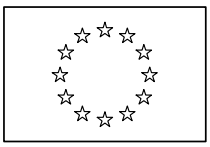

EUROPEISKA GEMENSKAPERNAS KOMMISSION

Bryssel den 17.11.2005
KOM(2005) 576 slutlig

GRÖNBOK

OM ETT EUROPEISKT PROGRAM FÖR SKYDD AV KRITISK INFRASTRUKTUR

(framlagt av kommissionen)

GRÖNBOK

OM ETT EUROPEISKT PROGRAM FÖR SKYDD AV KRITISK INFRASTRUKTUR

1. BAKGRUND

Kritisk infrastruktur kan skadas, förstöras eller utsättas för störningar genom planerade terrordåd, naturkatastrofer, försummelse, olyckor eller dataintrång, brottslig verksamhet och sabotage. För att rädda liv och egendom inom EU som utsätts för hot från terrorism, naturkatastrofer och olyckor bör eventuella störningar eller manipulationer av kritisk infrastruktur, om så är möjligt, vara kortvariga, sällsynta, hanterbara, geografiskt isolerade och minimalt skadliga för medlemsstaterna, deras medborgare och Europeiska unionen. Terroristattackerna i Madrid och London har accentuerat risken för terroristattacker mot europeisk infrastruktur. EU:s insatser måste vara snabba, samordnade och effektiva.

Europeiska rådet bad i juni 2004 kommissionen att utarbeta en övergripande strategi för skydd av kritisk infrastruktur. Med anledning av detta antog kommissionen den 20 oktober 2004 meddelandet ”Skydd av kritisk infrastruktur i kampen mot terrorismen” med tydliga förslag om vad som skulle kunna förbättra de förebyggande åtgärderna, beredskapen och insatserna i Europa gentemot terroristattacker som drabbar kritisk infrastruktur.

I rådets slutsatser när det gäller att förebygga, ha beredskap för och bemöta terroristattacker samt i EU:s solidaritetsprogram avseende konsekvenserna av terroristhot och terroristattacker, som antogs av rådet i december 2004, godkändes kommissionens avsikt att föreslå ett europeiskt program för skydd av kritisk infrastruktur (EPCIP – dvs. *European Programme for Critical Infrastructure Protection*) och vidare lämnades samtycke till att kommissionen inrättar ett nätverk för varningar om hot mot kritisk infrastruktur (CIWIN – dvs. *Critical Infrastructure Warning Information Network*).

Kommissionen arrangerade två seminarier och efterlyste idéer och kommentarer från medlemsstaterna. Det första seminariet om skydd av EU:s kritiska infrastruktur hölls den 6–7 juni 2005 med deltagande från medlemsstaterna. Efter seminariet lämnade medlemsstaterna kommissionen bakgrundsmaterial om sina upplägg ifråga om skyddet av kritisk infrastruktur samt kommentarer till de idéer som diskuterats under seminariet. Bidragen mottogs i juni och juli, och utgjorde basen för ytterligare utveckling av skyddet av kritisk infrastruktur. Det andra EU-seminariet om skydd av kritisk infrastruktur hölls den 12–13 september för att ge ytterliga tillfälle att dryfta frågor om skydd av kritisk infrastruktur. Både medlemsstaterna och näringslivsorganisationer deltog i detta seminarium. Som en följd därav har kommissionen beslutat att lägga fram denna grönbok som ger grunddragen till de olika alternativen för det europeiska programmet för skydd av kritisk infrastruktur.

2. GRÖNBOKENS SYFTE

Det huvudsakliga målet med grönboken är att få feedback avseende möjliga politiska alternativ i fråga om EPCIP genom att involvera ett stort antal berörda aktörer. För att reellt kunna skydda kritisk infrastruktur krävs kommunikation, samordning och samarbete både på nationell nivå och på EU-nivå mellan alla berörda parter – ägare och operatörer av

infrastruktur, tillsynsmyndigheter, yrkesorganisationer och näringslivsorganisationer i samarbete med alla nivåer inom statsapparaten samt med allmänheten.

Grönboken ger olika alternativ till hur kommissionen skulle kunna uppfylla rådets begäran om att inrätta EPCIP samt CIWIN och utgör den andra fasen i en samrådsprocess som skall utmynna i ett europeiskt program för skydd av kritisk infrastruktur. I och med publiceringen av denna grönbok förväntar sig kommissionen att få konkret feedback om de politiska alternativ som här skisseras. Beroende på resultatet från samrådsprocessen skulle ett politiskt paket med avseende på EPCIP kunna läggas fram under 2006.

3. SYFTE OCH RÄCKVIDD FÖR EPCIP

3.1. EPCIP:s övergripande mål

Målet för EPCIP skulle vara att se till att det finns adekvata och likvärdiga skyddsnivåer för kritisk infrastruktur, minsta möjliga antal svaga punkter och snabba, väl uttestade återhämtningsrutiner i hela EU. Skyddsnivån kan inte vara likvärdig för all kritisk infrastruktur och kan vara avhängig de konsekvenser som blir följden av störningar i den aktuella infrastrukturen. EPCIP skulle vara en fortlöpande process och regelbundna översyner krävs för att man skall kunna hålla jämna steg med nya frågor och farhågor.

EPCIP bör i möjligaste mån minimera eventuella negativa konsekvenser som ökade säkerhetsinvesteringar kan få på den specifika branschens konkurrenskraft. När man beräknar kostnadsproportionaliteten får man inte glömma bort behovet av en bibehållen marknadsstabilitet, vilket är avgörande för långsiktiga investeringar, säkerhetens inverkan på utvecklingen av fondbörserna samt den makroekonomiska dimensionen.

Fråga

Är detta ett lämpligt mål för EPCIP? Om inte, vad borde målet vara?

