COMMISSIE VAN DE EUROPESE GEMEENSCHAPPEN

Brussel, 17.11.2005
COM(2005) 576 definitief

GROENBOEK

BETREFFENDE EEN EUROPEES PROGRAMMA VOOR DE BESCHERMING VAN KRITIEKE INFRASTRUCTUUR

(door de Commissie ingediend)

GROENBOEK

BETREFFENDE EEN EUROPEES PROGRAMMA VOOR DE BESCHERMING VAN KRITIEKE INFRASTRUCTUUR

1. ACHTERGROND

Kritieke infrastructuur (CI) kan worden beschadigd, vernietigd of verstoord door terreurdaden, natuurrampen, nalatigheid, ongevallen of computerinbraak, criminele activiteiten en kwaadwillig gedrag. Teneinde het leven en de eigendommen van EU-burgers te beschermen en de schade die het gevolg is van terrorisme, natuurrampen en ongevallen zo beperkt mogelijk te houden voor de lidstaten, hun burgers en de Europese Unie, moet ervoor worden gezorgd dat storingen of manipulaties van kritieke infrastructuur zo kort mogelijk duren, zelden voorkomen, slechts in een geografisch beperkt gebied optreden en gemakkelijk beheersbaar zijn. Door de recente terreuraanslagen in Madrid en Londen is duidelijk het gevaar voor terreuraanslagen op Europese infrastructuur gebleken. De EU moet daarom snel, gecoördineerd en efficiënt reageren.

De Europese Raad van juni 2004 heeft de Commissie verzocht een algemene strategie ter bescherming van kritieke infrastructuur voor te bereiden. Naar aanleiding van dit verzoek heeft de Commissie op 20 oktober 2004 de mededeling "Terrorismebestrijding: bescherming van kritieke infrastructuur" goedgekeurd, waarin concrete voorstellen worden gedaan over de wijze waarop de preventie van, de paraatheid bij en de reactie op terreuraanslagen op kritieke infrastructuur in Europa kunnen worden versterkt.

Het voornemen van de Commissie om een Europees programma voor de bescherming van kritieke infrastructuur (EPCIP) voor te stellen, werd door de Raad bekrachtigd in zijn conclusies inzake "Preventie, paraatheid en reactie op terroristische aanslagen" en in zijn in december 2004 aangenomen "Solidariteitsprogramma van de EU betreffende de gevolgen van terroristische dreigingen en aanslagen". De Raad stemde voorts in met het voornemen van de Commissie om een netwerk voor waarschuwing en informatie inzake kritieke infrastructuur (CIWIN) op te zetten.

De Commissie heeft in dit verband twee seminars georganiseerd en de lidstaten verzocht haar hun ideeën en opmerkingen toe te zenden. Het eerste seminar over de bescherming van kritieke infrastructuur in de EU werd gehouden op 6 en 7 juni 2005. Aan dit seminar werd deelgenomen door de lidstaten, die de Commissie na afloop ervan relevante achtergronddocumenten betreffende hun aanpak van de bescherming van kritieke infrastructuur hebben verstrekt en nader zijn ingegaan op de tijdens het seminar besproken ideeën. Op grond van de bijdragen die de Commissie in juni en juli ontving werd de strategie ter bescherming van kritieke infrastructuur verder ontwikkeld. Het tweede seminar over de bescherming van kritieke infrastructuur werd op 12 en 13 september gehouden teneinde een impuls te geven aan de discussie over dit thema. Het werd niet alleen bijgewoond door de lidstaten, maar ook door organisaties uit het bedrijfsleven. In aansluiting daarop heeft de Commissie besloten dit groenboek te publiceren, waarin de opties voor een Europees beschermingsprogramma worden geschetst.

2. DOEL VAN HET GROENBOEK

Het hoofddoel van dit groenboek is feedback te verkrijgen over mogelijke beleidsopties voor het EPCIP door zoveel mogelijk belanghebbenden bij de discussie te betrekken. Voor een doeltreffende bescherming van kritieke infrastructuur is communicatie, coördinatie en samenwerking op nationaal niveau en op het niveau van de EU vereist tussen alle betrokken partijen – eigenaren en exploitanten van infrastructuur, regelgevende instanties, beroeps- en brancheorganisaties, in samenwerking met overheidsinstanties op alle niveaus en het publiek.

In dit groenboek worden verschillende opties voorgesteld voor de wijze waarop de Commissie kan tegemoetkomen aan het verzoek van de Raad om een Europees programma voor de bescherming van kritieke infrastructuur op te stellen en een Europees netwerk voor waarschuwing en informatie inzake kritieke infrastructuur op te zetten. Aldus wordt de tweede fase ingeleid van een raadplegingsproces dat erop is gericht een Europees beschermingsprogramma in te voeren. De Commissie hoopt dankzij de publicatie van dit groenboek concrete feedback over de in dit document voorgestelde beleidsopties te ontvangen. Afhankelijk van het resultaat van het raadplegingsproces zou in de loop van 2006 in het kader van het EPCIP een pakket beleidsmaatregelen kunnen worden voorgesteld.

3. DOEL EN TOEPASSINGSGEBIED VAN HET EPCIP

3.1. Algemeen doel van het EPCIP

Door het EPCIP zouden in de hele Unie adequate en uniforme veiligheidsniveaus voor kritieke infrastructuur, zo weinig mogelijk zwakke punten (single points of failure) en snelle, beproefde hulpverleningsvoorzieningen moeten worden gewaarborgd. Het beschermingsniveau hoeft wellicht niet hetzelfde te zijn voor alle kritieke infrastructuurinrichtingen en zou kunnen afhangen van de impact van het uitvallen van dergelijke infrastructuur. Het EPCIP zou continu verder moeten worden ontwikkeld en een geregelde herziening zal nodig zijn om gelijke tred te houden met nieuwe ontwikkelingen en problemen.

Een eventuele negatieve impact van verhoogde investeringen in veiligheid op het concurrentievermogen van een bepaalde bedrijfstak zou door het EPCIP tot een minimum moeten worden beperkt. Voorts mag bij de berekening van de proportionaliteit van de kosten de voor investeringen op lange termijn zo cruciale marktstabiliteit niet uit het oog worden verloren, evenmin als de invloed die veiligheid heeft op de effectenmarkten en op de macro-economische ontwikkelingen.

Vraag

Is dit een passende doelstelling voor het EPCIP? Zo niet, welk doel moet dan met het EPCIP worden nagestreefd?

