte teleudbyderes udbud af telenet og teletjenester kan udgøre en vis sårbarhed i relation til IT- og Telestyrelsens (og NALLA's) kompetence til at råde over telenettene og foretage prioriteringer i en beredskabssituation. Der er et behov for at styrke det operative samarbejde med teleudbyderne.

b. Sikringsordningen i bekendtgørelse om sikring af offentlige telenet og teletjenester gælder kun taletelefoni i faste telenet, og således ikke taletelefoni i mobilnettene. Sikringsordningen omhandler desuden kun fortrinsret til opkaldsmulighed. Der er ingen krav om eller garanti for, at opkaldet kan gennemføres. Sikringsordningen gælder desuden kun enkelttilsslutninger.

- Sendestationer til brug for *udsendelse af beredskabsmeddelelser* er meget sårbare over for fysiske angreb som terror eller krigshandlinger. Selv lette håndvåben kan ødelægge fødekablerne til antennerne og dermed stoppe udsendelserne. Et sendestop vil i givet fald være længerevarende, da antenner og fødekabler ikke er lagervare hos producenten. Hvor kritisk en sårbarhed der vil være tale om, afhænger af hvor mange og hvilke sendestationer, der sættes ud af drift.

3.4. It-området

Der er tradition for at arbejde med lokale beredskaber på it-området, og det betyder, at eksisterende lovgivning retter sig mod det lokale niveau. Et lokalt

beredskab betyder, at den enkelte myndighed eller virksomhed udarbejder en beredskabsplan, typisk som del af det generelle it-sikkerheds-arbejde.

Et nationalt perspektiv på sårbarheder er et nyt fokus på it-området, og et resultat af et ændret trusselsbillede. Det nye trusselsbillede har inden for de sidste par år fået en række lande til at gennemføre sårbarhedsanalyser på linie med den danske, herunder bl.a. USA[7], Sverige[8] og Norge[9].

Endelig har teknologiudviklingen været eksplosiv, og samfundets *anvendelse* af informations- og kommunikationsteknologi har gennemløbet en tilsvarende eksplosiv udvikling, og vi har i dag opnået en stor afhængighed af it.

Afhængighed fører til sårbarhed fordi der er risiko for, at det man er blevet afhængig af, ikke er tilstede eller ikke fungerer som forventet.

En sårbarhedsudredning på it-området kan meget hurtigt føre til at handle om alting, da der ikke er et system i dag der ikke på en eller anden måde er afhængig af it. Det er derfor vigtigt at afgrænse, hvad der menes med it, og hvad der menes med it som en del af infrastrukturen.

Beskrivelse af infrastruktur

It-området i relation til sårbarhedsudredningen omhandler computernetværk, dvs. internettet og andre offentligt tilgængelige netværk, samt hardware og software, som indgår heri. Der ses bort fra interne netværk og udstyr uden forbindelse til netværk.

I relation til sårbarhedsudredningen, er dette it-område defineret som:

- Applikationer (programmer der kører på en computer)
- Dataflow (de informationer der flyder mellem computerne og programmerne)

[7] The National Strategy to Secure Cyberspace, Feb. 2002
[8] SOU 2002, "Vulnerability and Security in a New Era – A Summary"
[9] Samfunnets sårbarhedet som følge av avhengighet til IT, oktober 2002. Den norske analyse er dog ligesom den danske, mere en ramme for en egentlig sårbarhedsanalyse.

- Netværket (de routere og protokoller der binder netværkene sammen). Der ses bort fra selve fremføringsmedierne (kabler, satellitter, etc.), da disse hører under teleområdet.

For hvert af disse områder er infrastrukturen beskrevet.

Netværket

Mange virksomheder og organisationer anvender eksterne netværk til at knytte deres forskellige afdelinger sammen og til at udveksle data og gennemføre transaktioner med samarbejdspartnere. Det mest alment kendte af disse netværk er internettet, der er beskrevet yderligere i næste afsnit.

Øvrige netværk omfatter en række lukkede net. Af disse kan bl.a. nævnes:

- Det danske sundhedsnet (Medcom)
- Supermarkedernes bestilling af varer

Internettet og andre offentlige netværk

Internettet er det mest kendte og mest åbne af de offentlige netværk. Internettet har traditionelt været benyttet til ikke-forretningskritisk datakommunikation, men forretningsmodeller har vist, at der er store økonomiske besparelser, hvis man kan acceptere en vis usikkerhed i ydeevne og stabilitet.

Internettets logiske infrastruktur er påvirket af, at internettet er skruet sammen af en række fysiske netværk, der drives af forskellige interessenter. Forskningsnettet og TDC har en stor del af det, man kalder det danske internets "backbone". UNI-C står for vedligeholdelse af DIX'en[10], som søger for kommunikation mellem de danske ISP'er.

Eksempler på andre offentlige netværk er:

- Forskningsnettet er en højhastigheds internetopkobling primært til forskningsinstitutioner

[10] Danish Internet Exchange, en omstillingscentral mellem de danske internetudbydere

- Sektornet tilbyder en række tjenester herunder Skolekom[11] til undervisningsverdenen

Der er en række mindre, nationale netværk koblet til kernedelen af det danske internet. Ikke mindst fra de mange bredsbåndsløsninger som ADSL og kabeltv, som er relevante i et trusselsperspektiv for eksempel i forbindelse med DoS[12]-angreb.

Noderne (de enkelte computere) sluttet til internettet har hver en unik maskinadresse (IP-adresse). De to vigtigste funktioner i den logiske infrastruktur eller IP-laget er:

1. Routningsprotokoller, der sikrer, at datatrafik mellem to maskiner, der alene er identificeret ved den unikke maskinadresse (IP-adressen) kan forekomme, uden at maskinerne ved, hvor den anden maskine rent fysisk befinder sig.

2. DNS-tabeller, der oversætter menneskesprogsnavngivning for services på internettet (en URL som f.eks. www.vtu.dk) til den unikke maskinadresse (IP-adressen).

Forsyning af udstyr

Der er ikke en standard for, hvordan en computer eller en komponent til en computer eller for den sags skyld en applikation skal se ud. It-branchen er kendetegnet ved mange leverandører og en ikke altid lige smidig sameksistens mellem forskellige producenters produkter. Forsyningen af software og hardware til virksomheder og organisationer foregår fra mange forskellige producenter via endnu flere forhandlere og løsningsleverandører.

[11] Skolekom er et mail- og konferencesystem med internetadgang, som benyttes af 250.000 brugere
[12] DOS, Denial of Service Attack, angreb der afbryder tilgængelighed til services på internettet

Public Key Infrastruktur – PKI

Med loven om kvalificerede certifikater fra år 2000, og ikke mindst med lanceringen af den fælles offentlige digitale signatur (OCES) foråret 2003, er der opbygget en national infrastruktur til behandling, udskrivning og inddrivelse af digitale signaturer og til udveksling af krypteringsnøgler.

Der indgår en række af virksomheder og andre typer af aktiver som væsentlige infrastruktur leverandører i netværket. Blandt virksomheder der indgår, er ISP'er (Internet Service Provider) kritiske aktiver, da de blandt tilbyder tjenester som internetadgang. Der indgår også andre typer aktiver som for eksempel landekode domain registrant og Danish Internet Exchange (DIX).

Dataflow

At opfatte data som strømme er et væsentligt perspektiv for at sikre tilgængelighed. Datastrømme forudsætter, at det grundlæggende netværk er til stede, og på den anden side, at der er applikationer, der kan sende, modtage og behandle data i applikationsniveauet.

En række virksomheder og offentlige institutioner benytter særligt sikrede intranet som for eksempel SDN (Statens Datanet), med særlige krav til opkobling til disse netværk. Det betyder, at store mængder trafik eller vigtig kommunikation skal passere udbydere af sådanne tjenester, hvorfor det kan være nødvendigt at lave flowanalyser som grundlag for at identificere aktiver. Udlandsafhængigheder, det vil sige afhængigheder af systemer placeret i udlandet, er et andet område, hvor flowanalyser kan afdække aktiver. Et eksempel er top level domainstrukturen, som også den danske del af internet er afhængigt af, eller ISP'er som router trafik rundt i deres egne netværk, også udenlandske netværk.

Applikationer

Behandlingen af data sker ved hjælp af applikationer. En applikation er et program, som kører på en computer, og som tilbyder en tjeneste. Programmer kan stille data til rådighed, samle og organisere data eller på anden måde understøtte håndtering af data.

Digital forvaltning

Den digitale forvaltning kræver digital kommunikation i alle tre lag, dvs, netværk, dataflow og applikationer, på tværs i den offentlige sektor. Digital forvaltning vil overordnet set sige elektronisk kommunikation mellem det offentlige og borger og mellem offentlige institutioner. Det må forventes, at der vil komme nye infrastrukturelementer til understøttelse af visionerne om den papirløse forvaltning, men den papirløse forvaltning stiller også krav om øget integration af offentlige it-systemer. I hvidbog om it-arkitektur for den offentlige forvaltning[13] er det muligt at finde yderligere beskrivelser af visioner for digital forvaltning.

XML og infostrukturdatabasen

Infostrukturdatabasen er et forholdsvist nyt element, der indgår i den nationale it-infrastruktur. Der er tale om en web-service, der kan anvendes til på korrekt vis at danne XML-skemaer, der skal benyttes, når to funktioner/databaser skal udveksle informationer første gang.

Store centrale database-installationer og andre centrale applikationer

Der findes store centrale databaser, som store dele af de offentlige forvaltninger ofte trækker på, eller som i perioder er meget vigtige. Som eksempel kan nævnes det Central Person Register (CPR), databaser hos ToldSkat og data hos Danmarks Statistik.

Vurdering af sårbarheder

Sårbarheder opstår, når kritiske aktiver er truet.

Følgende er en ikke udtømmende liste over trusler. Truslerne kommer fra tre kilder: De tilsigtede, de utilsigtede og tilfældigheder

[13] http://www.oio.dk/arkitektur/hvidbog

Tabel: 3.2. - trusler

Tilsigtede	**Utilsigtede**	**Tilfældige**
Hacking	Konfigurationsfejl	Oversvømmelse
DoS	Betjeningsfejl	Brand
Virus	Uhensigtsmæssig brug	Forsyningssvigt
Tyveri		
Spionage		

For at komme til bunds med en sårbarhedsudredning, skal eventuelle andre kritiske aktiver identificeres og hver for sig holdes op mod det samlede trusselsbillede i en risikovurdering.

Da sårbarhedsanalyse i et nationalt perspektiv er et nyt felt, og de samlede erfaringer så sparsomme, har det ikke været muligt indenfor den afsatte tid, på korrekt vis at identificere de reelle sårbarheder. Som det vil fremgå af afsnit 8.4, anbefales det, at der foretages en egentlig sårbarhedsvurdering af it-feltet, som beskrevet i afsnit 3.4.1 ovenfor.

3.5. Indbyrdes afhængigheder mellem områdets sektorer

I det følgende beskrives afhængigheder mellem områdets sektorer og sårbarheder i relation hertil. Det skal bemærkes, at der for så vidt angår de andre sektorers afhængighed af it-området, er tale om afhængigheder til den infrastruktur, som er defineret i afsnit 3.4, og altså ikke afhængigheder af it-anvendelse som sådan.

Elområdet

Elsektoren er i forskellig grad sårbar overfor problemer i de øvrige sektorer. Forsyningsafbrydelser for *naturgas* vil kunne indebære betydelige problemer for elsystemet af to årsager:

- *Elproduktionen er delvis afhængig af naturgas*. Ca. 25 % af den samlede danske elproduktion foretages således nu på grundlag af naturgas.

- *Elforbruget er delvis afhængigt af naturgas*. Hvis naturgasforsyningen ophører, forventes husholdningernes forbrug især erstattet med el, som for langt de fleste husholdninger er den energiform, som på kort sigt kan erstatte naturgasforbruget. For decentrale kraftvarmeværker og for afbrydelige erhvervskunder kan der være planlagt anvendelse af olie som alternativ til naturgas.

Bortfald af anden brændstofforsyning til produktionsanlæggene vil være mindre kritisk bortset fra kul, som anvendes i betydeligt, men dog aftagende omfang. For kul er risikoen for bortfald til gengæld beskeden, dels på grund af forholdene på det internationale kulmarked, dels som følge af de betydelige kullagre, som er etableret af de centrale elproduktionsvirksomheder.

En væsentlig sårbarhed for store dele af elsystemet skyldes desuden dets afhængighed af *tele*kommunikation, dels kommunikationen internt inden for virksomhederne og mellem virksomhederne indbyrdes, dels mellem virksomhederne og myndighederne samt andre eksterne parter.

Mest kritisk er dog systemdriften - dvs. driften af det overordnede elsystem, som er en forudsætning for, at alle andre dele af systemet kan fungere - hvor de væsentligste telekommunikationer omfatter:

a. Kommunikationen mellem de systemansvarlige virksomheders kontrolrum og andre kritiske kontrolrum, især produktionsvirksomhedernes kontrolrum, og derfra ud til værkerne, de regionale netkontrolrum samt kontrolrummene hos de systemansvarlige virksomheder i nabolandene

samt kommunikation i en krisesituation fra kontrolrummene til eksterne parter, herunder myndighederne; og

b. Fjernkontrolsystemer og online tilstandsinformation for transmissionsnettet, som er afgørende nødvendig både i normaldrift og ved en driftsforstyrrelse.

I Vestdanmark er transmissionsnettet stort set uafhængigt af de offentlige telenet, mens der i Østdanmark er en vis afhængighed heraf.

Vedrørende *it-afhængigheder* er der med indførelse af elmarkedet opstået et stort behov for dataudvekslinger mellem elsystemets markedsaktører og de systemansvarlige, hvorved der er blevet afhængighed af velfungerende internettjenester som e-mail og web-services. Markedsaktørerne skal eksempelvis sende næste døgns handels- og driftsplaner (nomineringer og renomineringer) til den systemansvarlige, som tilrettelægger systemdriften med hensyntagen hertil. Ved svigt af internettet findes der nødprocedurer for dataudveksling, men det vil under alle omstændigheder indebære betydelig gene for markedet og driftsplanlægningen, hvis internettet ikke fungerer. Systemdriften vil dog kunne gennemføres, også selvom internettet ikke fungerer.

Naturgasområdet

Naturgassektoren er i forskellig grad sårbar overfor problemer i de øvrige sektorer:

Forsyningsafbrydelser for *el* vil kunne indebære betydelige problemer for dele af naturgassystemet:

- *Gasforbrugerne vil ikke kunne bruge gassen*, da næsten alle gasforbrugende anlæg og apparater er afhængig af el.
- *Naturgasselskabernes kontrolcentre og M/R-stationer er afhængig af el*, men har i nogen grad no-break anlæg og nødstrømsanlæg, som for en periode vil kunne opretholde elforsyningen.

Afbrydelse af *tele*kommunikationen kan indebære store problemer for naturgassystemet, da kontrolcentrene vil kunne miste deres overvågning og styring af de ubemandede anlæg m.m. I så fald kan anlæg m.m. overvåges manuelt, men det kan under alle omstændigheder blive vanskeligt at opretholde naturgasforsyningen, hvis intern og ekstern kommunikation ophører.

Vedrørende *it-afhængigheder* er der med indførelse af gasmarkedet opstået et stort behov for dataudvekslinger mellem gassystemets markedsaktører og de systemansvarlige, hvorved der er blevet afhængighed af velfungerende internettjenester som e-mail og web-services. Markedsaktørerne skal eksempelvis sende næste døgns handels- og driftsplaner (nomineringer og renomineringer) til den systemansvarlige, som tilrettelægger systemdriften med hensyntagen hertil. Ved svigt af internettet findes der nødprocedurer for dataudveksling, men det vil under alle omstændigheder indebære betydelig gene for markedet og driftsplanlægningen, hvis internettet ikke fungerer. Systemdriften vil dog kunne gennemføres, også selvom internettet ikke fungerer.

Teleområdet

Telesektoren er grundlæggende afhængig af *elforsyning*, og dermed indirekte til en vis grad også af naturgasforsyning. Som det er beskrevet i afsnit 5.5, har teleudbyderne - herunder Broadcast Service Danmark - i et vist omfang sikret teleforsyningen mod strømsvigt ved nødstrømsanlæg, batteri backup og mobile nødstrømsgeneratorer. Sårbarhederne relateret til telesektorens afhængighed af el er dog meget svær at opgøre. Konsekvenserne af strømsvigt vil afhænge af, dels hvor stort et geografisk område, der er ramt af strømsvigtet, og dels af varigheden heraf. Konsekvenserne vil desuden afhænge af hvilket geografiske område, der rammes af strømsvigt, i forhold til teleudbydernes centrale placering af teleudstyr og sikringen heraf.

Landsdækkende strømsvigt eller strømsvigt, der rammer større dele af landet, vil generelt medføre betydelige nedbrud i teleforsyningen. Her er der tale om en meget høj sårbarhed. Om det er en kritisk sårbarhed, vil dog afhænge af varigheden af strømsvigtet og den konkrete beredskabssituation.

Der er tale om en kritisk sårbarhed i forhold til længerevarende strømsvigt, særligt hvis større dele af landet er ramt. Teleudbyderne har typisk sikret sig mod strømsvigt af en varighed på op til 4-6 timer. Inden for dette tidsrum er der tale om en minimal sårbarhed. Med mindre der er tale om et landsdækkende strømsvigt, vil et kortvarigt strømsvigt typisk kun medføre afbrydelser i teleforsyningen i et begrænset geografisk område. Men allerede ved strømsvigt på anslået over 4-6 timer, er der altså tale om en kritisk sårbarhed hos mange teleudbydere.

Ved meget langvarige strømsvigt, vil teleudbyderne være afhængige af opfyldning af tankanlæg til nødstrømsanlæg med diesel. Er en opfyldning mulig, vil teleforsyningen kunne opretholdes i visse geografiske områder - afhængigt af hvilke områder af landet, der er ramt af strømsvigt.

Generelt er mobilnettene mest sårbare, idet langt fra alle basisstationer i GSM-nettet er sikret med batteri backup. Der, hvor der er en sikring, er batteri kapaciteten typisk på 4-6 timer, det vil sige er strømsvigtet længerevarende kræver det, at teleudbyderne er i besiddelse af mobile nødstrømsgeneratorer til genopladning af batterierne. Dette er kun i mindre omfang tilfældet. Brug af mobiltelefoner kræver også el til genopladning af mobiltelefonens batteri, så længerevarende strømsvigt vil også ramme abonnenternes eget udstyr. Det samme gælder f.eks. brug af ISDN- og trådløse telefoner. Herved øges den samlede sårbarhed på området.

For så vidt angår *taletelefonitjenesterne* har de adspurgte teleudbydere oplyst, at de ikke er afhængige af *it-infrastrukturen*, som den er defineret i afsnit 3.4 ovenfor. Forhold vedrørende teleudbydernes interne it-systemer, der understøtter driften, er behandlet i afsnittet om netsikkerhed i afsnit 3.3.2 ovenfor.

It-området

It-området som forsyningsområde, som det er defineret i afsnit 3.4, er grundlæggende afhængig af *tele- og elforsyning*. Der er i forbindelse med dette udredningsarbejde ikke foretaget en nærmere analyse af sårbarheder, der kan relateres til - den ret åbenlyse - afhængighed af elforsyningen.

For så vidt angår afhængigheden af teleforsyning følger denne afhængighed allerede af afgrænsningen af infrastrukturen på it-området. Den del af samfundets it-anvendelse, der er baseret på it-infrastrukturen, som den er defineret i afsnit 3.4, er grundlæggende baseret på blandt andet teletjenester hos teleudbyderne og dermed teleinfrastrukturen. Teleinfrastrukturen leverer de fysiske lag i it-infrastrukturen, dvs. kabler m.v. De teleudbydere, der har egen infrastruktur - f.eks. TDC - også kaldet netoperatører, kan samtidig være ISP'ere (Internet Service Providere). Disse udbydere vil høre til såvel tele som it-området.

