Europaudvalget 2005
KOM (2005) 0576
Offentligt

KOMMISSIONEN FOR DE EUROPÆISKE FÆLLESSKABER

Bruxelles, den 17.11.2005
KOM(2005) 576 endelig

GRØNBOG

OM ET EUROPÆISK PROGRAM FOR BESKYTTELSE AF KRITISK INFRASTRUKTUR

(forelagt af Kommissionen)

GRØNBOG

OM ET EUROPÆISK PROGRAM FOR BESKYTTELSE AF KRITISK INFRASTRUKTUR

1. BAGGRUND

Kritisk infrastruktur kan beskadiges, ødelægges eller afbrydes ved forsætlige terrorhandlinger, naturkatastrofer, forsømmelser, ulykker eller computerhacking, kriminel aktivitet og destruktiv adfærd. For at beskytte EU-borgernes liv og ejendom mod terrorisme, naturkatastrofer og ulykker bør alle afbrydelser af kritisk infrastruktur eller alle utilsigtede ændringer heraf, som ikke afbryder den, så vidt muligt kun forekomme kortvarigt og sjældent, være relativ lette at forvalte, være geografisk afgrænsede og skade medlemsstaternes, deres borgeres og EU's velfærd mindst muligt. De seneste terrorangreb i Madrid og London satte fokus på risikoen for terrorangreb mod europæisk infrastruktur. EU's reaktion på terror skal være hurtig, koordineret og effektiv.

På Det Europæiske Råds møde i juni 2004 blev Kommissionen anmodet om at udforme en overordnet strategi til beskyttelse af kritisk infrastruktur. Som reaktion herpå vedtog Kommissionen den 20. oktober 2004 en meddelelse vedrørende beskyttelse af kritisk infrastruktur i forbindelse med bekæmpelse af terrorisme, der indeholder klare forslag til, hvordan EU kan forbedre forebyggelsen af, beredskabet i forbindelse med og reaktionen på terrorangreb, der påvirker kritisk infrastruktur.

Det Europæiske Råd gav i sine konklusioner af december 2004 vedrørende forebyggelse, beredskab og reaktion i forbindelse med terrorangreb og EU's solidaritetsprogram om følgerne af terrortrusler og –angreb sin støtte til Kommissionen om fremsættelse af et forslag til et europæisk program for beskyttelse af kritisk infrastruktur (EPCIP) og enedes om, at Kommissionen skal oprette et informations- og varslingsnetværk vedrørende kritisk infrastruktur.

Kommissionen har afholdt to seminarer og opfordret medlemsstaterne til at komme med idéer og bemærkninger. Det første EU-seminar vedrørende beskyttelse af kritisk infrastruktur blev afholdt den 6.-7. juni 2005 og havde deltagelse af medlemsstaterne. Efter seminaret sendte medlemsstaterne Kommissionen en række relevante dokumenter vedrørende deres strategi for beskyttelse af kritisk infrastruktur og deres bemærkninger til de idéer, der blev drøftet på seminaret. Medlemsstaterne sendte deres bidrag i juni og juli, og de udgjorde grundlaget for yderligere udvikling af beskyttelsen af kritisk infrastruktur. Det andet EU-seminar vedrørende beskyttelse af kritisk infrastruktur blev afholdt den 12.-13. september for at fremme diskussionen om beskyttelsen af kritisk infrastruktur. Både medlemsstaterne og faglige organisationer deltog i dette seminar. Som følge heraf har Kommissionen besluttet at fremlægge denne grønbog, hvori mulighederne for så vidt angår EPCIP-programmet opridses.

2. FORMÅLET MED GRØNBOGEN

Hovedformålet med grønbogen er at få feedback vedrørende mulighederne for en strategi for EPCIP-programmet, der involverer en lang række parter. En effektiv beskyttelse af kritisk infrastruktur kræver kommunikation, koordinering og samarbejde på nationalt plan og EU-plan mellem alle berørte parter - ejere og operatører af kritisk infrastruktur, lovgivere, erhvervs- og industriorganisationer i samarbejde med alle regeringsniveauer og offentligheden.

Grønbogen indeholder forslag til, hvad Kommissionen kan gøre for at efterkomme Det Europæiske Råds anmodning om udformning af EPCIP-programmet og oprettelse af et informations- og varslingsnetværk vedrørende kritisk infrastruktur, og udgør anden fase af konsultationen vedrørende udformning af EPCIP-programmet. Kommissionen forventer, at den ved fremlæggelsen af grønbogen vil få konkret feedback vedrørende de politiske muligheder, der er opridset heri. Afhængig af resultatet af konsultationen kan der i løbet af 2006 fremlægges en politisk pakke vedrørende EPCIP.

3. FORMÅLET MED EPCIP-PROGRAMMET

3.1. Det overordnede formål med EPCIP-programmet

Formålet med EPCIP-programmet er at sikre et hensigtsmæssigt og ensartet beskyttelsesniveau for kritisk infrastruktur, at mindske de svage punkter mest muligt og at etablere beredskabsordninger, der er afprøvet i hele EU. Beskyttelsesniveauet er ikke det samme for al kritisk infrastruktur og kan afhænge af, hvor store følger det vil få, at den pågældende kritiske infrastruktur svigter. EPCIP-programmet vil hele tiden blive videreudviklet, og der vil være behov for regelmæssige revideringer for at være på forkant med nye problemer.

EPCIP-programmet bør mindske de negative følger mest muligt, som øgede investeringer i sikkerhed har for en særlig industrisektors konkurrencedygtighed. Ved beregningen af disse omkostninger må der heller ikke ses bort fra behovet for at bevare markedsstabiliteten, som er vigtig for langsigtede investeringer, og den indflydelse, sikkerhed har på udviklingen på aktiemarkedet og den makroøkonomiske udvikling.

Spørgsmål

Er dette et hensigtsmæssigt mål for EPCIP-programmet? Hvis ikke, hvad bør målet så være?

3.2. Hvad bør EPCIP-programmet beskytte imod?

Selv om konsekvensstyringsforanstaltningerne er de samme eller ligner hinanden meget ved de fleste afbrydelser, kan sikkerhedsforanstaltningerne variere afhængig af truslens art. Trusler, der i væsentlig grad kan mindske kapaciteten til at sikre befolkningens væsentligste behov og sikkerhed, til at opretholde orden og yde et minimum af væsentlige offentlige tjenester eller en velfungerende økonomi, kan bl.a. være forsætlige angreb og naturkatastrofer. Der findes følgende alternative muligheder:

a) **En strategi, der dækker alt mod alle former for farer** – dette er en overordnet strategi, hvor der tages hensyn til den trussel, som såvel forsætlige angreb som naturkatastrofer udgør. Den sikrer, at synergien mellem beskyttelsesforanstaltningerne udnyttes maksimalt, men der lægges ikke særlig vægt på terrorisme.

b) **En strategi, der omfatter alle former for farer med vægt på terrorisme** - dette er en fleksibel strategi, der sikrer forbindelsen med andre typer farer såsom forsætlige angreb og naturkatastrofer, men hvor hovedvægten lægges på terrorisme. Hvis beskyttelsesniveauet i en bestemt industrisektor anses for passende, vil de berørte parter koncentrere sig om de trusler, de stadig er sårbare over for.

c) **Terrorbeskyttelse** – dette er en strategi, der fokuserer på terrorisme, og hvor der ikke lægges særlig vægt på mere almindelige trusler.

Spørgsmål

Hvilken strategi bør der vælges for EPCIP-programmet? Hvorfor?

4. HOVEDPRINCIPPER

Det foreslås, at følgende hovedprincipper danner grundlag for EPCIP-programmet:

- **Subsidiaritet** - Subsidiaritet udgør hovedkernen i EPCIP-programmet, hvor beskyttelsen af kritisk infrastruktur først og fremmest er et nationalt ansvar. Det er medlemsstaterne og ejerne/operatørerne, der handler inden for rammerne af fælles regler, som har hovedansvaret for beskyttelsen af kritisk infrastruktur. Kommissionen vil til gengæld koncentrere sig om forskellige aspekter i forbindelse med beskyttelsen af kritisk infrastruktur, hvis afbrydelse har virkning på tværs af grænserne i EU. Der bør ikke ændres ved det forhold, at det er ejere og operatører, der har ansvaret for deres egne beslutninger om og planer for beskyttelse af deres egne installationer.

