GRUNDNOTAT

om

Forslag til Rådets direktiv om indkredsning og klassificering af europæisk kritisk infrastruktur og vurdering af behovet for at beskytte dem

"EPCIP-forslaget" af 12. december 2006

KOM(2006)787

samt

Meddelelse fra Kommissionen om et europæisk program for beskyttelse af kritisk infrastruktur (EPCIP) af 12. december 2006

KOM(2006)786

1. Resumé

Kommissionen blev af Det Europæiske Råd i juni 2004 anmodet om at udsende et program for beskyttelse af kritisk infrastruktur (EPCIP) med baggrund i terroranslagene i Madrid marts 2004. Rådet gentog ønsket om et EPCIP-program i rådskonklusionerne fra den 16. – 17. december 2004 samt i EU's reviderede handlingsplan vedrørende indsatsen mod terrorisme af 10. juni 2005, og endvidere på rådsmødet (retlige og indre anliggender) den 1. – 2. december 2005. Kommissionen udsendte i november 2005 en grønbog vedrørende EPCIP. Den 12. december 2006 udsendte Kommissionen et forslag til direktiv og en meddelelse om EPCIP.

Meddelelsen beskriver rammerne for det samlede EPCIP-program, mens direktivet konkret fastlægger en procedure for udpegning af europæisk kritisk infrastruktur. Proceduren indebærer, at der via komitologi (beslutningsprocedure under Kommissionen) fastlægges sektorvise kriterier for udpegning af europæisk kritisk infrastruktur. Herefter indberetter medlemslandene til Kommissionen, hvilke infrastrukturer der opfylder kriterierne. Endelig vedtages en liste over europæisk kritisk infrastruktur ved komitologi-procedure. Operatører af europæisk kritisk infrastruktur skal udarbejde en sikkerhedsplan for operatører og udpege en sikkerhedsforbindelsesofficer. Medlemsstaterne skal herefter udarbejde risiko- og sårbarhedsvurderinger for sektorerne for europæisk kritisk infrastruktur.

Det fremgår af meddelelsen, at EPCIP udover proceduren for udpegning af europæisk kritisk infrastruktur blandt andet også omfatter informations- og varslingsnetværket vedrørende kritisk infrastruktur (CIWIN: Critical Infrastructure Warning Information Network), ekspertgrupper, identifikation af indbyrdes afhængigheder, fremme af nationale programmer for kritisk infrastrukturbeskyttelse, udvikling af en fælles tilgang til beredskabsplanlægning, en ydre dimension samt ledsagende finansielle tiltag.

Fra dansk side kan man støtte det overordnede mål om at sikre en forsvarlig beskyttelse af kritisk infrastruktur i Europa og bestræbelserne på at etablere et EPCIP-program.

2. Baggrund

Det Europæiske Råd anmodede i juni 2004 Kommissionen og den Højtstående Repræsentant om at udforme en overordnet strategi til beskyttelse af kritisk infrastruktur i Europa.

Kommissionen vedtog den 20. oktober 2004 en meddelelse vedrørende beskyttelse af kritisk infrastruktur i indsatsen mod terrorisme (KOM(2004)702). Meddelelsen indeholder forslag til, hvordan EU kan forbedre beredskabet bl.a. i forbindelse med terrorangreb, der påvirker kritisk infrastruktur, og den foreslår et program om europæisk kritisk infrastruktur beskyttelse (EPCIP) samt etablering af et informations- og varslingsnetværk vedrørende kritisk infrastruktur (CIWIN).

Rådet gentog ønsket om et EPCIP-program i EU's reviderede handlingsplan af 10. juni 2005 vedrørende indsatsen mod terrorisme, efter terrorangrebene i London den 7. juli 2005, samt på rådsmødet (retlige og indre anliggender) den 1. – 2. december 2005.

Rådskonklusionerne fra den 1. – 2. december 2005 slår bl.a. fast, at beskyttelse af kritisk infrastruktur er medlemsstaternes ansvar, at initiativer på EU-niveau skal respektere nærhedsprincippet, og at udgangspunktet for programmet bør være en "all hazards approach", dvs. alle typer af hændelser, med særligt fokus på terrorisme. Det konkluderes endvidere, at kritisk infrastrukturbeskyttelse i EU skal fremmes ved at styrke medlemsstaternes mulighed for at identificere og beskytte national kritisk infrastruktur, samt at den private sektor involveres aktivt.

Som forberedelse til udarbejdelsen af programmet udsendte Kommissionen den 17. november 2005 en grønbog om EPCIP. Derudover afholdt Kommissionen tre seminarer for repræsentanter for medlemsstaterne og den private sektor, samt uformelle møder med medlemsstaternes kontaktpersoner for kritisk infrastruktur og med repræsentanter for den private sektor (Telekommunikationsindustrien og Dansk Industri).

Kommissionen udsendte den 12. december 2006 "Forslag til Rådets direktiv om indkredsning og klassificering af europæisk kritisk infrastruktur og vurdering af behovet for at beskytte den" (KOM(2006)787) og "Meddelelse fra Kommissionen om et europæisk program for beskyttelse af kritisk infrastruktur" (KOM(2006)786).