3.2. Waartegen moet het EPCIP bescherming bieden?

Hoewel de gevolgenbeheersingsmaatregelen bij de meeste verstoringen van kritieke infrastructuur identiek of vergelijkbaar zijn, kunnen beschermingsmaatregelen verschillen naargelang van de aard van de dreiging. Aanslagen en natuurrampen zijn bijvoorbeeld dreigingen die kunnen leiden tot een aanzienlijke aantasting van de mogelijkheden om in de

essentiële behoeften en de veiligheid van de bevolking te voorzien, de orde te handhaven en een minimale openbare dienstverlening te garanderen. De opties voor het EPCIP zijn de volgende:

a) **bescherming bieden tegen alle gevaren in het algemeen:** bij deze aanpak zou rekening worden gehouden met zowel de dreiging van aanslagen als van natuurrampen. oor een dergelijke aanpak zou een maximale benutting van de synergieën tussen de beschermingsmaatregelen worden gegarandeerd, maar zou geen bijzondere nadruk worden gelegd op terrorisme;

b) **bescherming bieden tegen alle gevaren, waarbij echter prioriteit wordt gegeven aan terrorisme:** bij deze flexibele aanpak zou rekening worden gehouden met alle soorten van gevaren, van aanslagen tot natuurrampen, maar met terrorisme als prioriteit. Indien de beschermingsmaatregelen in een bepaalde bedrijfstak toereikend worden geacht, zouden de betrokken partijen zich in dit geval concentreren op die gevaren waarvoor zij nog kwetsbaar zijn;

c) **bescherming bieden tegen terrorisme:** bij deze aanpak zou terrorisme centraal staan en zou geen bijzondere aandacht worden besteed aan meer algemene gevaren.

Vraag

Welke aanpak moet voor het EPCIP worden gekozen? Waarom?

4. VOORGESTELDE UITGANGSPUNTEN

De volgende uitgangspunten worden als grondslag voor het EPCIP voorgesteld:

- **Subsidiariteit –** Subsidiariteit zou centraal staan in het EPCIP; de bescherming van kritieke infrastructuur zou in de eerste plaats een nationale verantwoordelijkheid zijn. De hoofdverantwoordelijkheid voor de bescherming van kritieke infrastructuur zou berusten bij de lidstaten en bij de eigenaren en exploitanten van infrastructuur die binnen een gemeenschappelijk kader optreden. De Commissie zou zich concentreren op de grensoverschrijdende aspecten van de bescherming van kritieke infrastructuur. Dat zou niets afdoen aan het feit dat de eigenaren en exploitanten verantwoordelijk zijn voor hun eigen beslissingen en plannen om hun activa te beschermen.

- **Complementariteit –** Het EPCIP zou reeds bestaande maatregelen aanvullen. Waar op het niveau van de Gemeenschap reeds mechanismen bestaan, zouden deze verder moeten worden gebruikt en tot de volledige uitvoering van het EPCIP moeten bijdragen.

- **Vertrouwelijkheid –** Informatie over de bescherming van kritieke infrastructuur zou op basis van vertrouwen en vertrouwelijkheid worden uitgewisseld. Dit is nodig, aangezien bepaalde gegevens over kritieke infrastructuur kunnen worden gebruikt om het functioneren ervan te verstoren of om feiten te plegen die onaanvaardbare gevolgen hebben voor deze installaties. Zowel op het niveau van de EU als van de lidstaten zou informatie over de bescherming van kritieke infrastructuur als vertrouwelijk moeten worden behandeld en zou deze slechts op een “need-to-know”-basis worden verstrekt.

- **Medewerking van de betrokken partijen –** Alle betrokken partijen, waaronder de lidstaten, de Commissie, bedrijfs- en brancheorganisaties, normalisatieorganen en eigenaren, exploitanten en gebruikers (als "gebruikers" worden beschouwd organisaties die de infrastructuur voor bedrijfsdoeleinden en voor het verlenen van diensten exploiteren en gebruiken) hebben een rol te spelen bij de bescherming van kritieke infrastructuur. Alle betrokken partijen zouden hun medewerking moeten verlenen en bijdragen tot de ontwikkeling en tenuitvoerlegging van het EPCIP in overeenstemming met hun specifieke rol en verantwoordelijkheden. De autoriteiten van de lidstaten zouden de leiding op zich nemen en zorgen voor de coördinatie bij de ontwikkeling en tenuitvoerlegging van een op nationaal niveau samenhangende aanpak van de bescherming van zich binnen hun bevoegdheidsgebied bevindende kritieke infrastructuur. De eigenaren, exploitanten en gebruikers verlenen daaraan zowel op nationaal niveau als op het niveau van de EU actief hun medewerking. Waar sectorale normen ontbreken of nog geen internationale normen zijn uitgewerkt, kunnen normalisatieorganisaties zonodig gemeenschappelijke normen vaststellen.

- **Evenredigheid –** Beschermingsstrategieën en –maatregelen zouden evenredig moeten zijn met de risico's, aangezien niet alle infrastructuren tegen alle dreigingen kunnen worden beschermd (stroomvoorzieningsnetwerken bijvoorbeeld zijn te omvangrijk om te worden omheind of bewaakt). Door de toepassing van risicomanagementtechnieken zou de aandacht in het bijzonder worden gevestigd op de gebieden waar het risico het grootst is, rekening houdend met de dreiging, de mate waarin infrastructuur als kritieke infrastructuur wordt beschouwd, de kosten-batenverhouding, het bestaande beschermingsniveau en de doeltreffendheid van de beschikbare strategieën ter vermindering van de risico's.

Vraag

Zijn deze uitgangspunten aanvaardbaar? Zijn sommige ervan overbodig? Moeten aanvullende uitgangspunten worden overwogen?

Bent u het ermee eens dat beschermingsmaatregelen evenredig moeten zijn met het risiconiveau, aangezien niet alle infrastructuur tegen alle dreigingen kan worden beschermd?

5. EEN GEMEENSCHAPPELIJK EPCIP-KADER

De beschadiging of het uitvallen van een bepaalde infrastructuurinrichting in een lidstaat kan negatieve gevolgen hebben voor verscheidene andere lidstaten en voor de Europese economie in het algemeen. De kans daarop wordt steeds groter, aangezien nieuwe technologieën (bijvoorbeeld internet) en de liberalisering van de markt (bijvoorbeeld van de markt voor de elektriciteits- en gasvoorziening) ertoe leiden dat veel infrastructuursystemen in een groter netwerk worden geïntegreerd. In die omstandigheden is de bescherming slechts even sterk als de zwakste schakel in het geheel van beschermingsmaatregelen. Dat betekent dat een gemeenschappelijk beschermingsniveau noodzakelijk kan zijn.

Voor een doeltreffende bescherming is communicatie, coördinatie en samenwerking zowel op nationaal niveau als (waar nodig) op EU-niveau en op internationaal niveau tussen alle betrokken partijen vereist. Er zou op het niveau van de EU een gemeenschappelijk kader voor de bescherming van kritieke infrastructuur in Europa kunnen worden ontwikkeld dat in elke lidstaat hetzelfde, adequate beschermingsniveau garandeert en waarborgt dat de mededinging binnen de interne markt niet wordt vervalst. Door het verschaffen van een gemeenschappelijk

kader voor de bescherming van kritieke infrastructuur zou de Commissie de vaststelling, de uitwisseling en de verspreiding van beproefde methoden vergemakkelijken en aldus de inspanningen van de lidstaten ondersteunen. Het toepassingsgebied van dit algemene kader dient te worden afgebakend.

Het gemeenschappelijke EPCIP-kader zou horizontale maatregelen omvatten, waarin de bevoegdheid en de verantwoordelijkheden van alle bij de bescherming van kritieke infrastructuur (CIP – critical infrastructure protection) betrokken partijen worden omschreven en de basis wordt gelegd voor een sectorspecifieke aanpak. De bedoeling is dat het gemeenschappelijke kader de op het niveau van de Gemeenschap en in de lidstaten bestaande sectorspecifieke maatregelen aanvult, teneinde aldus een maximale beveiliging van de kritieke infrastructuur in de Europese Unie te garanderen. Er zou bij voorrang een gemeenschappelijke lijst van definities en infrastructuursectoren moeten worden overeengekomen.