4. Sårbarheder vedr. it- og informationssikkerhed

Afsnit 3.4 indeholdt en definition af it-området samt en overordnet kortlægning af it-infrastrukturen som forsyningsområde ved identifikation af en række aktiver og trusler.

I dette afsnit behandles aspekter af it-sårbarheder ud fra velkendte trusler på it-området.

Emnerne beskrevet i afsnit 4 viser, at truslerne på it-området har en anden karakter end f.eks. den traditionelle måde at tænke teleberedskab på i Danmark i og med, at truslerne er globalt genkendelige, men rammer lokalt, og må derfor traditionelt siges at henhøre under den enkelte sektors ansvar. Historien har dog vist, at dette syn på it-beredskab (at det er et lokalt ansvar) ikke nødvendigvis giver en fornøden robusthed i interne kritiske it-systemer, og at der kan være et behov for øget koordinering og faglig udveksling af it-sikkerhedserfaringer på tværs af sektorerne. Primært fordi selve driften af it-systemerne ikke er kerneområdet for sektorerne, og der kan derfor ikke garanteres nødvendig og ensartet prioritering af beredskabsforanstaltninger.

Afsnittet handler om it-sikkerhed fremfor it-beredskab. Dette skyldes, at et en fornuftig afbalanceret it-sikkerhed er nødvendigt, for at give kritiske it-systemer den tilstrækkelige robusthed, så de kan modstå det pres, der måtte opstå under beredskabssituationer. Problemstillingerne listet i dette kapitel er valgt ud fra det alment genkendelige og umiddelbart vigtige, men beskriver kun en brøkdel af de forhold som den it-sikkerhedsbevidste organisation skal forholde sig til i dagligdagen og i planlægningen og styringen.

4.1. Beskrivelse af området

It-sikkerhedsområdet defineres ved tilgængelighed, integritet og fortrolighed, hvor tilgængelighed er behandlet i afsnit 3.4 i et infrastrukturperspektiv. Da fortrolighed og integritet primært er et fokus på data, bl.a. opbevaring og omgang med data, falder håndtering af sårbarheder ind under det mere veletablerede it-sikkerhedsområdes måde at håndtere trusler mod fortrolighed og integritet.

Begreberne tilgængelighed, integritet og fortrolighed defineres typisk som:

- *Tilgængelighed*, der skal sikre, at data og systemer er tilgængelige, når autoriserede brugere ønsker det.
- *Integritet*, der skal sikre, at dataene er korrekte og fuldstændige, og at programmer fungerer korrekt.
- *Fortrolighed*, der skal sikre, at data beskyttes mod uautoriseret anvendelse.

4.2. Vurdering af sårbarheder

Truslerne mod integritet og fortrolighed kan komme fra en række af kilder. Følgende er en gennemgang af en række trusler.

Medarbejdere som trussel

Hacking og virus er utvivlsomt nogle af de it-sikkerhedsemner, som oftest eksponeres i pressen. Denne eksponering er dog overdrevet, idet alle vurderinger peger i retning af, at det kun er 20% af virksomhedens hændelser, der er knyttet til angreb, som startes udenfor virksomheden. I modsætning hertil vurderes det, at 80% af truslerne stammer fra medarbejderes handlinger eller mangel på samme. Der er derfor i høj grad brug for at fokusere indsatsen mod medarbejdere og ikke kun mod tekniske foranstaltninger, som skal imødegå angreb udefra.

Medarbejdere kan handle uovervejet, i uvidenhed eller have deciderede ondsindede hensigter. Det er derfor vigtigt at beskytte organisationens it-installationer mod medarbejderne. En sådan beskyttelse kan udarbejdes i samarbejde med medarbejderne, så der er en klar forståelse af, hvad beskyttelsen går ud på og, hvorfor beskyttelsen er nødvendig.

Medarbejdere udgør en trussel på flere måder. For det første er det vigtigt, at medarbejdere har viden om hvilke handlinger, det er hensigtsmæssigt at undlade, hvis man skal bidrage til at forbedre organisationens it-sikkerhed - herun-

der skal medarbejderne også vide, hvilke handlinger, der eksplicit er forbudte. Der skal f.eks. specificeres regler for, hvordan internet og e-mail må anvendes på arbejdspladsen. Det skal også specificeres, hvordan brugerne identificerer sig unikt overfor organisationen - herunder regler for at passwords er personlige tillige med regler om, hvordan passwords udformes. Medarbejderne skal også oplyses om nogle af de mere bløde emner, som f.eks. at personer udenfor organisationen vil forsøge at lokke deres brugernavn og password fra dem gennem social engineering. Endelig skal medarbejderne også oplyses om, hvordan de afrapporterer fejl på systemerne.

Tidspunktet for ansættelsens forløb har betydning for de trusler organisationen står overfor. I starten af en persons ansættelse begås fejl ofte grundet uvidenhed, fordi de endnu ikke er ordentligt oplært i anvendelse af organisationens it-systemer. I midten af ansættelsens forløb begås de fleste fejl som følge af, at medarbejderne udfører opgaver, de har udført mange gange før, og derfor ikke har skærpet opmærksomhed rettet mod arbejdsopgaverne. I slutningen af et ansættelsesforhold er den største trussel mod organisationernes aktiver, at medarbejderen, på grund af problemer der er opstået i forbindelse med ansættelsens ophør eller af historiske årsager, vil hævne sig på organisationen og derfor kopierer eller destruerer elektroniske aktiver.

Det er imidlertid ikke kun organisationens egne medarbejdere opmærksomheden skal rettes imod. De medarbejdere, som ikke er ansat af organisationen, men som alligevel har sin regelmæssige gang i organisationen, udgør også en potentiel sikkerhedstrussel. Der kan f.eks. være tale om elektrikere, teknikere og rengøringspersonale. Denne gruppe kan være underlagt de samme sikkerhedskrav som organisationens egne medarbejdere. I særdeleshed kan der holdes øje med deres virke i organisationen, og de kan instrueres i hvilke konsekvenser deres aktiviteter kan have for organisationen. Der kan f.eks. være tale om begrænsninger i den fysiske adgang til el- og it-installationer. Tilsvarende gælder også for ansatte hos organisationens samarbejds- eller forretningspartnere. Her skal den adgang, som eksterne partnere har til organisationen, holdes under kontrol, og der skal holdes øje med, hvilke aktiviteter disse partnere foretager sig på organisationens it-systemer. En skade forvoldt af en ekstern

partner med adgang til f.eks. ordresystemet kan have lige store konsekvenser som en skade forvoldt af en af organisationens egne ansatte. Situationen kompliceres naturligvis af, at det for den enkelte organisation kan være meget vanskeligt at vurdere samarbejdspartnerens medarbejdere.

It-afdelingens ansatte skal have speciel fokus. Afdelingens behov for at kunne løse tekniske problemer betyder som regel, at de skal have noget nær ubegrænset adgang til alle organisationens it-systemer. Det betyder, at it-afdelingens ansatte (som den eneste personalegruppe) på baggrund af organisationens informationer kunne danne sig et overordnet billede af organisationens forretningsaktiviteter. Men det betyder også, at it-afdelingens ansatte er den eneste gruppe, som har mulighed for at anrette stor skade på organisationens elektroniske aktiver. Der kan derfor være behov for at have særlig opmærksomhed rettet mod denne gruppe ansatte. En mulighed er, at tavshedserklæringer som for mange af organisationens øvrige ansatte også kan bringes i anvendelse overfor it-personalet. Endelig kan der blandt de ansatte i afdelingen være en høj grad af funktionsadskillelse.

Bevidsthed om it-sikkerhed

Det er af stor betydning, at alle i organisationen har den nødvendige fokus på it-sikkerhed. Der skal være en konstant awarenes på it-sikkerhed således, at man kan tale om, at organisationen har en egentlig it-sikkerhedskultur. Denne awareness skal findes hos henholdsvis ledere og personalet.

Ledelsens awareness

Ledelsen har det øverste ansvar for it-sikkerheden. Det er således ledelsens ansvar at sikre, at organisationens ansatte har den rette awareness, at området it-sikkerhed har fået allokeret de rette ressourcer, at de rette politikker er blevet udarbejdet, at de rette tekniske sikkerhedsforanstaltninger er blevet installeret, at organisationens sikkerhedsbehov løbende vurderes og at nye nødvendige initiativer iværksættes.

Argumenter for at ledelsen bør interessere sig for it-sikkerhed:

- at minimere de økonomiske tab, som kan opstå hvis en it-sikkerhedshændelse indtræffer
- at sikre, at organisationen har et it-beredskab, som kan tages i anvendelse i tilfælde af nødsituationer og dermed sikre forretningens overlevelse
- at kunne udvikle forretningen under anvendelse af de nye forretningsmodeller, som er baseret på teknologisk innovation, som f.eks. understøttelse af webenablede e-business systemer, hjemmearbejdspladser og mobile arbejdspladser

En måde at sikre at organisationens ledelse kan leve op til sit ansvar kan være at gå frem i følgende faser:

Ledelsen kan først opstille en egentlig målsætning for it-sikkerheden. Denne skal bl.a. specificere, hvad formålet med it-sikkerheden er samt, hvordan denne skal implementeres i overensstemmelse med organisationens værdier og forretningsgrundlag. Organisationen kan herefter foretage en sikkerhedsanalyse, hvor organisationens elektroniske aktiver identificeres, hvor man vurderer hvilke sikkerhedsforanstaltninger man er i besiddelse, og hvilke ekstra sikkerhedsforanstaltninger man kan anskaffe sig. Det næste skridt er at fastlægge en it-sikkerhedspolitik, som dels beskriver hvem der har ansvaret for hvad, og hvilken politik der gælder for medarbejdernes anvendelse af it-systemerne. De initiativer, man på denne baggrund har besluttet sig at tage på it-sikkerhedsområdet, skal efterfølgende designes således, at de er i overensstemmelse med strategi, behov, politik og værdier. Desuden skal de testes og implementeres. Endelig er det af afgørende betydning at forstå, at it-sikkerhed ikke er noget man indfører en gang for alle. Den teknologiske udvikling gør, at der hele tiden findes nye sårbarheder, og derfor skal eksisterende installationer løbende opdateres og testes for disse nye sårbarheder.

Personalets awareness

De fleste fejl i organisationen sker, fordi de ansatte dobbeltklikker på en vedhæftet fil i en mail, glemmer at skifte backupbånd, besøger hjemmesider der indeholder vira o. lign. For at imødegå sådanne handlinger er det vigtigt at forsøge at sikre, at medarbejderne hele tiden har den fornødne viden og agtpågivenhed i forhold til anvendelse af organisationens it-systemer.

Der skal skrives en it-sikkerhedspolitik, og hver enkelt medarbejder skal instrueres i, hvad politikken går ud på og bibringes en forståelse af, hvorfor politikken ser ud, som den gør. Det betyder i praksis, at medarbejdere løbende skal efteruddannes i it-sikkerhed, således at de er opmærksomme på, hvad de skal passe på i forhold til netop de systemer, som de arbejder med. Dette kan ske i form af kurser. Det betyder også, at medarbejderne engang imellem kan blive præsenteret for elementer af politikken. På denne måde fastholdes den daglige awareness og på sigt vil en egentlig it-sikkerhedskultur opstå.

Softwaresikkerhed

Når it-programmer indeholder fejl, kan angribere udnytte fejlene til at få adgang til systemerne. Denne form for fejl betegnes ofte som "sårbarheder" eller "sikkerhedshuller". De senere år har vist en eksplosiv stigning i antallet af sikkerhedshuller. I år 2000 fandt sikkerhedsforskere på verdensplan 1.090 sårbarheder. Året efter var tallet 2.437. Det steg i 2002 til 4.129, oplyser det amerikanske CERT Coordination Center (Computer Emergency Response Team).

Ofte udsender softwareproducenterne rettelser til deres programmer, så snart de opdager et sikkerhedshul. Men mange administratorer af it-systemer undlader at installere disse rettelser. Den 25. januar 2003 blev internettet ramt af den såkaldte Slammer-orm, som inficerede mindst 75.000 computere på verdensplan. Den udnyttede et sikkerhedshul i et program fra Microsoft. Men allerede i juli 2002 udsendte Microsoft en advarsel om sikkerhedshullet sammen med en rettelse til det. Et halvt år efter var der altså mindst 75.000 computere, som ikke havde fået installeret denne rettelse, der kunne hentes gratis fra Microsofts web-sted.

Også de it-systemer, som organisationer selv udvikler, kan indeholde sårbarheder. For eksempel kan web-sider, der tilbyder offentlig adgang til en organisations interne systemer, misbruges, hvis de har sikkerhedshuller. Det skyldes ofte mangelfuld kontrol af de data, som brugerne kan indtaste i web-baserede formularer.

Sårbarheder findes både i serverprogrammer, der administreres af professionelle it-folk, og i de programmer, som private anvender. Sikkerhedsbranchen anbefaler tre metoder til at beskytte sig:

- Hold programmerne opdateret med de seneste rettelser
- Installer et antivirusprogram og hold det opdateret
- Installer en firewall, der blokerer for visse angrebstyper fra internettet

CERT Coordination Center anslår, at over 95 procent af alle vellykkede angreb fra hackere og orme udnytter velkendte sårbarheder, hvortil der findes rettelser. Når rettelserne ofte ikke installeres, skyldes det sandsynligvis tidsmangel eller manglende viden hos systemadministratorerne. Det kan også skyldes frygt for, at en programrettelse vil få et ellers velfungerende system til at fejle.

Industrispionage

Den hårde konkurrence i mange brancher medfører et øget behov for at tilegne sig konkurrenternes fortrolige informationer. Informationer der i stigende omfang indhentes gennem brug af industrispionage. Inden for de sidste 10-12 år er der således konstateret en væsentlig stigning i tilfælde af industrispionage. Dette fremgår bl.a. af en amerikansk undersøgelse, der viste en stigning på 323 % i økonomisk spionage blandt amerikanske organisationer fra 1992 til 1996. Af de deltagende organisationer angav 40 %, at de inden for en 2-års periode havde været udsat for spionage i større eller mindre omfang. En undersøgelse fra 2002 viste samtidig, at amerikanske organisationer i perioden fra 1. juli 2000 til 30. juni 2001 havde haft et tab på ca. 60 milliarder USD som følge af industrispionage. Endelig viste undersøgelsen, at alle organisationer er po-

tentielle ofre for industrispionage uanset størrelse, forretningsaktiviteter, og produktsortiment.

Hacking

Hackere er personer, der tiltvinger sig adgang til andres it-systemer. I langt de fleste tilfælde udnytter de sårbarheder (sikkerhedshuller) i systemerne.

Nogle tilfælde af hacking opdages med det samme. Det gælder web-graffiti (defacements), hvor hackerne erstatter indholdet på web-steder med deres egne budskaber. Her er formålet med hackingen at få omtale og vinde respekt fra andre hackere. Andre hackerangreb opdages først sent. DK-CERT oplyser, at man har set mange eksempler på, at hackere overtager computere for at udnytte dem til distribution af piratkopier. Når hackeren har overtaget kontrollen med computeren, kan han og andre hackere bruge den til at udveksle piratkopier af musik, film, spil og programmer. Da hackerne skjuler deres aktivitet bedst muligt, opdages angrebet ofte først længe efter, det er begyndt.

Nogle hackere anvender en særlig afart af orme (se nedenfor), der opbygger såkaldte "botnet". Det er netværk af computere, som ormen har inficeret. Alle de inficerede computere kan nu fjernstyres af hackeren, der kan bruge dem til at indlede et bombardement med datapakker mod en computer. På den måde sættes den angrebne computer ud af drift.

Afsendere af spam (uønskede reklamer via e-post) kan også benytte hackermetoder. De angriber computere, som de anvender til at udsende deres spam med. Derved kan de sløre deres spor, så de bliver sværere at forfølge.

Der er yderst sjældent eksempler på sager, hvor hackerne er interesserede i indholdet af de data, der ligger på de computere, de angriber. Derimod er de interesserede i at lære at udnytte de hackede systemer mest muligt til deres egne formål. Det er vanskeligt at anslå antallet af hackersager, da de sjældent anmeldes til politiet eller omtales offentligt. Da det ifølge Danmarks Statistik kun er halvdelen af danskerne, der bruger en firewall, er mange sårbare over for angreb. Det er sandsynligt, at mange ikke opdager, de er blevet ofre.

Varsling

Varslingssystemer giver besked, når ny, målrettet og specifik information om it-sikkerhed bliver tilgængelig. It-sikkerhedsbranchen tilbyder typisk varsling om tre slags begivenheder: Virus, sårbarheder og angreb.

Spørgsmålet om virusvarsling deler it-sikkerhedsbranchen i to lejre: Den ene mener, at det er nyttigt for organisationer og organisationer at få besked, hver gang der opdages en ny virus eller orm. Den anden lejr mener, at den bedste beskyttelse mod virusangreb er et opdateret antivirusprogram. Holder man sit program opdateret, behøver man til gengæld ikke få information om hver eneste ny trussel - den information har antivirusfirmaerne brug for, men ikke deres kunder.

Flere aktører på danske it-marked tilbyder varslingstjenester om sårbarheder. Typisk kan kunderne angive, hvilke systemer de ønsker overvåget, hvorefter de modtager besked, når der udkommer nye rettelser eller opdages nye sårbarheder i disse systemer. Kunderne kan anvende informationen til at sikre, at deres systemer er opdaterede.

Varsling om angreb går ud på at varsle, når et angreb finder sted. I stedet for at fortælle om alle nye vira og orme, fortæller man kun om de angreb, der rammer bredt. Endvidere kan man varsle om nye typer af hackerangreb, der opdages på netværkene. De organisationer, der kan tilbyde varsling om angreb, har som regel selv ansvaret for at drive et eller flere netværk. Erfaringerne fra driften af disse net giver den nødvendige viden.

På europæisk plan er fem stats-CERT'er ved at udarbejde standarder for, hvordan de kan udveksle informationer om aktuelle angrebstendenser. Fra Danmark deltager UNI-C via DK-CERT i projektet, der er støttet af EU.

Virusangreb og orme

Traditionelle virus spreder sig ved at inficere filer. De var især udbredte, da man primært udvekslede programmer via disketter. De findes stadig, men er nok stagnerende.

De senere år har der været mere aktivitet, når det gælder orme. De spreder sig ved at kopiere sig over netværk. De mest udbredte orme anvender e-post til at sprede sig med: En bruger modtager en e-mail med en vedhæftet fil. Når vedkommende dobbeltklikker på filen, inficeres pc'en, og den begynder at sende lignende mails ud til alle de adresser, der findes i computerens adressekartotek. Ofte forfalsker ormen afsenderadressen, så den er svær at spore.

De mest udbredte orme anvender flere metoder til at sprede sig: Foruden e-post udnytter de også kendte sikkerhedshuller i Windows og i web-serverprogrammer til at sprede sig med. Senest er de også begyndt at anvende chatprogrammer og fildelingsprogrammer. Det gælder således Fizzer-ormen, der har spredt sig siden starten af maj 2003. Den udnytter chat-programmer til at opbygge et "botnet" , som ormens bagmand kan fjernstyre.

Man kan beskytte sig mod angreb fra virus og orme ved at installere et antivirusprogram og holde det opdateret. Endvidere kan man anvende en firewall.