- **Komplementaritet** – De fælles regler under EPCIP-programmet vil supplere de eksisterende foranstaltninger. De steder, hvor der allerede findes EU-mekanismer, bør de fortsat anvendes og hjælpe med at sikre en generel gennemførelse af EPCIP-programmet.

- **Fortrolighed** – Informationsdeling vedrørende beskyttelse af kritisk infrastruktur bør ske i et klima af tillid og fortrolighed. Det er nødvendigt i lyset af, at specifikke oplysninger om kritisk infrastruktur kan anvendes til at afbryde dem eller begå handlinger med uacceptable følger for kritisk infrastruktur. På både EU-plan og medlemsstatsplan vil oplysninger om beskyttelse af kritisk infrastruktur blive hemmeligstemplet, og der vil kun blive givet adgang hertil til personer, der har behov for det.

- **Samarbejde mellem de berørte parter** – Alle berørte parter, inklusive medlemsstaterne, Kommissionen, erhvervsorganisationer, standardiseringsorganer og ejere, operatører og brugere ("brugere" defineres som organisationer, der udnytter og bruger infrastrukturen i forretningsøjemed og til levering af tjenesteydelser), har en rolle at spille i forbindelse med beskyttelsen af kritisk infrastruktur. Alle berørte parter bør samarbejde og bidrage til udviklingen og gennemførelsen af EPCIP-programmet afhængig af deres specifikke roller og ansvar. Medlemsstaternes myndigheder skal forestå ledelsen og koordineringen af udviklingen og gennemførelsen af en på nationalt plan sammenhængende strategi for

beskyttelse af kritisk infrastruktur inden for hver medlemsstats jurisdiktion. Ejere, operatører og brugere skal aktivt involveres på både nationalt plan og EU-plan. Når der ikke findes sektorbestemte standarder, eller der endnu ikke er blevet fastsat internationale standarder, kan standardiseringsorganisationerne vedtage fælles standarder, når det er hensigtsmæssigt.

- **Proportionalitet** – Beskyttelsesstrategierne og -foranstaltningerne skal stå i forhold til risikoens størrelse, da det ikke er muligt at beskytte al infrastruktur mod alle trusler (f.eks. er elnet for store at hegne ind eller bevogte). Ved at anvende hensigtsmæssige risikoforvaltningsteknikker kan der fokuseres på højrisikoområderne, idet der tages hensyn til truslen, den relative sårbarhed, cost/benefitforholdet, sikkerhedsgraden, og hvor effektive de til rådighed stående afhjælpningsstrategier er.

Spørgsmål

Er disse hovedprincipper acceptable? Er nogle af dem overflødige? Er der andre, der bør tages i betragtning?

Er De enig i, at beskyttelsesforanstaltninger bør står i et rimeligt forhold til den pågældende risikograd, da ikke al infrastruktur kan beskyttes mod alle trusler?

5. FÆLLES EPCIP-REGLER

Beskadigelse eller tab af et stykke infrastruktur i en medlemsstat kan have negative følger for mange andre medlemsstater og for europæisk økonomi som helhed. Dette bliver i stadig højere grad sandsynligt i takt med, at ny teknologi (f.eks. Internettet) og liberaliseringen af markedet (f.eks. el- og gasforsyningen) medfører, at megen infrastruktur indgår som en del af et større net. I en sådan situation er beskyttelsesforanstaltningerne kun så stærke som det svageste led. Det betyder, at det er nødvendigt med et fælles beskyttelsesniveau.

En effektiv beskyttelse af kritisk infrastruktur kræver kommunikation, koordinering og samarbejde på nationalt plan og EU-plan mellem alle berørte parter. Der kan fastsættes fælles EU-regler til beskyttelse af kritisk infrastruktur i Europa for at sikre, at hver medlemsstat har en passende og samme beskyttelse for så vidt angår deres infrastruktur, og at konkurrencereglerne på det indre marked ikke forvrides. For at støtte medlemsstaternes aktiviteter kan Kommissionen lette indkredsningen, udvekslingen og videreformidlingen af bedste praksis for så vidt angår beskyttelse af kritisk infrastruktur ved at fastsætte fælles regler for denne beskyttelse. Det er nødvendigt at overveje, hvor brede disse generelle regler skal være.

De fælles regler i et europæisk program for beskyttelse af kritisk infrastruktur vil omfatte generelle foranstaltninger, hvorved de forskellige berørte parters kompetence og ansvarsområde i forbindelse med beskyttelse af kritisk infrastruktur defineres, og som danner grundlag for sektorspecifikke strategier. Det er hensigten, at de fælles regler skal supplere de eksisterende sektorbestemte foranstaltninger på EU-plan og i medlemsstaterne for derved at sikre den størst mulige grad af sikkerhed for kritisk infrastruktur i EU. Arbejdet med at nå en aftale om en fælles liste over definitioner og de sektorer, hvori der findes kritisk infrastruktur, bør prioriteres.

Da de forskellige sektorer, hvori der findes kritisk infrastruktur, er meget forskellige, vil det være svært nøjagtigt at fastsætte, hvilke kriterier der bør anvendes til at identificere og beskytte dem alle i forbindelse med generelle regler. Dette bør ske på sektorbasis. Der er dog behov for en fælles forståelse af bestemte overordnede spørgsmål.

Det foreslås derfor at styrke kritisk EU-infrastruktur ved at fastsætte fælles regler i et europæisk program for beskyttelse af kritisk infrastruktur (fælles mål, fælles metoder for f.eks. at vurdere den indbyrdes afhængighed), og udveksle oplysninger om bedste praksis og mekanismer til kontrol af overholdelsen heraf. De fælles regler skal bl.a. omfatte følgende:

- fælles principper for beskyttelse af kritisk infrastruktur
- fælles aftalte koder/standarder
- fælles definitioner, som skal danne grundlag for sektorspecifikke definitioner (bilag 1 indeholder en vejledende liste over definitioner)
- fælles liste over sektorer med kritisk infrastruktur (bilag 2 indeholder en vejledende liste over sektorer)
- prioriterede områder for så vidt angår beskyttelse af kritisk infrastruktur
- beskrivelse af de berørte parters ansvar
- aftalte benchmarks
- metoder til at sammenligne infrastrukturen i forskellige sektorer og foretage en prioritering.

Sådanne fælles regler vil også mindske de potentielt konkurrenceforvridende virkninger heraf på det indre marked.

De fælles regler i et europæisk program for beskyttelse af kritisk infrastruktur kan være frivillige eller obligatoriske - eller en blanding afhængig af, hvad der er tale om. Begge typer regler kan supplere eksisterende sektorspecifikke og generelle foranstaltninger på EU-plan og medlemsstatsplan. Kun retlige regler kan imidlertid sikre et stærkt retligt fuldbyrdelsesgrundlag for en sammenhængende og ensartet gennemførelse af foranstaltninger til beskyttelse af kritisk infrastruktur og samtidigt tydeliggøre medlemsstaternes og Kommissionens respektive ansvar. Ikke-bindende frivillige foranstaltninger kan, selv om de er fleksible, ikke skabe klarhed om, hvem der gør hvad.

Afhængig af resultatet af en omhyggelig analyse og under behørig hensyn til proportionaliteten i forbindelse med de foreslåede foranstaltninger kan Kommissionen gøre brug af en række instrumenter, herunder retsforskrifter, i sit forslag vedrørende et europæisk program for beskyttelse af kritisk infrastruktur. Forslagene til specifikke foranstaltninger vil, når det er relevant, være ledsaget af konsekvensanalyser.

Spørgsmål

Vil fastsættelse af fælles regler være en effektiv måde at forbedre beskyttelsen af kritisk infrastruktur på?

Hvis der kræves retlige regler, hvad skal de så omfatte?

Er De enig i, at kriterierne for indkredsning af forskellige typer kritisk infrastruktur i EU og de beskyttelsesforanstaltninger, der betragtes som nødvendige, bør indkredses i hver enkelt sektor?