3.2. Vad bör EPCIP skydda mot?

Även om konsekvenshanteringsåtgärderna är identiska eller likartade för de flesta störningar, kan skyddsåtgärderna skilja sig åt allt efter hotets karaktär. Både planerade attacker och naturkatastrofer ingår bland de hot som avsevärt minskar möjligheterna att säkra befolkningens väsentliga behov och säkerhet, att vidmakthålla ordningen och att tillhandahålla ett minimum av viktiga offentliga tjänster eller se till att ekonomin fungerar ordentligt. Alternativen är de följande:

a) **Ett heltäckande upplägg för alla sorters risker** – Ett allsidigt upplägg som både tar hänsyn till hotet från planerade attacker och från naturkatastrofer. Det skulle innebära att synergierna mellan skyddsåtgärderna utnyttjas maximalt, men skulle inte särskilt betona terrorismen.

b) **Ett upplägg för alla risker, men med prioritering för terrorism** – Ett flexibelt upplägg som säkrar en koppling till andra risktyper, t.ex. hot från planerade attacker såväl som från naturkatastrofer, men med terrorism som en prioritering. Om nivån på skyddsåtgärderna inom en speciell näringslivssektor skulle befinnas vara adekvata, skulle de berörda aktörerna koncentrera sig på de hot som de fortfarande är sårbara inför.

c) **Ett upplägg för terrorismrisker** – Detta upplägg skulle koncentreras på terrorism och skulle generellt inte uppmärksamma de mer gängse hoten.

Fråga
Vilket upplägg bör EPCIP har? Varför?

4. FÖRESLAGNA HUVUDPRINCIPER

Följande huvudprinciper föreslås utgöra basen för EPCIP:

- **Subsidiaritet** – Subsidiariteten skulle inta en central plats i EPCIP, varvid skyddet av kritisk infrastruktur först och främst skulle vara ett nationellt ansvarsområde. Det främsta ansvaret för skyddet av kritisk infrastruktur skulle ligga på medlemsstaterna och ägarna/operatörerna som skulle agera inom en gemensam ram. Kommissionen skulle i sin tur koncentrera sig på de aspekter av detta skydd som har en gränsöverskridande effekt inom EU. Ägarnas och operatörernas ansvarighet när det gäller att fatta egna beslut och själv planera för skyddet av de egna anläggningarna skulle inte förändras.

- **Komplementaritet** – den gemensamma ramen för EPCIP skulle utgöra ett komplement till redan befintliga åtgärder. De gemenskapsmekanismer som redan införts bör fortsatt utnyttjas och de kommer att bidra till att garantera det övergripande genomförandet av EPCIP.

- **Konfidentialitet** – Utbytet av information om skyddet av kritisk infrastruktur skulle äga rum på ett förtroendefull och konfidentiellt sätt. Detta är nödvändigt med tanke på att fakta om kritisk infrastruktur kan användas för att orsaka störningar eller oacceptabla följder för kritiska infrastrukturanläggningar. På såväl EU-nivå nivå som nationell nivå skulle information om skyddet av kritisk infrastruktur vara hemligstämplad och tillgång beviljas endast till personer som verkligen behöver denna information.

- **Samarbete mellan berörda aktörer** – Alla berörda aktörer, bland vilka ingår medlemsstaterna, kommissionen, industri/näringslivsorganisationer, standardiseringsorgan och ägare, operatörer och användare (”användare” definieras som organisationer som utnyttjar och använder infrastrukturen för affärsändamål och för tillhandahållande av tjänster) har en roll att spela i skyddet av kritisk infrastruktur. Alla berörda aktörer bör samarbeta och bidra till utvecklingen och genomförandet av EPCIP i enlighet med deras specifika roller och ansvarsområden. Medlemsstaternas myndigheter skulle stå för ledarskapet och samordningen vid utvecklingen och genomförandet av ett nationellt konsekvent upplägg för skyddet av kritisk infrastruktur inom deras jurisdiktion. Ägarna, operatörerna och användarna skulle aktivt medverka både på nationell och unionell nivå. I de fall sektoriella normer inte finns eller om internationella normer ännu inte har fastställts skulle standardiseringsorganisationerna gemensamt kunna anta normer när så är lämpligt.

- **Proportionalitet** – Skyddsstrategier och -åtgärder skulle stå i proportion till den aktuella risknivån, eftersom all infrastruktur inte kan skyddas från alla hot (exempelvis är elöverföringsnäten för omfattande för att stängslas in eller att bevaka). Med hjälp av lämpliga riskhanteringsmetoder skulle uppmärksamheten kunna koncentreras på de mest utsatta riskområdena, med hänsyn till hotet, objektets relativa betydelse, förhållandet

mellan kostnaderna och nyttan, nivån på skyddet och graden av effektivitet hos de tillgängliga strategier som skall mildra verkningarna.

Fråga

Är dessa huvudprinciper godtagbara? Är en del överflödiga? Finns det andra som borde tas i övervägande?

Håller Ni med om att skyddsåtgärderna bör stå i proportion till den aktuella risknivån, eftersom ju all infrastruktur inte kan skyddas från alla hot?

5. EN GEMENSAM RAM FÖR EPCIP

En skada på eller förlust av en infrastrukturanläggning i en medlemsstat kan få negativa verkningar på flera andra medlemsstater och på den europeiska ekonomin som helhet. Detta blir alltmer sannolikt i takt med att den nya tekniken (t.ex. Internet) och avregleringen av marknaderna (t.ex. el- och gasleveranser) medför att mycket infrastruktur blir en del i ett större nät. I en sådan situation är skyddsåtgärderna inte effektivare än sin svagaste länk. Detta innebär att en gemensam skyddsnivå kan vara nödvändig.

För att ett skydd skall vara effektivt krävs kommunikation, samordning, och samarbete nationellt, på EU-nivå (när så krävs) och internationellt bland alla berörda aktörer. En gemensam EU-ram för skydd av kritisk infrastruktur i Europa skulle kunna införas för att se till att varje medlemsstats skydd av kritisk infrastruktur ligger på en lämplig och likvärdig nivå och att reglerna för konkurrensen inom den inre marknaden inte snedvrids. Som stöd för medlemsstaternas arbete skulle kommissionen underlätta identifiering, utbyte och spridning av de bästa lösningarna i frågor som berör skydd av kritisk infrastruktur genom att skapa en gemensam ram för skyddet av kritisk infrastruktur. Räckvidden för denna allmänna ram måste tas upp till behandling.

Den gemensamma ramen för EPCIP skulle innehålla övergripande åtgärder som definierar kompetens och ansvarsområden för alla berörda aktörer i fråga om skyddet av kritisk infrastruktur och dessutom lägga en grund för sektorsspecifika upplägg. Den gemensamma ramen är avsedd att komplettera de befintliga åtgärderna på gemenskapsnivå och i medlemsstaterna för att ge högsta möjliga nivå av säkerhet för den kritiska infrastruktur som finns inom Europeiska unionen. Arbetet med att nå en överenskommelse om en gemensam förteckning över definitioner och sektorer med kritisk infrastruktur bör få prioritet.