3. Hjemmelsgrundlag

Direktivforslagets hjemmel er EF-traktatens artikel 308, der forudsætter, at forslaget vedtages efter indhentet udtalelse fra Europa-Parlamentet med enstemmighed i Rådet. Endvidere henvises der i direktivforslaget til EURATOM, herunder artikel 203.

4. Nærhedsprincippet

Kommissionen har anført følgende vedrørende nærhedsprincippet i forhold til direktivet:

"Subsidiaritetsprincippet er respekteret, da de foranstaltninger, der træffes via dette forslag, ikke kan gennemføres af nogen enkelt medlemsstat og derfor bedre kan træffes på EU-plan. Selv om det er den enkelte medlemsstats ansvar at beskytte kritisk infrastruktur inden for dens jurisdiktion, er det vigtigt for EU's sikkerhed at sikre, at infrastruktur, hvis afbrydelse eller ødelæggelse kan have konsekvenser i to eller flere medlemsstater eller i en enkelt medlemsstat, hvis den kritiske infrastruktur er beliggende i en anden medlemsstat, er tilstrækkeligt beskyttet, og at en eller flere medlemsstater ikke gøres sårbare som følge af svagheder eller lave sikkerhedsstandarder i andre medlemsstater. Lignende regler vedrørende sikkerhed ville også være med til at sikre, at konkurrencereglerne på det indre marked ikke forvrides."

Regeringen lægger i sin vurdering af overholdelsen af nærhedsprincippet vægt på, at det overordnede ansvar for at beskytte kritisk infrastruktur inden for medlemsstaternes jurisdiktion forsat påhviler medlemsstaterne samt ejere og operatører af kritisk infrastruktur, også i forhold til den kritiske infrastruktur, som efter procedurerne i direktivet klassificeres som europæisk kritisk infrastruktur.

Kommissionens forslag til direktiv sigter på de dele af den kritiske infrastruktur, som vil kunne betegnes som "europæisk kritisk infrastruktur", dvs. de aktiver eller dele deraf, der er væsentlige for opretholdelsen af kritiske samfundsmæssige funktioner, herunder forsyningskæden og menneskers sundhed, sikkerhed og økonomisk eller social velfærd på europæisk niveau. Det er derfor vigtigt, at der anvendes gennemsigtige og ensartede metoder til at identificere kritisk infrastruktur på europæisk niveau.

Regeringen finder på det foreliggende grundlag, at direktivforslaget vil bidrage til at sikre, at medlemsstaterne fremover vil have en mere ensartet tilgang til beskyttelse af kritisk infrastruktur, der har betydning på det europæiske niveau. Det er regeringens målsætning at undgå, at sårbarheder i en medlemsstat medfører omfattende konsekvenser for andre medlemsstater. Regeringen vurderer, at dette mål mest hensigtsmæssigt kan opnås ved en koordineret indsats på europæisk plan.

Regeringens vurdering er på dette grundlag, at direktivforslaget ikke strider mod nærhedsprincippet.

Spørgsmålet om nærhedsprincippet er ikke relevant i forhold til meddelelsen.

5. Formål og indhold

Kommissionen har præsenteret en meddelelse om et europæisk program for kritisk infrastrukturbeskyttelse sammen med et direktivforslag om identifikation af europæisk kritisk infrastruktur. Meddelelsen beskriver rammerne for det samlede arbejde med beskyttelse af europæisk kritisk infrastruktur, mens direktivet konkret fastlægger metoden for udpegning af europæisk kritisk infrastruktur.

EPCIP-programmets generelle mål er at forbedre beskyttelsen af kritisk infrastruktur i EU gennem udformning af rammer på EU-plan. Programmet sigter på at beskytte kritisk infrastruktur i EU i forhold til alle former for farer, med prioriteret fokus på terror.

Meddelelsen beskriver de overordnede rammer i seks punkter:

- En procedure for udpegning af europæisk kritisk infrastruktur. Proceduren fastlægges i direktivet, som beskrives nedenfor.
- Foranstaltninger med henblik på at lette gennemførelsen af programmet, herunder en EPCIP handlingsplan (en tidsplan for gennemførelsen af EPCIP), et kommunikationsnetværk vedrørende kritisk infrastruktur (CIWIN), anvendelse af ekspertgrupper, procedurer for deling af oplysning om beskyttelse af kritisk infrastruktur samt analyse af indbyrdes afhængigheder.
- Støtte til medlemsstaterne vedrørende national kritisk infrastruktur. Hver medlemsstat opfordres til at udarbejde et nationalt program for beskyttelse af national kritisk infrastruktur, og meddelelsen opstiller en række spørgsmål, som et nationalt program kan tage op.
- Beredskabsplaner – herunder udarbejdelse af en sammenhængende strategi for udarbejdelse af beredskabsplaner.

- En ekstern dimension i form af et øget samarbejde ud over EU's grænser om beskyttelse af kritisk infrastruktur.
- Ledsagende finansielle foranstaltninger, navnlig programmet om forebyggelse, beredskab og konsekvensstyring i forbindelse med terrorisme og andre sikkerhedsrelaterede risici for perioden 2007-2013.