Aangezien de verschillende sectoren waarin kritieke infrastructuur te vinden is, zeer divers zijn, is het moeilijk om in een sectoroverschrijdende regeling precieze criteria voor het in kaart brengen en de bescherming van deze infrastructuur voor te schrijven. Deze zouden per sector moeten worden vastgesteld. Niettemin is overeenstemming over bepaalde sectoroverschrijdende kwesties nodig.

Daarom wordt voorgesteld ter verbetering van de bescherming van kritieke infrastructuur in de EU een gemeenschappelijk EPCIP-kader (gemeenschappelijke doelstellingen, methoden voor bijvoorbeeld vergelijkingen, en interdependentie) vast te stellen en beproefde methoden en controlemechanismen uit te wisselen. Dit gemeenschappelijke kader zou met name de volgende elementen kunnen omvatten:

- gemeenschappelijke beginselen voor de bescherming van kritieke infrastructuur;
- gezamenlijk overeengekomen regels/normen;
- gemeenschappelijke definities op grond waarvan sectorspecifieke definities kunnen worden overeengekomen (een indicatieve lijst van definities is opgenomen in bijlage 1);
- een gemeenschappelijke lijst van sectoren waarin kritieke infrastructuur te vinden is (een indicatieve lijst van sectoren is opgenomen in bijlage 2);
- prioritaire gebieden voor de bescherming van kritieke infrastructuur;
- beschrijving van de verantwoordelijkheden van de betrokken partijen;
- overeengekomen benchmarks;
- methoden om infrastructuur in verschillende sectoren te vergelijken en vast te stellen welke ervan prioritair is.

Een dergelijk gemeenschappelijk kader zou ook potentiële verstoringen van de interne markt tot een minimum beperken.

Het gemeenschappelijke EPCIP-kader zou een vrijwillig of een bindend karakter kunnen hebben - of een combinatie van beide, afhankelijk van de situatie. In beide gevallen zou het gemeenschappelijke kader bestaande sectorspecifieke en horizontale maatregelen op het niveau van de Gemeenschap en van de lidstaten kunnen aanvullen; alleen een wettelijk kader zou echter een sterke en afdwingbare rechtsgrond verschaffen voor een coherente en uniforme uitvoering van maatregelen om kritieke infrastructuur in de Europese Unie te beschermen en om de respectieve verantwoordelijkheden van de lidstaten en de Commissie duidelijk af te bakenen. Niet-bindende vrijwillige maatregelen zouden weliswaar flexibel zijn, maar geen duidelijkheid verschaffen over wie wat moet doen.

De Commissie zou, afhankelijk van het resultaat van een zorgvuldige analyse en er rekening mee houdend dat de voorgestelde maatregelen evenredig moeten zijn, in haar voorstel voor een Europees beschermingsprogramma gebruik kunnen maken van een aantal instrumenten, inclusief wetgeving. Voorstellen voor specifieke maatregelen moeten, waar nodig, vergezeld gaan van een effectbeoordeling.

Vragen

Is een gemeenschappelijk kader een doeltreffend instrument om de bescherming van kritieke infrastructuur te verbeteren?

Indien een wetgevend kader nodig blijkt, welke elementen moet dit dan omvatten?

Bent u het ermee eens dat de criteria om de verschillende soorten kritieke infrastructuur in de Europese Unie af te bakenen en de noodzakelijk geachte beschermingsmaatregelen per sector moeten worden vastgesteld?

Zou een gemeenschappelijk kader bijdragen tot de verduidelijking van de verantwoordelijkheden van de betrokken partijen? Moet een dergelijk gemeenschappelijk kader een bindend of een vrijwillig karakter hebben?

Wat moet het toepassingsgebied van het gemeenschappelijke kader zijn? Bent u het eens met de indicatieve lijst van termen en definities in bijlage I op grond waarvan (waar nodig) sectorspecifieke definities kunnen worden geformuleerd? Bent u het eens met de indicatieve lijst van CI-sectoren in bijlage II?

6. KRITIEKE INFRASTRUCTUUR IN DE EU (ECI)

6.1. Definitie van kritieke infrastructuur in de EU

Een belangrijk element in de definitie van Europese kritieke infrastructuur is of deze in geval van een incident ernstige grensoverschrijdende gevolgen zou hebben buiten het grondgebied van de lidstaat waar de installatie zich bevindt. Een ander element dat hier in aanmerking moet worden genomen is het feit dat bilaterale samenwerkingsprogramma's op het gebied van de bescherming van kritieke infrastructuur tussen lidstaten hun nut en doeltreffendheid hebben bewezen in geval van kritieke infrastructuur die zich in het grensgebied van twee lidstaten bevindt. Deze vorm van samenwerking zou het EPCIP aanvullen.

Onder Europese kritieke infrastructuur zou kunnen worden verstaan: materiële middelen, diensten, informatietechnologische voorzieningen, netwerken en infrastructuuractiva waarvan de verstoring of vernietiging ernstige gevolgen zou hebben voor de gezondheid, de veiligheid, de bescherming of het economische welzijn van de burgers van:

(a) twee of meer lidstaten - waardoor ook **bepaalde bilaterale kritieke infrastructuurinrichtingen er (eventueel) onder zouden vallen**;

(b) drie of meer lidstaten – waardoor **alle bilaterale kritieke infrastructuurinrichtingen ervan uitgesloten zouden zijn.**

Bij de toetsing van deze opties op hun respectieve voordelen, moet in gedachten worden gehouden dat:

– de aanmerking van een infrastructuurinrichting als ECI niet betekent dat noodzakelijkerwijze aanvullende beschermingsmaatregelen nodig zijn. De bestaande beschermingsmaatregelen, die ook kunnen zijn vastgelegd in bilaterale overeenkomsten tussen lidstaten, kunnen volledig aan de behoeften voldoen zodat zij door de aanmerking van infrastructuur als ECI niet hoeven te worden gewijzigd;

– optie (a) zou kunnen leiden tot de aanmerking van een groter aantal infrastructuurinrichtingen als ECI;

– optie (b) zou kunnen betekenen dat, ingeval infrastructuur voor slechts twee lidstaten van belang is, de Gemeenschap geen enkele rol zou spelen, zelfs indien het beschermingsniveau door één van deze beide lidstaten ontoereikend wordt geacht en de andere lidstaat weigert maatregelen te nemen. Optie (b) zou ook kunnen leiden tot een groot aantal bilaterale overeenkomsten of juist twistpunten tussen lidstaten. Het bedrijfsleven, dat vaak op pan-Europees niveau actief is, zou zich geconfronteerd kunnen zien met een lappendeken van uiteenlopende overeenkomsten, die bijkomende kosten ten gevolge zouden kunnen hebben.

Voorts wordt erkend dat ook kritieke infrastructuur die zich buiten het grondgebied van de EU bevindt, maar met een EU-lidstaat is verbonden of potentieel rechtstreekse gevolgen voor deze lidstaat kan hebben, in aanmerking moet worden genomen.