Eftersom de olika sektorerna med kritisk infrastruktur är mycket olikartade, vore det svårt att exakt föreskriva vilka kriterier som bör tillämpas för att identifiera och skydda all infrastruktur i en övergripande ram. Detta borde i stället ske i varje sektor för sig. Likväl finns det behov av en samsyn i vissa övergripande frågor.

Enligt förslaget skall därför förstärkningen av säkerheten för kritisk infrastruktur i EU uppnås genom att man fastställer en gemensam ram för EPCIP, (gemensamma mål och metoder t.ex. för jämförelser, interdependenser) utbyte av bästa lösningar och mekanismer för att övervaka efterlevnaden. Bland dessa element, som skulle utgöra en del av den gemensamma ramen, skulle följande ingå:

- Gemensamma principer för skyddet av kritisk infrastruktur.
- Gemensamt överenskomna förhållningssätt/normer.
- Gemensamma definitioner på grundval av vilka sektorsspecifika definitioner som man kan enas om (en vägledande förteckning över definitioner återfinns i bilaga 1).
- Gemensam förteckning över kritiska infrastruktursektorer (en vägledande förteckning över sektorer återfinns i bilaga 2).
- Prioriterade områden när det gäller skyddet av kritisk infrastruktur.
- Beskrivning av de medverkande berörda aktörernas ansvarsområden.
- Överenskomna benchmarks.
- Metoder för att jämföra och prioritera infrastruktur inom olika sektorer.

En sådan gemensam ram skulle också minimera potentiella snedvridande effekter på den inre marknaden.

Den gemensamma ramen för EPCIP skulle kunna vara frivillig eller obligatorisk – eller en blandning av båda, beroende på vad den avser. Båda typerna av ramverk skulle kunna komplettera redan existerande sektoriella och horisontella åtgärder på EG- och medlemsstatsnivå. Det är dock endast en lagstiftningsram som kan ge en rättslig grund för ett konsekvent och enhetligt genomförande av åtgärder till skydd för kritisk EU-infrastruktur, som är stark och möjlig att genomdriva, och samtidigt tydligt definierar medlemsstaternas och kommissionens respektive ansvarsområden. Icke bindande frivilliga åtgärder är visserligen flexibla, men skulle inte ge någon klarhet om vem som skall göra vad.

Med utgångspunkt i resultatet av en noggrann analys och med vederbörlig hänsyn till proportionaliteten hos de föreslagna åtgärderna kan kommissionen använda sig av ett antal instrument, också lagstiftning, i sitt EPCIP-förslag. I tillämpliga fall kommer förslag till särskilda åtgärder att åtföljas av konsekvensbedömningar.

Frågor

Skulle en gemensam ram effektivt stärka skyddet av kritisk infrastruktur?

Vilka olika beståndsdelar bör en eventuell lagstiftningsram innehålla?

Håller Ni med om att kriterierna för att identifiera olika typer av kritisk EU-infrastruktur samt de skyddsåtgärder som anses nödvändiga bör identifieras sektor för sektor?

Skulle en gemensam ram hjälpa till att klargöra vilka områden de berörda aktörerna ansvarar för? Vad i en sådan gemensam ram borde vara obligatoriskt och vad frivilligt?

Vad borde den gemensamma ramen ha för räckvidd?Instämmer Ni med förteckningen över vägledande termer och definitioner i bilaga I på vars grundval sektorsspecifika definitioner (i tillämpliga fall) kan skapas? Instämmer Ni med den vägledande förteckningen över sektorer med kritisk infrastruktur i bilaga II?

6. KRITISK EU-INFRASTRUKTUR

6.1. Definition av kritisk EU-infrastruktur

Definitionen av vad som är en kritisk EU-infrastruktur skulle avgöras av vilka gränsöverskridande verkningar av allvarlig art en incident kan få utanför den medlemsstat där anläggningen finns. En annan sak som här måste beaktas är att bilaterala samarbetsprogram mellan medlemsstaterna för skydd av kritisk infrastruktur utgör ett väletablerat och effektivt medel för att handskas med kritisk infrastruktur mellan två medlemsstaters gränser. Sådant samarbete skulle komplettera EPCIP.

Kritisk EU-infrastruktur kan inbegripa de fysiska resurser, tjänster, informationstekniska utrustningar, nät och infrastrukturanläggningar, som, om de utsätts för störningar eller förstörs skulle få allvarliga konsekvenser för hälsa, trygghet, säkerhet samt ekonomiska eller sociala förhållanden i antingen

(a) två eller fler medlemsstater – **detta skulle inkludera viss bilateral kritisk infrastruktur (när så är relevant),** eller

(b) tre eller fler medlemsstater **– detta skulle exkludera all bilateral kritisk infrastruktur.**

När man beaktar dessa alternativs respektive förtjänster är det viktigt att komma ihåg följande punkter:

– Det faktum att en infrastrukturanläggning skulle klassificeras som kritisk EU-infrastruktur, innebär inte att den nödvändigtvis skulle kräva några ytterligare skyddsåtgärder. Befintliga skyddsåtgärder, vari bilaterala avtal mellan medlemsstater skulle kunna ingå, kan vara fullkomligt adekvata och följaktligen lämnas oförändrade också efter det att anläggningen klassificerats som en kritisk EU-infrastruktur.

– Alternativ a) kan inbegripa att fler infrastrukturer klassificeras som kritiska för EU.

– Alternativ b) kan innebära att gemenskapen, i fråga om infrastruktur som endast berör två medlemsstater, inte skulle medverka även om en av dessa två medlemsstater skulle anse att skyddsnivån var inadekvat och den andra medlemsstaten skulle vägra att vidta några åtgärder. Alternativ b) skulle också kunna leda till en mängd bilaterala överenskommelser eller meningsskiljaktigheter mellan medlemsstater. Företagen, som ofta verkar över hela Europa, kan tvingas arbeta med ett lapptäcke av olika överenskommelser som kan medföra extrakostnader.

Dessutom har man enats om att kritisk infrastruktur härrörande från eller befintlig på platser utanför EU, men som är sammanlänkande eller har en potentiellt direkt effekt på EU:s medlemsstater även bör tas till övervägande.

Fråga

Bör kritisk EU-infrastruktur vara infrastruktur som har potentiellt allvarliga gränsöverskridande konsekvenser för två eller fler medlemsstater, eller tre eller fler medlemsstater? Varför?