Bortset fra proceduren for udpegning af europæisk kritisk infrastruktur er tiltagene frivillige for medlemslandene.

Direktivet om udpegning af europæisk kritisk infrastruktur skal sikre:

- Forsvarlige beskyttelsesniveauer for europæisk kritisk infrastruktur.
- At alle parter i europæisk kritisk infrastruktur er underlagt de samme rettigheder og pligter.
- At stabiliteten i det indre marked er opretholdt.

Europæisk kritisk infrastruktur defineres som infrastruktur, hvis afbrydelse eller ødelæggelse vil påvirke to eller flere medlemsstater eller en enkelt medlemsstat, hvis den pågældende infrastruktur er placeret i en anden medlemsstat.

Der eksisterer pt. i EU ingen foranstaltninger på tværs af sektorerne, om end der eksisterer en række forholdsregler på EU-niveau indenfor IT-sektoren, sundhedssektoren, den finansielle sektor, transportsektoren, den kemiske sektor samt den nukleare sektor.

Direktivet fastlægger, at Kommissionen i samarbejde med medlemsstaterne udvikler sektoropdelte og tværgående kriterier for identifikation af europæisk kritisk infrastruktur ud fra konsekvenserne af en ødelæggelse eller afbrydelse af en given infrastruktur. Det foreslås, at konsekvenserne skal vurderes ud fra størrelsen af befolkningen som påvirkes samt økonomiske, miljømæssige, politiske og psykologiske virkninger samt følger for folkesundheden.

Direktivet pålægger hver medlemsstat at identificere infrastruktur som opfylder kriterierne, og informere Kommissionen om disse. Herefter udarbejder Kommissionen et udkast til en liste over europæisk kritisk infrastruktur, som vedtages gennem komitologi-procedure. Arbejdet bygger på en liste over kritisk infrastruktur-sektorer, som findes i et bilag til direktivet. Listen kan revideres gennem komitologi-procedure.

Medlemsstaterne skal sikre at ejere/operatører af europæisk kritisk infrastruktur udarbejder en sikkerhedsplan for operatører (Operator Security Plan – OSP), som identificerer ejere og operatørers vigtige aktiver og etablerer relevante sikkerhedsløsninger for deres beskyttelse. Direktivet fastsætter en minimumsstandard for indholdet i en sikkerhedsplan for operatører. Sikkerhedsplanerne skal indsendes til medlemsstaten, som udarbejder generelle risiko- og sårbarhedsanalyser for hver sektor. Derudover skal ejere/operatører af kritisk infrastruktur udpege en sikkerhedsforbindelsesofficer, som skal være kontaktled til medlemsstaten for al information vedrørende beskyttelse af kritisk infrastruktur.

6. Europa-Parlamentets udtalelser

Europa-Parlamentet skal udtale sig om direktivforslaget i henhold til traktatens artikel 308. Der foreligger endnu ingen udtalelse fra Europa-Parlamentet.

7. Gældende dansk ret og forslagets konsekvenser herfor

Ansvaret for kritisk infrastrukturbeskyttelse i Danmark følger af sektoransvarsprincippet, jf. beredskabsloven § 24; "De enkelte ministre skal inden for deres område planlægge for opretholdelse og videreførelse af samfundets funktioner i tilfælde af ulykker og katastrofer (...)."

Ministerierne skal sørge for, at den nødvendige lovgivning, bekendtgørelser m.m. tilvejebringes i ressortlovgivningen. Regulering i ressortlovgivningen kan ske enten som en specifik beredskabsmæssig lovgivning eller som led i den almindelige lovgivning.

Beredskabskrav til operatører af kritisk infrastruktur kan blandt andet findes i:

- Havnesikringsbekendtgørelsen
- Elforsyningslovens § 85 b
- Naturgasforsyningslovens § 15 a
- Varmeforsyningslovens § 29 a
- Lov om pligtige lagre af mineralolie og mineralolieprodukter § 5 a
- Offshoresikkerhedslovens § 45, stk. 4-5
- Fødevarelovens § 59
- Sundhedsloven §§ 210-211
- Lov om konkurrence og forbrugerforhold på telemarkedet § 86

Vedtagelse af direktivforslaget vil medføre, at Danmark skal sikre dækkende lovgivning, som fastlægger, at operatører af europæisk kritisk infrastruktur skal udarbejde en sikkerhedsplan for operatører som opfylder kravene i direktivet, samt at operatører af europæisk kritisk infrastruktur skal udpege en sikkerhedsforbindelsesofficer.

Det er vurderingen, at implementeringen af Kommissionens forslag til direktiv vil kræve ændringer i dansk ret.

Det vurderes, at kravet om lovgivning kan opfyldes ved, at relevante bestemmelser indføjes i eksisterende sektorlovgivning eller ved at der indføres særskilt lovgivning om europæisk kritisk infrastruktur.