Vraag

Moet infrastructuur als Europese kritieke infrastructuur (ECI) worden beschouwd, wanneer zij potentieel ernstige grensoverschrijdende gevolgen kan hebben voor twee of meer lidstaten? Of voor drie of meer lidstaten? Waarom?

6.2. Interdependenties

Bij het in kaart brengen van alle ECI zou ook rekening moeten worden gehouden met interdependenties. Studies over dit onderwerp zouden ertoe kunnen bijdragen de potentiële impact van dreigingen in te schatten en vast te stellen welke lidstaten in geval van een ernstig incident zouden worden getroffen.

Er zou rekening worden gehouden met interdependenties binnen en tussen bedrijven, bedrijfstakken, geografische bevoegdheidsgebieden en autoriteiten van de lidstaten, in het bijzonder wanneer zij verband houden met informatie- en communicatietechnologieën (ICT). De Commissie, de lidstaten en de eigenaren/exploitanten van kritieke infrastructuur zouden deze interdependenties gezamenlijk moeten opsporen en analyseren, en passende strategieën moeten toepassen om de risico's zoveel mogelijk te beperken.

Vraag

Hoe kan rekening worden gehouden met interdependenties?

Kent u geschikte methoden om interdependenties te analyseren?

Op welk niveau moeten interdependenties in kaart worden gebracht – op het niveau van de EU en/of op het niveau van de lidstaten?

6.3. Stappenplan voor ECI

De Commissie stelt voor ECI het volgende stappenplan voor:

(1) de Commissie stelt samen met de lidstaten de criteria vast die voor het in kaart brengen van ECI per sector moeten worden gebruikt;

(2) vervolgens brengen de lidstaten en de Commissie de ECI in kaart en gaan zij over tot de verificatie ervan. De beslissing of een bepaalde kritieke infrastructuurinrichting als ECI moet worden aangemerkt, wordt wegens het grensoverschrijdende karakter van dergelijke infrastructuur op Europees niveau[1], genomen;

(3) de lidstaten en de Commissie analyseren per sector de bestaande leemten in de beveiliging van ECI;

(4) de lidstaten en de Commissie komen overeen in welke sectoren/voor welke infrastructuur, rekening houdend met de interdependenties, bij voorrang maatregelen moeten worden genomen;

(5) waar nodig stellen de Commissie en de belangrijkste betrokken partijen in de lidstaten voor elke sector minimumbeschermingsmaatregelen voor, die eventueel ook normen kunnen omvatten;

(6) deze maatregelen worden ten uitvoer gelegd na goedkeuring van de voorstellen door de Raad;

(7) de lidstaten en de Commissie oefenen een regelmatige controle uit. Zo nodig worden de maatregelen en de criteria voor het in kaart brengen van kritieke infrastructuur herzien.

Vragen

Is het stappenplan voor ECI aanvaardbaar?

Hoe moeten de Commissie en de lidstaten volgens u te werk gaan bij de gezamenlijke aanmerking van kritieke infrastructuur als ECI, rekening houdend met het feit dat de lidstaten over de nodige expertise beschikken en dat de Commissie een goed inzicht heeft in wat van Europees belang is? Is voor deze aanmerking als ECI een juridisch bindend besluit nodig?

[1] Dit geldt niet voor infrastructuur op het gebied van defensie.

Is een arbitragemechanisme nodig voor het geval dat een bepaalde lidstaat het niet eens is met de aanmerking van binnen zijn bevoegdheidsgebied vallende infrastructuur als ECI?

Is verificatie van de aanmerking van infrastructuur als ECI nodig? Wie moet met die verificatie worden belast?

Moeten de lidstaten de mogelijkheid hebben infrastructuur in andere lidstaten of in derde landen als voor hen kritieke infrastructuur aan te merken? Wat moet er gebeuren indien een lidstaat, een derde land of een bedrijfstak infrastructuur in een lidstaat als voor hem kritiek beschouwt?

Wat moet er gebeuren indien een lidstaat de betrokken infrastructuur niet als kritieke infrastructuur aanmerkt? Is een beroepsprocedure nodig? Zo ja, welke?

Moet een exploitant de mogelijkheid hebben om in beroep te gaan indien hij het niet eens is met de aanmerking van zijn infrastructuur als ECI? Zo ja, bij wie?

Welke methoden moeten worden ontwikkeld om vast te stellen in welke sectoren/voor welke infrastructuur bij voorrang maatregelen moeten worden genomen? Bestaan er reeds geschikte methoden die aan het Europese niveau kunnen worden aangepast?

Hoe kan de Commissie worden betrokken bij de analyse van leemten in de beveiliging van ECI?

7. NATIONALE KRITIEKE INFRASTRUCTUUR (NCI)

7.1. De rol van NCI in het EPCIP

Vele Europese ondernemingen zijn grensoverschrijdend actief en zijn bijgevolg onderworpen aan uiteenlopende, voor NCI geldende verplichtingen. Daarom wordt in het belang van de lidstaten en van de EU als geheel voorgesteld dat elke lidstaat zijn NCI zou beschermen op grond van een gemeenschappelijk kader, zodat eigenaren en exploitanten van dergelijke infrastructuur in Europa niet worden geconfronteerd met een groot aantal uiteenlopende regelingen en methoden, en de daaruit voortvloeiende bijkomende kosten. Hoewel de aandacht in het kader van het EPCIP vooral moet gaan naar kritieke infrastructuur in de EU, is de Commissie daarom van mening dat nationale kritieke infrastructuur niet volledig buiten beschouwing kan worden gelaten. Drie opties moeten hier worden onderzocht:

a) volledig integratie van NCI in het EPCIP;

b) volledige uitsluiting van NCI uit het toepassingsgebied van het EPCIP;

c) toepassing door de lidstaten, uit eigen beweging en zonder dat zij daartoe verplicht zijn, van delen van het EPCIP op NCI.

Vraag

Teneinde kritieke infrastructuur in de Europese Unie op doeltreffende wijze te kunnen beschermen, lijkt het nodig zowel ECI als NCI in kaart te brengen. Bent u het ermee eens dat hoewel het EPCIP vooral moet zijn toegespitst op ECI, NCI niet volledig buiten beschouwing kan worden gelaten?

Welke van deze opties lijkt u de meest geschikte voor het EPCIP?

7.2. Nationale programma's voor de bescherming van kritieke infrastructuur

De lidstaten zouden op grond van een gemeenschappelijk EPCIP-kader nationale programma's voor de bescherming van kritieke infrastructuur kunnen ontwikkelen voor hun NCI en strengere maatregelen opleggen dan die waarin het EPCIP voorziet.

Vraag

Is het wenselijk dat elke lidstaat een op het EPCIP gebaseerd nationaal programma voor de bescherming van kritieke infrastructuur goedkeurt?

7.3. Toezichthoudend orgaan

Om redenen van doeltreffendheid en coherentie zou elke lidstaat een enkel toezichthoudend orgaan moeten aanwijzen, dat belast is met de uitvoering van het EPCIP. Twee opties kunnen worden overwogen:

(a) Eén enkel toezichthoudend orgaan voor de bescherming van kritieke infrastructuur;

(b) Een nationaal contactpunt zonder bevoegdheid, waarbij het aan de lidstaten wordt overgelaten op welke wijze zij zich organiseren.