Nogle organisationer tilbyder scanning af al e-post til en virksomhed. Deres statistikker giver et billede af, hvor udbredte ormene er. Firmaet Comendo, der foretager virusscanning for over 800 danske organisationer, finder gennemsnitligt orme eller virus i 1,5 procent af de e-mails, det scanner. Hvis det tal er repræsentativt, vil der altså være virus eller orme i flere end en ud af 100 e-mails, en dansker modtager. Om pc'en så bliver smittet afhænger af, hvordan den er beskyttet. Hver fjerde dansker anvender ikke et antivirusprogram, fremgår det af opgørelser fra Danmarks Statistik.

5. Beredskabet

Det fremgår af beredskabsloven, at opgaven for den civile sektors beredskab er at planlægge og træffe foranstaltninger med henblik på i tilfælde af ulykker og katastrofer, herunder krigshandlinger, at videreføre samfundets funktioner samt yde støtte til forsvaret. Beredskabet på områderne el, naturgas, tele og it er en del af den civile sektors beredskab, og det er de enkelte ministres ansvar inden for hver sektor at planlægge og træffe foranstaltninger til udførelse af de beredskabsmæssige opgaver.

I det følgende beskrives beredskab for el, naturgas, tele og it. Der redegøres i den forbindelse for den gældende lovgivning på området samt for, hvordan området er organiseret. For så vidt angår organiseringen af området, redegøres der for myndighedsstruktur og regelbestemt organisering, men også for den organisering, der måtte følge af samarbejdsaftaler m.v. Der redegøres endelig for beredskabsforanstaltninger på området.

5.1. Beredskab på elområdet

Regelgrundlag

Beredskabsarbejdet inden for elsektoren er baseret på dels beredskabsloven, dels den sektorlovgivning, som er fastlagt gennem lov om elforsyning (jf. lovbekendtgørelse nr. 151 af 10. marts 2003), primært § 85 b.

For el forudsætter følgende former for virksomhed, at økonomi- og erhvervsministeren har meddelt bevilling hertil efter elforsyningsloven:

a. *Elproduktion*, dog kun for anlæg med en kapacitet på over 25 MW, dvs. bevilling er således ikke nødvendig for hovedparten af de decentrale elproduktionsanlæg (vindmøller, mindre kraftvarmeanlæg m.m.)

b. *Transmissions- og netvirksomhed*, dvs. dels transmission over store afstande, herunder import og eksport gennem udlandsforbindelserne (til Sverige, Norge og Tyskland), dels distribution til forbrugerne

c. *Systemansvarlig virksomhed*, hvis primære opgave er at sikre forsyningssikkerheden for el, herunder at opretholde elnettets tekniske kvalitet og balance samt at sikre, at der er tilstrækkelig produktionskapacitet

For disse former for virksomhed, som er baseret på centrale dele af elsektorens infrastruktur, fastsætter elforsyningslovens § 85 b, stk. 1, at *de enkelte virksomheder* skal have det nødvendige beredskab. Dette beredskab skal omfatte dels forudgående planlægning, dels operative foranstaltninger i en krisesituation. Disse krisesituationer svarer til den ændrede beredskabslov pr. 1. juli 2003. Beredskabets nærmere indhold forudsættes fastlagt gennem bekendtgørelser og andre regler.

Sikring af, at de enkelte virksomheders beredskab er indbyrdes afstemt og koordineret, varetages af de to systemansvarlige virksomheder (Eltra og Elkraft System for henholdsvis Vest- og Østdanmark) efter lovens § 85 b, stk. 2. Også her gælder, at det nærmere indhold af denne overordnede og koordinerende opgave forudsættes fastlagt gennem bekendtgørelser og andre regler.

Derudover indeholder bestemmelsen en hjemmel til, at økonomi- og erhvervsministeren kan fastsætte nærmere regler om beredskabsopgaverne. Denne hjemmel er indtil nu alene anvendt til fastsættelse af regler om lagerberedskab for brændstoffer inden for elsektoren, herunder om

a. udarbejdelse af planer for, hvorledes elforsyningen kan videreføres i tilfælde af manglende brændstofforsyning til landet som følge af krisesituationer

b. løbende overvågning af omfanget af brændstoflagre inden for den samlede elsektor og vurdering af, om disse lagre i den under punkt a nævnte situation vil kunne danne grundlag for at videreføre elforsyningen i en periode på 3 måneder samt underretning af Energistyrelsen herom

c. beføjelse for økonomi- og erhvervsministeren til i den under punkt b nævnte situation om nødvendigt at pålægge de systemansvarlige virksomheder at etablere særskilte brændstoflagre for en nærmere fastsat periode

Sådanne regler om beredskab påregnes udarbejdet af Energistyrelsen i samarbejde med de systemansvarlige virksomheder samt andre berørte parter.

Organisatoriske forhold

Organisationen af beredskabsarbejdet er således baseret på, at arbejdet primært udføres af sektoren selv inden for rammer, som fastsættes af myndighederne i et samarbejde med sektoren:

a. *De enkelte virksomheder* varetager beredskabet for deres egen aktivitet

b. *De systemansvarlige virksomheder* varetager de overordnede og koordinerende opgaver inden for sektoren

c. *Myndighederne* (dvs. Energistyrelsen på vegne af økonomi- og erhvervsministeren) varetager relationerne til denne og andre energisektorer, til de centrale myndigheder på beredskabsområdet og til internationale organisationer samt udarbejder udkast til bekendtgørelser og andre regler

Med henblik på drøftelser af beredskabsforhold inden for elsektoren er der etableret et *Danske Elselskabers Beredskabsudvalg*, hvori de forskellige former for virksomhed er repræsenteret og hvori Energistyrelsen deltager. Formandskab og sekretæropgaver varetages af de systemansvarlige virksomheder. Udvalget afholder normalt 2-3 årlige møder.

Den nævnte opgavevaretagelse inden for elsektoren er baseret på det sektoransvar, som er grundlag for beredskabsarbejdet. Denne struktur bør være koordineret med det regionale samarbejde om beredskab, som foretages gennem arbejdet i de nye regionale stabe.

I de nye regionale stabe - hvis opgaver skal fastlægges efter civilregionernes nedlæggelse pr. 1. juli 2003 - forventes der at indgå repræsentanter for de relevante civile myndigheder, herunder Energistyrelsen, således at disse repræsentanter udpeges af Energistyrelsen. Disse repræsentanter vil dermed have en funktion som en form for forbindelsesofficerer i forhold til den udpegende myndighed og forudsættes derfor at have en løbende kommunikation med

denne med henblik på at sikre, at drøftelserne i de regionale stabe af energiforhold foretages i overensstemmelse med sektoransvaret.

Beredskabsforanstaltninger

Forholdet til forsyningssikkerhed

Som nævnt i afsnit 1.3 er der traditionelt lagt afgørende vægt på, at der for elsektoren skal være en stor grad af *forsyningssikkerhed* og sektoren har derfor set under ét et betydeligt driftsberedskab, som ikke alene er rettet mod at kunne håndtere de almindeligt forekommende driftsforstyrrelser som følge af uheld m.m., men også er rettet mod mere alvorlige hændelser som følge af vejrforhold m.m. Den civile sektors beredskab ses derfor som en overbygning på og et supplement til det generelle driftsberedskab, rettet mod de meget alvorlige og kritiske hændelser, som nu indgår i beredskabsbegrebet. Som følge af det generelt høje niveau i driftsberedskabet er der ret få enkeltforanstaltninger i elsektorens øvrige beredskab. Dertil kommer, at det historisk set hidtil har været muligt hurtigt at opskalere driftsberedskabet til et tilfredsstillende beredskab i katastrofelignende situationer. Orkanen i 1999 blev eksempelvis håndteret med stor entusiasme og villighed fra personalets side og der blev ydet en stor ekstraordinær indsats. Blandt elselskaberne har der endvidere altid været tradition for omfattende gensidig hjælp i ekstraordinære situationer.

Elsektoren har i en årrække haft en *Beredskabshåndbog* med retningslinier for virksomhedernes arbejde med beredskabsforhold, herunder deres udarbejdelse af beredskabsplaner. Denne beredskabshåndbog er p.t. under revision, bl.a. under hensyntagen til det ændrede beredskabsbegreb.

Gennemgangen nedenfor af beredskabsforhold inden for elsektoren er derfor ret summarisk og er baseret på følgende opdeling af beredskabet:

a. *Forebyggende beredskab* (security) på virksomhedsniveau, dvs. indhegning, alarmering, adgangskontrol, begrænset antal adgangsveje osv. for de kritiske dele af virksomheden

a. *Konsekvensreducerende beredskab* på virksomhedsniveau, dvs. bekæmpelse af person- og materielskader i form af evakueringsplaner, brandbekæmpelsesplaner osv.

a. *Reetableringsberedskab* på virksomhedsniveau, dvs. hurtig udbedring af skader, især reetablering af energiforsyning

a. *Robusthed og fleksibilitet* i dimensionering af produktions-, transmissions og distributionsforhold

Forebyggende beredskab

Det forebyggende beredskab omfatter dels den overvågning og styring, som foretages fra systemets kontrolcentre, dels en række andre forhold.

De systemansvarlige virksomheder, større elproducenter samt større transmissionsselskaber har således døgnbemandede kontrolrum, hvorfra der foretages en kontinuerlig overvågning og hvorfra der hurtigt kan reageres på unormale forhold. De øvrige netvirksomheder har typisk bemandede kontrolrum indenfor normal arbejdstid og hjemmevagt overvågning resten af tiden med hurtig reaktion, hvis der indtræffer fejl. En del virksomheder har endvidere nødkontrolrum, som kan anvendes, hvis det normale kontrolrum ikke fungerer.

De systemansvarlige virksomheder holder løbende de enkelte virksomheder orienteret om beredskabsmæssige forhold af betydning for elsektoren. Efter drøftelse med Energistyrelsen skal de systemansvarlige virksomheder således kunne aktivere de enkelte virksomheders operative beredskab ved en opgradering af det generelle driftsberedskab, afstemt efter situationen.

En af de generelle driftsforanstaltninger i driftsberedskabet, som i særlig grad kan have betydning for den civile sektors beredskab, er således muligheden for, at elsystemet overgår til *Skærpet Drift*, der bl.a. indebærer, at alle planlagte og igangværende afbrydelser af elsystemet annulleres og der kun foretages absolut nødvendigt arbejde på transformerstationer o.lign. og på produktionsanlæg. Derudover indeholder den skærpede drift bl.a. særlige instrukser til at tage højde for kendte sårbarheder, der kan opstå i særlige situationer.

Det forebyggende beredskab omfatter endvidere indhegning, aflåsning og overvågning af anlæg, løbende overvågning af elsektorens brændstoflager samt instrukser og procedurer i driftsberedskabet, herunder f.eks. procedurer for håndtering af telefoniske bombetrusler.

Konsekvensreducerende beredskab

Det konsekvensreducerende beredskab (udover det forebyggende) ligger i driftsberedskabet i form af anlæg og procedurer for en række foranstaltninger som f.eks. relæbeskyttelse, indsættelse af automatiske produktionsreserver, automatisk frekvensaflastning m.m. Disse foranstaltninger vil f.eks. kunne begrænse et netsammenbrud og dermed reducere antallet af berørte forbrugere og reducere den tid, som det vil tage et komme tilbage til normal drift.

Reetableringsberedskab

Reetableringsberedskabet findes i både distributions- og transmissionsnettet i form af planer for tilkald og indsættelse af mandskab til reetablering i løbet af kort tid. Det er ikke muligt at dimensionere dette beredskab til at kunne håndtere enhver situation og der kan være situationer med så mange ødelæggelser, at der kan gå dage, før alt er reetableret, f.eks. efter en usædvanlig voldsom storm.

Både på distributions- og transmissionsniveau er der reservedelslagre til reetablering og udbedring af skader i elnettet. Nogle elselskaber har mobile transformerstationer til indsættelse ved alvorlige ødelæggelser.

Robusthed og fleksibilitet

Robusthed og fleksibilitet er som tidligere beskrevet nøglebegreber for elsektorens dimensionering og udbygning af elsystemet. Normalt designes elsystemet således med sigte på at opnå stor robusthed og fleksibilitet inden for de givne energipolitiske og økonomiske rammer. Det bedste eksempel herpå er n minus 1-princippet, jf. afsnit 3.2.2, som er grundlag for planlægningen af anlægs- og driftssituationer.

Det har dog ikke været muligt at gennemføre n minus 1-princippet helt uden afvigelser, bl.a. er transmissionslinier og transformeranlæg i mange tilfælde ikke i væsentlig grad adskilt fra de reservesystemer, som skal fungere i tilfælde af udfald af de pågældende linier og anlæg. Ved planlægning af nye anlæg og net, herunder ikke mindst nye udlandsforbindelser, bør det derfor sikres, at n minus 1-princippet gennemføres på en måde, så der er reel uafhængighed mellem reservesystemerne og de systemer, som de skal erstatte, dvs. at der sikres en reel reservekapacitet.

Generelt må det således forventes, at beredskabshensyn i højere grad fremover bør indgå blandt de hensyn, som skal danne grundlag for design og dimensionering af elsystemet.

Afhængighed af telekommunikation

Med hensyn til afhængigheden af telekommunikation har nogle virksomheder opnået en vis robusthed dels gennem dublering af teleforbindelser, dels gennem etablering af egne telekommunikationsforbindelser, som er uafhængige af det offentlige telenet, jf. afsnit 5.5. For hovedparten af elsektorens virksomheder gælder dog, at der er en betydelig afhængighed af den offentlige telekommunikation, både fastnet og mobilnet, og at denne afhængighed er steget kraftigt gennem de senere år, bl.a. som følge af en øget brug af hjemmevagtsordninger, hvor overvågning og styring foretages fra hjemmet.

Kortlægning af elsektorens beredskab

De systemansvarlige virksomheder har i slutningen af 2002 efter anmodning af Energistyrelsen udarbejdet såkaldte temarapporter om beredskabsforhold inden for elsektoren for henholdsvis Vest- og Østdanmark. I disse temarapporter indgår bl.a. en indledende kortlægning af beredskabet hos de enkelte produktions-, transmissions- og netvirksomheder i elsektoren. Konklusionerne af denne kortlægning - udført som en spørgeskemaundersøgelse omfattende alle de nævnte virksomheder i elsektoren i Vest- og Østdanmark - kan sammenfattes således:

a. Virksomhedernes egen vurdering af deres beredskab varierer meget

b. Kun få virksomheder har foretaget en egentlig risiko- og sårbarhedsvurdering

c. Kun få virksomheder har holdt beredskabsøvelser i 2001 eller øvelser siden 1995

d. Virksomhederne fremkommer med en del forslag til effektivisering og forbedring af deres beredskab, især peges på forbedret sikring af kommunikationsforhold og afholdelse af øvelser som mulige indsatsområder

e. Nogle virksomheder har egentlige beredskabsplaner, andre ikke. I de tilfælde, hvor der foreligger beredskabsplaner, er de ikke ensartede. Nogle virksomheder opererer med et niveauopdelt beredskab, andre ikke

f. De fleste virksomheder har eget kontrolrum, resten styres fra andet kontrolrum

- Der er store forskelle mellem virksomhederne med hensyn til døgnbemanding af kontrolrum, men inden for normal arbejdstid er så godt som alle kontrolrum bemandet
- Virksomheder uden døgnbemandet kontrolrum har typisk i stedet en hjemmevagtordning med overvågning og styring
- De største virksomheder har sikret sig med nødkontrolrum, dog normalt med en reduceret funktionsdygtighed i forhold til det almindeligt anvendte kontrolrum
- Mange virksomheder har sikret elforsyning af vitale kontrolrumsfunktioner (af en varighed på mindst 10 timer)
- Kontrolrummene er i forskellig grad aflåste for net- og produktionsselskaber

g. Netanlæg er generelt sikret ved aflåsning, men derudover er der kun begrænset omfang etableret elektronisk overvågning eller alarmering i tilfælde af utilladt adgang

h. Produktionsanlæg er for de flestes vedkommende indhegnet, men indenfor normal arbejdstid er de ofte åbne uden adgangskontrol

i. Undersøgelsen giver et ufuldstændigt billede af virksomhedernes afhængighed af offentlig telekommunikation i krisesituationer, men giver dog indikationer på en stigende afhængighed af det offentlige fastnet eller mobilnet. Dette gælder både den interne og eksterne kommunikation

j. Undersøgelsen giver endvidere et ufuldstændigt billede af virksomhedernes sikring af deres vitale it-systemer

k. I en krisesituation er der normalt mulighed for at opnå mandskabsmæssig bistand gennem etablerede tilkaldeordninger eller gennem aftaler om udlån af personale fra andre virksomheder

l. I en krisesituation har virksomhederne en rimelig inddækning for almindelige reservedele, men ikke for større eller sjældnere anvendte reservedele. For de største anlægsdele findes således normalt ingen reserver. For netvirksomheder er reserverne derimod indbygget i nettet. For produktionsanlæg vil havari af turbiner, generatorer o.lign. normalt medføre lang udetid indtil reparation. Samtidig er det usikkert, om de normale leverandøraftaler vil fungere i en sådan situation.

Kortlægningen danner grundlag for det videre beredskabsarbejde inden for elsektoren.

Sikring over for afbrydelse af elforsyningen

Det er som nævnt elsystemets målsætning, at elforsyningen i tilfælde af en krisesituation opretholdes i videst muligt omfang og at den i tilfælde af afbrydelser genetableres hurtigst muligt. Elsystemet er imidlertid sårbart i en række henseender. Det kan derfor ikke udelukkes, at der i ekstraordinære situationer

vil kunne opstå elafbrydelser i mindre eller større geografisk omfang samt af kortere eller længere varighed.

Såfremt en virksomhed eller myndighed vurderer, at det for dem er af afgørende betydning at opretholde elforsyningen under almindelige eller ekstraordinære forhold, er det derfor nødvendigt, at sådanne elforbrugere i tilfælde af en elafbrydelse etablerer en nødelforsyning inden for den nødvendige tidshorisont. I de tilfælde, hvor det vurderes, at en sådan nødelforsyning skal etableres hurtigt, f.eks. på sundhedsområdet, bør dette ske f.eks. ved installation af nødstrømsanlæg, som automatisk overtager elforsyningen, mens det i de tilfælde, hvor en sådan hurtig etablering af nødelforsyning ikke anses for nødvendig, kan ske gennem en tilvejebringelse af mobile nødstrømsanlæg. I begge tilfælde bør sådanne elforbrugere have planer for etablering og opretholdelse af en sådan nødelforsyning.

Det må forventes, at elafbrydelser som oftest ikke kan varsles. I tilfælde af afbrydelse vil oplysning om afbrydelsens forventede varighed kunne fås ved kontakt til det pågældende netselskab og eventuelt også til den systemansvarlige virksomhed.

5.2. Beredskab på naturgasområdet

Naturgassektoren har som nævnt traditionelt et samarbejde med bygassektoren om beredskab, sikkerhed m.m. De to sektorer behandles derfor samlet nedenfor.

Regelgrundlag

Beredskabsarbejdet inden for naturgas- og bygassektorerne er baseret på dels beredskabsloven, dels den sektorlovgivning, som er fastlagt for

a. *naturgas* i lov om naturgasforsyning (jf. lovbekendtgørelse nr. 130 af 27. februar 2003), primært § 15 a

b. *bygas* i lov om varmeforsyning (jf. lovbekendtgørelse nr. 772 af 24. juli 2000 som ændret ved § 3 i lov nr. 316 af 22. maj 2002), primært § 29 a

For *naturgas* forudsætter følgende former for virksomhed, at økonomi- og erhvervsministeren har meddelt bevilling eller tilladelse hertil efter naturgasforsyningsloven:

a. *Naturgastransmission og -distribution*, dvs. dels transmission over store afstande, herunder eksport og eventuel import gennem udlandsforbindelserne (til Sverige og Tyskland), dels distribution til forbrugerne

b. *Lagervirksomhed*, dvs. drift af naturgaslagre (p.t. ved Stenlille og Ll. Torup)

c. *LNG-virksomhed* (LNG står for *Liquified Natural Gas*, dvs. nedkølet, flydendegjort naturgas), idet der dog p.t. ikke er iværksat sådan virksomhed her i landet

For *bygas* etableres anlæg til produktion og fremføring af bygas efter beslutning af den enkelte kommunalbestyrelse.