6.2. Interdependenser

Det har föreslagits att man i den successiva kartläggningen av all kritisk EU-infrastruktur särskilt skall beakta interdependenser. Studier av interdependenser skulle bidra till bedömningen av de potentiella konsekvenserna av hot mot specifik kritisk infrastruktur och särskilt till att utröna vilka medlemsstater som skulle påverkas vid en större incident som berör kritisk infrastruktur.

Man skulle till fullo beakta interdependenserna inom och mellan företag, näringslivssektorer, geografiska jurisdiktioner och medlemsstaternas myndigheter, i synnerhet de som är beroende av informations- och kommunikationsteknik för att fungera. Kommissionen, medlemsstaterna och ägare/operatörer av kritisk infrastruktur skulle arbeta tillsammans för att identifiera dessa interdependenser och tillämpa lämpliga strategier för att reducera riskerna där så är möjligt.

Fråga

Hur kan man ta hänsyn till interdependenser?

Känner Ni till några lämpliga metoder för analys av interdependenser?

På vilken nivå bör kartläggningen av interdependenser ske – på EU-nivå och/eller på nationell nivå?

6.3. Det stegvisa genomförandet för kritisk EU-infrastruktur

Kommissionen vill föreslå följande genomförandesteg för kritisk EU-infrastruktur:

(1) Kommissionen utarbetar tillsammans med medlemsstaterna de särskilda kriterier som skulle användas för att urskilja kritisk EU-infrastruktur på sektorsspecifik basis.

(2) Medlemsstaterna och kommissionen kartlägger och verifierar successivt den nationellt kritiska infrastrukturen sektor för sektor. Beslutet om att klassificera viss kritisk infrastruktur som kritisk EU-infrastruktur kommer att fattas på europeisk nivå[1] på grundval av den aktuella infrastrukturens gränsöverskridande karaktär.

(3) Medlemsstaterna och kommissionen analyserar existerande luckor i säkerheten i fråga om kritisk EU-infrastruktur i sektor för sektor.

(4) Medlemsstaterna och kommissionen enas om prioriterade sektorer/infrastrukturer, under beaktade av interdependenser.

[1] Med undantag för försvarsrelaterad infrastruktur.

(5) När så krävs enas kommissionen och de viktigaste berörda aktörerna i medlemsstaterna i sektor efter sektor om förslag till minimiskyddsåtgärder, eventuellt även normer.

(6) Efter antagandet av förslagen i rådet genomförs åtgärderna därefter.

(7) För en regelbunden övervakning ansvarar medlemsstaterna och kommissionen. Revideringar (åtgärder samt kartläggning av kritisk infrastruktur) görs när så är påkallat.

Frågor

Är förteckningen över stegen i genomförandet av kritisk EU-infrastruktur godtagbar?

Hur föreslår Ni att kommissionen och medlemsstaterna tillsammans skall avgöra vad som är kritisk EU-infrastruktur – medlemsstaterna har sakkunskapen, medan kommissionen har överblicken över vad som ligger i det europeiska intresset? Borde det finnas ett rättsligt bindande beslut?

Behövs det en förlikningsmekanism om en viss medlemsstat inte går med på att klassificera en infrastruktur under sin jurisdiktion som kritisk EU-infrastruktur?

Finns det behov för att verifiera beslut om att klassificera en infrastruktur som kritisk? Vem bör vara ansvarig?

Bör en medlemsstat kunna klassificera infrastruktur i andra medlemsstater eller tredjeländer såsom kritiska för dem? Vad skulle hända om en medlemsstat, ett tredjeland eller en bransch anser att en infrastruktur i en medlemsstat är kritisk ur för dem?

Vad skulle hända om denna medlemsstat inte fattar motsvarande beslut? Behövs det en mekanism för överklaganden? Om så är fallet, varför?

Bör en operatör kunna överklaga om han inte instämmer i att hans infrastruktur klassificeras eller inte klassificeras som kritisk? Om så är fallet, till vem?

Vilka metoder behöver tas fram för att avgöra prioritetsordningen mellan sektorer/infrastrukturer? Finns det redan lämpliga metoder som kan anpassas till EU-nivå?

Hur kan kommissionen medverka i analyserna av säkerhetsluckor, när det gäller kritisk EU-infrastruktur?

7. NATIONELLT KRITISK INFRASTRUKTUR

7.1. Den nationellt kritiska infrastrukturens roll i EPCIP

Många europeiska företag verkar i andra länder än det egna och är därför underkastade olika skyldigheter i fråga om den nationellt kritiska infrastrukturen. I medlemsstaternas och hela EU:s intresse bör därför varje medlemsstat skydda sin nationellt kritiska infrastruktur med utgångspunkt i en gemensam ram så att ägare och operatörer överallt i Europa slipper lyda under ett lapptäcke av regelverk som medför en mängd olika förfaranden och extrakostnader. Därför föreslår kommissionen att EPCIP visserligen primärt skall koncentreras på EU-kritisk

infrastruktur, men ändå inte helt skulle kunna utelämna nationellt kritisk infrastruktur. Likväl kan tre alternativ tänkas:

(a) Nationellt kritisk infrastruktur är fullt integrerad inom EPCIP

(b) Nationellt kritisk infrastruktur ligger utanför EPCIP:s räckvidd

(c) Medlemsstaterna kan av egen fri vilja använda sig av delar av det europeiska programmet för nationellt kritisk infrastruktur, men de är inte skyldiga att göra så.

Fråga

Ett verkningsfullt skydd av kritisk infrastruktur i Europeiska unionen verkar kräva att man kartlägger både kritisk EU-infrastruktur och nationellt kritisk infrastruktur. Instämmer Ni med att även om EPCIP skulle koncentreras på kritisk EU-infrastruktur så kan nationellt kritisk infrastruktur inte helt lämnas åt sidan?

Vilket av dessa alternativ anser Ni vara mest lämpligt för EPCIP?

7.2. Nationella program för skydd av kritisk infrastruktur

På grundval av en gemensam EPCIP-ram skulle medlemsstaterna kunna ta fram egna inhemska program för skydd av kritisk infrastruktur för sin nationellt kritiska infrastruktur. Medlemsstaterna skulle kunna tillämpa strängare bestämmelser än dem som ingår i EPCIP.

Fråga

Är det önskvärt att varje medlemsstat på grundval av EPCIP skall anta ett nationellt program för skydd av kritisk infrastruktur?