Vil det være nyttigt med fælles regler for at tydeliggøre de berørte parters ansvar? I hvilket omfang bør sådanne fælles regler være obligatoriske og i hvilket omfang frivillige?

Hvor meget skal de fælles regler dække? Går De ind for listen med vejledende betingelser og definitioner i bilag I, på grundlag af hvilken der kan fastsættes sektorspecifikke definitioner (når det er relevant)? Går De ind for den vejledende liste over sektorer med kritisk infrastruktur i bilag II?

6. KRITISK EU-INFRASTRUKTUR

6.1. Definition af kritisk EU-infrastruktur

Det afgørende for definitionen af, hvad der udgør kritisk EU-infrastruktur, er, hvorvidt det vil have en alvorlig virkning på tværs af grænserne, at der indtræffer et uheld i forbindelse med en installation, der befinder sig på en medlemsstats område. Et andet element, der skal tages hensyn til, er det forhold, at de bilaterale samarbejdsordninger vedrørende beskyttelse af kritisk infrastruktur udgør et afprøvet og effektivt middel til forvaltning af kritisk infrastruktur, der befinder sig i et grænseområde mellem to medlemsstater. Dette samarbejde vil supplere EPCIP-programmet.

Kritisk EU-infrastruktur kan omfatte fysiske ressourcer, tjenester, informations-teknologifaciliteter, netværker og infrastruktur, hvis afbrydelse eller ødelæggelse vil have alvorlige virkninger for sundheden, sikkerheden og den økonomiske eller sociale velfærd i:

a) to eller flere medlemsstater – **dette vil omfatte visse typer bilateral kritisk infrastruktur (når dette er relevant)**

b) tre eller flere medlemsstater – **dette vil udelukke alle typer bilateral kritisk infrastruktur.**

I forbindelse med overvejelserne om disse alternativers respektive fordele er det vigtigt at være opmærksom på følgende:

- Det forhold, at en infrastruktur klassificeres som kritisk EU-infrastruktur, betyder ikke, at der nødvendigvis kræves supplerende beskyttelsesforanstaltninger. De eksisterende beskyttelsesforanstaltninger, der kan omfatte bilaterale aftaler mellem medlemsstaterne, kan være fuldt ud tilstrækkelige og skal derfor ikke ændres, hvis infrastrukturen klassificeres som kritisk EU-infrastruktur.

- Alternativ a) kan medføre, at flere installationer klassificeres som kritisk EU-infrastruktur.

- Alternativ b) kan medføre, at i forbindelse med infrastruktur, der kun vedrører to medlemsstater, har EU ingen rolle at spille, selv om en af medlemsstaterne anser beskyttelsesniveauet for utilstrækkeligt, og den anden nægter at gøre noget ved det. Alternativ b) kan også føre til indgåelse af en lang række bilaterale aftaler eller uenighed mellem medlemsstaterne. Erhvervslivet, der ofte har sit virke i hele Europa, kan være nødt til at arbejde med et virvar af forskellige aftaler, hvilket kan medføre yderligere omkostninger.

Man må heller ikke glemme kritisk infrastruktur, der udgår fra eller befinder sig i et tredjeland uden for EU, men som er forbundet med eller kan have indvirkning på EU-medlemsstaterne.

Spørgsmål

Bør kritisk EU-infrastruktur defineres som infrastruktur, hvis afbrydelse eller ødelæggelse kan have alvorlige virkninger på tværs af grænserne for to eller flere medlemsstater eller tre eller flere medlemsstater? Hvorfor?

6.2. Indbyrdes afhængighed

Det foreslås, at der i forbindelse med den gradvise indkredsning af al kritisk EU-infrastruktur navnlig tages hensyn til den indbyrdes afhængighed. Undersøgelser af den indbyrdes uafhængighed vil bidrage til at vurdere de potentielle virkninger af trusler mod særlig infrastruktur, navnlig for at finde ud af, hvilke medlemsstater der vil blive berørt i tilfælde af et større uheld i forbindelse med kritisk infrastruktur.

Der bør i fuld udstrækning tages hensyn til den indbyrdes afhængighed inden for og mellem virksomheder, industrisektorer, geografisk kompetence og medlemsstaternes myndigheder, navnlig dem, der anvender informations- og kommunikationsteknologi. Kommissionen, medlemsstaterne og ejere/operatører af kritisk infrastruktur skal arbejde sammen om at indkredse denne indbyrdes afhængighed og anvende passende strategier til at mindske risikoen, når det muligt.

Spørgsmål

Hvordan kan der tages hensyn til indbyrdes afhængighed?

Kender De nogen hensigtsmæssige metoder til analysering af indbyrdes afhængighed?

På hvilket niveau bør indkredsningen af den indbyrdes afhængighed finde sted – på EU-plan og/eller medlemsstatsplan?

6.3. Gennemførelsesforanstaltninger vedrørende kritisk EU-infrastruktur

Kommissionen foreslår følgende gennemførelsesforanstaltninger i forbindelse med kritisk EU-infrastruktur:

(1) Kommissionen fastsætter sammen med medlemsstaterne specifikke kriterier, der kan anvendes til at indkredse kritisk EU-infrastruktur på sektorspecifik basis.

(2) Medlemsstaterne og Kommissionen indkredser og kontrollerer gradvis de forskellige sektorer med kritisk EU-infrastruktur. Beslutningen om at klassificere bestemt kritisk infrastruktur som kritisk EU-infrastruktur vil blive truffet på europæisk plan[1], da der er tale om infrastruktur, der går på tværs af grænserne.

(3) Medlemsstaterne og Kommissionen analyserer de eksisterende huller i sikkerheden i forbindelse med kritisk EU-infrastruktur i de forskellige sektorer.

(4) Medlemsstaterne og Kommissionen enes om, hvilke sektorer/hvilken infrastruktur der skal prioriteres under hensyntagen til den indbyrdes afhængighed.

---

[1] Med undtagelse af forsvarsrelateret infrastruktur.

(5) Når det er relevant, enes Kommissionen og de væsentligste berørte parter i medlemsstaterne om forslag til minimumsbeskyttelsesforanstaltninger, der kan omfatte standarder.

(6) Efter vedtagelsen af Rådets forslag, gennemføres foranstaltningerne.

(7) Medlemsstaterne og Kommissionen foretager regelmæssig overvågning. Der foretages ændringer (foranstaltninger og indkredsning af kritisk infrastruktur), når og hvor det er hensigtsmæssigt.

Spørgsmål

Er listen over de forskellige trin i gennemførelsen af beskyttelse af kritisk infrastruktur acceptabel?

Hvordan foreslår De, at Kommissionen og medlemsstaterne sammen klassificerer infrastrukturer som kritisk EU-infrastruktur (medlemsstaterne har ekspertisen og Kommissionen overblikket over europæiske interesser)? Bør det være en retlig afgørelse?

Er der brug for en mæglingsordning, hvis en medlemsstat ikke er enig i at klassificere infrastruktur inden for dens jurisdiktion som kritisk EU-infrastruktur?

Er der brug for at kontrollere klassificeringen af kritisk EU-infrastruktur? Hvem skal være ansvarlig herfor?

Bør medlemsstaterne kunne klassificere infrastruktur i andre medlemsstater eller tredjelande som værende kritisk infrastruktur for dem? Hvad bør der ske, hvis en medlemsstat, et tredjeland eller en virksomhed anser en bestemt infrastruktur i en medlemsstat som værende kritisk for dem?

Hvad bør der ske, hvis denne medlemsstat ikke indkredser infrastrukturen som kritisk? Er der brug for klagemuligheder? Hvis ja, hvilke?

Bør en operatør have mulighed for at klage, hvis han ikke er enig i, at infrastruktur klassificeres som værende kritisk eller ikke kritisk infrastruktur? Hvis ja, til hvem?

Hvilke metoder vil det være nødvendigt at udvikle for at fastsætte, hvilke sektorer/hvilken infrastruktur der skal prioriteres, og hvor der bør gøres en indsats? Findes der allerede hensigtsmæssige metoder, der kan tilpasses, så de kan anvendes på EU-plan?