Een dergelijk orgaan zou de uitvoering van het EPCIP binnen zijn bevoegdheidsgebied kunnen coördineren en controleren. Voorts zou het in aangelegenheden die de bescherming van kritieke infrastructuur betreffen kunnen dienen als belangrijkste institutioneel contactpunt met de Commissie, andere lidstaten en eigenaren en exploitanten van kritieke infrastructuur. Het zou kunnen zorgen voor de nationale vertegenwoordiging in deskundigengroepen die zich bezighouden met aangelegenheden die betrekking hebben op de bescherming van kritieke infrastructuur en de verbinding kunnen vormen met het netwerk voor waarschuwing en informatie inzake kritieke infrastructuur. Hoewel in een lidstaat reeds andere organen of instanties actief kunnen zijn op het gebied van de bescherming van kritieke infrastructuur, zou een dergelijk nationaal orgaan voor de coördinatie van de bescherming van kritieke infrastructuur (NCCB – National CIP coordination body) kunnen zorgen voor de coördinatie van nationale acties op dit gebied.

Door de eigenaren en exploitanten van infrastructuur de verplichting op te leggen het NCCB in kennis te stellen van elke bedrijvigheid op het gebied van de bescherming van kritieke infrastructuur moet het mogelijk zijn geleidelijk alle NCI in kaart te brengen.

Het NCCB zou kunnen worden belast met het nemen van het besluit waardoor infrastructuur binnen zijn bevoegdheidsgebied op bindende wijze als NCI wordt aangemerkt. Alleen de betrokken lidstaat zou over deze informatie kunnen beschikken.

Aan dit orgaan zouden de volgende bevoegdheden kunnen worden toevertrouwd:

a) coördinatie en controle van, alsmede toezicht op de uitvoering van het EPCIP in een lidstaat;

b) fungeren als het belangrijkste institutionele contactpunt voor kwesties die de bescherming van kritieke infrastructuur betreffen, met:

   i. de Commissie

   ii. de andere lidstaten

   iii. de eigenaren en exploitanten van kritieke infrastructuur

c) medewerking bij de aanmerking van kritieke infrastructuur als Europese kritieke infrastructuur (ECI);

d) het nemen van het besluit waarbij infrastructuur binnen zijn bevoegdheidsgebied op bindende wijze als nationale kritieke infrastructuur wordt aangemerkt;

e) fungeren als beroepsinstantie voor eigenaren/exploitanten die het er niet mee eens zijn dat hun infrastructuur als "kritieke infrastructuur" wordt aangemerkt;

f) medewerking verlenen bij het opstellen van het nationale programma voor de bescherming van kritieke infrastructuur en van de sectorspecifieke beschermingsprogramma's;

g) het in kaart brengen van interdependenties tussen de verschillende CI-sectoren;

h) bijdragen aan de sectorspecifieke aanpak van de bescherming van kritieke infrastructuur door deel te nemen aan deskundigengroepen. Ook vertegenwoordigers van de eigenaren en exploitanten zouden kunnen worden uitgenodigd een bijdrage te leveren tot de besprekingen. Er zouden regelmatig bijeenkomsten kunnen worden gehouden;

i) toezien op de uitwerking van noodplannen voor kritieke infrastructuur.

Vragen

Bent u het ermee eens dat alleen de lidstaten voor de aanmerking van infrastructuur als NCI en en het beheer van NCI op grond van een gemeenschappelijk EPCIP-kader verantwoordelijk moeten zijn?

Is het wenselijk dat in elke lidstaat een coördinatieorgaan voor de bescherming van kritieke infrastructuur (NCCB) wordt aangewezen, dat de volledige verantwoordelijkheid draagt voor maatregelen ter bescherming van kritieke infrastructuur, zonder dat wordt geraakt aan in de verschillende sectoren bestaande verantwoordelijkheden (van de burgerluchtvaartautoriteiten, de verantwoordelijkheden die voortvloeien uit de Seveso-richtlijn, enz.)?

Acht u de voorgestelde bevoegdheden passend voor een dergelijk coördinatieorgaan? Zijn andere bevoegdheden vereist?

7.4. Stappenplan voor NCI

De Commissie stelt voor NCI het volgende stappenplan voor:

(1) de lidstaten stellen op grond van het EPCIP de criteria vast die voor het in kaart brengen van NCI moeten worden gebruikt;

(2) vervolgens brengen de lidstaten de NCI in kaart per sector en gaan over tot de verificatie ervan;

(3) de lidstaten analyseren per sector de bestaande leemten in de beveiliging van NCI;

(4) de lidstaten stellen vast in welke sectoren bij voorrang maatregelen moeten worden genomen, waar nodig rekening houdend met interdependenties en op EU-niveau overeengekomen prioriteiten;

(5) waar nodig stellen de lidstaten voor elke sector minimumbeschermingsmaatregelen vast;

(6) de lidstaten zien erop toe dat de eigenaren/exploitanten binnen hun bevoegdheidsgebied de nodige uitvoeringsmaatregelen nemen;

(7) de lidstaten oefenen een regelmatige controle uit. Zo nodig worden de maatregelen en de criteria voor het in kaart brengen van kritieke infrastructuur herzien.

Vraag

Acht u het stappenplan voor de NCI doeltreffend? Zijn bepaalde stappen overbodig? Zijn aanvullende stappen nodig?

8. ROL VAN DE EIGENAREN, EXPLOITANTEN EN GEBRUIKERS VAN KRITIEKE INFRASTRUCTUUR

8.1. Verantwoordelijkheden van de eigenaren, exploitanten en gebruikers van kritieke infrastructuur

De aanmerking van infrastructuur als kritieke infrastructuur brengt voor de eigenaren en exploitanten bepaalde verantwoordelijkheden met zich mee. Voor eigenaren en exploitanten van infrastructuur die is aangemerkt als NCI of ECI kunnen vier verantwoordelijkheden worden overwogen:

(1) **kennisgeving aan het orgaan dat in de betrokken lidstaat bevoegd is voor de bescherming van kritieke infrastructuur van het feit dat een infrastructuurinrichting als kritieke infrastructuur zou kunnen worden aangemerkt;**

(2) **aanwijzing van een of meer hooggeplaatste vertegenwoordiger(s) als veiligheids-verbindingsfunctionaris (SLO - Security Liaison Officer) tussen de eigenaar/exploitant en de autoriteit die in de betrokken lidstaat bevoegd is voor de bescherming van kritieke infrastructuur.** Deze verbindingsfunctionaris zou veiligheids- en rampenplannen helpen opstellen. Hij zou de belangrijkste

gesprekspartner zijn van het in de lidstaat in een bepaalde sector voor de bescherming van kritieke infrastructuur bevoegde orgaan en, zo nodig, van de wetshandhavingsinstanties;

(3) **vaststelling, uitvoering en herziening van veiligheidsplannen voor de exploitanten (OSP - Operator Security Plan)**. Een modelplan is opgenomen in bijlage 3;

(4) **samenwerking** met de in de betrokken lidstaat met de civiele bescherming belaste instanties en wetshandhavingsinstanties **bij het opstellen van een noodplan voor kritieke infrastructuur,** indien daarom wordt verzocht**.**

Het veiligheidsplan zou, onder toezicht van het NCBB, ter goedkeuring aan de in de betrokken lidstaat in de sector voor de bescherming van kritieke infrastructuur bevoegde instanties kunnen worden voorgelegd, ongeacht of het gaat om een NCI of een ECI, hetgeen de coherentie zou garanderen van de veiligheidsmaatregelen die door bepaalde eigenaren en exploitanten en door de betrokken sectoren in het algemeen worden genomen. Het NCBB, en, in voorkomend geval, de Commissie zouden eigenaren en exploitanten van hun kant nuttige informatie kunnen verstrekken en dezen passende steun kunnen verlenen in verband met op hen betrekking hebbende dreigingen of bij de ontwikkeling van beproefde methoden. Zo nodig zouden zij hen kunnen helpen bij het beoordelen van interdependenties en zwakke plekken.