8. Forslagets konsekvenser for statsfinanserne, samfundsøkonomien, miljøet og beskyttelsesniveauet

Direktivforslaget vil forpligte den danske stat til at identificere europæisk kritisk infrastruktur i Danmark samt kritisk infrastruktur i udlandet, hvis afbrydelse eller ødelæggelse vil have væsentlige konsekvenser for Danmark. EPCIP vil medføre en række nye opgaver, hvor det er vanskeligt på det nuværende grundlag at vurdere, hvor omfattende opgaven vil være. Disse opgaver vil involvere alle myndigheder med ansvar for kritisk infrastruktur. Opgavens karakter og omfang vil afhænge af de kriterier, der skal vedtages for at udpege europæisk kritisk infrastruktur. Dertil kommer, at arbejdet med den øvrige nationale kritiske infrastruktur må ventes påvirket af det arbejde, som udgøres af den europæiske kritiske infrastruktur.

Det er ligeledes vanskeligt at vurdere, hvor omfattende dette arbejde vil være og tilsvarende gælder arbejdet med at udarbejde risiko- og trusselsvurderinger for hver af sektorerne for europæisk kritisk infrastruktur i Danmark, herunder i hvilket omfang der er tale om udvidelser i forhold til det arbejde, der allerede gennemføres i dag.

Kravet i direktivforslaget om, at operatører af europæisk kritisk infrastruktur skal implementere en sikkerhedsplan for operatører, kan pålægge de udpegede virksomheder yderligere arbejdsopgaver. Kravet kan derfor betyde, at disse operatører pålægges særskilte udgifter, dog afhængigt af i hvilket omfang de opstillede krav reelt indebærer ændrede og øgede opgaver i forhold til det sikkerhedsarbejde, som operatørerne udfører i dag.

De potentielle økonomiske og administrative byrder for operatørerne mindskes, hvis direktivforslaget ændres, så kravene til sikkerhedsplaner kan opfyldes ved at tilføje de nødvendige elementer til allerede eksisterende beredskabs- og sikkerhedsplaner. Der vil i sektorerne være forskel på, i hvor høj grad enkelte elementer i sikkerhedsplanen er omfattet af eksisterende sektorspecifikke krav, og dermed hvor store ekstra byrder kravet om en sikkerhedsplan for operatører vil kunne indebære.

Forslaget indebærer ikke i sig selv væsentlige udgifter på EU's budget, men det er forudsat, at der kan opnås EU-tilskud fra programmet "Forebyggelse, beredskabs og konsekvenshåndtering i forbindelse med terrorisme og andre sikkerhedsrelaterede risici", der har en samlet bevilling på 137,5 mio. EUR i perioden 2007-2013. Danmark betaler 2% af EU's udgifter. Programmet kan ikke (med)finansiere egentlige investeringer i hardware og udstyr, men blandt andet tiltag til fremme af risikovurderinger, evalueringer med hensyn på identificering af trusler m.v., udvikling af minimumstandarder og værktøjer, risikoanalyser, samt udgifter vedrørende samarbejde og udvikling af bedste praksis.

9. Høring

Direktivforslaget og meddelelsen er sendt i høring i EU Specialudvalget på Civilbeskyttelsesområdet m.fl. den 10. januar 2007 med tidsfrist for bemærkninger den 24. januar 2007.

Bemærkninger fra interesseorganisationer m.fl.

Naviair anfører, at direktivforslagets artikel 5 om sikkerhedsplaner og håndteringen af disse, herunder etablering af et overvågningssystem til feedback/kontrol af operatører af kritisk infrastruktur, giver stor risiko for dobbeltarbejde, i og med at de fleste relevante virksomheder allerede har udarbejdet specifikke beredskabsplaner, og som meget vel kan være mere detaljerede end det, der foreskrives i direktivforslaget.

Herudover finder Naviair, at de enkelte operatører er de nærmeste til at vide, hvilke elementer, der skal indeholdes i en beredskabsplan, og det bør derfor være tilstrækkeligt, såfremt det af et givet direktiv på området fremgår, at operatørerne skal sikre, at elementerne i sikkerhedsplanen er til stede.

Endvidere er lufttrafiktjeneste området allerede omfattet af de såkaldte Common Requirement, som er en del af EU's Single European Sky regelsæt. Det fremgår heraf, at der skal udarbejdes nødplaner for alle de tjenester, som den pågældende virksomhed udøver, i tilfælde af, at der indtræder begivenheder, som fører til væsentlig forringelse eller afbrydelse af den pågældendes tjenester. Common Requirements giver ikke detaljerede regler for, hvordan beredskabsplaner skal udarbejdes, og hvad de nærmere skal indeholde, men reglerne skal sikre, at planerne foreligger.

Hvorvidt der skal udpeges en sikkerhedforbindelsessofficer bør være den enkelte operatørs eget valg, og ikke noget, der fremgår af direktivet.

Til indberetningskravet i artikel 7 anfører Naviair, at også i henhold til Common Requirements er lufttrafiktjenesteudbyderne forpligtet til at oprette et Security Management System, der bl.a. skal indeholde procedurer for risikovurderinger, korrigerende tiltag og registreringer af uregelmæssigheder. Såfremt der med EPCIP direktivet indføres krav om endnu et system,

hvorefter der skal udarbejdes risiko- og sårbarhedsanalyser, eventuelt efter en fælles EU-metode, vil dette pålægge en lufttrafiktjenesteudbyder en yderligere byrde, i fald en konkret tjeneste udpeges som kritisk europæisk infrastruktur. Dette vil betyde flere administrative byrder for de berørte virksomheder.