Hvordan kan Kommissionen inddrages i analysen af, hvor der er huller i sikkerheden i forbindelse med kritisk EU-infrastruktur?

7. NATIONAL KRITISK INFRASTRUKTUR

7.1. National kritisk infrastrukturs rolle i forbindelse med EPCIP-programmet

Mange europæiske virksomheder arbejder på tværs af grænserne og er som sådan underkastet forskellige forpligtelser for så vidt angår national kritisk infrastruktur. Det foreslås derfor i medlemsstaternes og hele EU's interesse, at hver medlemsstat beskytter sin nationale kritiske infrastruktur ved hjælp af fælles regler, således at ejere og operatører i hele Europa kan undgå

at være underlagt et puslespil af forskellige regler, hvilket medfører mange forskellige fremgangsmåder og ekstra omkostninger. Med henblik herpå foreslår Kommissionen, at der i EPCIP-programmet, hvor der hovedsageligt fokuseres på kritisk EU-infrastruktur, ikke ses helt bort fra national kritisk infrastruktur. Der er dog tre muligheder:

a) National kritisk infrastruktur medtages fuldt og helt i EPCIP-programmet

b) National kritisk infrastruktur omfattes ikke af EPCIP-programmet

c) Medlemsstaterne kan efter eget ønske anvende dele af EPCIP-programmet i forbindelse med national kritisk infrastruktur, men er ikke forpligtet til at gøre det.

Spørgsmål

En effektiv beskyttelse af kritisk infrastruktur i EU synes at kræve, at både kritisk EU-infrastruktur og national kritisk infrastruktur indkredses. Er De enig i, at selv om EPCIP-programmet bør fokusere på kritisk EU-infrastruktur, kan der ikke ses helt bort fra national kritisk infrastruktur?

Hvilke af disse løsninger finder De det mest hensigtsmæssigt at vælge i forbindelse med EPCIP-programmet?

7.2. Nationale programmer for beskyttelse af kritisk infrastruktur

På grundlag af fælles regler i EPCIP-programmet kan medlemsstaterne udvikle nationale programmer for beskyttelse af national kritisk infrastruktur. Medlemsstaterne kan anvende strengere bestemmelser end dem, der findes i EPCIP-programmet.

Spørgsmål

Er det ønskeligt, at hver medlemsstat vedtager et nationalt program for beskyttelse af kritisk infrastruktur baseret på EPCIP-programmet?

7.3. Et enkelt overvågningsorgan

Behovet for effektivitet og sammenhæng taler for, at det er nødvendigt, at hver medlemsstat udpeger et enkelt overvågningsorgan, der skal forestå den overordnede gennemførelse af EPCIP-programmet. Der er to muligheder:

a) Et enkelt overvågningsorgan for beskyttelse af kritisk infrastruktur

b) Et nationalt kontaktpunkt uden myndighed, der overlader det til medlemsstaterne selv at organisere sig.

Et sådant organ kan koordinere, overvåge og tilse gennemførelsen af EPCIP-programmet inden for medlemsstatens jurisdiktion og fungere som det væsentligste institutionelle kontaktpunkt i forbindelse med spørgsmål vedrørende beskyttelse af kritisk infrastruktur for Kommissionen, andre medlemsstater og ejere og operatører af kritisk infrastruktur. Organet kan fungere som national repræsentant i ekspertgrupper vedrørende beskyttelse af kritisk infrastruktur og knyttes til informations- og varslingsnetværket vedrørende kritisk infrastruktur. Det nationale koordineringsorgan for beskyttelse af kritisk infrastruktur kan

koordinere nationale foranstaltninger i forbindelse med beskyttelse af kritisk infrastruktur, uden at dette har indflydelse på den indsats, som andre organer eller enheder i en medlemsstat gør på området.

Det er muligt gradvis at indkredse national kritisk infrastruktur ved at pålægge infrastrukturejere og –operatører at informere det nationale koordineringsorgan for beskyttelse af kritisk infrastruktur om alle aktiviteter, der vedrører beskyttelse af kritisk infrastruktur.

Det nationale koordineringsorgan kan have ansvaret for den retlige beslutning om at klassificere en infrastruktur inden for medlemsstatens jurisdiktion som national kritisk infrastruktur. Disse oplysninger vil udelukkende stå til rådighed for den pågældende medlemsstat.

Koordineringsorganet kan have følgende beføjelser:

a) Koordinering, overvågning og tilsyn med den overordnede gennemførelse af EPCIP-programmet i en medlemsstat.

b) Fungere som det væsentligste institutionelle kontaktpunkt vedrørende spørgsmål om beskyttelse af kritisk infrastruktur i forhold til:

   i. Kommissionen

   ii. andre medlemsstater

   iii. ejere og operatører af kritisk infrastruktur.

c) Deltage i klassificering af infrastruktur som kritisk EU-infrastruktur.

d) Træffe en retlig beslutning om klassificering af infrastruktur inden for medlemsstatens jurisdiktion som national kritisk infrastruktur.

e) Fungere som klageorgan for ejere/operatører, der ikke er enige i, at deres infrastruktur klassificeres som "kritisk infrastruktur".

f) Deltage i udformningen af et program for beskyttelse af national kritisk infrastruktur og de sektorspecifikke programmer for beskyttelse af kritisk infrastruktur.

g) Indkredse indbyrdes afhængighed mellem specifikke sektorer med kritisk infrastruktur.

h) Bidrage til sektorspecifikke strategier for beskyttelse af kritisk infrastruktur via deltagelse i ekspertgrupper. Repræsentanter for ejere og operatører kan opfordres til at bidrage til diskussionen. Der kan afholdes regelmæssige møder.

i) Overvåge bestræbelserne for at udforme en beredskabsplan i forbindelse med kritisk infrastruktur.

Spørgsmål

Er De enig i, at medlemsstaterne alene skal være ansvarlige for klassificeringen og forvaltningen af national kritisk infrastruktur inden for rammerne af reglerne i EPCIP-programmet?

Er det ønskeligt at udpege et koordineringsorgan for beskyttelsen af kritisk infrastruktur i hver medlemsstat, som har det overordnede ansvar for koordineringen af foranstaltninger i forbindelse med beskyttelse af kritisk infrastruktur, samtidig med at det skal respektere de allerede eksisterende sektorspecifikke ansvarsområder (civile luftfartsmyndigheder, Seveso-direktivet m.m.)?

Er de foreslåede beføjelser passende for et koordineringsorgan? Er det nødvendigt at tilføje andre?

7.4. Gennemførelsesforanstaltninger i forbindelse med national kritisk infrastruktur

Kommissionen foreslår følgende gennemførelsesforanstaltninger i forbindelse med national kritisk infrastruktur:

(1) På grundlag af EPCIP-programmet fastsætter medlemsstaterne særlige kriterier for indkredsning af, hvad der er national kritisk infrastruktur.

(2) Medlemsstaterne indkredser og kontrollerer gradvis de forskellige sektorer med national kritisk infrastruktur.

(3) Medlemsstaterne analyserer de eksisterende huller i sikkerheden i forbindelse med national kritisk infrastruktur i de forskellige sektorer.

(4) Medlemsstaterne beslutter, hvilke sektorer der skal prioriteres, og hvor der skal træffes foranstaltninger, idet de tager hensyn til den indbyrdes afhængighed og de prioriterede områder, der er opnået enighed om, når det er relevant.

(5) Når det er relevant, enes medlemsstaterne for hver sektor om minimumsbeskyttelsesforanstaltninger.

(6) Medlemsstaterne har ansvaret for inden for deres jurisdiktion at sikre, at ejere/operatører træffer de nødvendige gennemførelsesforanstaltninger.

(7) Medlemsstaterne sikrer en regelmæssig kontrol. Der foretages ændringer (foranstaltninger og indkredsning af kritisk infrastruktur), når og hvor det er hensigtsmæssigt.

Spørgsmål

Er listen over de forskellige trin i gennemførelsen af beskyttelse af national kritisk infrastruktur acceptabel? Er nogen af trinnene overflødige? Bør der tilføjes andre?