Elke lidstaat zou een termijn kunnen vaststellen waarbinnen de eigenaren en exploitanten van NCI en ECI hun veiligheidsplan moeten uitwerken (in geval van ECI zou ook de Commissie daarbij worden betrokken) en administratieve boetes kunnen opleggen ingeval deze termijn niet wordt nageleefd.

In het veiligheidsplan zou een nauwkeurig overzicht worden gegeven van de kritieke infrastructuur van de eigenaar/exploitant en zouden passende oplossingen ter bescherming ervan worden voorgesteld. Voorts zouden de methoden en procedures erin worden beschreven die moeten worden gevolgd om te waarborgen dat het EPCIP, de nationale programma's voor de bescherming van kritieke infrastructuur en de relevante sectorspecifieke programma's voor de bescherming van kritieke infrastructuur in acht worden genomen. Door het veiligheidsplan zou de bescherming van kritieke infrastructuur ook vanuit de basis kunnen worden geregeld, hetgeen de particuliere sector meer speelruimte (en ook meer verantwoordelijkheid) zou geven.

In bepaalde situaties, met name wanneer het gaat om bepaalde infrastructuurinrichtingen zoals elektriciteitsvoorzienings- en informatienetwerken, zou het (uit praktisch en financieel oogpunt) onrealistisch zijn te verwachten dat de eigenaren en exploitanten voor alle delen van hun infrastructuur hetzelfde veiligheidsniveau waarborgen. In dergelijke gevallen zouden de eigenaren en exploitanten, samen met de bevoegde autoriteiten, kunnen vaststellen welke de kritieke punten van een fysiek netwerk of een informatienetwerk zijn waarop de beveiligingsmaatregelen zouden kunnen worden geconcentreerd.

In het veiligheidsplan zouden twee categorieën van veiligheidsmaatregelen kunnen worden onderscheiden:

- **permanente beveiligingsmaatregelen,** waarbij wordt omschreven welke investeringen in beveiliging en welke middelen absoluut noodzakelijk zijn, maar die door de eigenaar/exploitant niet op korte termijn kunnen worden gedaan,

respectievelijk ter beschikking kunnen worden gesteld. De eigenaar/exploitant zou permanent alert blijven op mogelijke dreigingen, zonder dat zijn normale economische bedrijvigheid en zijn activiteiten op administratief en sociaal gebied daardoor worden verstoord;

- **graduele beveiligingsmaatregelen,** die zouden kunnen worden aangepast naargelang van het bedreigingsniveau. In het veiligheidsplan zou derhalve moeten worden voorzien in verscheidene veiligheidsscenario's, die zijn aangepast aan mogelijke dreigingsniveaus in de lidstaat waar de infrastructuur zich bevindt.

Ingeval de eigenaar/exploitant van kritieke infrastructuur niet voldoet aan de verplichting een veiligheidsplan op te stellen, bij te dragen aan de uitwerking van rampenplannen en een verbindingsfunctionaris aan te wijzen, zou hem een geldboete worden opgelegd.

Vragen

Zijn de verantwoordelijkheden die mogelijk aan de eigenaren/exploitanten van kritieke infrastructuur zouden worden toegekend aanvaardbaar als daardoor de veiligheid van kritieke infrastructuur verhoogt? Welke kosten zouden daaraan vermoedelijk zijn verbonden?

Moeten de eigenaren en exploitanten ertoe worden verplicht kennis te geven van het feit dat hun infrastructuur kritieke infrastructuur kan zijn? Acht u een veiligheidsplan nuttig? Waarom?

Zijn de voorgestelde verplichtingen evenredig met de ermee gemoeide kosten?

Welke rechten kunnen door de autoriteiten van de lidstaten en door de Commissie aan de eigenaren en exploitanten van kritieke infrastructuur worden toegekend?

8.2. Dialoog met eigenaren, exploitanten en gebruikers van kritieke infrastructuur

Het EPCIP zou de eigenaren en exploitanten ertoe kunnen aanzetten partnerschappen aan te gaan. Het succes van elk beschermingsprogramma hangt af van de mate waarin de eigenaren en exploitanten samenwerken en zich bij het programma betrokken voelen. Op het niveau van de lidstaten zouden de eigenaren en exploitanten van kritieke infrastructuur door geregelde contacten met het NCCB nauw bij de ontwikkelingen op het gebied van de bescherming van die infrastructuur kunnen worden betrokken.

Op het niveau van de EU zouden forums kunnen worden georganiseerd om de uitwisseling van standpunten over algemene en sectorspecifieke kwesties op het gebied van de bescherming van kritieke infrastructuur te vergemakkelijken. Een gemeenschappelijke aanpak met het oog op de inschakeling van de particuliere sector bij kwesties op het gebied van de bescherming van kritieke infrastructuur teneinde alle betrokken partijen van de openbare en de particuliere sector samen te brengen, zou de lidstaten, de Commissie en het bedrijfsleven een belangrijk platform verschaffen voor overleg over welke nieuwe kwestie op het gebied van de infrastructuurbescherming dan ook. De eigenaren, exploitanten en gebruikers van kritieke infrastructuur zouden kunnen bijdragen tot de vaststelling van gemeenschappelijke richtsnoeren, normen voor beproefde methoden en, waar nodig, de uitwisseling van informatie. Een dergelijke dialoog zou toekomstige herzieningen van het EPCIP vergemakkelijken.

Waar nodig zou de Commissie de oprichting van bedrijfs- of brancheorganisaties voor de bescherming van kritieke infrastructuur in de EU kunnen aanmoedigen. De twee doelstellingen waar het uiteindelijk om gaat, zijn: garanderen dat het Europese bedrijfsleven zijn concurrentiepositie behoudt en dat de burgers van de EU een veiliger leven kunnen leiden.

Vraag

Hoe moet de dialoog met de eigenaren, exploitanten en gebruikers van kritieke infrastructuur worden gestructureerd?

Wie moet de eigenaren, exploitanten en gebruikers vertegenwoordigen bij de publiek/private dialoog?

9. MAATREGELEN TER ONDERSTEUNING VAN HET EPCIP

9.1. Het netwerk voor waarschuwing en informatie inzake kritieke infrastructuur (CIWIN)

De Commissie heeft een aantal systemen voor snelle waarschuwing ontwikkeld, die het mogelijk maken in noodsituaties, ook als die door een terreuraanslag zijn veroorzaakt, op concrete, gecoördineerde en doeltreffende wijze te reageren. Op 20 oktober 2004 kondigde de Commissie de oprichting van een centraal netwerk bij de Commissie aan (ARGUS) dat een snelle informatiestroom tussen alle systemen voor snelle waarschuwing en de bevoegde diensten van de Commissie moet waarborgen.