Post Danmark har noteret, at postområdet er faldet ud i det fremlagte direktivforslag som et relevant område, hvorefter hele området Civil Administration er fjernet, hvilket tidligere indgik i grønbogen om kritisk infrastrukturbeskyttelse.

Sund & Bælt anfører, at det er uhyre vigtigt, at kriterierne for identifikation af europæisk kritisk infrastruktur på transportområdet bliver fastlagt, inden arbejdet med EPCIP i øvrigt kommer for langt. Det påpeges, at bl.a. alternative transportmuligheder har indflydelse på, om en given infrastruktur kan anses for kritisk, og analyse af dette bør derfor være en af de forudsætninger, der skal være opfyldt, før kritisk infrastruktur kan udpeges.

Det påpeges, at der som regel pågår omfattende risikoanalyser i forbindelse med infrastrukturanlæg, særligt i relation til trusler som naturkatastrofer og andre ulykkesårsager. Sådanne analyser fastlægger et passende sikkerhedsniveau for anlæggene. Uanset, at terrortrusler i sin natur ikke kan underkastes tilsvarende risikoanalyser, så er der på Storebæltsforbindelsen etableret nogle grundlæggende beskyttelsesforanstaltninger, som kan suppleres med en række graduerede sikringstiltag, der kan iværksættes i takt med at terrortruslen identificeres og gradvist øges. Dette princip bør også være bærende på europæisk plan, da permanente sikringsforanstaltninger overfor terror bør holdes på et passende lavt niveau for at undgå omfattende etablerings- og driftsudgifter til foranstaltninger, der ikke afspejler en reel terrortrussel.

Sund & Bælt finder, at det er vigtigt at få slået fast, at handlingsplaner for beskyttelse mod terror er af særdeles fortrolig karakter. Dette betyder dog ikke, at der ikke indenfor transportområdet kan være behov blandt de sikringsansvarlige operatører for at etablere en generel erfaringsudveksling om principper og metoder. Dette sker allerede i dag i nogen udstrækning, men Sund & Bælt kan støtte en egentlig platform, der på en sikker måde kan anvendes til udveksling af bedste praksis.

Vedrørende de ikke-bindende foranstaltninger, indkredsning og analyse af den indbyrdes afhængighed, bemærker Sund & Bælt, at en sådan analyse skal baseres på et åbent og konstruktivt samarbejde mellem de berørte parter i forhold til den kritiske transportinfrastruktur. Afhængigt af kriterierne for udpegning af kritisk transportinfrastruktur, kan opgaven gøres meget stor, og det er derfor vigtigt, at der sikres en top-down proces, således at analysen kun beskæftiger sig med de allermest væsentlige elementer.

For så vidt angår ledsagedokumentets bemærkninger om sårbarheds-, trussels- og risikovurderinger i forbindelse med europæisk kritisk infrastruktur, bemærker Sund & Bælt, at det er væsentligt, at der er metodefrihed til at gennemføre sådanne analyser, idet der kan være knyttet særdeles mange ressourcer til gennemførelse af den slags analyser. Trusselsvurdering er i den forbindelse et separat emne, som Sund & Bælt går ud fra bliver håndteret i PET-regi.

Øresundsbron finder, at det er fornuftigt og hensigtsmæssigt, at der forefindes ensartede retningslinier for beskyttelse af og beredskab for kritisk infrastruktur. Fælles retningsliner i form af Operator Security Plans eller lignende vil på sigt sikre en form for "best practice" for beskyttelse og beredskab i forbindelse med europæisk kritisk infrastruktur.

Det er til gengæld vigtigt, at der er metodefrihed ved gennemførelse af sårbarheds-, trussels- og risikovurderinger, samt ved udarbejdelse af Operator Security Plans, så allerede eksisterende og omfattende vurderinger, beregninger og planer kan anvendes. Ved udpegning af kontaktpunkt og sikkerhedsforbindelsesofficer antager Øresundsbron, at Kommissionen her

tager andre EU-regelsæt med tilsvarende krav i betragtning, således at der ikke dannes unødvendigt stort bureaukrati i de enkelte medlemsstater.

Øresundsbron påpeger, at direktivforslaget giver Kommissionen mulighed for at kræve specifikke beskyttelsesforanstaltninger for europæisk kritisk infrastruktur, og dette kan betyde, at udpeget infrastruktur kan blive belastet med betydelige økonomiske omkostninger, som meget vel kan andrage to cifrede millionbeløb. Øresundsbron forudsætter derfor, at der i EU-regi eller på nationalt plan afsættes særlige midler til dækning af sådanne omkostninger, således at en eventuel udpegning af Øresundsbron som europæisk kritisk infrastruktur ikke får økonomiske følger for selskabet.

Øresundsbron påpeger det vigtige i, at selskabet selv får indflydelse i forbindelse med en eventuel fremtidig udpegningsproces.