7.3. Ett enda övervakningsorgan

Behovet av effektivitet och koherens talar för nödvändigheten av att varje medlemsstat utser ett övervakningsorgan som tar hand om det övergripande genomförandet av EPCIP. Två alternativ kan tänkas:

(a) Ett enda organ har hand om uppsikten över kritisk infrastruktur.

(b) En nationell kontaktpunkt utan befogenheter, medan medlemsstaterna själva får sköta organisationen.

Ett sådant organ skulle inom sin jurisdiktion kunna samordna, övervaka och ha uppsikt över genomförandet av EPCIP och skulle kunna tjäna som huvudsaklig institutionell kontaktpunkt i fråga om skyddsfrågor i förhållande till kommissionen, andra medlemsstater samt ägare och operatörer av kritisk infrastruktur. Detta organ skulle kunna utgöra basen för den nationella representationen i expertgrupper som behandlar frågor i ämnet och skulle kunna vara kopplad till informationsnätverket för kritisk infrastruktur (CIWIN). Det nationella samordnings-organet för skyddet av kritisk infrastruktur skulle kunna samordna frågor rörande det nationella skyddet av kritisk infrastruktur trots att andra organ eller enheter inom en medlemsstat eventuellt redan är inblandade i frågor rörande detta skydd.

Den successiva kartläggningen av nationellt kritisk infrastruktur skulle kunna ske genom att man förpliktigar ägare och operatörer att meddela det nationella samordningsorganet all relevant verksamhet som rör kritisk infrastruktur.

Det nationella samordningsorganet för skyddet av kritisk infrastruktur skulle kunna vara ansvarigt för det rättsliga beslutet att klassificera en infrastruktur under dess jurisdiktion som en nationellt kritisk infrastruktur. Denna information skulle vara tillgänglig endast för den berörda medlemsstaten.

Specifika befogenheter skulle kunna inbegripa

a) att samordna, övervaka och ha uppsikt över det övergripandet genomförandet av EPCIP i en medlemsstat,

b) att agera som huvudsaklig institutionell kontaktpunkt angående frågor som gäller skydd av kritisk infrastruktur för:

   i. kommissionen

   ii. andra medlemsstater

   iii. ägare och operatörer av kritisk infrastruktur.

c) att delta i besluten om vad som skall klassificeras som kritisk EU-infrastruktur,

d) att fatta rättsligt bindande beslut när en infrastruktur under landets jurisdiktion klassificera som en nationellt kritisk infrastruktur,

e) att agera som besvärsinstans för ägare/operatörer som inte håller med om att deras infrastruktur klassificeras som ”kritisk infrastruktur”,

f) att delta i utarbetandet av skyddsprogrammet för nationellt kritisk infrastruktur och de sektorsspecifika skyddsprogrammen för kritisk infrastruktur,

g) att ange interdependenser mellan specifika kritiska infrastruktursektorer,

h) att bidra till sektorsspecifika upplägg för skydd av kritisk infrastruktur genom medverkan i expertgrupper. Företrädare för ägarna och operatörerna skulle kunna uppmanas lämna sina bidrag till diskussionerna. Regelbundna möten skulle kunna hållas,

i) att ha tillsyn över processen med att utarbeta beredskapsplaner för kritisk infrastruktur.

Frågor

Håller Ni med om att medlemsstaterna ensamma bör vara ansvariga för att utse och handha nationellt kritisk infrastruktur på grundval av en gemensam EPCIP-ram?

Är det önskvärt att i varje medlemsstat skapa ett samordningsorgan för skydd av kritisk infrastruktur med övergripande samordningsansvar för åtgärder som berör detta skydd samtidigt som den respekterar redan existerande sektorsbaserade ansvarsområden (civila luftfartsmyndigheter, Seveso-direktivet etc.)?

Är de föreslagna befogenheterna lämpliga för ett sådant samordningsorgan? Är andra befogenheter nödvändiga?

7.4. Det stegvisa genomförandet för nationellt kritisk infrastruktur

Kommissionen vill föreslå följande stegvisa genomförande när det gäller nationellt kritisk infrastruktur:

(1) Med hjälp av EPCIP utarbetar medlemsstaterna de specifika kriterier som skulle användas för att kartlägga nationellt kritisk infrastruktur.

(2) Medlemsstaterna kartlägger och verifierar successivt sektor för sektor den nationellt kritiska infrastrukturen.

(3) Medlemsstaterna analyserar sektor för sektor existerande luckor i säkerheten vad gäller nationellt kritisk infrastruktur.

(4) Medlemsstaterna beslutar om prioriterade insatssektorer och beaktar, i tillämpliga fall, därvid interdependenser samt prioriteringar man enats om på EU-nivå.

(5) I tillämpliga fall enas medlemsstaterna om minimiskyddsåtgärder för varje sektor.

(6) Medlemsstaterna är ansvariga för att se till att ägare/operatörer inom deras jurisdiktion vidtar de nödvändiga genomförandeåtgärderna.

(7) Regelbunden övervakning sköts av medlemsstaterna. Revideringar (åtgärder och kartläggning av kritisk infrastruktur) görs när så är påkallat.

Fråga

Är förteckningen över stegen i genomförandet när det gäller nationellt kritisk infrastruktur lämplig? Är några steg överflödiga? Borde några steg läggas till?

8. DEN ROLL SOM SPELAS AV ÄGARE, OPERATÖRER OCH ANVÄNDARE AV KRITISK INFRASTRUKTUR

8.1. Ägarnas, operatörernas och användarnas ansvarsområden

När en infrastruktur klassificeras såsom kritisk innebär detta att ägare och operatörer åläggs ett visst ansvar. Man kan tänka sig fyra ansvarsområden för ägare och operatörer av infrastruktur som klassificerats som nationellt kritisk infrastruktur eller kritisk EU-infrastruktur:

(1) Anmälan till medlemsstatens relevanta organ för skydd av kritisk infrastruktur av att en infrastruktur kan vara kritisk.

(2) **Utnämning av en eller flera högre representanter som skall agera som sambandsansvarig i säkerhetsfrågor mellan ägaren/operatören och den relevanta medlemsstatens myndighet för skydd av kritisk infrastruktur**. Den sambandsansvarige skulle delta i utarbetandet av säkerhets- och beredskapsplaner. Den sambandsansvarige skulle ha huvudansvaret för sambandet med det relevanta sektorsorganet för skydd av kritisk infrastruktur i medlemsstaterna och vid behov med brottsbekämpningsmyndigheterna.