For disse former for virksomhed, som er baseret på centrale dele af infrastrukturen i de to sektorer, fastsætter naturgasforsyningslovens § 15 a, stk. 1 og varmeforsyningslovens § 29 a, stk. 1, at *de enkelte virksomheder* skal have det nødvendige beredskab. Dette beredskab skal omfatte dels forudgående planlægning, dels operative foranstaltninger i en krisesituation. Disse krisesituationer svarer til den ændrede beredskabslov pr. 1. juli 2003. Beredskabets nærmere indhold forudsættes fastlagt gennem bekendtgørelser og andre regler.

Sikring af, at de enkelte virksomheders beredskab er indbyrdes afstemt og koordineret, varetages p.t. af DONG Transmission. Også her gælder, at det nærmere indhold af denne overordnede og koordinerende opgave forudsættes fastlagt gennem bekendtgørelser og andre regler.

Derudover indeholder de to lovbestemmelser en hjemmel til, at økonomi- og erhvervsministeren kan fastsætte nærmere regler om beredskabsopgaverne. Denne hjemmel er ikke anvendt indtil nu. Sådanne regler om beredskab påregnes udarbejdet af Energistyrelsen i samarbejde med DONG Transmission samt andre berørte parter.

Organisatoriske forhold

Organisationen af beredskabsarbejdet er således baseret på, at arbejdet primært udføres af de to sektorer selv inden for rammer, som fastsættes af myndighederne i et samarbejde med sektorerne:

a. *De enkelte virksomheder* varetager beredskabet for deres egen aktivitet

b. *DONG Transmission* varetager de overordnede og koordinerende opgaver inden for sektorerne

c. *Myndighederne* (dvs. Energistyrelsen på vegne af økonomi- og erhvervsministeren) varetager relationerne til disse og andre energisektorer, til de centrale myndigheder på beredskabsområdet og til internationale organisationer samt udarbejder udkast til bekendtgørelser og andre regler

Med henblik på drøftelser af beredskabsforhold inden for naturgas- og bygassektorerne er der etableret et *Naturgasselskabernes Beredskabsudvalg*, hvori deltager alle 9 naturgas- og bygasvirksomheder samt Energistyrelsen. Formandskab og sekretæropgaver varetages af DONG Transmission. Udvalget har nedsat et forretningsudvalg. Naturgasselskabernes Beredskabsudvalg påregnes at holde møde 1 gang årligt med hyppigere møder i forretningsudvalget.

Det er hensigten at foretage vurderinger af de enkelte selskabers beredskabsplaner og -struktur og at afholde en fælles øvelse ca. hvert andet år med fokus på samarbejdet mellem virksomhederne. Det er endvidere hensigten at koordinere virksomhedernes ajourføring af deres beredskabsplaner.

Den nævnte opgave varetagelse inden for naturgas- og bygassektorerne er baseret på det sektoransvar, som er grundlag for beredskabsarbejdet. Denne struktur bør være koordineret med det regionale samarbejde om beredskab, som foretages gennem arbejdet i de nye regionale stabe.

I de nye regionale stabe - hvis opgaver skal fastlægges efter civilregionernes nedlæggelse pr. 1. juli 2003 - forventes der at indgå repræsentanter for de relevante civile myndigheder, herunder Energistyrelsen, således at disse repræsen-

tanter udpeges af Energistyrelsen. Disse repræsentanter vil dermed have en funktion som en form for forbindelsesofficerer i forhold til den udpegende myndighed og forudsættes derfor at have en løbende kommunikation med denne med henblik på at sikre, at drøftelserne i de regionale stabe af energiforhold foretages i overensstemmelse med sektoransvaret.

Beredskabsforanstaltninger

Gennemgangen af beredskabsforhold inden for naturgas- og bygassektorerne er koncentreret om naturgassystemet. Gennemgangen nedenfor er baseret på følgende opdeling af beredskabet:

a. *Forebyggende beredskab* (security) på virksomhedsniveau, dvs. indhegning, alarmering, adgangskontrol, begrænset antal adgangsveje osv. for de kritiske dele af virksomheden

b. *Konsekvensreducerende beredskab* på virksomhedsniveau, dvs. bekæmpelse af person- og materielskader i form af evakueringsplaner, brandbekæmpelsesplaner osv.

c. *Reetableringsberedskab* på virksomhedsniveau, dvs. hurtig udbedring af skader, især reetablering af energiforsyning

d. *Robusthed og fleksibilitet* i dimensionering af produktions- og distributionsforhold

Forebyggende beredskab

Det forebyggende beredskab omfatter dels den overvågning og styring, som foretages fra systemets kontrolcentre, dels en række andre forhold.

Transmissionssystemet og de enkelte distributionssystemer overvåges således fra et centralt placeret kontrolcenter i de enkelte selskaber. Overvågningen er baseret på såkaldte *Scada-systemer*, der gennem telekommunikationsnet overfører data mellem kontrolcentrene og anlæg, stationer og procesanlæg. Kontrolcentrenes primære aktiviteter er:

- overvågning af tryk og flow i de enkelte ledningssystemer
- overvågning af eventuelle ledningsbeskadigelser
- styring af linieventiler (ledningssektionering)
- overvågning af gasbalancen i systemerne
- emergency shut down af anlæg og stationer
- overvågning af gaskvaliteten og gassammensætningen
- aktivering og koordinering af beredskabsindsats

Scada-systemerne er dublerede og er sikret mod afbrydelse af elforsyningen gennem no-break anlæg og nødstrømsgeneratorer.

Kontrolcentrene for DONG's transmissionssystem og for HNG er døgnbemandet. De øvrige virksomheders kontrolcentre er dagbemandet, hvor overvågningen efter normal arbejdstid varetages af hjemmegående vagtpersonale, som får overført alarmer til en terminal i hjemmet.

Alle virksomhederne har en vagtordning med tekniker på tilkaldevagt. Vagtberedskabet er dimensioneret ud fra selskabernes ledningsnet, antal stationer og kundemassens omfang og karakter. Tilkaldevagterne kan om nødvendigt tilkalde ledelsesvagter, der træffer de nødvendige beslutninger og koordinerer det videre forløb.

Produktions- og behandlingsanlæg er døgnbemandet, indhegnet og forsynet med et adgangskontrolsystem. De ubemandede M/R-stationer m.m. er udført som robuste, aflåste bygninger og de større stationer er indhegnet og aflåst. De fleste stationer er forsynet med alarmsystemer for utilladt adgang, hvor alarmen videresendes til kontrolcentrene.

Alle virksomheder har drifts- og beredskabsmanualer for egne anlæg og rørledningssystemer.

Virksomhederne afholder årligt et antal øvelser med efterfølgende evaluering. Nogle øvelser omfatter samarbejdet mellem transmissionssystemet og distributionssystemerne med hensyn til forsyningssikkerheden for naturgas.

Konsekvensreducerende beredskab

Det konsekvensreducerende beredskab er primært baseret på den *forsyningsstrategi*, som er grundlaget for transmissionsnettets dimensionering og drift. Da de øvrige naturgas- og bygasselskaber forsynes gennem transmissionssystemet, er deres forsyningssikkerhed afhængig af dettes robusthed.

Den forsyningsstrategi, som anvendes af DONG Transmission og som samlet set er dimensionerende for virksomhedens beredskab over for nødsituationer, består af to forsyningsmålsætninger:

a. En *korttidsmålsætning*, der fastlægger krav til, hvor hurtigt naturgas kan leveres ved driftsforstyrrelser og dermed i praksis den rate, hvormed naturgas kan udtrækkes fra de to naturgaslagre

b. En *langtidsmålsætning*, der fastlægger krav til opretholdelse af leverancer ved længerevarende uheld og i praksis mængden af naturgas, som skal være til rådighed på naturgaslagrene

Disse forsyningsmålsætninger skal ses på baggrund af, at DONG indtil 1999 fik leverancer af naturgas fra én leverandør gennem én søledning. I 1999 blev der etableret endnu en ledning fra den danske del af Nordsøen, hvilket forbedrede nødberedskabet væsentligt.

Korttids-målsætningen går ud på, at der under både normale og unormale forsyningsforhold, dvs. fuldstændig afbrydelse af leverancerne fra den største leverandør, skal være tilstrækkelig udtrækskapacitet fra lagrene til i 3 sammenhængende dage at kunne klare forsyningen af det uafbrydelige marked i Danmark ned til en døgngennemsnitstemperatur på -14° C.

Statistisk set indtræffer et døgn med en gennemsnitlig døgntemperatur på ca. -14° C én gang for hver ca. 20 år. Inden for de sidste 45 år er dette indtruffet tre gange, sidste gang i 1987. Hændelsen med 3 sammenhængende døgn med -14° C er ikke indtruffet inden for denne periode.

Langtids-målsætningen går ud på, at der under unormale forsyningsforhold, dvs. fuldstændig afbrydelse af leverancerne fra den største leverandør, skal være tilstrækkeligt volumen til at kunne klare forsyningen af naturgas til det uafbrydelige marked i Danmark i op til ca. 60 dage (svarende til den forventede reparationstid i tilfælde af et søledningsbrud) i en temperaturmæssig normal vinter.

Tilstrækkelig volumen betyder i denne sammenhæng dels leverancer fra andre leverandører og dels tilstrækkelig lagergasmængde. Lagergasmængde består dels af en mængde til belastningsudjævning, da vinterafsætningen er større end leverancerne, dels af en mængde til nødforsyning, der skal sikre forsyningen under et 60 døgns forsyningssvigt fra den største forsyningskilde på det værst tænkelige tidspunkt af året. Hertil kommer et balancelager, som er reserveret dels til systembalance og dels til optagelse af mindre driftsforstyrrelser.

Siden 1999, hvor DONG har modtaget leverancer af naturgas fra to uafhængige leverandører gennem to søledninger, baseres forsyningssikkerheden på, at der kan ske fuldstændig afbrydelse af den største, uafhængige leverandør, dvs. DUC. I tilfælde af et søledningsbrud på Tyra - Nybro rørledningen vil DUC levere de aftalte nødforsyningsmængder gennem den nye søledning via Harald.

DONG får i dag leveret gas gennem to offshore-ledninger med følgende mulige leverancer i normalsituationer:

- Tyra - Nybro rørledningen (DUC) ca. 24 mill. m^3/døgn
- Syd Arne - Nybro rørledningen (Syd Arne) ca. 13 mill. m^3/døgn

Ved det værst tænkelige forsyningssvigt regnes der med, at forsyningen fra den største leverandør svigter, dvs. at DONG mister leverancer fra DUC gennem Tyra - Nybro rørledningen.

DONG har fysisk mulighed for at kompensere for de manglende offshore leverancer således:

- Nødforsyning Tyra - Harald - Nybro rørledningen, hvor det gennem aftale med DUC er muligt at få leverancer på 11 mill. m^3/døgn, forudsat faciliteterne på Tyra er intakte, dvs. at der er tale om en skade på søledningen og ikke platformen. Leverancerne er kun mulige ved længerevarende forsyningssvigt (udover 1 døgn) og har således kun betydning for størrelsen af DONG's nødforsyningsvolumen og ikke for udtrækskapaciteten. Ved leverancer af 11 mill. m^3/døgn gennem Tyra - Harald - Nybro rørledningen leveres ingen gas fra Syd Arne.

- Leverancer fra Tyskland gennem DEUDAN-rørledningen er en teknisk mulighed, selvom både ledningssystem og kompressor ved den dansk-tyske grænse er etableret med udgangspunkt i, at der skal leveres naturgas fra Danmark til Tyskland. Det er således muligt at levere gas fra Tyskland til Danmark ved anvendelse af kompressorerne i Ellund. Hvor store mængder, der kan leveres, afhænger af trykforholdene i det tyske transmissionssystem. Der er ikke i dag indgået kommercielle aftaler om leverancer af naturgas fra Tyskland til Danmark i nødsituationer.

Tabel 5.1

DONG's naturgaslagre i Stenlille og Ll. Torup har isoleret set følgende tekniske maksimale kapaciteter. .	Lagervolumen (mill. m^3)	Udtrækskapacitet (mill. m^3/døgn)	Injektionskapacitet (mill. m^3/døgn)
Stenlille	300	10,8	2,4
Ll. Torup	410	14,4	3,6

Transmissionssystemets *ventilstyring* sikrer, at systemet i tilfælde af uheld kan opdeles i uafhængige sektioner. Systemet er således forsynet med linieventiler, placeret med passende mellemrum, således at afstanden og gasvolumen mellem to linieventiler er af en overskuelig størrelse. Ved en ledningsbeskadigelse kan det beskadigede ledningsafsnit derfor sektioneres fra, således at det øvrige ledningsnet kan opretholde forsyningen enten ved brug af de to gaslagre eller ved at udnytte den såkaldte *linepack*, der er i ledningssystemet, dvs. en form for bufferkapacitet. Linieventiler i kritiske punkter kan fjernbetjenes fra kontrolcentret. Øvrige linieventiler skal manuelt betjenes.

Alle gasvirksomhederne har indbyggede linieventiler efter samme princip, enkelte fjernbetjente.

Alle naturgas- og bygasvirksomheder har *specifikke beredskabsmanualer*, udarbejdet og indøvet for de enkelte ledningstyper og stationstyper samt behandlingsanlæg og produktionsanlæg. Beredskabsstyring og koordinering foretages fra

de respektive kontrolcentre. Kommunikationen mellem virksomhederne og til myndighederne koordineres ligeledes i kontrolcentrene.

Retableringsberedskab

Reetableringsberedskabet omfatter *reparationsplaner og procedurer* herfor, hvilket er udarbejdet af alle naturgas- og bygasvirksomheder for de enkelte anlæg og rørledningstyper. Planerne og procedurerne afprøves og ajourføres med passende intervaller. Mange af procedurerne er udarbejdet i fællesskab af naturgasvirksomhederne i regi af naturgasselskabernes fagudvalgssamarbejde. De enkelte virksomheders erfaring er indbygget i procedurerne, idet systemerne er ens med hensyn til opbygning og materialer.

Som et led i beredskabet har gasselskaberne lavet aftaler med entreprenører om ydelser i situationer, hvor større ressourcer er påkrævet. Det kan være i form af grave-, reparations- og kontroludstyr, f.eks. NDT udstyr. Disse firmaer har en vagtordning, således at de kan rekvireres i alle døgnets 24 timer.

DONG har mobile M/R-stationer, som kan indsættes på strategisk vigtige steder med relativ kort varsel. Alle virksomhederne har reservestrenge og reserveudstyr til M/R-stationerne, som kan forsyne begrænsede områder, samt reserverør og -fittings til reparation af alle ledningsnet.

Selskaberne har endvidere tradition for udveksling af reservedele, udstyr og mandskab i nødsituationer. Det er hensigten fremover at udarbejde mere formelle aftaler om gensidig træk på reservedele, udstyr og ressourcer.

Robusthed og fleksibilitet

Robusthed og fleksibilitet i dimensionering af produktions- og distributionsforhold er i nogen grad opnået gennem ringforbindelser i nettene.

Transmissionsnettet har dog ikke ringforbindelser, bortset fra, at de to bæltkrydsninger er dublerede. Derimod er 40/19 bars fordelingsledninger, som er det overordnede system for de øvrige naturgasselskaber, i begrænset omfang udført som ringforbindelser. 4 bars distributionsledninger er i større omfang

udført som ringforbindelser, især ved de større bysamfund, og 0,1 bars distributions-ledninger og bygasledninger er i endnu større omfang udført som ringforbindelser, ofte forsynet fra to eller flere M/R- D/R-stationer, hvilket giver yderligere forsyningssikkerhed.

Alle ledningssystemer har en bufferkapacitet i form af såkaldt *linepack*. Linepack har den effekt, at et ledningsnet kan opretholde forsyningen til forbrugerne fra halve timer til flere dage, afhængig af ledningstype og tryktrin samt årstid (forbrug). Transmissionssystemet (80 bar) har størst linepack.

Forsyningssikkerheden for naturgas øges ved, at mange erhvervskunder er afbrydelige, dvs. kan afbrydes med et aftalt varsel og overgå til anden energiform.

5.3. Beredskab på teleområdet

Som nævnt i afsnit 1.2 omhandler udredningen kun *offentlige* telenet og teletjenester. Gennemgangen i det følgende omhandler desuden kun forhold vedrørende *udbydere* af offentlige telenet og teletjenester. Der er således ikke sat fokus på, hvorledes den enkelte statslige myndighed eller private virksomhed har planlagt sit beredskab vedrørende eget telekommunikationsbehov. En myndigheds interne teleberedskab vil afhænge af myndighedens behov for telekommunikation generelt samt i beredskabssituationer. Myndigheder som Beredskabsstyrelsen, Forsvaret eller politiet, har f.eks. et særligt behov for telekommunikation i beredskabssituationer. Problemstillingen er nærmere belyst i afsnit 7.3. og 8.3.

Regelgrundlag

Lov nr. 413 af 31. maj 2000 om konkurrence- og forbrugerforhold på telemarkedet

Det lovmæssige grundlag for teleberedskabet følger af lov om konkurrence- og forbrugerforhold på telemarkedet. Der er i henhold til § 86 hjemmel til, at Videnskabsministeren kan fastsætte nærmere regler om, at udbydere af offentlige

telenet og teletjenester skal foretage nødvendig planlægning og træffe nødvendige foranstaltninger til sikring af samfundsvigtig telekommunikation i beredskabssituationer og i andre ekstraordinære situationer, herunder pligt til etablering af særlige faciliteter uden omkostninger for staten. Videnskabsministeren kan fastsætte tilsvarende regler for offentlige myndigheder samt offentlige og private virksomheder og institutioner.

Det følger af denne bestemmelse og af bemærkningerne til lovforslaget, at reglerne ikke blot skal omfatte sikring vedrørende hændelser i forbindelse med krise og krig, men også andre ekstraordinære situationer i fredstid, hvor der f.eks. kan være en fare for overbelastning af telenettene eller svigt i telekommunikationssystemerne som følge af naturkatastrofer etc.

Bemyndigelsen giver mulighed for, at der kan fastsættes regler vedrørende pligter for udbydere af offentlige telenet og teletjenester i forbindelse med teleberedskabet inden for hovedområderne

- Prioriteringer i telenet og teletjenester
- Fysisk beskyttelse af telenet og teletjenester
- Retningslinier for tilvejebringelse og opretholdelse af samfundsvigtig telekommunikation

Bekendtgørelse nr. 1045 af 13. december 2001 om teleberedskab

Bekendtgørelse om teleberedskabet er udstedt af Videnskabsministeriet med hjemmel i lov om konkurrence- og forbrugerforhold på telemarkedet. Bekendtgørelsen har som formål at sikre planlægningen og gennemførelsen af det civile beredskab [14] på telekommunikationsområdet. Bekendtgørelsen finder anvendelse med henblik på under krise eller krig samt katastrofer og andre ekstraordinære situationer i fredstid, at videreføre samfundets funktioner samt at yde støtte til beredskabsmyndighederne.