DONG Energy bemærker, at meget allerede er på plads, idet beredskabsloven, den nationale beredskabsplan og de to beredskabsbekendtgørelser fra Energistyrelsen dækker meget. Udfordringen bliver at gennemføre analyserne af, hvad der er kritisk infrastruktur. Sårbarhedsvurderingerne på udvalgte anlæg bør nok gennemføres i et tættere samarbejde mellem aktørerne, end det til nu har været tilfældet. Direktivforslaget indeholder nogle fornuftige bestemmelser omkring videnbeskyttelse og sikkerhedsgodkendelse. Det kunne pege på, at der måske bør tages et initiativ til at vurdere på behovet for at sikkerhedsgodkende nøgledeltagere i processerne.

Oliebranchens Fællesrepræsentation (OFR) finder det hensigtsmæssigt, at der udarbejdes en overordnet ramme for sikring af europæisk kritisk infrastruktur i relation til energiområdet. OFR kan derfor støtte Kommissionens forslag til program for beskyttelse af kritisk infrastruktur. Det påpeges, at det må sikres, at der ikke pålægges unødige byrder på operatøren af den omhandlende kritiske infrastruktur.

North Sea Operators Committee - Denmark (NSOC-D) finder at EPCIP alene bør omfatte terrortrusler, da der allerede eksisterer lovgivning og beredskabsplanlægning for de andre typer af hændelser, som pålægges politiet og redningsberedskabet. Ejere/operatører bør fortsætte med at bidrage til at identificere kritisk infrastruktur, og om nødvendigt at opstille kriterier for beskyttelsesforanstaltninger.

Dansk Erhverv

Den af Kommissionen foreslåede fremgangsmåde til at løse de konkrete sikkerhedsspørgsmål på infrastrukturområdet er atypisk, idet man ikke i EU systemet umiddelbart har mulighed for at iværksætte et samarbejde/arbejde, der de facto svarer til en efterretningstjenestes. Dansk Erhverv rejser derfor overordnet tvivl om selve den foreslåede proces til indkredsning og klassificering af europæisk kritisk infrastruktur.

Den foreslåede fremgangsmåde er den samme som et almindeligt kommissionsforslag til lovgivning. Det vil sige en politisk proces, hvor resultatet afhænger af politisk enighed. Identifikationen af udsatte mål foretages således ikke af eksperter i sikkerhed, der kan udarbejde den mest optimale sikkerhedsløsning, men derimod politikere som søger en politisk løsning.

Dansk Erhverv finder det endvidere væsentligt at skelne mellem, hvorvidt der er tale om sikring imod terror eller sikring imod naturkatastrofer eller lignende. Konsekvenserne kan være de samme, men der stor forskel på risiko og sikringsforanstaltninger.

For så vidt angår terrorangreb foretages den forudgående risikovurdering bedst i de nationale efterretningstjenester og det er afgørende vigtigt for funktionen af disse tjenester, at de har adgang til et intensivt internationalt samarbejde med deres søsterorganisationer i andre lande også ud over EU's grænser.

Efterretningstjenesternes primære funktion på dette område er at opdage og optrevle eventuelle terrorangreb før de finder sted. På den baggrund er det helt afgørende for Dansk Erhverv, at tjenesternes effektivitet og interoperabilitet som absolut mindstemål bibeholdes og helst forbedres ved ethvert tiltag på området.

Der findes allerede internationalt samarbejde både på efterretningsområdet og på området for naturkatastrofer. Dansk Erhverv afholder sig fra at vurdere, om samarbejdet er tilstrækkeligt og effektivt nok, men henleder opmærksomheden på, at en evt. oprettelse af et europæisk agentur for infrastruktursikring, der fungerer sideordnet med disse systemer hverken vil være hensigtsmæssigt eller effektivt.

Dansk Erhverv påpeger, at koordination og integration mellem sikkerhedsinitiativer er helt afgørende for deres samlede effektivitet. Dansk Erhverv anser sikring og afholdelse af omkostninger til sikring som en myndighedsopgave. Selvfølgelig skal erhvervet inddrages, men der må ikke blive tale om, at der sker en udlicitering af ansvaret for rigets sikkerhed.

Endelig finder Dansk Erhverv, at man ved udarbejdelse af dette og lignende forslag helt overordnet gør sig klart, at man ikke kan skabe et samfund helt uden risici. Terror har netop til formål at sætte samfundet i stå. Opbygning af komplicerede sikkerhedssystemer kan netop bremse et samfund – dels som følge af den økonomiske byrde systemet medfører og dels som følge af de administrative og praktiske besværligheder det kan medføre.

Dansk Erhverv finder det positivt, at man forsøger, at harmonisere nationale regler for kritiske infrastruktur. Dette kan forhåbentlig sætte nationale myndigheder i stand til at samarbejde bedre med forenkling og ressourcebesparelser som resultat. Endvidere er det positivt, at det anerkendes, at kritisk infrastruktur har en transeuropæisk dimension.

Ligeledes findes det positivt, at EU med forslaget fokuserer på infrastruktur snarere end operatører, der anvender infrastrukturen. Det foreliggende forslag om terrorsikring i transportkæden har vist, hvor vanskeligt og omkostningstungt det vil være at etablere et system, der skal dække alle operatører i transportkæden. Det synes umiddelbart mere omkostningseffektivt at rette indsatsen mod den del af infrastrukturen, der er kritisk. Dermed omfattes også den del af de relevante parter, der er af kritisk betydning for kædens fortsatte funktion og retablering.

