COMMISSIE VAN DE EUROPESE GEMEENSCHAPPEN

Brussel, 12.12.2006
COM(2006) 787 definitief

2006/0276 (CNS)

Voorstel voor een

RICHTLIJN VAN DE RAAD

inzake de inventarisatie van Europese kritieke infrastructuur, de aanmerking van infrastructuur als Europese kritieke infrastructuur en de beoordeling van de noodzaak de bescherming van dergelijke infrastructuur te verbeteren

(door de Commissie ingediend)

{SEC(2006) 1648}
{SEC(2006) 1654}

TOELICHTING

1) ACHTERGROND VAN HET VOORSTEL

- **Motivering en doel van het voorstel**

De Europese Raad van juni 2004 heeft de Commissie verzocht een algemene strategie ter bescherming van kritieke infrastructuur voor te bereiden. De Commissie heeft op 20 oktober 2004 een mededeling over "Terrorismebestrijding: de bescherming van kritieke infrastructuur" aangenomen, waarin voorstellen worden gedaan over de wijze waarop de preventie van, de paraatheid bij en de reactie op terreuraanslagen op kritieke infrastructuur (CI) 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.

In november 2005 hechtte de Commissie haar goedkeuring aan een Groenboek betreffende een Europees programma voor de bescherming van kritieke infrastructuur (EPCIP), waarin beleidsopties zijn opgenomen in verband met de wijze waarop de Commissie het EPCIP en het CIWIN tot stand zou kunnen brengen.

In december 2005 verzocht de Raad Justitie en Binnenlandse Zaken (JBZ) de Commissie tegen juni 2006 een voorstel betreffende het EPCIP in te dienen.

In het onderhavige voorstel voor een richtlijn worden de maatregelen beschreven die door de Commissie worden voorgesteld voor de inventarisatie van Europese kritieke infrastructuur (ECI), voor de aanmerking van infrastructuur als ECI en voor de beoordeling van de noodzaak de bescherming van deze infrastructuur te verbeteren.

- **Algemene context**

De Europese Unie telt een aantal infrastructuurvoorzieningen waarvan de verstoring of vernietiging invloed zou hebben op twee of meer lidstaten. Het is ook mogelijk dat het uitvallen van dergelijke kritieke infrastructuur in een lidstaat effecten heeft in een ander lidstaat. Zulke vitale infrastructuurvoorzieningen met een transnationale dimensie moeten in kaart worden gebracht en als ECI worden aangemerkt. Dat is alleen mogelijk via een gemeenschappelijke procedure voor de inventarisatie van ECI en voor de beoordeling van de noodzaak de bescherming ervan te verbeteren.

Gezien de transnationale dimensie van deze infrastructuur zou een geïntegreerde aanpak op EU-niveau bij het onderzoek naar de zwakke en kwetsbare plekken ervan en bij de opsporing van leemten in de beschermingsmaatregelen niet alleen een nuttige aanvulling vormen op de reeds in de lidstaten bestaande nationale programma's voor de bescherming van kritieke infrastructuur, die daardoor een meerwaarde zouden krijgen, maar er ook in belangrijke mate toe bijdragen dat de Europese interne markt levensvatbaar blijft en welvaart blijft scheppen.

Aangezien in verschillende sectoren specifieke ervaring en deskundigheid op het gebied van de bescherming van kritieke infrastructuur (CIP) beschikbaar is en er op dat gebied specifieke behoeften bestaan, zou een EU-aanpak van de CIP moeten worden uitgewerkt en ten uitvoer gelegd, waarbij rekening wordt gehouden met de specifieke kenmerken van de sector waartoe de kritieke infrastructuur (CI) behoort. Daarbij zouden de reeds in de verschillende sectoren bestaande maatregelen als uitgangspunt moeten worden genomen. Ter vergemakkelijking van deze sectorale aanpak van de bescherming van kritieke infrastructuur dient een gemeenschappelijke lijst van sectoren met kritieke infrastructuur te worden opgesteld.

- **De behoefte aan een gemeenschappelijk kader**

Alleen een gemeenschappelijk kader kan de basis verschaffen die vereist is om de maatregelen ter verbetering van de bescherming van ECI op coherente en uniforme wijze ten uitvoer te leggen en om de respectieve verantwoordelijkheden van de partijen die betrokken zijn bij de bescherming van ECI duidelijk af te bakenen. Niet-bindende vrijwillige maatregelen zouden weliswaar flexibel zijn, maar niet voldoende duidelijkheid verschaffen over wie wat moet doen en zij zouden evenmin bijdragen tot de verduidelijking van de rechten en plichten van de betrokken partijen.

Een procedure voor de inventarisatie van Europese kritieke infrastructuur en voor de aanmerking van infrastructuur als ECI, alsmede een gemeenschappelijke aanpak om te beoordelen of het nodig is de bescherming van dergelijke infrastructuur te verbeteren, kunnen enkel door middel van een richtlijn worden vastgesteld. Het doel is immers:

- een adequaat niveau van bescherming van ECI te garanderen;
- ervoor te zorgen dat alle betrokken partijen vergelijkbare rechten en plichten hebben;
- te garanderen dat de stabiliteit van de interne markt wordt gehandhaafd.

De beschadiging of het uitvallen van een bepaalde infrastructuurvoorziening in een lidstaat kan negatieve effecten 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 infrastructuurvoorzieningen 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.

- **Een sectorale dialoog met de betrokken partijen**

Voor een doeltreffende bescherming is communicatie, coördinatie en samenwerking op nationaal niveau en op EU-niveau tussen alle betrokken partijen vereist.