8. EJERES, OPERATØRERS OG BRUGERES ROLLE

8.1. Ejeres, operatørers og brugeres ansvar

Når en infrastruktur klassificeres som kritisk infrastruktur, pålægger det ejere og operatører visse forpligtelser. Der kan være tale om fire forpligtelser for ejere og operatører af infrastruktur, der er klassificeret som national kritisk infrastruktur eller kritisk EU-infrastruktur:

(1) **Indberetning til det relevante organ i medlemsstaten, der tager sig af beskyttelse af kritisk infrastruktur, om, at en infrastruktur kan være af kritisk art.**

(2) **Udpegelse af (en) højtstående repræsentant(er), der skal fungere som sikkerhedsforbindelsesofficer(er) mellem ejer/operatør og en medlemsstats relevante myndighed med ansvar for beskyttelse af kritisk infrastruktur.** Sikkerhedsforbindelsesofficererne deltager i udviklingen af sikkerheds- og beredskabsplaner. En sikkerhedsforbindelsesofficer vil være hovedforbindelses-officeren i forbindelse med det relevante sektororgan for beskyttelse af kritisk infrastruktur i medlemsstaten, og når det er relevant, med de retshåndhævende myndigheder.

(3) **Udformning, gennemførelse og ajourføring af en sikkerhedsplan for operatører.** Bilag 3 indeholder et forslag til model til en sikkerhedsplan for operatører.

(4) **Deltagelse i udviklingen af en beredskabsplan** vedrørende kritisk infrastruktur sammen med de relevante civilbeskyttelsesmyndigheder og retshåndhævende myndigheder i medlemsstaterne, når det er påkrævet.

Sikkerhedsplanen for operatører kan forelægges medlemsstatens sektorspecifikke myndighed for beskyttelse af kritisk infrastruktur til godkendelse under tilsyn af det nationale koordineringsorgan, uanset om der er tale om national kritisk infrastruktur eller kritisk EU-infrastruktur, således at der sikres sammenhæng i de sikkerhedsforanstaltninger, som såvel specifikke ejere og operatører som de relevante sektorer generelt har truffet. Til gengæld kan det nationale koordineringsorgan og, når det er relevant, Kommissionen give ejere og operatører en række nyttige oplysninger og støtte i forbindelse med de trusler, de er udsat for, og hvad angår udvikling af bedste praksis. De kan desuden, når det er hensigtsmæssigt, hjælpe med at vurdere den indbyrdes afhængighed og infrastrukturens sårbarhed.

Hver medlemsstat kan fastsætte en tidsfrist for ejeres og operatørers udformning af en sikkerhedsplan for operatører af både national kritisk infrastruktur og kritisk EU-infrastruktur (i tilfælde af kritisk EU-infrastruktur skal Kommissionen inddrages) og fastsætte administrative bøder, hvis tidsfristerne ikke overholdes.

Det foreslås, at ejerens/operatørens kritiske infrastruktur indkredses i sikkerhedsplanen for operatører, og at der fastsættes hensigtsmæssige løsninger for så vidt angår sikkerheden for at beskytte infrastrukturen. Sikkerhedsplanen for operatører kan indeholde en beskrivelse af metoder og den procedure, der skal følges for at sikre, at kravene i EPCIP-programmet, programmerne for beskyttelse af national kritisk infrastruktur og relevante sektorspecifikke programmer for beskyttelse af kritisk infrastruktur overholdes. Med en sikkerhedsplan er det muligt at tilrettelægge beskyttelsen af kritisk infrastruktur helt fra grunden, hvilket giver den private sektor større frihed (men også større ansvar).

I særlige tilfælde, når der er tale om bestemt infrastruktur, f.eks. elnet og informationsnet, vil det være urealistisk (ud fra både et praktisk og økonomisk synspunkt) at forvente, at ejere og operatører tilvejebringer samme sikkerhed overalt for deres infrastruktur. I disse tilfælde foreslås det, at ejere og operatører sammen med de relevante myndigheder indkredser de kritiske punkter i forbindelse med et fysisk netværk eller et informationsnetværk, som sikkerhedsforanstaltningerne kan koncentreres om.

En sikkerhedsplan for operatører kan indeholde to typer sikkerhedsforanstaltninger:

- **Permanente sikkerhedsforanstaltninger** med præcisering af, hvilke investeringer og midler der er nødvendige for sikkerheden, men som ejeren/operatøren ikke kan træffe med kort varsel. Ejeren/operatøren skal hele tiden være opmærksom på eventuelle trusler, men på en måde, der ikke forstyrrer de normale økonomiske, administrative og sociale aktiviteter.

- **Gradvise sikkerhedsforanstaltninger**, der kan iværksættes afhængig af fareniveauet. Sikkerhedsplanen for operatører kan derfor omfatte forskellige sikkerhedsordninger, der er tilpasset mulige trusselsniveauer i de medlemsstater, hvor infrastrukturen befinder sig.

Det foreslås, at en ejer eller operatør af kritisk infrastruktur kan pålægges en bøde, hvis den pågældende ikke efterkommer kravet om at udforme en sikkerhedsplan for operatører, ikke bidrager til at udvikle beredskabsplaner og ikke udpeger en sikkerhedsforbindelsesofficer.

Spørgsmål

Er det potentielle ansvar, der påhviler ejere/operatører af kritisk infrastruktur, acceptabelt for så vidt angår en forbedring af sikkerheden omkring kritisk infrastruktur? Hvor meget skønnes det at koste?

Bør ejere og operatører være forpligtet til at give meddelelse om, at deres infrastruktur kan være kritisk infrastruktur? Finder De idéen med en sikkerhedsplan for operatører nyttig? Hvorfor?

Står de foreslåede krav i et rimeligt forhold til de omkostninger, de afstedkommer?

Hvilke rettigheder kan medlemsstaternes myndigheder og Kommissionen give ejere og operatører af kritisk infrastruktur?

8.2. Dialog med ejere, operatører og brugere

Ejere og operatører kan i EPCIP-programmet opfordres til at indgå partnerskaber. Hvor vellykket et beskyttelsesprogram er, afhænger af, hvor meget ejere og operatører samarbejder og er involveret. I medlemsstaterne kan ejere og operatører af kritisk infrastruktur gennem regelmæssig kontakt med det nationale koordineringsorgan inddrages i udviklingen af beskyttelse af kritisk infrastruktur.

På EU-plan kan der dannes fora for at lette udvekslingen af synspunkter om generelle og sektorspecifikke spørgsmål vedrørende beskyttelse af kritisk infrastruktur. Gennem en fælles strategi for den private sektors inddragelse i spørgsmål vedrørende beskyttelse af kritisk infrastruktur for at samle alle berørte parter i den offentlige og den private sektor vil

medlemsstaterne, Kommissionen og erhvervslivet kunne drøfte nye spørgsmål vedrørende beskyttelse af kritisk infrastruktur. Ejere, operatører og brugere af kritisk infrastruktur kan bidrage til udviklingen af fælles retningslinjer og standarder for bedste praksis og dele oplysninger, når det er relevant. En sådan dialog vil være nyttig i forbindelse med fremtidige ændringer af EPCIP-programmet.

Når det er relevant, kan Kommissionen opfordre til, at der dannes erhvervssammenslutninger vedrørende beskyttelse af kritisk EU-infrastruktur. De sidste to mål vil være at sikre, at europæisk industri bevarer sin konkurrencedygtighed, og at EU-borgernes sikkerhed øges.

Spørgsmål

Hvordan bør dialogen mellem ejere, operatører og brugere af kritisk infrastruktur struktureres?

Hvem bør repræsentere ejere, operatører og brugere i dialogen mellem den offentlige og den private sektor?

9. FORANSTALTNINGER TIL STØTTE FOR EPCIP-PROGRAMMET

9.1. Informations- og varslingsnetværk vedrørende kritisk infrastruktur

Kommissionen har udviklet en række systemer for hurtig varsling, der gør det muligt at sikre en konkret, koordineret og effektiv reaktion i tilfælde af nødsituationer, herunder som følge af terrorisme. Den 20. oktober 2004 meddelte Kommissionen, at der i Kommissionen ville blive oprettet et centralt net, der skal sikre en hurtig strøm af informationer mellem alle Kommissionens systemer for hurtig varsling og berørte tjenestegrene i Kommissionen (ARGUS).