Dansk Erhverv finder dog, at det foreliggende forslag ikke tager stilling til en række konkrete spørgsmål:

Definitionen af infrastruktur er meget bred og kan omfatte ukonkrete begreber såsom "transportkæden". Dermed er der risiko for, at forslaget reelt ender med at være en detailregulering af transportkæden og omfatter både, hvad man traditionelt vil opfatte som infrastruktur (vej, broer, jernbane) og andre elementer, der indgår i transportkædens funktion: lagerhaller, omladningsstationer, garager, overvågningssystemer m.v.

Denne problemstilling får yderligere relevans i lyset af, at forslaget synes at lægge op til, at myndigheder fastsætter, hvad der er kritiske infrastruktur og hvilken sikkerhedsplan, der skal laves for den pågældende infrastruktur.

Men forslaget er tavst om hvilke forhold, der gør sig gældende, når der er tale om infrastruktur, der for eksempel er privatejet. I tilfælde af koncessioneret ejendom - motorveje, betalingsbroer med videre - kan der formentlig findes løsninger, men i tilfælde af, at et privatejet lageranlæg, transitanlæg eller lignende defineres som kritisk infrastruktur og dermed pålægges at skulle lave en sikkerhedsplan, er situationen en anden. Forslaget har end ikke sikret ejeren af dette anlæg ret til at blive inddraget i beslutningen, ligesom forslaget ikke tager stilling til eventuelle spørgsmål om kompensation, ansvar med videre. Endelig risikerer forslaget

ved denne fremgangsmåde at skabe konkurrenceforvridning mellem private operatører, hvor nogle belastes mere end andre af byrder, der har fælles gavn.

Et positivt element er, at forslaget entydigt pålægger medlemsstaterne at udføre en risiko- og trusselsvurdering. Det er Dansk Erhvervs generelle opfattelse, at opgaver som risiko- og trusselsvurdering kræver en indsigt og viden som kun offentlige myndigheder kan have. Risiko- og trusselsvurderinger er derfor efter vores opfattelse klart en myndighedsopgave. Det er endvidere vigtigt at fremhæve, at myndigheders ansvar rækker videre, da sikkerhed i sidste ende er en samfundsopgave.

Endelig udtrykker Dansk Erhverv en vis bekymring i forbindelse med den kompetence, som forslaget synes at tillægge Kommissionen i relation til kontrol og opsyn med de konkrete opgaver. Der kan i den forbindelse sættes spørgsmålstegn ved Kommissionens faglig kompetence til at foretage risikovurderinger og vurderinger af sikkerhedsplaner. Dansk Erhverv sætter spørgsmålstegn ved værdien af etablering af endnu en terrorsikringsmyndighed, når ressourcerne kunne anvendes bedre på konkrete opgaver til sikring af infrastruktur og borgere.

Telekommunikationsindustrien (TI) peger på, at uagtet det ikke er muligt at vurdere omfanget af økonomiske eller andre belastninger for ejere af 'europæisk kritisk infrastruktur' (ECI), er det formentlig givet, at der vil blive tale om øgede administrative og økonomiske belastninger for disse. Estimater af omfanget forudsætter imidlertid afklaring af en række elementer i direktivudkastet.

TI gør opmærksom på, at spørgsmålet om mulig identifikation af dansk ECI vil rejse spørgsmål om integration mellem national og europæiske planlægning, som det af prioriteringsmæssige grunde er vigtigt at få afklaret. TI understreger, at sigtet med ECI og dermed i første omgang udpegning af prioriterede sektorer og dernæst identifikation af specifikke ECI fastholdes, således at der med ECI kun er tale om de specifikke infrastrukturer, hvis sikring reelt har vidtrækkende og pan-euroæpisk betydning.

TI udtrykker i sine bemærkninger betænkelighed ved definitionen, der vedrører kun to medlemslande. Sådanne forhold vil ofte være sikret via bilaterale aftaler, og det vil ikke være proportionalt at klassificere sådanne infrastrukturer som ECI. Der peges især på infrastruktur, der vedrører et medlemsland og er lokaliseret i andet medlemsland. TI anbefaler derfor - ud fra en proportionalitetsmæssig betragtning - at definitionen ændres til at gælde minimum tre lande.

Endvidere er ECI defineret ved 'afbrydelse el. ødelæggelse', der er karakteriseret ved 'truslens alvor', men uden at de elementer som f.eks. antal brugere, politiske og miljømæssige, der indgår i definitionen af 'truslens alvor', er præciseret kvantitativt eller kvalitativt. Dermed er det reelt uklart, hvilke horisontale eller sektorspecifikke kriterier for udpegning af ECI, der kan opstilles af Kommissionen og i komitologiudvalget. TI opfordrer til, at disse elementer præciseres - eksempelvis med minimumsgrænser og under alle omstændigheder vha. et 3 lande kriterium, således at ECI begrebet ikke udvandes til at omfatte, hvilke som helst forstyrrelser, der i ikke nærmere bestemt omfang medfører ulemper.