[14] I beredskabsloven betegnet den civile sektors beredskab

Bekendtgørelsen indeholder regler om organisatoriske forhold, herunder regler vedrørende IT- og Telestyrelsens beføjelser og forvaltningsorganet NALLA's beføjelser, når NALLA aktiveres. Herudover indeholder bekendtgørelsen særligt regler om, hvilke vilkår for udbud af telenet og teletjenester IT- og Telestyrelsen kan fastsætte.

IT- og Telestyrelsen kan således fastsætte nærmere regler om forpligtelser af udførelsesmæssig, driftsmæssig og vedligeholdelsesmæssig art, herunder regler om:

- Tilvejebringelse af mulighed for at give særligt udpegede abonnenter en fortrinsstilling ved benyttelsen af offentlige telenet og teletjenester - om fornødent ved begrænsning af den almindelige adgang til telenet og teletjenester
- Fysisk beskyttelse af offentlige telenet og teletjenester, herunder senderstationer
- Retningslinier for tilvejebringelse og opretholdelse af samfundsvigtig telekommunikation til brug for beredskabsmyndighederne
- Opretholdelse af senderstationer der anvendes til spredning af Danmarks Radio's og TV2's lyd- og billedprogrammer med henblik på, at Danmarks Radio og TV2 kan opfylde den forpligtelse til at udsende meddelelser af beredskabsmæssig betydning, som påhviler dem efter lov om radio- og fjernsynsvirksomhed

Ved bekendtgørelse om sikring af offentlige telenet og teletjenester, jf. nedenfor, er der udstedt regler om fortrinsstilling for særligt udpegede abonnenter ved benyttelsen af offentlige telenet og teletjenester. Ved bekendtgørelse om faste kredsløb til beredskabsmæssige formål, jf. nedenfor, er der udstedt regler om tilvejebringelse og opretholdelse af samfundsvigtig telekommunikation til brug for beredskabsmyndighederne. Der er p.t. ikke udstedt regler om fysisk beskyttelse af telenet og teletjenester eller om opretholdelse af senderstationer til brug for meddelelser af beredskabsmæssig art til befolkningen.

Bekendtgørelsen indeholder også regler om teleudbydernes beredskabspligt. Teleudbyderne skal planlægge og sikre, at det nødvendige personale er til rådighed ved gennemførelse af teleberedskabet. Herved forudsættes det, at teleudbyderne har foretaget en beredskabsplanlægning til gennemførelse af teleberedskabet, men der er ikke fastsat nærmere krav til karakteren og omfanget heraf.

Der er samtidig hjemmel til, at personale, der varetager nøglefunktioner hos teleudbyderen, ved ansøgning herom kan fritages for mødepligt i Forsvaret i forbindelse med krise eller krig, også benævnt designeringsordningen. Personale, der ønsker at deltage i det frivillige hjemmeværnsarbejde, vil indgå i virksomhedshjemmeværnet. Det er hensigten, at personalet herved skal kunne passe deres arbejde under krise og krig indtil det tidspunkt, hvor hjemmeværnet/Forsvaret eventuelt overtager ansvaret i forbindelse med bevogtning og beskyttelse af det pågældende tjenestested.

Bekendtgørelse nr. 1056 af 14. december 2001 om sikring af offentlige telenet og teletjenester

Bekendtgørelse om sikring af offentlige telenet og teletjenester er udstedt af IT- og Telestyrelsen med hjemmel i bekendtgørelse om teleberedskabet. Bekendtgørelsen har til formål at tilvejebringe en sikring af offentlige taletelefonitjenester i faste telenet, der opfylder beredskabsmyndighedernes behov for anvendelse af sådanne tjenester i beredskabssituationer. Sikringen giver abonnenter, der er særligt udpeget af beredskabsmyndighederne, en fortrinsstilling ved adgangen til at benytte offentlige taletelefonitjenester i faste telenet.

Ved sikring af offentlige taletelefonitjenester i faste telenet forstås to foranstaltninger: Sikret fortrinsret og sikret adgang. Ved sikret fortrinsret forstås en fast etableret mulighed for adgang til at benytte offentlige taletelefonitjenester i faste telenet til at gennemføre opkald forud for ikke udpegede abonnenter. Ved sikret adgang forstås en særlig foranstaltning, der indebærer, at ikke udpegede abonnenter midlertidigt udelukkes fra at anvende offentlige taletelefonitjenester i faste telenet. Sikret adgang indføres i de tilfælde, hvor sikret fortrinsret ikke giver tilstrækkelig sikker og hurtig trafikafvikling.

Bekendtgørelsen indeholder krav til teleudbyderne om etablering, effektuering og vedligeholdelse af administrative og tekniske foranstaltninger til gennemførelse af sikret fortrinsret og sikret adgang, herunder procedurer vedrørende en sikret abonnents flytning fra én udbyder til en anden (nummerportering).

Sikringsordningen gælder som nævnt i afsnit 3.3.2 kun taletelefoni i faste telenet, og giver kun fortrinsret til opkaldsmulighed. Opkaldet er ikke sikret prioritet frem til modtager af opkaldet. Sikringsordningen gælder desuden kun for enkelttilslutninger.

Bekendtgørelse nr. 620 af 19. juli 2002 om faste kredsløb til beredskabsmæssige formål

Bekendtgørelse om faste kredsløb til beredskabsmæssige formål er udstedt af IT- og Telestyrelsen med hjemmel i bekendtgørelse om teleberedskab. Bekendtgørelsen har til formål at sikre retningslinier for tilvejebringelse og opretholdelse af samfundsvigtig telekommunikation til brug for beredskabsmyndighederne. Bekendtgørelsen omhandler i den forbindelse kun beredskabsmyndighedernes mulighed for at leje *faste kredsløb* hos teleudbyderne. Bekendtgørelsen omfatter en række krav til de teleudbydere, der udbyder faste kredsløb til beredskabsmæssige formål, vedrørende proceduren for etablering, ændring, nedkobling samt fejlretning af faste kredsløb.

Faste kredsløb til beredskabsmæssige formål registreres løbende i NALLA. Når et kredsløb er registreret i NALLA, vil bestilleren af kredsløbet kunne sikre sig, at kredsløbet prioriteres forud for andre kredsløb og teleforbindelser i en beredskabssituation. Prioritering af de registrerede kredsløb indgår i IT- og Telestyrelsens og NALLA's bemyndigelse til at råde over alle offentlige telenet og teletjenester i en beredskabssituation.

Såfremt brugeren af et kredsløb konstaterer fejl ved kredsløbet, skal brugeren fejlmelde dette til den teleudbyder, der har ansvaret for kredsløbet. Brugeren skal i den forbindelse blandt andet oplyse hvorvidt, der er tale om et kredsløb af særlig væsentlig beredskabsmæssig betydning. Såfremt dette er tilfældet, skal teleudbyderen i en beredskabssituation foretage fejlretning af kredsløbet forud for andre fejlretninger.

I beredskabssituationer skal teleudbyderen i øvrigt følge IT- og Telestyrelsens eller NALLA's anvisninger vedrørende etablering, ændring og nedkobling af faste kredsløb til beredskabsmæssige formål.

Denne ordning betyder, at de registrerede kredsløb er sikret en *høj* prioritet, hvis der er knappe ressourcer i forhold til fejlretning af kredsløb eller reetablering af teleanlæg m.v. Opretholdelse af samfundsvigtig telekommunikation ved brug af disse kredsløb afhænger dog af teleudbyderens generelle teleberedskab og funktionsevnen af større dele af net og tjenester hos teleudbyderen.

Det skal bemærkes, at det register over samfundsvigtige teleforbindelser, som NALLA er i besiddelse af, ikke kun udgør et prioriteringsværktøj i forbindelse med krise eller krig eller hvor NALLA i øvrigt er aktiveret, jf. afsnit 5.3.2 nedenfor. Hvor NALLA ikke er aktiveret, vil IT- og Telestyrelsen kunne anvende dette register som et prioriteringsværktøj om nødvendigt i en beredskabssituation.

Organisatoriske forhold

Ministeriet for Videnskab, Teknologi og Udvikling

Det overordnede ansvar for teleberedskabet påhviler i henhold til beredskabsloven og lov om konkurrence- og forbrugerforhold på telemarkedet, jf. § 86, Videnskabsministeren. Videnskabsministeren har i § 86 i lov om konkurrence- og forbrugerforhold på telemarkedet, hjemmel til at fastsætte nærmere regler om, at udbydere af offentlige telenet og teletjenester skal foretage nødvendig planlægning og træffe nødvendige foranstaltninger til sikring af samfundsvigtig telekommunikation. Tilsvarende regler kan fastsættes for offentlige myndigheder samt offentlige og private virksomheder.

I bekendtgørelse om teleberedskabet, jf. afsnit 5.3.1 ovenfor, er der på den baggrund fastsat bestemmelser, der har til formål at sikre planlægning og gennemførelse af det civile beredskab på telekommunikationsområdet.

IT- og Telestyrelsen

Det følger af § 87 i lov om konkurrence- og forbrugerforhold på telemarkedet, at IT- og Telestyrelsen er tilsynsmyndighed på teleberedskabsområdet. IT- og Telestyrelsen fører således tilsyn med de regler, der fastsættes i medfør af lovens § 86, herunder med, at teleudbyderne planlægger og gennemfører de nødvendige beredskabsforanstaltninger, som følger af den gældende lovgivning. Dette gælder indtil forvaltningsorganet NALLA aktiveres, jf. nedenfor. Når NALLA aktiveres, overgår tilsynsbeføjelsen til NALLA.

Bekendtgørelse om teleberedskabet giver desuden IT- og Telestyrelsen bemyndigelse til at fastsætte nærmere regler om teleberedskabet og angiver samtidig rammerne herfor. I afsnit 5.3.1 ovenfor er disse rammer og de nærmere regler om teleberedskabet beskrevet.

Det følger endelig af bekendtgørelse om teleberedskabet, at IT- og Telestyrelsens overordnede opgave er at koordinere og prioritere beredskabsmyndighedernes[15] skiftende behov for samfundsvigtig telekommunikation indtil NALLA aktiveres.

IT- og Telestyrelsen kan på den baggrund:

- Modtage og ekspedere ønsker fra beredskabsmyndighederne om faste kredsløb
- Afgøre hvilke forbindelser hos teleudbyderne der skal dækkes af telenettenes fremføringsmuligheder, når disse ikke kan tilgodese alle behov
- Give fornødne direktiver til teleudbyderne vedrørende prioritering af reetablering af ødelagte teleanlæg

[15] Ved beredskabsmyndighederne forstås her det militære forsvar, redningsberedskabet, politiet og øvrige civile myndigheder

- Pålægge teleudbyderne generel begrænsning af trafikken i telenet og teletjenester

- Samarbejde med tilsvarende organer i andre lande om løsning af tilsvarende opgaver

Det betyder blandt andet, at IT- og Telestyrelsen har kompetence til at råde over de offentlige telenet og teletjenester i en beredskabssituation, indtil NALLA aktiveres.

IT- og Telestyrelsen har samtidig ansvaret for planlægningen af al NALLA-virksomhed, indtil NALLA aktiveres.

NALLA og NALLA-sekretariatet

NALLA er et forvaltningsorgan, oprettet til at varetage beredskabsmyndighedernes behov for udnyttelse af telekommunikationsnet under kriser og krig. NALLA kan aktiveres på regeringens eller Videnskabsministerens ordre eller i øvrigt ved angreb på landet eller under krig.

NALLA etableres som to ensartet opbyggede organer, NALLA og alternativt NALLA (ALTNALLA), et på hver side af Storebælt. ALTNALLA forberedes til at kunne overtage NALLA's opgaver helt eller delvist. NALLA består af en komité og et sekretariat. Sekretariatet virker i fredstid og er placeret i IT- og Telestyrelsen, ligesom det er styrelsen, der fastlægger de nærmere retningslinier for sekretariatets virke.

NALLA-komiteen består af en formand og en repræsentant for teleudbyderne, der begge udpeges af Videnskabsministeren, en repræsentant for forsvarschefen, en repræsentant for NATO samt en repræsentant for Beredskabsstyrelsen. ALTNALLA sammensættes på samme måde som NALLA, og er underlagt NALLA, så længe dette fungerer.

Når NALLA aktiveres, afgiver IT- og Telestyrelsen kompetence til NALLA. Det betyder særligt, at det er NALLA, der koordinerer og prioriterer beredskabsmyndighedernes behov for samfundsvigtig telekommunikation i krise el-

ler krig. NALLA-komitéen overtager i den forbindelse den samlede ledelse af teleberedskabet og råderetten over landets teleressourcer.

Teleudbyderne

I afsnit 3.3.1 er telemarkedet og teleinfrastrukturen beskrevet nærmere. Med det liberaliserede telemarked er det nu de private teleudbydere, der ejer teleinfrastrukturen. Det er teleudbydernes ansvar at overholde lovgivningen på teleområdet. For så vidt angår de beredskabsmæssige forhold, er der tale om egentlige vilkår for udbuddet, og selvom teleudbyderne nu selv ejer teleinfrastrukturen, har henholdsvis IT- og Telestyrelsen og NALLA som nævnt fuld råderet over de offentlige telenet og teletjenester i en beredskabssituation, uden udgifter for staten.

Beredskabsforanstaltninger

Beredskabsforanstaltninger i henhold til gældende lovgivning

IT- og Telestyrelsen fører som beskrevet under afsnit 5.3.2 ovenfor tilsyn med, at teleudbyderne overholder de regler, der er fastsat på teleberedskabsområdet. Hverken lovgivningenen på området eller forarbejderne hertil giver nogen anvisning for, hvorledes dette tilsyn bør tilrettelægges. I praksis er tilsynet tilrettelagt på den måde, at IT- og Telestyrelsen kontakter teleudbyderne, og anmoder dem om at redegøre for, hvorvidt og eventuelt på hvilken måde, reglerne efterleves. Der er således som udgangspunkt ikke tale om en egentlig kontrol af, om reglerne efterleves, f.eks. ved besigtigelse af teleudbydernes virksomhed og systemer. Det er teleudbydernes eget ansvar at efterleve reglerne.

Der er ikke registreringspligt for teleudbyderne i Danmark. Enhver kan udbyde offentlige telenet og teletjenester, blot skal reglerne på teleområdet efterleves. For så vidt angår de beredskabsmæssige forhold, er der i reglerne tale om vilkår for udbuddet. Oplysninger om teleudbyderne til brug for IT- og Telestyrelsens tilsyn får styrelsen blandt andet via ansøgninger om frekvenstilladelser og telefonnumre, samtrafikaftaler etc. og via en række samarbejdsfora. Det er derfor IT- og Telestyrelsens vurdering, at der er et tilfredsstillende overblik

over de teleudbydere, der må antages at have betydning for teleberedskabet og dermed teleforsyningen i landet i kritiske situationer.

IT- og Telestyrelsens tilsyn med foranstaltningerne sikret fortrinsret og sikret adgang, som beskrevet i afsnit 5.3.1 ovenfor, har vist, at teleudbyderne overholder bekendtgørelsen på området.

Vedrørende faste kredsløb til beredskabsmæssige formål, føres der et løbende tilsyn via registreringen af kredsløbene i NALLA-sekretariatet. For tiden er det kun TDC, der udbyder disse kredsløb.

Hvad angår teleudbydernes beredskabspligt efter bekendtgørelse om teleberedskabet, sikkerhedsgodkender IT- og Telestyrelsen løbende personel hos en række teleudbydere, og styrelsen er påbegyndt et arbejde med at etablere et beredskabsnetværk til teleudbyderne. Formålet med dette netværk er at kunne udveksle informationer i beredskabssituationer med henblik på, at IT- og Telestyrelsen kan prioritere teleressourcerne om nødvendigt i en beredskabssituation.

Andre beredskabsmæssige tiltag

Teleudbyderne har en kommerciel interesse i at sikre telenet og teletjenester. Med liberaliseringen af telemarkedet er det blevet et konkurrenceparameter at kunne udbyde driftsstabile telenet og teletjenester til kunderne. Dette gælder ikke mindst udbuddet til de store erhvervskunder og statslige myndigheder. Teleudbyderne har derfor en interesse i af egen drift at sikre kommunikationssystemerne.

I det følgende beskrives de *typer af sikringstiltag*, teleudbyderne har etableret på den baggrund og de *typer af hændelser*, man har valgt at sikre sig mod. Ikke alle adspurgte teleudbydere har etableret alle de nævnte former for sikringsforanstaltninger, men det er i forbindelse med udredningsarbejdet vurderet, at de oplysninger, de enkelte teleudbydere er fremkommet med, giver et fornuftigt generelt billede af beredskabet - og dermed de styrker og sårbarheder, der måtte være i de offentlige telenet og teletjenester, jf. afsnit 3.3.2, hvor sårbarhederne er sat i fokus.

Det skal bemærkes, at sikringsforanstaltninger vedrørende udsendelse af beredskabsmeddelelser via radio og tv også er behandlet i det følgende, idet Broadcast Service Danmark, som har ansvaret for de senderstationer, der blandt andet anvendes hertil, også betragtes som udbyder af offentlige telenet i medfør af lov om konkurrence- og forbrugerforhold på telemarkedet. De særlige forhold, der måtte gøre sig gældende vedrørende udsendelse af beredskabsmeddelelser, er behandlet i henholdsvis afsnit 3.3.1 og 3.3.2.

Teleudbyderne har alle en høj bevidsthed og viden om beredskabsforhold. De har i vidt omfang udarbejdet beredskabsplaner og foretager risiko- og konsekvensanalyser i forhold til trusler mod driftsstabiliteten. Generelt er beredskabet dog rettet mod vejrfænomener og utilsigtede hændelser som f.eks. lynnedslag og menneskelige og tekniske fejl. Der er ikke i samme omfang sikret mod bevidste angreb som terror- og krigshandlinger. Bag valget af sikringsforanstaltninger er typisk en bevidst prioritering baseret på et forretningsmæssigt hensyn. Teleudbyderne er nødt til at prioritere sikringstiltagene i forhold til det konkrete udbud af net og tjenester og i forhold til rentabiliteten i virksomheden. Der er relativ stor forskel på sikringsniveauet hos de adspurgte teleudbydere. Man har valgt at sikre sig på forskellig vis og på forskellige områder. De forskellige sikringstiltag vil i den forbindelse også afhænge af den teknologi, udbyderne anvender ved det konkrete udbud af net og tjenester.

Ved personale til brug for teleberedskabet sondrer teleudbyderne typisk mellem et beredskab i dagligdagen, der skal håndtere mindre forstyrrelser i driften, og et udvidet beredskab, som typisk består af en form for krisestab, der kaldes sammen i ekstraordinære, kritiske beredskabssituationer. Selve sikringsniveauet er dog forskelligt udbyderne imellem. Ressourcemæssigt må der generelt anslås kun at være tilstrækkeligt personale til brug for teleberedskabet i mindre kritiske beredskabssituationer. De adspurgte teleudbydere har alle sikkerhedsgodkendt personale.

Teleudbyderne har i vidt omfang sikret bygninger og installationer i teleinfrastrukturen mod naturkatastrofer og utilsigtede hændelser. Dette er særligt tilfældet for så vidt angår backbone- og transportnettene. Accessnettene er ikke

sikret i samme omfang, men skader på disse net vil til gengæld typisk kun betyde eventuelle driftsforstyrrelser eller nedbrud i et begrænset geografisk område. Der kan f.eks. være tale om, at et kabel graves over i forbindelse med vejarbejde. På grund af strukturen i backbone- og transportnettene, jf. afsnit 3.3.1, er der desuden i meget høj grad tale om redundans i disse net. Det betyder, at hvis f.eks. et hovedkabel eller en sendermast beskadiges, vil trafikken kunne dirigeres en anden vej i nettet. Bygninger og installationer er kun i mindre omfang sikret mod terror- og krigshandlinger. Bygninger, som indeholder udstyr, der udgør vigtige knudepunkter i teleinfrastrukturen, er f.eks. i vidt omfang sikret mod uvedkommendes indtrængen i form af fysisk og eller logisk adgangskontrol, videoovervågning og skalsikring. Derimod er bygninger og installationer stort set ikke sikrede mod terror- eller militære angreb.