Kommissionen foreslår, at der oprettes et informations- og varslingsnetværk vedrørende kritisk infrastruktur, der skal fremme udviklingen af hensigtsmæssige beskyttelsesforanstaltninger ved at lette udvekslingen af oplysninger om bedste praksis på en sikker måde, og være et middel til videreformidling af umiddelbare trusler og varsler. Systemet skal sikre, at de rigtige personer får de rigtige oplysninger i rette øjeblik.

Informations- og varslingsnetværket vedrørende kritisk infrastruktur kan udformes på tre måder:

(1) **Et forum, der kun omfatter udveksling af idéer og bedste praksis for så vidt angår beskyttelse af kritisk infrastruktur** med henblik på at støtte ejere og operatører af kritisk infrastruktur. Et sådant forum kan have form af et net af eksperter og et elektronisk forum for udveksling af relevante oplysninger inden for sikre rammer. Kommissionen skal spille en væsentlig rolle ved at indsamle og videreformidle oplysninger. Denne løsning gør det ikke muligt hurtigt at videreformidle varsler om umiddelbare trusler. Der er dog grundlag for senere at udvide informations- og varslingsnetværket.

(2) **Et system for hurtig varsling, der forbinder medlemsstaterne med Kommissionen.** Dette vil øge sikkerheden i forbindelse med kritisk infrastruktur, idet det er muligt at videreformidle advarsler om umiddelbare trusler og varsler. Målet vil

være at lette en hurtig udveksling af oplysninger om potentielle trusler til ejere og operatører af kritisk infrastruktur. Systemet indebærer ikke informationsdeling på lang sigt. Det kan anvendes til hurtig deling af oplysninger om umiddelbare trusler mod specifik infrastruktur.

(3) **Et kommunikations- og varslingssystem med flere niveauer og med to særskilte funktioner:** a) et system for hurtig varsling, der forbinder medlemsstaterne med Kommissionen, og b) et forum for udveksling af idéer og bedste praksis for så vidt angår beskyttelse af kritisk infrastruktur med henblik på at støtte ejere og operatører af kritisk infrastruktur og bestående af et net af eksperter og et forum for elektronisk udveksling af oplysninger.

Uanset hvilken løsning der vælges, skal informations- og varslingsnetværket supplere de eksisterende net, og der skal undgås overlapninger. På lang sigt kan informations- og varslingsnetværket kobles til alle ejere og operatører af kritisk infrastruktur i hver medlemsstat, f.eks. gennem det nationale koordineringsorgan. Varsler og bedste praksis kan videreformidles gennem dette organ, der bliver den eneste tjeneste, der er direkte knyttet til Kommissionen og dermed til alle medlemsstater. Medlemsstaterne vil kunne bruge de eksisterende informationssystemer til at opbygge deres nationale informations- og varslingsnetværk vedrørende kritisk infrastruktur, der forbinder myndighederne med specifikke ejere og operatører. De nationale netværker kan desuden tjene som et tovejskommunikationssystem mellem medlemsstaternes kompetente myndigheder på området beskyttelse af kritisk infrastruktur og ejere og operatører.

Der vil blive iværksat en undersøgelse for at afgøre, hvilke aspekter informations- og varslingsnetværkets fremtidige grænseflade med medlemsstaterne skal dække og de tekniske specifikationer for netværket.

Spørgsmål

Hvilken form bør informations- og varslingsnetværket have for at støtte målsætningerne i forbindelse med EPCIP-programmet?

Bør ejere og operatører af kritisk infrastruktur være koblet til informations- og varslingsnetværket?

9.2. Fælles metoder

De forskellige medlemsstater har forskellige varslingsniveauer svarende til forskellige situationer. På nuværende tidspunkt er det ikke muligt at vide, om f.eks. et "højt" varslingsniveau i en medlemsstat svarer til et "højt" varslingsniveau i en anden. Det gør det svært for tværnationale virksomheder at prioritere investeringer i beskyttelsesforanstaltninger. Det kan derfor være nyttigt at forsøge at harmonisere eller kalibrere de forskellige niveauer.

For hvert trusselsniveau kan der være et beredskabsniveau, hvor der iværksættes fælles sikkerhedsforanstaltninger generelt, og der om nødvendigt anvendes graduerede sikkerhedsforanstaltninger. Medlemsstater, der ikke ønsker at træffe en bestemt foranstaltning, vil kunne imødegå en specifik trussel ved hjælp af alternative sikkerhedsforanstaltninger.

Det kan overvejes at fastsætte en fælles metode til indkredsning og klassificering af trusler, kapacitet, risici og sårbarhed og til at drage en række konklusioner om, hvorvidt truslen udgør en reel, sandsynlig og alvorlig fare for, at infrastrukturen afbrydes. Dette kan omfatte risikoklassificering og -ranking, hvor risici defineres ud fra, hvor sandsynlige de er, deres virkninger og forbindelsen til andre risikoområder eller –processer.

Spørgsmål

I hvor høj grad er det ønskeligt og muligt at harmonisere eller kalibrere forskellige varslingsniveauer?

Bør der være en fælles metode til indkredsning og klassificering af trusler, kapacitet, risici og sårbarhed og til at drage en række konklusioner om, hvorvidt truslen udgør en reel, sandsynlig og alvorlig fare?

9.3. Finansiering

Som reaktion på Europa-Parlamentets initiativ (oprettelse af en ny budgetpost – pilotprojekt vedrørende bekæmpelse af terrorisme – i budgettet for 2005) traf Kommissionen den 15. september beslutning om at afsætte 7 mio. EUR til finansiering af en række foranstaltninger, der vil forbedre forebyggelsen af, beredskabet i forbindelse med og reaktionen på terrorangreb i EU, herunder konsekvensstyring, beskyttelse af kritisk infrastruktur, finansiering af terrorisme, sprængstoffer og voldelig radikalisering. Mere end to tredjedele af budgettet skal gå til udformningen af det fremtidige europæiske program for beskyttelse af kritisk infrastruktur, integrering og udvikling af den kapacitet, der er nødvendig for at styre kriser af tværnationalt omfang som følge af mulige terrorangreb og nødforanstaltninger, som kan være påkrævet for at imødegå en alvorlig trussel eller et angreb. Det forventes, at der også vil blive stillet midler til rådighed hertil i 2006.

Fra 2007-2013 vil finansieringen ske over rammeprogrammet om sikkerhed og beskyttelse af frihedsrettigheder. Det vil omfatte et særprogram om forebyggelse, beredskab og konsekvensstyring i forbindelse med terrorisme. Kommissionen har foreslået en finansieringsramme på 137,4 mio. EUR, der skal anvendes til at afdække behovene og udvikle fælles tekniske standarder til beskyttelse af kritisk infrastruktur.

Via programmet vil der blive ydet EU-støtte til projekter vedrørende beskyttelse af kritisk infrastruktur, som nationale, regionale og lokale myndigheder fremlægger. I programmet fokuseres der på at indkredse behovene for beskyttelse og tilvejebringe oplysninger med henblik på at udforme fælles standarder og at vurdere trusler og risici for at beskytte kritisk infrastruktur eller udvikle specifikke beredskabsplaner. Kommissionen kan udnytte sin nuværende ekspertise eller hjælpe med at finansiere undersøgelser vedrørende indbyrdes afhængighed i specifikke sektorer. Det er hovedsageligt medlemsstaternes eller ejernes og operatørernes ansvar at ajourføre sikkerheden omkring deres infrastruktur på grundlag af de indkredsede behov. Via programmet selv ydes der ikke støtte til ajourføring af beskyttelse af kritisk infrastruktur. Der kan f.eks. ydes banklån til ajourføring af sikkerheden omkring infrastruktur i medlemsstaterne på grundlag af de behov, der er indkredset via programmet, og til gennemførelse af fælles standarder. Kommissionen vil være villig til at støtte sektorbaserede undersøgelser for at vurdere de finansielle virkninger, en ajourføring af sikkerheden omkring kritisk infrastruktur vil få for erhvervslivet.