De Commissie stelt voor CIWIN op te zetten. Dit netwerk zou de uitwerking van passende beschermingsmaatregelen kunnen stimuleren door ervoor te zorgen dat beproefde methoden op een veilige manier kunnen worden uitgewisseld en dat informatie over onmiddellijke dreigingen en waarschuwingen wordt doorgegeven. Op die manier zou ervoor worden gezorgd dat de juiste personen op het juiste ogenblik over de juiste informatie beschikken.

Er zijn drie mogelijkheden:

(1) **het CIWIN zou kunnen worden opgezet als een forum uitsluitend voor de uitwisseling van ideeën en beproefde methoden** inzake de bescherming van kritieke infrastructuur, ter ondersteuning van de eigenaren en exploitanten van dergelijke infrastructuur. Een dergelijk forum zou kunnen worden opgezet in de vorm van een netwerk van deskundigen en een elektronisch platform voor de uitwisseling van nuttige informatie in een veilige omgeving. De Commissie zou een belangrijke rol spelen bij het verzamelen en verspreiden van dergelijke informatie. In dit geval zou het niet mogelijk zijn snel te waarschuwen voor imminente dreigingen. Een latere verdere ontwikkeling van het CIWIN is echter denkbaar;

(2) **het CIWIN zou kunnen worden opgezet als een systeem voor snelle waarschuwing tussen de lidstaten en de Commissie.** In dit geval zou de veiligheid van kritieke infrastructuur worden verhoogd omdat voor onmiddellijke dreigingen en alarmsituaties wordt gewaarschuwd. Het doel in dit geval zou zijn de snelle uitwisseling van informatie over mogelijke dreigingen met de eigenaren en exploitanten van kritieke infrastructuur te vergemakkelijken. In het kader van dit

systeem voor snelle waarschuwing zouden geen inlichtingen worden uitgewisseld op op lange termijn. Dit systeem zou worden gebruikt voor de snelle uitwisseling van informatie over onmiddellijke dreigingen voor bepaalde infrastructuurinrichtingen;

(3) **het CIWIN zou als een communicatie-/waarschuwingssysteem met verscheidene niveaus en met twee verschillende functies kunnen worden opgezet:** a) een systeem voor snelle waarschuwing tussen de lidstaten en de Commissie en b) een forum voor de uitwisseling van ideeën en beproefde methoden op het gebied van de bescherming van kritieke infrastructuur in de vorm van een netwerk van deskundigen en een elektronisch platform voor de uitwisseling van gegevens ter ondersteuning van de eigenaren en exploitanten van dergelijke infrastructuur.

Het CIWIN zou, ongeacht voor welke van de drie mogelijkheden wordt gekozen, bestaande netwerken aanvullen en dubbel werk voorkomen. Op lange termijn zouden alle eigenaren en exploitanten van kritieke infrastructuur in alle lidstaten, bijvoorbeeld via het NCCB, met het CIWIN worden verbonden. Waarschuwingen en beproefde methoden zouden kunnen worden doorgegeven via dit orgaan, dat als enige rechtstreeks zou verbonden zijn met de Commissie, en bijgevolg met alle andere lidstaten. De lidstaten zouden hun bestaande informatiesystemen kunnen gebruiken om hun eigen nationale CIWIN-capaciteit tussen de autoriteiten en de eigenaren en exploitanten van kritieke infrastructuur op te zetten. Belangrijk is ook dat deze nationale netwerken door de nationale NCCB en de eigenaren en exploitanten van kritieke infrastructuur als tweerichtingscommunicatiesysteem zouden kunnen worden gebruikt.

In een studie zal worden onderzocht welke de opzet en welke de technische kenmerken moeten zijn van de toekomstige interface tussen het CIWIN en de lidstaten.

Vragen

Welke vorm zou het CIWIN-netwerk moeten krijgen ter ondersteuning van de doelstellingen van het EPCIP?

Zouden eigenaren en exploitanten van kritieke infrastructuur met het CIWIN-netwerk verbonden moeten zijn?

9.2. Gemeenschappelijke methoden

De verschillende lidstaten hanteren verschillende alerteringsniveaus, afhankelijk van de situatie. Op dit ogenblik is onmogelijk te bepalen of bijvoorbeeld een “hoge” staat van alertheid in een lidstaat overeenkomst met een “hoge” staat van alertheid in een andere lidstaat. Dit kan het voor transnationale ondernemingen moeilijk maken prioriteiten voor hun uitgaven voor beschermingsmaatregelen vast te stellen. De harmonisering of uniformisering van de verschillende alerteringsniveaus kan bijgevolg nuttig zijn.

Voor elk niveau van dreiging zou een niveau van paraatheid kunnen worden vastgesteld, dat bepaalde veiligheidsmaatregelen in het algemeen en, eventueel, graduele veiligheidsmaatregelen in het bijzonder ten gevolge heeft. Lidstaten die in geval van een bepaalde dreiging een bepaalde maatregel niet wensen te nemen, zouden in de plaats daarvan alternatieve veiligheidsmaatregelen kunnen treffen.

Er zou een gemeenschappelijke methode kunnen worden overwogen om dreigingen, risico’s, zwakke punten en reactiemogelijkheden in kaart te brengen en te classificeren, en om

conclusies te trekken betreffende de ernst van de dreiging en de mogelijkheid of de waarschijnlijkheid dat de werking van infrastructuur erdoor wordt verstoord. Het zou daarbij kunnen gaan om risico-beoordeling en het vaststellen van prioriteiten, waarbij risico's zouden kunnen worden gedefinieerd op grond van de waarschijnlijkheid dat zij zich zullen voordoen, hun impact en de vraag of zij verband houden met andere risicogebieden en –processen.

Vragen

In hoeverre moeten de verschillende alerteringsniveaus worden geharmoniseerd of geüniformiseerd?

Is een gemeenschappelijke methode nodig om dreigingen, reactiemogelijkheden, risico's en zwakke plekken in kaart te brengen en te classificeren, en om conclusies te trekken betreffende de mogelijkheid of de waarschijnlijkheid dat een dreiging zich voordoet of betreffende de ernst ervan?

9.3. Financiering

Naar aanleiding van een initiatief van het Europees Parlement (invoering van een nieuw begrotingsonderdeel – proefproject "Terrorismebestrijding" – in de begroting 2005), besloot de Commissie op 15 september 7 miljoen EUR toe te kennen voor de financiering van een reeks maatregelen die ten doel hebben de preventie van, de paraatheid bij en de reactie op terreuraanslagen te verbeteren. Dit maatregelenpakket omvat ook gevolgenbeheersing, de bescherming van kritieke infrastructuur en de bestrijding van de financiering van terroristische activiteiten, het gebruik van explosieven en gewelddadige radicalisering. Meer dan twee derde van deze middelen is bestemd voor de uitwerking van het toekomstige Europese programma voor de bescherming van kritieke infrastructuur, de integratie en de ontwikkeling van de capaciteit die vereist is om crisissen van transnationaal belang die het gevolg zijn mogelijke terreuraanslagen te beheersen, en voor de noodmaatregelen die nodig kunnen zijn om het hoofd te bieden aan een ernstige dreiging of een aanslag. Verwacht wordt dat deze financiering ook in 2006 zal worden voortgezet.