Hvad angår selve nettene - netsikkerheden - er der generelt tale om et højt sikringsniveau og udbyderne har en høj bevidsthed omkring it-sikkerhed i forhold til driften. Teleudbyderne har 24 timers netovervågning, restriktioner omkring adgang til systemer og data, dublerede systemer, backup af kritiske data etc. På enkelte områder er der foretaget en - bevidst - nedprioritering af sikkerheden af økonomiske årsager. Igen er sikringsniveauet højest for så vidt angår de mindre kritiske beredskabssituationer og de mindre sandsynlige trusler som f.eks. et militært angreb.

5.4. Beredskab på it-området

Som omtalt i afsnit 3.4 er it-beredskab i et nationalt perspektiv et nyt område, både i Danmark og i andre lande. Der findes dog særlovgivning, som regulerer lokal håndtering af it-beredskab, f.eks. fastsætter Finanstilsynet krav til anvendelsen af it i finanssektoren, herunder krav om it-beredskab for de finansielle virksomheder.

Der er ikke i dag en myndighed, der koordinerer forhold vedrørende samfundets behov for it-beredskaber, men Videnskabsministeriet har en styrket koordinerende rolle på it-sikkerheds-området. Videnskabsministeriet har desuden i efteråret 2002 iværksat et projekt, der skal klarlægge opgaver og kompetencer for et eventuelt nationalt it-beredskab, jf. afsnit 8.4.

5.5. Beredskab vedrørende afhængigheder mellem sektorerne

Der eksisterer ikke i dag et egentligt formaliseret samarbejde eller en koordinering af beredskabet mellem sektorerne i Underudvalget for el-, naturgas- og teleforsyning samt it-forhold.

I det følgende beskrives de beredskabsmæssige tiltag, der er planlagt eller iværksat inden for de enkelte sektorer med henblik på at reducere de sårbarheder, jf. afsnit 3.5, der kan relateres til afhængigheder sektorerne imellem.

Elområdet

Elsektorens beredskab overfor *naturgasområdet* omfatter primært:

- Naturgasfyrede centrale elproduktionsanlæg i Vestdanmark med en kapacitet på ca. 750MW og 200 MW i Østdanmark. Ved naturgassvigt er det for disse anlæg muligt at skifte til indfyring med alternativt brændsel.

- Naturgasfyrede decentrale kraftvarmeanlæg i Vestdanmark med en kapacitet på ca. 1250 MW og 450 MW i Østdanmark. Ved naturgassvigt er der ikke umiddelbart et brændselsalternativ, men et landsdækkende pludseligt svigt af naturgas vurderes ikke sandsynligt. Centrale elproduktionsanlæg kan i løbet af relativ kort tid bidrage med alternativ produktion, så elforsyningen kan opretholdes. Fjernvarmeforsyningen kan derimod blive et problem og mange fjernvarmekunder kan i situation forventes at substituere med elvarme.

Elsektorens beredskab med hensyn til *tele- og datakommunikation* omfatter primært:

- Der er foretaget dublering af teleforbindelser mellem kontrolrum og til de vigtigste net- og produktionsknudepunkter.

- Der er etableret egne teleforbindelser, som er uafhængige af de offentlige telenet. For transmissionssystemet i Vestdanmark er der

etableret et uafhængigt telefonsystem med egne telefoncentraler og uafhængige datakommunikationsforbindelser, for Østdanmark er der etableret uafhængigt taletelefoni mellem de væsentlige kontrolrum i transmission og produktion, samt det Svenske telefonsystem. Herved er der uafhængige forbindelser mellem den systemansvarlige virksomheds kontrolrum, de regionale transmissionskontrolrum, de centrale produktionskontrolrum og de vigtigste stationer i transmissionsnettet.

- Der er etableret egne radio-telefonisystemer hos netvirksomhederne til driftsmæssig kommunikation internt i virksomheden (mellem kontrolrum og driftspersonalet som arbejder ude i anlæggene). Der er tendens til, at flere og flere virksomheder bruger offentlig mobiltelefoni til den normale driftskommunikation, hvilket indebærer, at deres egne radiosystemer mest anvendes i ekstraordinære situationer.

- Der er i offentlige telenet oprettet en række sikrede telefoner, jf. afsnit 3.3.2, hvorfra der er prioritet til at foretage opkald i tilfælde af overbelastning af telenettene. Telefonerne er ikke sikret mod nedbrud i telenettene.

- Der er hos NALLA, jf. afsnit 3.3.2. og 5.3.2, registreret en del faste kredsløb, der hermed er sikret høj prioritet i en beredskabssituation.

Elsektorens beredskab på *it-området* som forsyningsområde, som defineret i afsnit 3.4.1, omfatter i øvrigt primært:

- Sikker adskillelse mellem it-systemer til fjernkontrol og elvirksomhedernes øvrige it-systemer tilkoblet internettet.

- Fjernkontrolanlæg til styring og overvågning af elsystemet er uafhængige af internettet. En del fjernkontrolanlæg anvender derimod alarmnettet (tekniknettet) til dataudveksling og det vurderes som et sikkert datanet sammenlignet med internettet.

- El-markedsfunktionerne anvender i udstrakt grad den offentlige it-infrastruktur i form af internet tjenester til dataudveksling. De systemansvarlige er centrale parter i markedsaktørernes dataudveksling og afhængigheden af internet er reduceret med flere geografisk adskilte tilkoblinger til internettet. Ved internet svigt findes nødprocedurer for alternativ gennemførelse af dataudveksling.

Naturgasområdet

Naturgassektorens beredskab overfor *elområdet* omfatter primært:

- De store behandlingsanlæg er forsynet med nødstrømsgeneratorer og kan opretholde gasforsyningen ved svigt i elforsyningen. Disse anlæg opgraderes jævnligt. Dertil kommer, at der er tegnet serviceaftaler med døgntilkald.

- De mindre anlæg er forsynet med nødstrømsanlæg, der kan opretholde elforsyningen og dermed kommunikationen i ca. et til to døgn. Disse anlæg opgraderes med kommunikationsudstyr, der har et lavere strømforbrug og giver dermed en længere oppetid for kommunikationen.

- Selskaberne har mobile nødstrømsgeneratorer, som kan forsyne anlæggene i et begrænset område ved svigt i elforsyningen.

Naturgassektorens beredskab med hensyn til *tele- og datakommunikation* omfatter primært:

- DONG's kontrolcenter har sin egen telefoncentral. Hvis der sker et nedbrud af denne central, kan dispatcherne derfor straks benytte de to nødtelefoner i kontrolcentret. Disse nødtelefoner er forbundet til den administrative telefoncentral i nærheden. TDC kan med meget kort varsel omstille alle indgående samtaler til kontrolcentret til disse to nødtelefoner. Som et alternativ hertil har alle vagtgående dispatchere mobiltelefon, der også kan benyttes.

- Der er etableret egne radio-telefonisystemer hos enkelte af distributionsselskaberne til driftsmæssig kommunikation internt i virksomheden (mellem kontrolrum og driftspersonalet som arbejder ude i anlæggene). Der er tendens til, at flere og flere virksomheder bruger offentlig mobiltelefoni til den normale driftskommunikation, hvilket indebærer, at deres egne radiosystemer mest anvendes i ekstraordinære situationer.

- Der er oprettet flere direkte linier til kontrolcentrene udenom omstillingsbordene som alternativ kommunikationsmulighed.

- Der er hos NALLA, jf. afsnit 5.3.2, registreret et begrænset antal faste kredsløb, der hermed er sikret høj prioritet.

Teleområdet

Teleforsyning er grundlæggende afhængig af *elforsyning*. Teleudbyderne - herunder Broadcast service Danmark - har i vidt omfang planlagt eller iværksat beredskabsmæssige tiltag vedrørende teleinfrastrukturens afhængighed af elforsyning. Teleudbyderne har således i vidt omfang etableret nødstrømsanlæg i vigtige knudepunkter (switch/server lokationer) i telenettene. Andre lokationer - f.eks. basisstationer i GSM-nettet - er i et vist omfang forsynet med batteri backup. Teleudbyderne er i mindre omfang i besiddelse af mobile nødstrømsgeneratorer samt har indgået aftale om leje heraf. Sikringsniveauet er meget forskelligt udbyderne imellem. Der er typisk tale om en bevidst forretningsmæssigt prioritering, da disse sikringsforanstaltninger udgør en relativ dyr investering. Beredskabet er derfor kun rettet mod kortvarige og geografisk begrænsede strømafbrydelser. Den anslåede kapacitet af nødstrøm til opretholdelse af teleforsyningen er behandlet i afsnit 3.5.

For så vidt angår *taletelefonitjenesterne* har de adspurgte teleudbydere oplyst, at de ikke er afhængige af it-infrastrukturen, som den er defineret i afsnit 3.4. De sikringstiltag, der typisk er omfattet af teleudbydernes it-beredskab, vedrører interne it-systemer, der understøtter drift og administrative procedurer, altså den interne it-sikkerhed. En beskrivelse af dette beredskab falder for så vidt angår

de administrative procedurer (f.eks. billingsystemer) uden for denne udredning, mens systemer, der understøtter driften - og dermed selve teleinfrastrukturen, er behandlet i afsnit 5.3.3 i forbindelse med netsikkerheden.

It-området

It-området som forsyningsområde, som det er defineret i afsnit 3.4, er grundlæggende afhængig af tele- og el-forsyning. Der er i forbindelse med dette udredningsarbejde ikke foretaget en nærmere analyse af det beredskab, der på it-området måtte være planlagt eller iværksat hos de enkelte, relevante aktører til at imødegå eventuelle sårbarheder, der kan relateres til afhængighedsforholdene.

6. Internationalt samarbejde og regler m.v. af betydning for beredskabet

I afsnit 6 beskrives internationalt samarbejde, regler og aftaler, der måtte indvirke på beredskabsplanlægningen nationalt, samt i den forbindelse i hvilket omfang, man kan "trække på udlandet" med hensyn til assistance i en beredskabssituation. Eventuelle sårbarheder relateret til internationale forhold behandles ikke i dette afsnit, men er anført i de øvrige afsnit i udredningen.

6.1. Elområdet

Der findes ikke for elsektoren internationale regler og aftaler om beredskab, som påvirker elsektorens planlægning af beredskab eller som i en krisesituation indebærer dels pligt til at yde bistand til andre lande, dels ret til at kunne få bistand fra andre lande. Dog er der naturligvis internationalt samarbejde, som kan have betydning for beredskabsforhold, og som kan indebære mulighed for, at der i en krisesituation kan indgås konkrete aftaler om bistand.

Endvidere er der et formaliseret driftssamarbejde henover landegrænser med henblik på at optimere driftsplanlægning og systemdrift af de sammenkoblede elsystemer. Grænsen mellem unormale driftsforhold - spændende fra driftsforstyrrelser til egentlige krisesituationer - er ikke skarp og derfor diskuteres beredskabsforhold jævnligt i det internationale driftssamarbejde, ikke mindst i forbindelse med aktuelle begivenheder.

EU-forhold

Det centrale EU-direktiv for elsektoren er *Europaparlamentets og Rådets direktiv 2003/54/EF af 26. juni 2003 om fælles regler for det indre marked for elektricitet og om ophævelse af direktiv 96/92/EF.* Direktivet indeholder primært regler om det indre marked for el og indeholder ikke bestemmelser om beredskabsforhold med en enkelt undtagelse, nemlig direktivets artikel 24.

Ifølge artikel 24 kan en medlemsstat midlertidigt træffe de nødvendige beskyttelsesforanstaltninger, såfremt der opstår ;

a. en pludselig krise på energimarkedet,

b. fare for personers fysiske sikkerhed,

c. fare for apparaters eller anlægs driftssikkerhed eller for systemets integritet.

Sådanne foranstaltninger må dog ikke mere end højst nødvendigt forstyrre den måde, hvorpå det indre marked fungerer, og må ikke være mere vidtgående, end det er strengt nødvendigt for at afhjælpe de pludselige vanskeligheder, der er opstået.

I tilfælde af sådanne foranstaltninger skal den pågældende medlemsstat omgående underrette dels de øvrige medlemsstater, dels Kommissionen. Kommissionen kan beslutte, at medlemsstaten skal ændre eller ophæve de nævnte foranstaltninger, hvis de medfører konkurrenceforvridning og påvirker samhandelen negativt på en måde, som strider imod den fælles interesse.

Udgangspunktet er således, at markedsmekanismerne i EU's indre marked skal fungere længst muligt, også i tilfælde af vanskeligheder, men at markedshensynet kan tilsidesættes midlertidigt, hvis håndteringen af en krisesituation nødvendiggør dette. Sådanne foranstaltninger skal dog rapporteres til Kommissionen og kan ændres eller ophæves af denne som anført i bestemmelsen.

Nordisk samarbejde om beredskab

Der er ikke et formaliseret beredskabssamarbejde mellem de nordiske energimyndigheder, men der har i en række år været en løbende gensidig orientering om de enkelte landes initiativer og foranstaltninger vedrørende beredskabsforhold.

Endvidere er der i nordisk regi etableret et vist samarbejde i det såkaldte *Nordisk Elberedskaps- og Säkerhetsforum* (NEF), som er et forum for erfaringsud-

veksling og drøftelser i øvrigt om beredskab inden for elsektoren mellem energimyndigheder, systemansvarlige virksomheder og brancheorganisationer. De drivende kræfter i NEF og dens arbejdsgrupper er Norge, Finland og Sverige, mens Danmark normalt primært deltager i møder for at holde sig orienteret.

Internationalt driftssamarbejde for de danske systemansvarlige

Som nævnt er der et formaliseret driftssamarbejde mellem landene, hvor beredskabsforhold jævnligt drøftes, men som ikke omfatter egentlige aftaler om beredskabsforhold.

De relevante internationale driftsprincipper aftales primært i de to samarbejdsorganisationer Nordel og UCTE, som er samarbejdsorganisationer for de systemansvarlige virksomheder og transmissionsselskaber i henholdsvis Skandinavien og Centraleuropa. For de systemansvarlige virksomheder er Nordel det primære samarbejdsforum. Derudover er der bilateralt internationalt driftssamarbejde med udenlandske nabosystemansvarlige omfattende Svenska Kraftnät i Sverige, Statnett i Norge, Vattenfall Europe Transmission i Tyskland, E.ON Netz i Tyskland og Stadtwerke Flensburg i Tyskland.

I *Nordel* behandles fællesnordiske driftsforhold af Nordels Driftskomité, som mødes typisk 8-10 gange årligt. Både Elkraft System og Eltra er medlemmer af Nordel. Under driftskomitéen findes et antal arbejdsgrupper og alle relevante fællesnordiske driftsanliggender behandles i driftskomitéens regi. Der er indgået en fællesnordisk systemdriftsaftale (se www.nordel.org) mellem Nordelmedlemmerne, som fastlægger driftsprincipper for samkøring af de nordiske elsystemer med henblik på at sikre udnyttelse af fordelene ved samkøring. I aftalen fastlægges krav med henblik på sikring af tilfredsstillende driftssikkerhed og forsyningskvalitet:

- Hver systemansvarlig er grundlæggende ansvarlig for eget område (§ 5).
- Ved driftsforstyrrelser skal parterne bistå hinanden for at minimere konsekvenserne af indtrufne forstyrrelser (§ 11), men et fejlramt delsystem er ultimativt selv ansvarlig for eget område.

- Ved effektbrist skal parterne samarbejde, så tilgængelige ressourcer i det sammenkoblede nordiske elsystem udnyttes for at minimere omfanget af tvangsmæssig bortkobling af forbrug (§ 15 og bilag 9). Ved effektbrist med utilstrækkelige reserver og forsyningsunderskud skal forbrug bortkobles i underskudsområdet.

Beredskabsforhold og disses håndtering indgår ikke direkte i systemdriftsaftalen, men der sker i driftskomiteen en gensidig orientering herom.

I *UCTE* (*Union for the Co-ordination of Transmission of Electricity*) fastlægges operative fælles regler for de samkørende elsystemer dækkende størstedelen af det kontinentale Europa. De driftsmæssige regler er samlet i en *UCTE Operation Handbook*, der udarbejdes af den permanente arbejdsgruppe *Operations and Security* (se www.ucte.org). Eltra er associeret medlem af UCTE, da Vestdanmark vekselstrømsmæssigt er tilkoblet UCTE. Dansk operativt samarbejde med UCTE varetages primært gennem Nordel og via den tyske systemansvarlige E.ON Netz, som der er et tæt bilateralt samarbejde med. Hovedprincippet i UCTE er, at hvert land skal bidrage forholdsmæssigt til opretholdelse af det samkørende systems reserver og sikkerhed. Der er ikke UCTE-regler om beredskabsforhold, der betragtes som opgaver for de nationale myndigheder.

E.ON Netz og Eltra har et løbende driftssamarbejde og har indgået en bilateral systemdriftsaftale for sammenkoblingen af det vestdanske elsystem med det tyske. I aftalen fastlægges de gensidige driftssamarbejdsregler med henblik på optimal udnyttelse af samkøringen mellem parternes elsystemer. Hver part er ansvarlig for eget system og der ydes assistance til naboen i muligt omfang, men uden at der er forpligtende sikkerhed herfor. Beredskabsforhold indgår ikke i aftalen, men parterne orienterer hinanden herom. Også her ses beredskabsforhold som opgaver for de nationale myndigheder.

Stadtwerke Flensburg og Eltra har indgået en systemdriftsaftale, bl.a. om at de to systemansvarlige virksomheder i størst mulig omfang vil støtte hinanden i tilfælde af unormale driftstilstande. Beredskabsforhold indgår ikke i aftalen.

Vattenfall Europe Transmission og Elkraft System har indgået en aftale, der bl.a. indeholder bestemmelser om systemdrift, herunder om udveksling af momentanreserve, som indgår i den daglige driftsplanlægning. Derudover er der også bestemmelser, som i tilfælde af truende blackout giver tilladelse til at standse en eventuel eksport.

Øvrige internationale samarbejdsfora

ETSO (*European Transmission System Operators*) er det europæiske samarbejdsorgan for specielt de markedsorienterede forhold mellem systemansvarlige virksomheder. I Skandinavien findes der i Nordel en markedskomité, som tager sig af disse forhold. I en krisesituation kan det ikke udelukkes, at der kan opstå et dilemma mellem markedshensyn og forsyningssikkerhed. Der findes ikke internationale retningslinier herfor.

CIGRE er en international organisation med det formål at udvikle og udbrede teknisk viden inden for området elproduktion og -transmission i store højspændingssystemer. Et stort antal studiekomitéer er aktive, bl.a. komiteen *System Control and Operation*. Her er der tradition for et højt niveau af gensidig orientering om driftsforstyrrelser og beredskabsforhold for eltransmission, bl.a. er der her givet orienteringer om elsystemernes påvirkning under Balkankonflikterne.

6.2. Naturgasområdet

Der findes ikke for naturgassektoren internationale regler og aftaler om beredskab, som påvirker naturgassektorens planlægning af beredskab eller som i en krisesituation indebærer dels pligt til at yde bistand til andre lande, dels ret til at kunne få bistand fra andre lande. Dog er der naturligvis internationalt samarbejde, som kan have betydning for beredskabsforhold, og som kan indebære mulighed for, at der i en krisesituation kan indgås konkrete aftaler om bistand.