Der bør opstilles sektorspecifikke kriterier for udpegning af ECI inden for de prioriterede sektorer. Det er uklart i hvilken grad, det reelt er overladt til Kommissionen at fastlægge ECI via identifikationen af sektorspecifikke kriterier. Den meget centrale rolle for Kommissionen understreger vigtigheden af, at definitionerne præciseres og der opstilles tærskelværdier. Teleområdet er formentlig allerede på en række områder fyldestgørende dækket af andre sektorspecifikke redskaber, idet netop teleområdet udgør, i kraft af etableringen af alternative net, kun i begrænset grad én sårbar infrastruktur.

For så vidt angår udpegning af ECI på IT- og teleområdet gælder, at på dette område er de umiddelbart samfundsmæssigt kritiske elementer eksempelvis adresseringssystemer, applikationer (netbank, elektroniske betalingssystemer) samt andre IT-systemer, der anvender egne net snarere end de i stigende grad redundante telenet. TI anbefaler, at dette tydeliggøres og eksemplificeres, således at det sikres, at en eventuel efterfølgende dansk udmøntning ikke alene gennemføres i telelovgivningen.

Det er vigtigt, at nationale kritiske infrastrukturer, hvor der allerede er etableret procedurer for håndtering i tilfælde af krise, fortsat håndteres nationalt. Der bør ikke etableres et unødvendigt dobbelt system mellem nationale forholdsregler og de i direktivet omtalte sikkerhedsplaner for operatører, som de enkelte ejere af mulige ECI skal udarbejde. TI påpeger, at omfanget og detaljeringsniveauet af evt. sikkerhedsplaner for operatører skal vurderes meget nøje, da disse let kan komme til at indeholde særdeles fortrolige data om kunder, opbygning af systemer og organisation. Sådanne planer bør derfor kun indeholde data på et overordnet niveau, hvilket bør fremgå af forslaget.

Hvad angår telekommunikationens grundlæggende tvær- eller internationale egenskaber, kan det være påkrævet at indrette procedurer og tilrettelægge krav, der fremmer grænseoverskridende infrastrukturløsninger, og hvis fornødent, erstatter eller supplerer nationale jurisdiktions- og andre krav. TI påpeger behovet for at tage hensyn til opretholdelse af telekommunikationen med tredjelande under kritiske forhold.

For IT-området, påpeger TI, at selve 'netdelen' ikke kan være den eneste kritiske komponent på dette område. Eksempelvis er adresseringssystemer, applikationer (netbank, elektroniske betalingssystemer) samt systemer, der anvender egne net, i stigende omfang kritiske for samfundet. Disse områder bør derfor beskrives mere generelt, så det ikke giver indtryk af, at kritiske komponenter for IT-området alene findes på teletjenesteområdet. Det betyder efter TIs opfattelse, at en eventuel efterfølgende dansk udmøntning ikke alene kan gennemføres i telelovgivningen.

TI understreger, at eventuelle omkostninger for de enkelte ejere af kritisk infrastruktur, der kan blive pålagt med forpligtigelser som følge af Direktivet, bør søges begrænset bl.a. ved, at der ikke indføres uhensigtsmæssige rapporteringskrav. Det vil eksempelvis være meget omkostningskrævende, hvis selv mindre mobilstationer skal sikres mod terror. Omkostningerne skal sættes i forhold til effekten af, at en mobilstation går ned og antallet af mennesker, det vil påvirke. På dette område bør der principielt tilstræbes fælles retningslinier for hele EU og nationale krav som vil virke konkurrenceforvridende, bør undgås.

10. Regeringens foreløbige generelle holdning

Regeringen stiller sig positivt over for et program om beskyttelse af europæisk kritisk infrastruktur, og regeringen støtter derfor overordnet meddelelsen og direktivforslaget om udpegning af europæisk kritisk infrastruktur. Regeringen finder det positivt, at det i direktivforslaget understreges, at hovedansvaret for beskyttelse af kritisk infrastruktur påhviler medlemsstaterne og ejere/operatører af kritisk infrastruktur.

Regeringen finder det dog vigtigt at få præciseret kriterierne for udpegning af europæisk kritisk infrastruktur samt at mindske risikoen for unødige administrative byrder for operatører og myndigheder.

11. Generelle forventninger til andre landes holdninger

Der foreligger ingen officielle tilkendegivelser af andre landes holdninger. På baggrund af de tidligere drøftelser af grønbogen, er regeringens forventning, at de andre medlemslande overordnet vil støtte et program for europæisk kritisk infrastruktur, men at medlemslandene vil være delte med hensyn til omfanget af rækkevidden af programmet.

12. Tidligere forelæggelser for Folketingets Europaudvalg

Foreløbigt nærhedsnotat om EPCIP-programmet er den 12. januar 2007 fremsendt til Folketingets Europaudvalg samt sendt til orientering for Folketingets Forsvarsudvalg og Folketingets Retsudvalg.

Grundnotat for grønbog om et europæisk program for beskyttelse af kritisk infrastruktur er 4. januar 2006 fremsendt Folketingets Europaudvalg samt sendt til orientering for Folketingets Retsudvalg og Folketingets Forsvarsudvalg.