Van 2007 tot 2013 zullen de maatregelen worden gefinancierd via het kaderprogramma betreffende "Veiligheid en bescherming van de vrijheden". Dit zal een specifiek programma "Terrorisme: preventie, paraatheid en beheersing van de gevolgen" omvatten. De Commissie heeft voorgesteld een bedrag van 137,4 miljoen EUR uit te trekken om vast te stellen welke de behoeften zijn en om gemeenschappelijke technische normen voor de bescherming van kritieke infrastructuur vast te stellen te ontwikkelen.

Dit programma zal het mogelijk maken financiële steun te verstrekken voor projecten voor de bescherming van kritieke infrastructuur van nationale, regionale en plaatselijke autoriteiten. Het programma heeft in de eerste plaats ten doel vast te stellen welke de behoeften zijn en informatie te verstrekken met het oog op de vaststelling van gemeenschappelijke normen en dreigings- en risico-beoordelingen, teneinde kritieke infrastructuur te beschermen of specifieke rampenplannen uit te werken. De Commissie kan hiervoor gebruikmaken van bestaande expertise of bijdragen in de financiering van studies betreffende de interdependenties in bepaalde sectoren. Het is dan in de eerste plaats de verantwoordelijkheid van de eigenaren en exploitanten de veiligheid van hun infrastructuur te verhogen overeenkomstig de vastgestelde behoeften. Het programma zelf voorziet niet in de mogelijkheid financiële steun te verstrekken voor de verhoging van de veiligheid van kritieke infrastructuur. De Commissie is bereid steun te verlenen voor sectorale studies die ten doel

hebben de financiële gevolgen van de verhoging van de veiligheid van infrastructuur voor het bedrijfsleven te evalueren.

De Commissie financiert onderzoeksprojecten op het gebied van de bescherming van kritieke infrastructuur in het kader van de voorbereidende actie voor veiligheidsonderzoek[2] (2004-2006) en voorziet in meer substantiële activiteiten op het gebied van veiligheidsonderzoek in haar voorstel voor een besluit van de Raad en het Europees Parlement betreffende het zevende kaderprogramma op het gebied van onderzoek van de EG (COM(2005)119 def.)[3] en haar voorstel voor een besluit van de Raad betreffende het specifieke programma "Samenwerking" ter uitvoering van het zevende kaderprogramma (COM(2005)440 def.). Gericht onderzoek dat ten doel heeft praktische strategieën of instrumenten uit te werken om de risico's te beperken is van het grootste belang voor de beveiliging van Europese kritieke infrastructuur op middellange of lange termijn. Elke vorm van veiligheidsonderzoek, ook op dit gebied, zal worden onderworpen aan een ethische evaluatie teneinde de verenigbaarheid ervan met het Handvest van de grondrechten te garanderen. De vraag naar onderzoek zal alleen maar toenemen naarmate de het aantal interdependenties tussen infrastructuurinrichtingen toeneemt.

Vragen

Welke zouden volgens u de kosten en de gevolgen van de uitvoering van de in dit groenboek voorgestelde maatregelen zijn voor de overheidsdiensten en het bedrijfsleven? Acht u deze evenredig?

9.4. Evaluatie en monitoring

Voor de evaluatie van en het toezicht op de uitvoering van het EPCIP is een proces op verscheidene niveaus nodig, waarbij alle belanghebbende partijen moeten worden betrokken:

- **op EU-niveau zou een mechanisme van onderlinge toetsing kunnen worden ingevoerd,** waarin de lidstaten en de Commissie zouden samenwerken bij de evaluatie van het algemene niveau van uitvoering van het EPCIP in elke lidstaat. De Commissie zou jaarlijkse voortgangsverslagen over de uitvoering van het EPCIP kunnen opstellen;

- **de Commissie zou de lidstaten en de andere instellingen elk kalenderjaar** in een werkdocument van de diensten van de Commissie **op de hoogte brengen van de geboekte vooruitgang;**

- **op het niveau van de lidstaten zou het NCCB in elke lidstaat kunnen toezien op de algemene uitvoering van het EPCIP binnen zijn bevoegdheidsgebied, waarbij het zich ervan vergewist of het/de nationale programma('s) voor de bescherming van kritieke infrastructuur en sectorspecifieke programma's in acht worden genomen,** teneinde door middel van jaarlijkse verslagen aan de Raad en de Commissie te garanderen dat deze daadwerkelijk worden uitgevoerd.

---

2 Het totale bedrag aan kredieten in de begroting 2004 en 2005 beliep 30 miljoen EUR. De Commissie heeft voor 2006 het bedrag van 24 miljoen EUR voorgesteld. Dit voorstel wordt momenteel door de begrotingsautoriteit onderzocht.

3 Voor onderzoeksactiviteiten op het gebied van veiligheid en ruimtevaart in het kader van het zevende kaderprogramma op het gebied van O&O heeft de Commissie een bedrag van 570 miljoen EUR aan begrotingsmiddelen voorgesteld (COM(2005)119 def.)

De uitvoering van het EPCIP zou een dynamisch proces zijn dat constant evolueert en wordt geëvalueerd zodat gelijke tred kan worden gehouden met de veranderende wereld en kan worden voortgebouwd op de opgedane ervaring. Er zou gebruik kunnen worden gemaakt van door deskundigen uitgevoerde evaluaties en van controleverslagen van de Commissie als instrumenten om het EPCIP te herzien en nieuwe maatregelen voor te stellen om de bescherming van kritieke infrastructuur te verbeteren.

Door de lidstaten zou relevante informatie betreffende Europese kritieke infrastructuur (ECI) ter beschikking van de Commissie kunnen worden gesteld met het oog op de ontwikkeling van gemeenschappelijke kwetsbaarheidsanalyses, gevolgenbeheersingsplannen, gemeenschappelijke normen voor de bescherming van kritieke infrastructuur, de vaststelling van de prioriteit die onderzoeksactiviteiten moeten krijgen en, waar nodig, regelgeving en harmonisatie. Dergelijke informatie zou als geclassificeerde informatie worden beschouwd en strikt vertrouwelijk worden gehouden.

De Commissie zou verschillende initiatieven van de lidstaten van nabij kunnen volgen, in het bijzonder die in het kader waarvan financiële gevolgen worden verwacht voor eigenaren en exploitanten die niet in staat zijn binnen een bepaalde maximumtermijn essentiële diensten te hervatten.

Vraag

Welk soort evaluatiemechanisme acht u nodig voor het EPCIP? Acht u het hiervoor beschreven mechanisme toereikend?

Reacties dienen uiterlijk op 15 januari 2006 elektronisch naar het volgende e-mailadres te worden gezonden: **JLS-EPCIP@cec.eu.int**. Deze antwoorden zullen vertrouwelijk worden behandeld, tenzij de auteur ervan uitdrukkelijk verklaart dat hij wenst dat deze openbaar worden gemaakt. In dat geval zullen zij op de internetsite van de Commissie worden gepubliceerd.

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.