(3) **Fastställande, genomförande och uppdatering av operatörens säkerhetsplan (*Operator Security Plan* - OSP).** En föreslagen OSP-mall återfinns i bilaga 3.

(4) **Medverkan i utarbetandet av en beredskapsplan** gällande kritisk infrastruktur med relevanta civilförsvars- och brottsbekämpningsmyndigheter i medlemsstaterna när så begärs.

Operatörens säkerhetsplan skulle kunna lämnas in för godkännande av medlemsstatens relevanta sektorsmyndighet för det aktuella skyddet, som står under det nationella samordningsorganets övergripande tillsyn, oavsett om det är en nationellt kritisk infrastruktur eller kritisk EU-infrastruktur. Detta skulle garantera en enhetlighet i de säkerhetsåtgärder som generellt vidtas av specifika ägare och operatörer och inom de relevanta sektorerna. I gengäld skulle ägare och operatörer kunna få feedback och stöd när det gäller hot som är relevanta för dem, förändringar i fråga om de bästa lösningarna och, i tillämpliga fall, hjälp med att bedöma interdependenser och sårbara punkter via det nationella samordningsorganet för skydd av kritisk infrastruktur och, vid behov, av kommissionen.

Varje medlemsstat skulle kunna bestämma en egen tidsfrist för när en OSP skall ha upprättats av ägarna och operatörerna av nationellt kritisk infrastruktur och kritisk EU-infrastruktur (i fallet kritisk EU-infrastruktur skulle kommissionen också medverka) och bestämma administrativa böter om dessa tidsfrister inte iakttas.

Operatörens säkerhetsplan föreslås ange ägarens/operatörens kritiska infrastrukturanläggningar och ställa upp relevanta säkerhetslösningar för deras skydd. Operatörens säkerhetsplan skulle innehålla en beskrivning av metoder och förfaranden som skall följas för att säkerställa efterlevnaden av EPCIP, de nationella programmen för skydd av kritisk infrastruktur och relevanta program för sektorsspecifikt skydd av kritisk infrastruktur. Operatörens säkerhetsplan skulle kunna erbjuda en reglering ”nedifrån och uppåt” när det

gäller skyddet av kritisk infrastruktur, vilket ger större spelrum (men också mer ansvar) till den privata sektorn.

I specifika situationer skulle det i fråga om viss infrastruktur – t.ex. kraftledningsnät och informationsnät – vara orealistiskt (ur praktisk och ekonomisk synvinkel) att förvänta sig att ägare och operatörer skall åstadkomma en likvärdig nivå på säkerheten för alla sina anläggningar. I dessa fall föreslås att ägare och operatörer tillsammans med berörda myndigheter skulle kunna ange de kritiska punkterna (knutpunkterna) i ett fysiskt nät eller ett informationsnät som säkerhetsåtgärderna skulle kunna koncentreras på.

Operatörens säkerhetsplan kan innehålla säkerhetsåtgärder under två olika rubriker:

- **Permanenta säkerhetsåtgärder**, som skulle identifiera oundgängliga säkerhetsinvesteringar och medel som inte kan installeras av ägare/operatörer med kort varsel. Ägaren/operatören skulle ständigt vara vaksamma på potentiella hot, vilket inte skulle störa deras normala ekonomiska, administrativa och sociala verksamheter.

- **Graderade säkerhetsåtgärder**, som skulle kunna aktiveras i enlighet med varierande hotnivåer. Operatörens säkerhetsplan skulle därför förutse olika säkerhetsordningar anpassade till möjliga hotnivåer i den medlemsstat där infrastrukturen är belägen.

Ägare och operatörer av kritisk infrastruktur underlåter att uppfylla sin skyldighet att ta fram en OSP och bidra till utarbetandet av beredskapsplaner samt att utse en sambandsansvarig i säkerhetsfrågor skulle kunna bötfällas.

Frågor

Är det potentiella ansvaret för ägare/operatörer av kritisk infrastruktur godtagbart med tanke på den därigenom ökade säkerheten för kritisk infrastruktur? Vad skulle det sannolikt komma att kosta?

Bör ägare och operatörer vara skyldiga att meddela om deras infrastruktur kan vara kritisk? Anser Ni att OSP-konceptet är användbart? Varför?

Står de föreslagna skyldigheterna i proportion till kostnaderna?

Vilka rättigheter skulle ägarna och operatörerna av kritisk infrastruktur kunna få av medlemsstaternas myndigheter och kommissionen?

8.2. Dialog med ägare, operatörer och användare av kritisk infrastruktur

EPCIP skulle kunna involvera ägarna och operatörer i partnerskap. Huruvida ett skyddsprogram bli framgångsrikt beror på hur mycket samarbete och medverkan som kan uppnås med ägarna och operatörerna. I medlemsstaterna skulle ägare och operatörer av kritisk infrastruktur nära kunna medverka i utvecklingen av skyddet genom regelbundna kontakter med det nationella samordningsorganet för skydd av kritisk infrastruktur.

På EU-nivå skulle man kunna skapa fora för att underlätta utbyte av åsikter om allmänna och sektorsspecifika frågor om skyddet av kritisk infrastruktur. Ett gemensamt upplägg i fråga om privatsektorns medverkan i de aktuella skyddsfrågorna för att sammanföra alla berörda aktörer inom den offentliga och privata sfären skulle ge medlemsstaterna, kommissionen och näringslivet en viktig plattform för kontakter angående alla nya frågor som väcks. Ägarna, operatörerna och användarna av kritisk infrastruktur skulle kunna hjälpa till med utvecklingen av gemensamma riktlinjer, normer för bästa lösningar och, när så är lämpligt, informationsutbyte. En sådan dialog skulle hjälpa till att gestalta framtida revideringar av EPCIP.

När så är lämpligt skulle kommissionen kunna uppmuntra till bildandet av näringslivs-/företagssammanslutningar för skydd av kritisk EU-infrastruktur. De två yttersta målen skulle vara att säkra att det europeiska näringslivet bibehåller sin konkurrenskraft och att EU-medborgarnas säkerhet förbättras.

Fråga

Hur bör dialogen med ägare, operatörer och användare av kritisk infrastruktur vara strukturerad?