Kommissionen finansierer forskningsprojekter til støtte for beskyttelse af kritisk infrastruktur via det forberedende program for sikkerhedsforskning[2] (2004-2006) og har planlagt omfattende aktiviteter på området sikkerhedsforskning i sit forslag til Europa-Parlamentets og Rådets afgørelse om Det Europæiske Fællesskabs syvende rammeprogram for forskning, teknologisk udvikling og demonstration (KOM(2005) 119 endelig)[3] og dens forslag til Rådets beslutning om særprogrammet "Samarbejde" til gennemførelse af Det Europæiske Fællesskabs syvende rammeprogram for forskning, teknologisk udvikling og demonstration (KOM(2005) 440 endelig). Målrettet forskning med henblik på at finde frem til praktiske strategier eller redskaber til mindskelse af risikoen er af allerstørste betydning for at sikre kritisk EU-infrastruktur på mellemlang og lang sigt. Al sikkerhedsforskning, inklusive dette område, vil blive omfattet af etisk kontrol for at sikre, at den er i overensstemmelse med chartret om grundlæggende rettigheder. Behovet for forskning vil kun stige i takt med, at omfanget af afhængighed mellem infrastruktur vokser.

Spørgsmål

Hvor store bliver omkostningerne og virkningerne af gennemførelsen af de forslag, der fremsættes i denne grønbog efter Deres mening for administrationerne og erhvervslivet? Finder De dem forholdsmæssigt rimelige?

9.4. Evaluering og overvågning

For at sikre evalueringen og overvågningen af EPCIP-programmet kræves der en procedure på flere niveauer med inddragelse af alle berørte parter:

- **På EU-plan: der kan indføres en ekspertvurderingsmekanisme**, hvor medlemsstaterne og Kommissionen arbejder sammen om at vurdere den overordnede grad af gennemførelse af EPCIP-programmet i hver medlemsstat. Kommissionen kan udarbejde årlige statusrapporter vedrørende gennemførelsen af programmet.

- **Kommissionen kan rapportere om fremskridt til medlemsstaterne og de andre institutioner hvert kalenderår** i et arbejdsdokument fra dens tjenestegrene.

- **På medlemsstatsniveau: det nationale koordineringsorgan i hver medlemsstat kan overvåge den overordnede gennemførelse af EPCIP-programmet inden for dens jurisdiktion og sikre, at der er overensstemmelse med programmet/programmerne for beskyttelse af national kritisk infrastruktur og programmerne for beskyttelse af sektorspecifik kritisk infrastruktur** for at kontrollere, at de reelt er blevet gennemført, og rapportere hvert år til Rådet og Kommissionen.

Gennemførelsen af EPCIP-programmet vil blive en dynamisk proces under konstant udvikling, der hele tiden evalueres for at holde trit med forandringerne i verden og bygge videre på de indhøstede erfaringer. Ekspertvurderinger og medlemsstaternes overvågningsrapporter kan udgøre en del af de instrumenter, der anvendes til at ændre EPCIP-programmet og foreslå nye foranstaltninger for at øge beskyttelsen af kritisk infrastruktur.

---

[2] De samlede midler på budgettet i 2004 og 2005 var på 30 mio. EUR. For 2006 har Kommissionen fremsat et forslag om 24 mio. EUR, som budgetmyndigheden er ved at behandle.

[3] Kommissionens forslag til budget for sikkerheds- og rumfartsrelaterede forskningsaktiviteter under det syvende rammeprogram er på 570 mio. EUR (KOM(2005) 119 endelig).

Medlemsstaterne kan stille relevante oplysninger vedrørende kritisk EU-infrastruktur til rådighed for Kommissionen med henblik på udvikling af fælles vurderinger af sårbarhed, konsekvensstyringsplaner, fælles standarder for beskyttelse af kritisk infrastruktur, prioritering af forskning og om nødvendigt lovgivning og harmonisering. Disse oplysninger vil blive klassificeret som strengt fortrolige og behandlet som sådan.

Kommissionen kan overvåge forskellige medlemsstaters initiativer, herunder de, der får økonomiske konsekvenser for ejere og operatører, der ikke er i stand til at genoptage leveringen af væsentlige tjenester til borgerne inden for en fastsat maksimal tidsramme.

Spørgsmål

Hvilken type evalueringsmekanisme kan der anvendes i forbindelse med EPCIP-programmet? Vil ovennævnte mekanisme være tilstrækkelig?

Svarene skal sendes elektronisk inden 15. januar 2006 til følgende e-mail-adresse: **JLS-EPCIP@cec.eu.int**. De vil blive behandlet fortroligt, medmindre besvareren udtrykkeligt gør opmærksom på, at de kan offentliggøres. I så tilfælde vil de blive sat på Kommissionens Internetsted.

BILAG

ANNEX 1

CIP TERMS AND DEFINITIONS

This indicative list of definitions could be further built upon depending on the individual sectors for the purpose of identification and protection of Critical Infrastructure (CI).

Alert

Notification that a potential disaster situation will occur, exists or has occurred. Direction for recipient to stand by for possible escalation or activation of appropriate measures.

Critical infrastructure protection (CIP)

The ability to prepare for, protect against, mitigate, respond to, and recover from critical infrastructure disruptions or destruction.

Critical Information Infrastructure (CII):

ICT systems that are critical infrastructures for themselves or that are essential for the operation of critical infrastructures (telecommunications, computers/software, Internet, satellites, etc.).

Critical Information Infrastructure Protection (CIIP)

The programs and activities of infrastructure owners, operators, manufacturers, users, and regulatory authorities which aim at keeping the performance of critical information infrastructures in case of failures, attacks or accidents above a defined minimum level of services and aim at minimising the recovery time and damage.

CIIP should therefore be viewed as a cross-sector phenomenon rather than being limited to specific sectors. CIIP should be closely coordinated with Critical Infrastructure Protection from a holistic perspective.

Contingency plan

A plan used by a MS and critical infrastructure owner/operator on how to respond to a specific systems failure or disruption of essential service.

Contingency plans would typically include the development, coordination, and execution of service- and site-restoration plans; the reconstitution of government operations and services; individual, private-sector, nongovernmental and public-assistance programs to promote restoration; long-term care and treatment of affected persons; additional measures for social, political, environmental, and economic restoration as well as development of initiatives to mitigate the effects of future incidents.

Critical Information

Specific facts about a critical infrastructure asset, vitally needed to plan and act effectively so as to guarantee failure or cause unacceptable consequences for critical infrastructure installations.

Critical Infrastructure (CI)

Critical infrastructure include those physical resources, services, and information technology facilities, networks and infrastructure assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of Citizens or the effective functioning of governments.

There are three types of infrastructure assets:

- Public, private and governmental infrastructure assets and interdependent cyber & physical networks.
- Procedures and where relevant individuals that exert control over critical infrastructure functions.
- Objects having cultural or political significance as well as "soft targets" which include mass events (i.e. sports, leisure and cultural).

Essential service

Often applied to utilities (water, gas, electricity, etc.) it may also include standby power systems, environmental control systems or communication networks that if interrupted puts at risk public safety and confidence, threatens economic security, or impedes the continuity of a MS government and its services.

European critical infrastructure (ECI)

European critical infrastructure include those physical resources, services, and information technology facilities, networks and infrastructure assets, which, if disrupted or destroyed would have a serious impact on the health, safety, security, economic or social well-being of two or more MS.

The definition of what constitutes an EU critical infrastructure is determined by its cross border effect which ascertains whether an incident could have a serious impact beyond two or more MS national territories. This is defined as the loss of a critical infrastructure element and is rated by the:

- extent of the geographic area which could be affected by the loss or unavailability of a critical infrastructure element beyond three or more Member State's national territories;
- effect of time (i.e. the fact that a for example a radiological cloud might, with time, cross a border);
- level of interdependency (i.e. electricity network failure in one MS effecting another);

Impact

Impacts are the total sum of the different effects of an incident. This needs to take into account at least the following qualitative and quantitative effects:

- *Scope* - The loss of a critical infrastructure element is rated by the extent of the geographic area which could be affected by its loss or unavailability - international, national, regional or local.