EU-forhold

Det centrale EU-direktiv for naturgassektoren er *Europaparlamentets og Rådets direktiv 2003/55/EF af 26. juni 2003 om fælles regler for det indre marked for naturgas og*

om ophævelse af direktiv 98/30/EF. Direktivet indeholder primært regler om det indre marked for naturgas og indeholder ikke bestemmelser om beredskabsforhold med en enkelt undtagelse, nemlig direktivets artikel 26.

Ifølge artikel 26 kan en medlemsstat midlertidigt træffe de nødvendige beskyttelsesforanstaltninger, såfremt der opstår

a. en pludselig krise på energimarkedet;

b. fare for personers fysiske sikkerhed;

c. fare for apparaters eller anlægs driftssikkerhed eller for systemets integritet.

Sådanne foranstaltninger må dog ikke mere end højst nødvendigt forstyrre den måde, hvorpå det indre marked fungerer, og må ikke være mere vidtgående, end det er strengt nødvendigt for at afhjælpe de pludselige vanskeligheder, der er opstået.

I tilfælde af sådanne foranstaltninger skal den pågældende medlemsstat omgående underrette dels de øvrige medlemsstater, dels Kommissionen. Kommissionen kan beslutte, at medlemsstaten skal ændre eller ophæve de nævnte foranstaltninger, hvis de medfører konkurrenceforvridning og påvirker samhandelen negativt på en måde, som strider imod den fælles interesse.

Udgangspunktet er således, at markedsmekanismerne i EU's indre marked skal fungere længst muligt, også i tilfælde af vanskeligheder, men at markedshensynet kan tilsidesættes midlertidigt, hvis håndteringen af en krisesituation nødvendig dette. Sådanne foranstaltninger skal dog rapporteres til Kommissionen og kan ændres eller ophæves af denne som anført i bestemmelsen.

Internationalt samarbejde

DONG deltager i en række internationale organisationer, der beskæftiger sig med økonomiske, tekniske og sikkerhedsmæssige forhold inden for naturgassektoren. Disse organisationer gennemfører eksempelvis projekter inden for

forebyggelse af uheld, statistik over gasudslip og årsagerne hertil. Andre projekter kunne være udvikling af nyt reparationsudstyr til at sikre hurtigere eller mere sikker retablering efter skader.

Ingen af disse organisationer beskæftiger sig med beredskabsforhold, men der kan være enkelte projekter, som tangerer dette begreb. Beredskabsforhold varetages som hovedregel af de enkelte transmissionsselskaber.

Mellem transmissionsselskaberne foreligger der ingen deciderede aftaler om beredskab, men der er en forståelse for, at selskaberne bistår hinanden i muligt omfang. Eksempelvis kunne man forestille sig, at tyske gasselskaber bistod med gasforsyning i det sønderjyske område i tilfælde af ledningshavari på strækningen mellem Egtved og grænsen.

Ligeledes er der mellem de forskellige operatører af offshoreledninger aftaler om gensidig bistand om udveksling af teknisk udstyr m.m.

Der er således mulighed for at trække på internationale samarbejdsparter, men der foreligger ikke eller kun i meget begrænset omfang skriftlige aftaler herom.

6.3. Teleområdet

Beredskabsplanlægning på teleområdet foregår, som det fremgår af afsnit 5.3, på to "niveauer". Den mere overordnede planlægning af teleberedskabet - i forhold til sikring af samfundsvigtig telekommunikation i beredskabssituationer - foregår på myndighedsniveau. Teleudbyderne gennemfører denne beredskabsplanlægning i praksis, og har samtidig i større eller mindre omfang etableret et driftberedskab af kommercielle årsager.

For så vidt angår teleudbydernes beredskabsplanlægning, eksisterer der ifølge det oplyste ikke et internationalt samarbejdsorgan. Dog har teleudbyderne mulighed for at deltage i visse arbejdsgrupper i internationale statslige organisationer, jf. nedenfor. I organisationen GSM Association, som er en international handelsorganisation for primært teleudbydere af trådløse tjenester, drøftes desuden visse forhold, der kan have karakter af beredskabsforhold. I dette forum udveksles bl.a. erfaringer vedrørende netsikkerhed og ny teknologi på

mobilområdet i arbejdsgruppen "Security Group". Det er ikke muligt at opgøre nærmere, hvorvidt internationalt samarbejde indvirker på teleudbydernes beredskabsplanlægning.

Af større betydning må anses teleudbydernes mulighed for at indgået aftaler om eller fastlægge procedurer for assistance fra moderselskaber, forskellige leverandører eller fra andre nationale teleudbydere. IT- og Telestyrelsen er bekendt med, at der hos nogle teleudbydere er indgået sådanne aftaler, men der er ikke i forbindelse med denne udredning foretaget en nærmere undersøgelse af dette forhold.

Beskrivelsen i det følgende omhandler internationale forhold af betydning for den planlægning af det nationale teleberedskab, der foregår på *myndighedsniveau*.

North Atlantic Council Organisation (NATO)

På området for elektroniske kommunikationsnet og -tjenester har IT- og Telestyrelsen gennem mange år deltaget i et NATO-samarbejde på følgende hovedområder:

- Under NATO's *Consultation, Command and Control Organisation (NC3O)* består et sam-arbejde i relation til National Long Lines Agency (NALLA). Der er primært tale om et samarbejde mellem NALLA i de enkelte NATO-lande om tilvejebringelse af faste kredsløb NATO-landene imellem i forhold til militære og civile NATO-myndigheders behov herfor. NATO-procedurer vedrørende NALLA har været implementeret i den nationale beredskabsplanlægning i årtier, og procedurerne er kendte og gennemgår løbende en tilpasning til udviklingen i sektoren. Faste kredsløbs betydning for teleberedskabet er behandlet nærmere i afsnit 5.3.1.

- Under NATO's *Civil Emergency Planning (CEP)* består et samarbejde i *Civil Communications Planning Committee (CCPC)*. CCPC dækker post- og telekommunikationsområdet og har bl.a. til opgave at støtte myndigheder i NATO medlems- og partnerlande. Opgaven løses for-

trinsvis ved udarbejdelse af vejledninger og anbefalinger om sikring og fortsat drift af post og tele til støtte for samfundet i beredskabssituationer. Større teleudbydere bistår deres nationale myndighed i samarbejdet.

Ved planlægning af teleberedskabet vurderes de anbefalinger m.m., som udarbejdes i CCPC-regi.

IT- og Telestyrelsens teleberedskab udgør en del af CCPC's krisestyringsberedskab under Civil Emergency Planning som en del af NATO's krisestyrings- og beredskabssystem.

CCPC har gennem de seneste år bl.a. set på forhold vedrørende følgende emner:

- New risks and threats to civil communications
- Critical communications infrastructure protection
- Consequences of the Tampere Convention
- International emergency preference scheme
- National (emergency) legislation
- Vulnerability of communications systems to weapons of mass destruction – EMP, man-made EMP, high power microwave and directed energy weapons/systems
- Reviewed crise management arrangements.

United Nations (FN)

I FN-regi blev i 1998 vedtaget en konvention om beredskab på teleområdet. Den såkaldte Tampere Konvention (Tampere Convention on the Provision of Telecommunication Resources for Disaster Mitigation and Relief Operations) har til formål at skabe rammerne for, at andre lande kan bistå med midlertidige

kommunikationssystemer, hvis de(t) eksisterende telekommunikationsnet bryder ned i forbindelse med f.eks. naturkatastrofer.

Konventionen anbefaler, at de lande, som deltager i samarbejdet, sikrer, at personer og organisationer, som bidrager med eller betjener telekommunikationsudstyr i sådanne situationer, undtages fra told og afgifter og blandt andet sikres immunitet over for beslaglæggelse og rekvisition af telekommunikationsudstyr. Endvidere skal der etableres nødprocedurer for allokering af frekvenser til mobile systemer. Konventionen indeholder endvidere en række bestemmelser om fremsættelse af anmodninger om assistance, betaling og refusion af omkostninger ved bistanden, samt etablering af et katalog over mulige ressourcer, som kan stilles til rådighed.

Det skal bemærkes, at konventionen ikke sikrer bistand på teleområdet fra andre lande i en national beredskabssituation, men alene har til formål at sikre en samarbejdsstruktur for håndtering af henvendelser om assistance på teleområdet og for minimering af hindringer i forbindelse med en sådan assistance. Danmark har ratificeret konventionen, som dog formelt først træder i kraft, når den er ratificeret af 30 medlemslande.

International Telecommunication Union (ITU)

ITU er en mellemstatslig organisation under FN, hvis formål primært er at fremme og koordinere udviklingen af teknologi på verdensplan inden for telekommunikationsområdet. Der optages kun suveræne stater som medlemmer af ITU. Operatører, producenter m.fl. kan dog i et vist omfang deltage i arbejdet i ITU som såkaldte sektormedlemmer.

ITU består af et generalsekretariat og følgende tre sektorer:

- Telecommunication Standardization Sector (ITU-T)
- Radiocommunication Sector (ITU-R)
- Telecommunication Development Sector (ITU-D)

ITU-T arbejder med standardisering inden for telekommunikation med undtagelse af radioområdet.

Videnskabsministeriet ved IT- og Telestyrelsen følger aktiviteterne i ITU, med henblik på at vurdere muligheden for at indføre anbefalinger herfra i det nationale sektorberedskab.

Et eksempel på drøftelser i ITU, som har haft betydning for overvejelser om planlægningen af teleberedskabet i Danmark, er drøftelserne omkring sikring af mobiltelefoni (prioriterede kald).

European Telecommunications Standards Institute (ETSI)

ETSI er en organisation, hvis formål er at udarbejde tekniske standarder til brug for det europæiske telekommunikationsmarked. Instituttet er anerkendt af EU-kommissionen som den europæiske standardiseringsorganisation på teleområdet. Medlemmer af ETSI kan være administrationer, offentlige eller private netoperatører, tjenesteudbydere, fabrikanter, brugere samt forskningsinstitutioner inden for teleområdet.

På baggrund af navnlig hændelserne 11. september 2001 i USA har ETSI iværksat aktiviteter på bl.a. "emergency-området" benævnt "Emergency Telecommunications (EMTEL).

EMTEL dækker et bredt spektrum af emner relateret til tilvejebringelse af elektroniske kommunikationstjenester i beredskabssituationer (emergencies). F.eks. kan nævnes samfundets behov for tilvejebringelse af de nødvendige ressourcer til sikring af offentlig sikkerhed - herunder f.eks. politi-, brand-, ambulance- og sundhedstjenester, og i den forbindelse at integrere elektroniske kommunikationsnet og -tjenester på områderne.

IT- og Telestyrelsen følger som medlem af ETSI intensivt dette arbejde, med henblik på at vurdere muligheden for at indføre anbefalinger herfra i det nationale sektorberedskab.

EU

Såvel it- som teleområdet er for så vidt angår beredskabs- og sikkerhedsspørgsmål et forholdsvist nyt område i EU-sammenhæng. Der har i EU-regi gennem de seneste år været drøftelser og der er iværksat analyser om emner som "Critical Infrastructure" og "Network Security". Dette har indtil videre ikke ført til konkrete anbefalinger, samarbejdsaftaler eller reguleringstiltag - og ses heller ikke i øvrigt at have haft væsentlig konkret indflydelse på beredskabsplanlægningen i Danmark på myndighedsniveau.

6.4. It-området

På it-området er der som tidligere nævnt ikke i dag etableret et nationalt, koordineret it-beredskab med henblik på at sikre samfundsvigtig it-anvendelse i beredskabssituationer. Videnskabsministeriet og IT- og Telestyrelsen har dog en styrket rolle på området, og et projekt er iværksat med henblik på en politisk stillingtagen til et sådant beredskab. Der er på den baggrund ikke på myndighedsniveau tale om internationalt samarbejde m.v., der påvirker en overordnet og koordineret beredskabsplanlægning.

Videnskabsministeriets og IT- og Telestyrelsens deltagelse i diverse internationalt samarbejde er dog til inspiration for planlægningen af rammerne for et nationalt it-beredskab. Det skal desuden bemærkes, at det kan være vanskeligt at drage en skillelinje mellem it- og teleberedskabet. Som beskrevet i afsnit 3.3, udgør teleinfrastrukturen en væsentlig del af it-infrastrukturen. Det betyder, at internationale forhold, der har indvirkning på beredskabsplanlægningen på teleområdet, indirekte også vil have indvirkning på it-området. Der skal derfor henvises til gennemgangen i afsnit 6.3 ovenfor.

Det er ikke i forbindelse med denne udredning undersøgt, hvorvidt de enkelte statslige myndigheder eller offentlige eller private virksomheder med et særligt behov for it-anvendelse i beredskabssituationer, har indgået internationale aftaler med henblik på assistance i beredskabssituationer, eller om internationale forhold indvirker på den beredskabsplanlægning, der foregår på lokalt niveau.

For så vidt angår de private aktører på it-markedet - netoperatører, hostmastere, ISP'ere m.fl. - der indgår i it-infrastrukturen, er det ikke muligt at foretage

en fuldstændig afdækning af eventuelt internationalt samarbejde m.v., der måtte indvirke på en beredskabsplanlægning. Det skyldes navnlig, at der ikke er foretaget en egentlig sårbarhedsanalyse for it-området - herunder en nærmere kortlægning af it-infrastrukturen, og i den forbindelse en endelig listning af væsentlige aktiver, som indgår heri. Oplysningerne i det følgende er derfor baseret på en rundspørge blandt andet nogle af de virksomheder og organisationer, som har medvirket ved dette udredningsarbejde.

Det generelle billede for virksomheder og organisationer som indgår i it-området er, at omfanget af internationale relationer er bestemt af virksomhedens størrelse og funktion i it-infrastrukturen.

For større internationale virksomheder gælder, at de baserer deres it-sikkerheds- og beredskabsarbejde på internationalt kendte standarder som BS 7799 og ISO 17799, og evt. deltagelse i internationale fora spiller kun en mere indirekte rolle.

Organisationer, der behandler sikkerhedshændelser og varsling, har et veludbygget internationalt netværk af samarbejdspartnere, som både dækker forskningssektoren og den private sektor.

Virksomheder, der udbyder væsentlige infrastruktur elementer som f.eks. navneservices eller backbone kapacitet, benytter sig af internationale aftaler for at sikre høj tilgængelighed til kommunikationstjenesterne, og deltager i en række internationale fora afhængig af hvilke type tjenester virksomheden udbyder.

7. Udviklingstendenser

7.1. Udviklingstendenser på elområdet

Udviklingstendenserne på elområdet vil stille nye udfordringer til beredskabet fremover. De systemansvarlige elvirksomheder (Eltra og Elkraft System) udgiver hvert år en systemplan, hvor der sættes fokus på elsystemernes udvikling, herunder opfyldelse af målsætninger som forsyningssikkerhed, tilstrækkelig produktionskapacitet, teknisk kvalitet og balance, transportkapacitet m.v. I systemplanen for 2003 er der eksempelvis fokus på elsystemets langsigtede mål, systemarkitektur, systemdesign, systemsikkerhed, systemkontrol og en sikkerhedsstrategi.

Af særlig relevans for beredskabsområdet fremhæves nogle udviklingstendenser i det følgende.

Der er en fortsat udvikling mod øget andel af decentral produktionskapacitet. Udover decentral kraftvarme og vindkraft kan der forventes mikrokraftværker i husstandene og solcelleanlæg. Hvad det betyder for systemets sårbarhed bør vurderes. Konceptet i dag for den decentrale produktion betyder, at disse anlæg ikke kan forsyne delområder, men forudsætter, at centrale produktionsenheder og transmissionsnettet er i drift. Fremover kunne sårbarheden reduceres, hvis den decentrale produktion alene kunne forsyne delområder. Der arbejdes på at få den decentrale produktion til at bidrage til systemstabiliteten og dermed øge robustheden i elsystemet.

Med vedvarende energikilder er elproduktionen typisk bestemt af meteorologiske betingelser og ikke af elforbruget. De danske elsystemer er i dag afhængige af kraftige udlandsforbindelser bl.a. for at kunne udligne forskelle mellem forbrug og vindkraftproduktion. En øgning af vedvarende energikilder ser ud til at øge udlandsafhængigheden. I beredskabssammenhæng kunne overvejes eventuelle krav til selvstændig drift af landets elsystemer.

Med indførelse af markedsvilkår for elforsyningen er der hos elmarkedsaktørerne og de systemansvarlige virksomheder øget brug af offentlige email og

web-tjenester. En øget markedsorientering forventes at betyde en yderligere øget anvendelse af internet-tjenester. Det bliver derfor mere og mere vigtigt for markedsfunktion og driftsplanlægning, at disse offentlige tjenester altid fungerer. For driften af elsystemet betyder internetsvigt væsentlige gener, uden at det dog har afgørende indflydelse på systemdriften.

Liberaliseringen af elsektoren har givet øget fokus på omkostningsbevidsthed og konkurrenceevne hos elselskaberne. Netselskabernes indtægtsrammeregulering og producenternes konkurrencevilkår kan indebære risiko for, at der gradvis afsættes færre ressourcer til beredskabsopgaver.

Koordineringen med myndighederne anses for væsentlig for beredskabet i krisesituationer. I dag anvendes hertil alene offentligt tilgængelige teletjenester. Det bør overvejes, om udviklingen indikerer et behov for særlig sikre telekommunikationsforbindelser.

7.2. Udviklingstendenser på naturgasområdet

Det danske naturgassystem er fuldt udbygget for så vidt angår det overordnede transmissionssystem. På det regionale plan sker der mindre udbygninger i lokalområder. Naturgassektoren er fortsat stærkt afhængig af en enkelt leverandør i Nordsøen. På kortere sigt forventes afhængigheden af denne leverandør gradvist at aftage som følge af liberaliseringen af naturgassektoren og deraf følgende stigende import af gas fra Tyskland (der vil fortsat være en fysisk nettoeksport). På længere sigt kan det forventes, at der kommer flere udlandsforbindelser, hvilket må forventes at medføre en større spredning af gastilførslen til Danmark og bevirke en yderligere styrkelse af forsyningssikkerheden.

Fra 1. januar 2004 gennemføres den fulde liberalisering af naturgassektoren. Dette vil medføre en voldsom forøgelse af brugen af internettjenester og dermed stigende afhængighed af disse tjenester. Svigt af disse tjenester vil kunne give væsentlige gener for gasbestilling, afregning, leverandørskift m.m., men selve gasforsyningen vil ikke umiddelbart blive berørt.

Liberaliseringen i naturgassektoren medfører opsplitning i mindre selskaber. Det stiller nye krav til koordinering af beredskabet i krisesituationer mellem de nye selskaber. Samtidig er der en risiko for, at der som følge af øget omkostningsbevidsthed afsættes færre ressourcer til beredskabsopgaver.

7.3. Udviklingstendenser på teleområdet

Udviklingstendenserne på teleområdet stiller store udfordringer til teleberedskabet fremover. Telemarkedet er et meget dynamisk marked, hvor særligt konkurrencesituationen og den teknologiske udvikling er med til at sætte farten.

Den teknologiske udvikling og fremkomsten af nye accessteknologier og nye typer af teletjenester, og i den forbindelse tendensen til konvergens mellem de elektroniske medier, gør det stadig mere vanskeligt at overskue de samlede teleressourcer og at lovgive på teleområdet. Denne udviklingstendens skaber blandt andet et behov for at integrere it- og teleberedskabet, som på længere sigt kun vanskeligt lader sig adskille. Konvergenstendensen må også antages at kunne medføre en øget sårbarhed efterhånden, som de forskellige teletjenester smelter sammen og fremføres i samme net, kontrolleres og styres fra samme enheder etc.