Vem skulle representera ägarna, operatörerna och användarna i den offentlig-privata dialogen?

9. ÅTGÄRDER TILL STÖD FÖR EPCIP

9.1. Nätverket för varningar om hot mot kritisk infrastruktur (CIWIN)

Kommissionen har tagit fram ett antal förvarningssystem som möjliggör konkreta, samordnade och verkningsfulla insatser vid nödlägen, inklusive sådana som uppstår genom terrordåd. Den 20 oktober 2004 meddelade kommissionen att man skapat ett centralt nät inom kommissionen för ett snabbt informationsflöde mellan alla kommissionens förvarningssystem och inblandade tjänsteenheter inom kommissionen (Argus).

Kommissionen föreslår att man skapar CIWIN, vilket skulle kunna stimulera utvecklingen av lämpliga skyddsåtgärder genom att underlätta ett säkert utbyte av de bästa lösningarna och samtidigt vara ett medel för att vidarebefordra överhängande hot och larm. Systemet skulle se till att rätt personer får rätt information vid rätt tidpunkt.

Följande tre alternativ är möjliga för utvecklingen av CIWIN:

(1) **CIWIN skulle existera som ett forum som inskränker sig till utbyte av idéer och bästa lösningar** i fråga om skyddet av kritisk infrastruktur som ett stöd för ägare och operatörer av kritisk infrastruktur. Ett sådant forum skulle kunna ta formen av ett nätverk av experter och en elektronisk plattform för utbyte av relevant information under säkra förhållanden. Kommissionen skulle spela en viktig roll vid insamling och spridning av denna information. Detta alternativ skulle inte göra det möjligt att utfärda erforderliga snabba larm vid överhängande hot. Det skulle dock kunna finnas utrymme för att bredda CIWIN i framtiden.

(2) **CIWIN skulle vara ett förvarningssystem som sammanlänkar medlemsstaterna med kommissionen.** Detta alternativ skulle öka säkerheten för kritisk infrastruktur genom att det ge varningar som begränsar sig till omedelbara hot och larm. Målet skulle vara att underlätta ett snabbt utbyte av information om potentiella hot mot ägare och operatörer av kritisk infrastruktur. Detta förvarningssystem skulle inte handha utbyte av långsiktiga underrättelseuppgifter. Det skulle användas för snabb spridning av information om överhängande hot mot specifik infrastruktur.

(3) **CIWIN skulle vara ett kommunikations-/larmsystem med flera nivåer bestående av två distinkta funktioner:** a) ett förvarningssystem som sammanlänkar medlemsstaterna med kommissionen och b) ett forum för utbyte av idéer om skydd av kritisk infrastruktur och de bästa lösningarna inom området till stöd för ägare och operatörer av sådan infrastruktur i form av ett nätverk av experter och en elektronisk plattform för utbyte av data.

Oavsett vilket alternativ som väljs skulle CIWIN komplettera de befintliga nätverken och vederbörlig omsorg skulle tas för att undvika dubbla system. På lång sikt kunde CIWIN vara kopplat till alla relevanta ägare och operatörer av kritisk infrastruktur i varje medlemsstat via exempelvis det nationella samordningsorganet för skydd av kritisk infrastruktur. Larm och uppgifter om de bästa lösningarna skulle kunna kanaliseras genom detta organ som skulle vara den enda tjänst direkt kopplad till kommissionen och därigenom till alla medlemsstaterna. Medlemsstaterna kunde utnyttja sina redan befintliga informationssystem för att inrätta sin nationella CIWIN-kapacitet som länkar myndigheterna till specifika ägare och operatörer. I första hand skulle dessa nationella nätverk användas av medlemsstaternas organ för skydd av kritisk infrastruktur samt av ägarna och operatörerna som ett system för tvåvägskommunikation.

En studie kommer att inledas för att avgöra räckvidden och de tekniska specifikationerna för CIWIN:s framtida gränssnitt till medlemsstaterna.

Frågor

Vilken form bör CIWIN-nätet ha för att understödja målen för EPCIP?

Bör ägare och operatörer av kritisk infrastruktur var uppkopplade till CIWIN?

9.2. Gemensamma metoder

Olika medlemsstaterna har olika larmnivåer avpassade till olika situationer. För närvarande är det omöjligt att veta exempelvis om beteckningen ”hög beredskap” i en medlemsstat är det samma som en ”hög beredskap” i en annan. Detta gör det svårt för företag med verksamhet i flera länder att prioritera sina utgifter för skyddsåtgärder. Det kan därför vara av nytta att försöka harmonisera eller ”kalibrera” de olika nivåerna.

Varje hotnivå skulle kunna motsvaras av en beredskapsnivå som utlöser generella gemensamma säkerhetsåtgärder och, i tillämpliga fall, speciellt att graderade säkerhetsåtgärder används. En medlemsstat som i en specifik hotsituation inte vill vidta en viss åtgärd skulle kunna agera med hjälp av alternativa säkerhetsåtgärder.

En gemensam metod kan tas under övervägande för att identifiera och klassificera hot, reaktionskapacitet, risker och sårbara punkter samt för att dra slutsatser om ett hot är reellt,

sannolikt och nog allvarligt för att kunna störa en infrastrukturanläggning. Detta skulle inkludera riskgradering och riskprioritering i enlighet med hur sannolika riskerna är, deras konsekvenser och förhållandet till andra riskområden eller -processer.

Frågor

I vilken omfattning är det önskvärt och genomförbart att harmonisera eller ”kalibrera” olika larmnivåer?

Borde det finnas en gemensam metod för att identifiera och klassificera hot, reaktionskapacitet, risker, och sårbara punkter och för att dra slutsatser om ett hot är reellt, sannolikt och nog allvarligt?

9.3. Finansiering

Efter ett initiativ från Europaparlamentet (den nya budgetposten – pilotprojekt ”Kampen mot terrorismen” – i 2005 års budget) beslöt kommissionen den 15 september att anslå 7 miljoner euro till finansiering av en rad insatser som kommer att förbättra EU:s förebyggande åtgärder, beredskap och insatser mot terroristattacker, inklusive konsekvenshantering, skydd av kritisk infrastruktur, terroristfinansiering, sprängämnen och radikalisering. Mer än två tredjedelar av denna budget är avsedd för förberedelserna av det framtida europeiska programmet för skydd av kritisk infrastruktur, för integrering och vidareutveckling av den kapacitet som krävs för att hantera kriser som drabbar flera länder och som är resultatet av eventuella terroristattacker och för nödåtgärder som kan behövas för att agera mot betydande hot eller förekomsten av en sådan attack. Dessa anslag förväntas också för år 2006.