- *Severity* - The degree of the loss can be assessed as None, Minimal, Moderate or Major. Among the criteria which can be used to assess impact are:

  – Public (number of population affected, loss of life, medical illness, serious injury, evacuation);

  – Economic (GDP effect, significance of economic loss and/or degradation of products or services, interruption of transport or energy services, water or food shortages);

  – Environment (effect on the public and surrounding location);

  – Interdependency (between other critical infrastructure elements).

  – Political effects (confidence in the ability of government);

  – Psychological effects (may escalate otherwise minor events). both during and after the incident and at different spatial levels (e.g. local, regional, national and international)

- *Effects of time* - This criteria ascertains at what point the loss of an element could have a serious impact (i.e. immediate, 24-48 hours, one week, other).

Interdependency

Identified connections or lack thereof between and within infrastructure sectors with essential systems and assets.

Occurrence

The term "occurrence" in the CIP context is defined as an event (either human caused or by natural phenomena) that requires a serious emergency response to protect life or property or puts at risk public safety and confidence, seriously disrupts the economy, or impedes the continuity of a MS government and its services. Occurrences include negligence, accidents, deliberate acts of terrorism, computer hacking, criminal activity and malicious damage, major disasters, urban fires, floods, hazardous materials spills, nuclear accidents, aircraft accidents, earthquakes, storms, public health and medical emergencies and other occurrences requiring a major emergency response.

Operator Security Plan

The Operator Security Plan (OSP) identifies all of the operator's critical infrastructure assets and establishes relevant security solutions for their protection. The OSP describes the methods and procedures which are to be followed by the owner/operator.

Prevention

The range of deliberate, critical tasks and activities necessary to build, sustain, and improve the operational capability to prevent, protect against, respond to, and recover from an incident. Prevention involves efforts to identify threats, determine vulnerabilities and identify required resources.

Prevention involves actions to protect lives and property. It involves applying intelligence and other information to a range of activities that may include such countermeasures as deterrence operations; heightened inspections; improved surveillance and security operations; investigations to determine the full nature and source of the threat; public health and agricultural surveillance and testing processes; immunizations, isolation, or quarantine; and as appropriate specific law enforcement operations aimed at deterring, pre-empting, interdicting, or disrupting illegal activity, and apprehending potential perpetrators and bringing them to justice. Prevention involves the stopping of an incident before it happens with effective processes, guidelines, standards and certification. Seamless interactive systems, and comprehensive threat- and vulnerability analysis.

Prevention is a continuous process of ongoing actions to reduce exposure to, probability of, or potential loss from hazards.

Response

Activities that address the short-term direct effects of an incident. Response includes immediate actions to save lives, protect property, and meet basic human needs. As indicated by the situation, response activities include applying intelligence and other information to lessen the effects or consequences of an incident; increased security operations; continuing investigations into nature and source of the threat; ongoing public health and agricultural surveillance and testing processes; immunizations, isolation, or quarantine; and specific law enforcement operations aimed at pre-empting, interdicting, or disrupting illegal activity, and apprehending actual perpetrators and bringing them to justice.

Risk

The possibility of loss, damage or injury. The level of risk is a condition of two factors: (1) the value placed on the asset by its owner/operator and the impact of loss or change to the asset, and (2) the likelihood that a specific vulnerability will be exploited by a particular threat.

Threat

Any indication, circumstance, or event with the potential to disrupt or destroy critical infrastructure, or any element thereof. An all-hazards approach to threat includes accidents, natural hazards as well as deliberate attacks. It can also be defined as the intention and capability of an adversary to undertake actions that would be detrimental to critical assets.

Vulnerability

A characteristic of an element of the critical infrastructure's design, implementation, or operation that renders it susceptible to destruction or incapacitation by a threat.

ANNEX 2

INDICATIVE LIST OF CRITICAL INFRASTRUCTURE SECTORS

Sector		Product or service	
I	Energy	1	Oil and gas production, refining, treatment and storage, including pipelines
		2	Electricity generation
		3	Transmission of electricity, gas and oil
		4	Distribution of electricity, gas and oil
II	Information, Communication Technologies, ICT	5	Information system and network protection
		6	Instrumentation automation and control systems (SCADA etc.)
		7	Internet
		8	Provision of fixed telecommunications
		9	Provision of mobile telecommunications
		10	Radio communication and navigation
		11	Satellite communication
		12	Broadcasting
III	Water	13	Provision of drinking water
		14	Control of water quality
		15	Stemming and control of water quantity
IV	Food	16	Provision of food and safeguarding food safety and security
V	Health	17	Medical and hospital care
		18	Medicines, serums, vaccines and pharmaceuticals
		19	Bio-laboratories and bio-agents
VI	Financial	20	Payment services/payment structures (private)
		21	Government financial assignment
VII	Public & Legal Order and Safety	22	Maintaining public & legal order, safety and security
		23	Administration of justice and detention
VIII	Civil administration	24	Government functions
		25	Armed forces
		26	Civil administration services
		27	Emergency services
		28	Postal and courier services
IX	Transport	29	Road transport
		30	Rail transport
		31	Air traffic
		32	Inland waterways transport
		33	Ocean and short-sea shipping
X	Chemical and nuclear industry	34	Production and storage/processing of chemical and nuclear substances
		35	Pipelines of dangerous goods (chemical substances)
XI	Space and Research	36	Space
		37	Research

ANNEX 3

OPERATOR SECURITY PLAN

The possible contents of the OSP should include an introduction and a classified detail part (not accessible outside the relevant MS authorities). The classified part would begin with a presentation of the operator and describe the legal context of its CI activities. The OSP would then go on to presenting the details on the criticality of the infrastructure concerned, taking into consideration the operator's objectives and the Member State's interests. The critical points of the infrastructure would be identified and their security requirements presented. A risk analysis based on major threat scenarios, vulnerability of each critical point, and potential impact would be conducted. Based on this risk analysis, relevant protection measures should be foreseen.

Introduction)

Contains information concerning the pursued objectives and the main organisational and protection principles.

Detailed part *(classified)*

– **Presentation of the operator**

Contains a description of the operator's activities, organization and connections with the public authorities. The details of the operator's Security Liaison Office (SLO) are given.

– **Legal context**

The operator addresses the requirements of the National CIP Programme and the sector specific CIP programme where relevant.

– **Description of the criticality of the infrastructure**

The operator describes in detail the critical services/products he provides and how particular elements of the infrastructure come together to create an end-product. Details should be provided concerning:

- material elements;
- non-material elements (sensors, command, information systems);
- human elements (decision-maker, expert);
- access to information (databases, reference systems);
- dependence on other systems (energy, telecoms);
- specific procedures (organisation, management of malfunctions, etc.).

– **Formalisation of security requirements**

The operator identifies the critical points in the infrastructure, which could not be easily replaced and whose destruction or malfunctioning could significantly disrupt the operation of the activity or seriously endanger the safety of users, customers or employees or result in essential public needs not being satisfied. The security of these critical points is then addressed.

The owners, operators and users ('users' being defined as organizations that exploit and use the infrastructure for business and service provision purposes) of critical infrastructure would have to identify the critical points of their infrastructure, which would be deemed restricted areas. Access to restricted areas should be monitored in order to ensure than no unauthorised persons and vehicles enter such areas. Access would only be granted to security cleared personnel. The relevant background security checks (if deemed necessary by a MS CIP sector authority) should be carried out by the Member State in which the critical infrastructure is located.

– **Risk analysis and management**

The operator conducts and risk analysis concerning each critical point.

– **Security measures**

The operator presents the security measures arranged around two headings:

- Permanent security measures, which will identify indispensable security investment and means, which cannot be installed by the owner/operator in a hurry. The owner/operator will maintain a standing alertness against potential threats, which will not disturb its regular economic, administrative and social activities. This heading will include information concerning general measures; technical measures (including installation of detection, access control, protection and prevention means); organizational measures (including procedures for alerts and crisis management); control and verification measures; communication; awareness raising and training; and security of information systems.

- Graduated security measures, which may be activated according to varying threat levels. The OSP will therefore foresee various security regimes adapted to possible threat levels existing in the Member State.

– **Presentation and application**

The operator will prepare detailed information sheets and instructions on how to react to various situations.

– **Monitoring and updating**

The operator sets out the relevant monitoring and updating mechanisms which will be used.