Den teknologiske udvikling kan generelt betyde flere valgmuligheder i forhold til telekommunikationsløsninger, hvilket er en styrke, men det betyder også, at man i forhold til f.eks. en lovgivningsindsats hele tiden skal være på forkant med udviklingen. Det betyder også, at det løbende bør overvejes, hvorledes nye teknologier kan anvendes til beredskabsmæssige formål.

Med liberaliseringen af teleområdet spiller markedsmekanismerne en afgørende rolle for udviklingen på området. Driftsstabilitet er også blevet et konkurrenceparameter. Men det er driftsstabilitet i dagligdagen, der konkurreres på. Der "regnes på" de nærliggende risici, beredskabet indrettes - naturligt nok - efter de mest sandsynlige trusler - i den henseende er f.eks. terrorangreb ifølge teleudbyderne ikke altid med i regnestykket. Når markedsmekanismerne styrer udviklingen, er det, der er gældende i dag, ikke nødvendigvis gældende i morgen.

Den sårbarhed i teleinfrastrukturen, der kan relateres til det beredskab, teleudbyderne har planlagt eller etableret ud fra kommercielle hensyn, kan på den baggrund være svær at følge over tid. Det er derfor vigtigt, at der gennem lovgivning sikres et vist minimumsniveau for teleberedskabet hos alle teleudbyderne.

En væsentlig udviklingstendens på telemarkedet er også den stigende globalisering. Teleudbyderne på det danske telemarked er i vid udstrækning udenlandsk ejet selskaber. Teleinfrastrukturen er i vidt omfang fortsat placeret inden for landets grænser, men stadig flere opgaver udføres fra moderselskaber m.v. i udlandet. Dette udgør en vis sårbarhed. Dels kan man forestille sig en konflikt mellem Danmark og det land, hvori udstyret er placeret eller hvorfra en opgave løses, dels en konflikt i det andet land, som Danmark ikke er involveret i, men som vil kunne ramme danske interesser. Selvom teleudbyder i forhold til sit udbud af telenet og teletjenester i Danmark vil være ansvarlig efter den danske lovgivning, er problemet dog, at der vil bestå en afhængighed af sikringsniveauet i det pågældende land.

En tendens på telemarkedet, hvis effekt ligner effekten af globaliseringstendensen, er teleudbydernes tendens til at outsource opgaver som f.eks. netovervågning og fejlretning af visse systemer til andre private virksomheder. Teleudbyderne vil i den situation fortsat bære ansvaret for de pågældende opgaver i forhold til kunderne og i forhold til efterlevelse af lovgivningen på teleområdet, men sikkerheden vil nu også afhænge af forholdene hos de virksomheder, hvortil opgaverne er outsourcet. Der vil desuden kunne indtræde forskellige interessekonflikter, f.eks. hvis der er knappe ressourcer i en virksomhed, som derfor må prioritere hvilke kunder, der skal betjenes. Der kan også opstå problemer, hvis en virksomhed, der udfører en opgave, er placeret i udlandet, jf. synspunkterne skitseret ovenfor i forbindelse med globaliseringstendensen.

Der ses endelig en tendens til centralisering i forhold til opgaver og placering af udstyr. Den teknologiske udvikling på teleområdet har betydet, at f.eks. styring og overvågning af net kan foregå centralt fra et kontrol- eller situationscenter, som herved vil være et oplagt mål for f.eks. terrorvirksomhed.

Udviklingstendenserne betyder navnlig, at det er meget vanskeligt at følge udviklingen i teleområdets sårbarhed. Sårbarheden er ikke statisk - og der kan for nærværende ikke foreslås egentlige redskaber til at følge denne udvikling. En mulig løsning med hensyn til at sikre et tidssvarende teleberedskab er dog også at fokusere på *ansvaret* for sikring af samfundsvigtig telekommunikation i beredskabssituationer.

Videnskabsministeriet og IT- og Telestyrelsen har, som det er beskrevet i afsnit 5.3.2, kompetence - et sektoransvar - i forhold til et nationalt teleberedskab og i den forbindelse for navnlig lovgivning og tilsyn på området. Teleudbyderne har et ansvar for et beredskab i forhold til dels en efterlevelse af lovgivningen, men også i forhold til kunderne. Men det er kunderne - f.eks. beredskabsmyndigheder m.fl. - der er nærmest til at klarlægge eget kommunikationsbehov, dels i forhold til en myndigheds funktion og konkrete opgaver, og dels i forhold til et særligt behov i en beredskabssituation. Den enkelte myndighed har et selvstændigt ansvar i medfør af beredskabsloven for et beredskab i relation til eget kommunikationsbehov - og myndighedens valg af telekommunikationsløsninger har betydning for sikringen af samfundsvigtig telekommunikation i forhold til myndighedens funktion i samfundet.

IT- og Telestyrelsens og Videnskabsministeriets indsats på teleberedskabsområdet har i det seneste årti været rettet mod teleudbyderne. Dette har været et naturligt fokusområde med liberaliseringsprocessen og tilkomsten af de mange nye teleudbydere. Det har været - og er stadig - en væsentlig opgave at sikre et beredskab hos disse teleudbydere. Der er dog behov for fremover at sætte myndighedernes individuelle ansvar for eget kommunikationsbehov i fokus. IT- og Telestyrelsen bør i den forbindelse vejlede myndighederne, hjælpe dem med at løfte dette ansvar, jf. afsnit 8.3. Herved sikres bedre en løbende vurdering af sårbarheder i forhold til myndighedernes eget beredskab. Og hvis myndighederne sætter sikkerhed i fokus ved f.eks. indkøb af teleydelser hos teleudbyderne, så efterspørgslen herfor med andre ord stiger, vil dette også kunne være med til at påvirke teleudbydernes interne sikringsniveau, foretaget af kommercielle hensyn.

7.4. Udviklingstendenser på it-området

På **it-området** er det en tydelig udviklingstendens, at den økonomiske omkostning ved at benytte internettet til transport af data er stadig faldende. Økonomiske omkostninger ved at opbygge lukkede net, og de ekstra omkostninger der er forbundet med at skulle udvikle egne programmer hertil gør, at der kan iagttages en konvergens mod at benytte internettet. De sikkerhedsproblemstillinger, der er forbundet med at benytte åbne net frem for lukkede net, er velkendte, og kan håndteres økonomisk på en sådan måde, at det stadig er billigere at benytte internettet. Samfundets generelle afhængighed af internettet vil derfor være stigende.

Den offentlige forvaltnings ønske om øget effektivitet gennem digitalisering af forvaltningen og samtidig åbne den kommunale forvaltning for digitale henvendelser 24 timer i døgnet, vil også stille store krav til den digitale forvaltnings robusthed mod it-sikkerhedshændelser. Et væsentligt aspekt af den digitale forvaltning er, at datasystemer i en myndighed i stigende omfang vil være afhængige af dataføde fra andre myndigheders datasystemer. Det må forventes, at den offentlige forvaltnings sårbarhed overfor it-sikkerhedshændelser vil stige efterhånden som integrationen mellem systemerne stiger.

På den teknologiske front vil vi indenfor de næste 10 år se nye teknologiervinde indpas i dagligdagen. Hvad vi kan se i dag er, at it bevæger sig ind i flere og flere dele af dagligdagen. Man kan måske forestille sig en fremtid, hvor tøjet bliver mere intelligent og kan fortælle vaskemaskinen hvor meget sæbe og vand, der skal bruges under vask, hvor legetøjet bliver mere intelligent og kan gøre opmærksom på, at det er blevet glemt og hvem det tilhører, og hvor selv kaffemaskinen indenfor en overskuelig fremtid vil kunne fungere som en webserver . I et sårbarhedsperspektiv fører denne udvikling af »it i alt«, blandet sammen med nye trådløse kommunikationsteknologier til, at f.eks. maskiner, pumper og lignede udstyr får et web-interface, hvor det er muligt at omkonfigurere udstyret. Disse "i-lagte" (embedded) computere kaldes på engelsk for *pervasive computing*, og de vil være sårbare over for hacking, virusangreb og alle andre velkendte trusler på it-området. Pervasive computing har endnu ikke realiserede anvendelsesmuligheder, og deraf endnu ikke erkendte sårbarheder.

8. Problemstillinger der bør belyses nærmere

I afsnit 8 beskrives først kort de problemstillinger inden for hver sektor, der bør belyses nærmere fremover - samt i den forbindelse fokusområder med forslag til en række konkrete initiativer. Herefter følger et afsnit med forslag om koordinering og samarbejde på tværs af sektorerne.

8.1. Elområdet

Der er kontinuert behov for fokus på de væsentligste områder af betydning for elsektorens beredskab. De seneste år har betydet en ændring af trusselsbilledet og for elsektoren bør det indebære en revurdering af de generelle beredskabskrav til sektoren. De systemansvarlige virksomheder har fokus på denne opgave, og har taget opgaven op i Danske Elselskabers Beredskabsudvalg. Myndighederne og de systemansvarlige virksomheder har således en opgave med at formulere, hvad der fremover vil være et rimeligt beredskabsniveau. I de seneste år er elsektoren liberaliseret, og det har medført store ændringer af opgaverne hos forskellige typer af elselskaber. Der er nu en øget omkostningsbevidsthed hos selskaberne, som kan få indflydelse på de ressourcer, som afsættes til beredskabsforhold.

Nogle af de mest aktuelle fokusområder for elsektoren er:

- En mere detaljeret undersøgelse af elselskabernes afhængighed af offentlige tele- og it-systemer samt af de offentlige systemers forventede driftsegenskaber og sårbarhed bl.a. ved svigt af elforsyning.
- En vurdering af behovet for at etablere adgangskontrol med alarmering i elsystemets stationer.
- En vurdering af behovet for fælles retningslinier for elselskabernes fremtidige beredskab.

8.2. Naturgasområdet

Der er kontinuert behov for fokus på de væsentlige områder af betydning for naturgassektorens beredskab. Nogle af de mest aktuelle fokusområder for naturgassektoren er:

- Transmissionssystemet blev etableret for ca. 20 år siden under hensyntagen til de daværende forhold og kendte planer. Siden da har transmissionsnettets udbygning og infrastruktur ændret sig. Det kan derfor være relevant at gennemføre en samlet vurdering af de kritiske dele af gasledningssystemet med henblik på reparationsforhold, metoder og tider.

- Der kan være anledning til at foretage en revurdering af behovet for udstyr og reparationsmetoder vedrørende offshore-rørledninger i de kystnære farvande.

- Revurdering af minimumskrav til nødstrømsforsyning af elsektorens produktions-, stations- og fjernkontrolanlæg

8.3. Teleområdet

Udviklingstendenserne på teleområdet betyder, at det bliver stadigt mere vanskeligt at følge udviklingen i sårbarhederne, som ikke er statiske. Også trusselsbilledet vil ændre sig over tid. Fokus bør rettes mod ikke kun teleudbyderne, men også mod de myndigheder, der har et særligt behov for telekommunikation i beredskabssituationer - deres sikringsbehov og mulighed for at tilvejebringe alternative kommunikationsløsninger, jf. afsnit 7.3. Myndighederne bør i den forbindelse f.eks. vejledes om udarbejdelse af en individuel kommunikationsplan.

Sikringsniveauet teleudbyderne imellem, hvad angår de sikringstiltag, udbyderne har etableret ud fra kommercielle hensyn, er generelt relativt forskelligt - dog overholder de alle de krav, der følger af lovgivningen. Bag valget af sikringsniveau ligger typisk en bevidst prioritering - en balance i forhold til henholdsvis sikring af driftsstabilitet og økonomi. Det betyder, at der er enkelte -

men væsentlige - sikringstiltag, der er nedprioriteret. Henset til, at sikringsniveauet også fremover må forventes at afhænge af udviklingen på telemarkedet og teleudbydernes kommercielle prioritering, bør det overvejes med udgangspunkt i den eksisterende lovgivning på området, jf. afsnit 5.4.1, at fastsætte krav til et minimumsniveau for sikring af netsikkerhed samt fysisk og logisk sikring af bygninger og installationer m.v. Et mere præcist niveau herfor forudsætter en politisk stillingtagen, men det vurderes på baggrund af denne udredning, at disse krav bør omfatte sikring mod hændelser i fredstid som f.eks. naturkatastrofer, utilsigtede hændelser og visse former for terrorangreb (f.eks. logiske angreb). For så vidt angår it-sikkerhed hos teleudbyderne kunne overvejes et krav om certificering af selskabets systemer og procedurer. Sådanne krav er ikke mindst vigtige i forhold til de nye udbydere, der løbende kommer til på telemarkedet.

Vedrørende den gældende lovgivning på teleberedskabsområdet er der behov for en ændring af bekendtgørelsen om sikring af offentlige telenet og teletjenester. Der bør således snarest muligt iværksættes et samarbejde med teleudbyderne med henblik på at undersøge mulighederne for sikring af mobiltelefoni, således at særligt udpegede abonnenter, som ved den gældende ordning for fastnetstelefoni, sikres en fortrinsstilling ved brug af tjenesten. For såvel mobiltelefoni som fastnets-telefoni bør det desuden undersøges, hvorvidt opkald kan prioritetsmarkeres i telenettene, således at man sikrer prioritet af opkald helt frem til modtager. Der er allerede iværksat en undersøgelse i IT- og Telestyrelsen af, hvorvidt det er teknisk muligt - og hensigtsmæssigt - at sikre digitale PABC'ere.

For så vidt angår teleudbydernes beredskabspligt efter bekendtgørelse om teleberedskabet, sikkerhedsgodkender IT- og Telestyrelsen løbende personel hos en række teleudbydere, og styrelsen er påbegyndt et arbejde med at etablere et beredskabsnetværk til teleudbyderne. Formålet med dette netværk er at kunne udveksle informationer med henblik på, at styrelsen kan prioritere teleressourcerne om nødvendigt i en beredskabssituation. Dette samarbejde med teleudbyderne bør styrkes. Styrelsen bør i den forbindelse f.eks. også vejlede teleud-

byderne om, hvorledes udbydernes beredskab bør indrettes i forhold til regler på området, det aktuelle trusselsbillede etc.

Som nævnt indledningsvis til afsnit 3.4, har fokus været på sikring af taletelefoni. Der er ikke foretaget en nærmere undersøgelse specifikt for så vidt angår teleudbydernes udbud af internet- og datatjenester. Undersøgelsen af teleudbydernes beredskab, jf. afsnit 5.4.3, omfatter i et vist omfang også disse tjenester, idet en større del af udbydernes sikringstiltag gælder alle tjenestetyper, og idet TDC, som har bidraget til denne udredning, også er langt den største udbyder af disse tjenester. Der er dog behov for specifikt at fokusere på sårbarhed og beredskab for disse tjenester. For det første fordi disse tjenester er helt afgørende for it-infrastrukten, og for det andet fordi disse tjenester er baseret på anden teknologi og delvist udbydes i andre typer net end taletelefonitjenesterne. En sådan undersøgelse vil indgå i en egentlig sårbarhedsvurdering på it-området, jf. afsnit 8.4.

Det bør endelig vurderes, i hvilket omfang it- og teleberedskabet fremover skal integreres. It og teleområdet er allerede tæt forbundet, idet den del af samfundets it-anvendelse, der er baseret på it-infrastrukturen, som den er defineret i afsnit 3.4, som nævnt i vid udstrækning er baseret på teletjenester hos teleudbyderne. Konvergenstendensen betyder desuden, at det bliver stadig mere vanskeligt at adskille it- og teletjenester.

Fokusområder på teleområdet er på den baggrund følgende:

- Udarbejdelse af vejledning om kommunikationsplan for beredskabsmyndigheder og andre med særligt behov for telekommunikation i en beredskabssituation
- Eventuelle krav til teleudbyderne ved bekendtgørelse om minimumsniveau for netsikkerhed samt fysisk og logisk sikring af bygninger og installationer m.v.
- Ændring af bekendtgørelse om sikring af offentlige telenet og teletjenester (undersøge mulighed for henholdsvis sikring af mobiltelefoni, prioritetsmarkering af opkald og sikring af digitale PABC'ere)

- Styrkelse af samarbejdet med teleudbyderne
- Integration af it- og teleberedskabet

8.4. It-området

It-anvendelse og elektronisk kommunikation indgår i drift og udvikling i alle sektorer i samfundet. Der er behov for et tværgående overblik over de it- og telerelaterede sårbarheder og trusler, samt de modforanstaltninger, der bør iværksættes ved hændelser i de enkelte sektorer, som kan have store tværgående konsekvenser for øvrige sektorer. Der er m.a.o. behov for en overordnet koordination, herunder at der kan rådgives om og påpeges mangler i de enkelte sektorers beredskabsplanlægning.

Der er i den forbindelse behov for en yderligere afklaring af kompetence og ansvarsfordeling vedrørende beredskabet på it-området. Den it-sektor ansvarlige myndighed bør have en generel koordinerende rolle i forhold til et nationalt it-beredskab. Det anbefales, at den koordinerende rolle som minimum indebærer ansvar for at udarbejde generelle vejledninger om planlægning, udarbejdelse, vedligeholdelse og gennemførelse af et internt it-beredskab og øvrige værktøjer til understøttelse af dette. Det anbefales derudover, at der udarbejdes tilstandsrapporter, der på it-området afdækker afhængigheder mellem sektorer, og som bør udarbejdes således, at alle sektorer behandles over en fastsat periode.

Ved etablering af denne funktion, kan det overvejes at gøre som i Sverige eller USA, hvor en integreret og tværgående it- og teleberedskabsplanlægning bl.a. skal tage højde for ændringer i det generelle trusselsbillede og stigende konvergens på it- og teleområdet.

Der bør indledningsvis udarbejdes en egentlig identificering af samfundskritiske it-systemer og efterfølgende en sårbarhedsvurdering af disse.

Fokusområder på it-området er på den baggrund følgende:

- Igangsættelse af en analyse af sårbarheder på it-området som beskrevet i afsnit 3.4
- Udarbejdelse af en beskrivelse af den koordinerende myndigheds rolle og mandat på it-beredskabsområdet
- Integration af it- og teleberedskabet, jf. pkt. 8.3

Videnskabsministeriet har som tidligere nævnt igangsat et projekt, hvis overordnede mål er at fastlægge en myndighedsstruktur på it-beredskabsområdet - herunder at kortlægge en organisering af et nationalt it-beredskab. Projektet tager udgangspunkt i en placering af ansvaret for koordinering af it-beredskabet i Videnskabsministeriet ved IT- og Telestyrelsen.

8.5. Koordinering og samarbejde på tværs af sektorer

Arbejdet i forbindelse med denne udredning har vist, at der er et behov for et vist samarbejde på tværs af sektorerne i underudvalget. De enkelte sektorer er i vidt omfang afhængige af forsyningsvirksomheden i de øvrige sektorer og dermed også af beredskabet i sektorerne. Et større eller længerevarende nedbrud i en eller flere af sektorerne vil potentielt kunne føre til større forsyningssvigt i de øvrige sektorer, hvorved der kan være risiko for en slags dominoeffekt, som vil kunne forstærke konsekvenserne for samfundets øvrige sektorer og potentielt øge forsyningssektorernes problemer.

Fokusområder for et videre samarbejde fremover sektorerne imellem er på den baggrund følgende:

- Regelmæssig opdatering af vurderingerne af de indbyrdes afhængigheder sektorerne imellem og sårbarheder relateret hertil
- Regelmæssig drøftelse om sårbarheder og beredskabsforhold vedrørende de indbyrdes afhængigheder sektorerne imellem

- Generel erfaringsudveksling om beredskabsforhold - herunder vedrørende beredskabet inden for egen sektor