Mellan 2007 och 2013 kommer utbetalningen av anslagen att skötas inom ramprogrammet för säkerhet och skydd av friheter. Här kommer ett särskilt program att ingå som gäller förebyggande åtgärder, beredskap och konsekvenshantering av terroristdåd. I kommissionens förslag anslogs 137,4 miljoner euro för kartläggning av relevanta behov och för att arbeta fram gemensamma tekniska normer för skydd av kritisk infrastruktur.

Programmet kommer att bevilja gemenskapsmedel till projekt som läggs fram av nationella, regionala och lokala myndigheter till skydd för kritisk infrastruktur. Programmet koncentreras på att kartlägga skyddsbehov och på att ge sådan information att gemensamma normer, hot- och riskbedömningar kan utvecklas till skydd för kritisk infrastruktur, eller för utarbetandet av specifika beredskapsplaner. Kommissionen kan använda sig av sin redan befintliga sakkunskap eller hjälpa till att finansiera studier av interdependenser inom specifika sektorer. Huvudsakligen är det medlemsstaterna eller ägare och operatörer som ansvarar för att uppgradera säkerheten i sin infrastruktur i enlighet med de identifierade behoven. Inom programmet finns inte några medel för att finansiera uppgraderingen av skyddet av kritisk infrastruktur. Lån från finansinstitut skulle kunna användas för att uppgradera säkerheten i medlemsstaternas infrastruktur i enlighet med de behov som identifierats genom programmet och för att införa gemensamma normer. Kommissionen är villig att stödja sektorsbaserade studier för att bedöma vilka ekonomiska konsekvenser uppgraderingen av infrastrukturens säkerhet kan ha på branschen.

Kommissionen finansierar forskningsprojekt till stöd för skydd av kritisk infrastruktur i den förberedande åtgärden för säkerhetsforskning[2] (2004–2006), och har planerat mer omfattande säkerhetsforskning i sitt förslag till rådets och Europaparlamentets beslut om EU:s sjunde ramprogram för forskning (KOM(2005)119 slutlig)[3] och i sitt förslag till rådsbeslut om det särskilda programmet ”Samarbete” som genomför sjunde ramprogrammet (KOM(2005)440 slutlig). Riktad forskning som skall utmynna i praktiska strategier eller verktyg för att minska riskerna är av primär betydelse för att säkra kritisk EU-infrastruktur på medellång och lång sikt. All säkerhetsforskning, även på detta område, kommer att underkastas en etisk granskning, så att man kan garantera att den överensstämmer med stadgan om de grundläggande rättigheterna. Forskningsbehovet kommer bara att växa allt eftersom avhängigheten av olika infrastrukturer utökas.

Frågor

Hur stor blir kostnaden och vad blir konsekvenserna för förvaltningar och näringsliv, anser Ni, om de åtgärder som förs fram i denna grönbok skulle vidtas? Anser Ni att de är proportionerliga?

9.4. Utvärdering och övervakning

Utvärderingen och övervakningen av genomförandet av EPCIP innebär en process på flera nivåer med medverkan från samtliga berörda aktörer:

- **EU-nivå: En kollegial utvärderingsmekanism skulle kunna inrättas**, där medlemsstaterna och kommissionen tillsammans arbetar med att bedöma den övergripande nivån på genomförandet av EPCIP i varje medlemsstat. Kommissionen skulle kunna utarbeta årliga resultatrapporter om genomförandet av det europeiska programmet för skydd av kritisk infrastruktur.

- **Kommissionen skulle varje kalenderår rapportera hur arbetet framskrider till medlemsstaterna och andra institutioner** i ett arbetsdokument från sina tjänsteenheter.

- **Nationell nivå: Varje medlemsstats egna samordningsorgan för skydd av kritisk infrastruktur skulle med hjälp av årliga rapporter till rådet och kommissionen kunna övervaka det övergripande genomförandet av det europeiska programmet inom den egna jurisdiktionen och se till att de nationella programmen för skydd av kritisk infrastruktur och de sektorsspecifika programmen för skydd av kritisk infrastruktur,** verkligen förverkligas.

Genomförandet av det europeiska programmet skulle vara en dynamisk process, i ständig rörelse och ständigt utvärderat både för att hålla samma takt som en föränderlig värld och för att kunna utnyttja de lärdomar som dragits. Kollegiala utvärderingar och medlemsstaternas övervakningsrapporter skulle kunna utgöra en del av de instrument som används för att se över det europeiska programmet och ge förslag till nya åtgärder för att stärka skyddet av kritisk infrastruktur.

---

[2] Totalt uppgick anslagen i 2004 och 2005 års budgetar till 30 miljoner euro. För 2006 har kommissionen föreslagit ett belopp på 24 miljoner euro, som f.n. granskas av budgetmyndigheten.

[3] Kommissionens budgetförslag för säkerhets- och rymdforskning inom sjunde ramprogrammet uppgår till 570 miljoner euro (KOM(2005)119 slutlig)

Relevant information från medlemsstaterna om kritisk EU-infrastruktur skulle kunna göras tillgänglig för kommissionen vid utarbetandet av gemensamma sårbarhetsbedömningar, konsekvenshanteringsplaner, gemensamma normer för skyddet av kritisk infrastruktur, prioriteringar av forskning och, om så är nödvändigt, reglering och harmonisering. Sådan information skulle vara hemligstämplad och hållas strikt konfidentiell.

Kommissionen skulle kunna övervaka olika medlemsstatsinitiativ, inklusive dem som får finansiella följder för ägare och operatörer som inte klarar av att åter tillhandahålla väsentliga tjänster till medborgarna inom en specificerad maximal tidsrymd.

Fråga

Vilken typ av utvärderingsmekanism skulle behövas för det europeiska programmet för skydd av kritisk infrastruktur? Skulle den ovan nämnda mekanismen vara tillräcklig?

Svaren bör sändas elektroniskt senast den 15 januari 2006 till följande e-postadress: **JLS-EPCIP@cec.eu.int**. De kommer att vara konfidentiella, såvida inte den som lämnar in uppgifterna uttryckligen önskar att de skall bli offentliga. I så fall placeras de på kommissionens webbplats på Internet.

ANNEXES

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.