De volledige betrokkenheid van de particuliere sector is belangrijk, aangezien de meeste kritieke-infrastructuurvoorzieningen eigendom zijn van de particuliere sector en door deze sector worden beheerd. Elke exploitant dient op de beheersing van de risico's toe te zien, aangezien normaal gezien uitsluitend de exploitant beslist welke beschermende maatregelen en bedrijfscontinuïteitsplannen ten uitvoer worden gelegd. Bij de continuïteitsplanning

moeten de normale bedrijfsprocessen en de normale bedrijfslogica in acht worden genomen en moeten, waar mogelijk, oplossingen op gangbare commerciële regelingen worden gebaseerd.

De sectoren beschikken over specifieke ervaring en deskundigheid op het gebied van de bescherming van hun kritieke infrastructuur en hebben specifieke behoeften op dat gebied.

De particuliere sector zou derhalve, overeenkomstig de reacties op het groenboek betreffende een Europees programma voor de bescherming van kritieke infrastructuur, ten volle moeten worden betrokken bij de EU-aanpak, in het kader waarvan rekening zou moeten worden gehouden met de specifieke kenmerken per sector. De in de verschillende sectoren bestaande beschermingsmaatregelen zouden als uitgangspunt voor deze EU-aanpak moeten worden genomen.

- **Bestaande bepalingen op het door het voorstel bestreken gebied**

Momenteel bestaan er op EU-niveau geen horizontale bepalingen inzake de bescherming van kritieke infrastructuur. Bij deze richtlijn wordt een procedure ingesteld voor de inventarisatie van Europese kritieke infrastructuur en voor de aanmerking van infrastructuur als Europese kritieke infrastructuur. Daarnaast wordt in deze richtlijn een gemeenschappelijke aanpak vastgesteld om te beoordelen of het nodig is de bescherming van dergelijke infrastructuur te verbeteren.

Er bestaat een aantal sectorspecifieke maatregelen, onder meer:

- in de IT-sector:

  (a) de Universeledienstrichtlijn (Richtlijn 2002/22/EG), die onder meer de integriteit van openbare elektronische communicatienetwerken betreft;

  (b) de Machtigingsrichtlijn (Richtlijn 2002/20/EG), die onder meer de integriteit van openbare elektronische communicatienetwerken betreft;

  (c) de richtlijn inzake e-privacy (Richtlijn 2002/58/EG), die onder meer de beveiliging van openbare elektronische communicatienetwerken betreft;

  (d) Kaderbesluit 2005/222/JBZ van de Raad van 24 februari 2005 over aanvallen op informatiesystemen;

  (e) Verordening (EG) nr. 460/2004 van 10 maart 2004 tot oprichting van het Europees Agentschap voor netwerk- en informatiebeveiliging (ENISA).

- in de sector van de gezondheidszorg:

  (a) Beschikking nr. 2119/98/EG van het Europees Parlement en de Raad van 24 september 1998 tot oprichting van een netwerk voor epidemiologische surveillance en beheersing van overdraagbare ziekten in de Europese Gemeenschap;

(b) Richtlijn 2003/94/EG van de Commissie van 8 oktober 2003 tot vaststelling van de beginselen en richtsnoeren inzake goede praktijken bij het vervaardigen van geneesmiddelen voor menselijk gebruik en geneesmiddelen voor onderzoek voor menselijk gebruik.

- in de financiële sector:

(a) Richtlijn 2004/39/EG van het Europees Parlement en de Raad van 21 april 2004 betreffende markten voor financiële instrumenten (MiFID);

(b) De oversightnormen voor euro-retailbetalingssystemen, die in juni 2003 door de Raad van bestuur van de Europese Centrale Bank (ECB) werden goedgekeurd;

(c) Richtlijn 2006/48/EG van het Europees Parlement en de Raad van 14 juni 2006 betreffende de toegang tot en de uitoefening van de werkzaamheden van kredietinstellingen;

(d) Richtlijn 2006/49/EG van het Europees Parlement en de Raad van 14 juni 2006 inzake de kapitaaltoereikendheid van beleggingsondernemingen en kredietinstellingen;

(e) Voorstel voor een richtlijn betreffende betalingsdiensten in de interne markt tot wijziging van de Richtlijnen 97/7/EG, 2001/12/EG en 2002/65/EG (COM(2005) 603);

(f) Richtlijn 2000/46/EG van het Europees Parlement en de Raad van 18 september 2000 betreffende de toegang tot, de uitoefening van en het bedrijfseconomisch toezicht op de werkzaamheden van instellingen voor elektronisch geld;

(g) Richtlijn 1998/26/EG van het Europees Parlement en de Raad van 19 mei 1998 betreffende het definitieve karakter van betalingen en effectentransacties.

- in de transportsector:

(a) Verordening (EG) nr. 725/2004 van het Europees Parlement en de Raad van 31 maart 2004 betreffende de verbetering van de beveiliging van schepen en havenfaciliteiten;

(b) Verordening (EG) nr. 884/2005 van de Commissie van 10 juni 2005 tot vaststelling van procedures voor inspecties van de Commissie op het gebied van maritieme beveiliging;

(c) Richtlijn 2005/65/EG van het Europees Parlement en de Raad van 26 oktober 2005 betreffende het verhogen van de veiligheid van havens;

(d) Verordening (EG) nr. 2320/2002 van het Europees Parlement en de Raad van 16 december 2002 tot vaststelling van gemeenschappelijke regels op het gebied van de beveiliging van de burgerluchtvaart;

(e) Verordening (EG) nr. 622/2003 van de Commissie van 4 april 2003 tot vaststelling van maatregelen voor de tenuitvoerlegging van de gemeenschappelijke basisnormen op het gebied van de beveiliging van de luchtvaart;

(f) Verordening (EG) nr. 1217/2003 van de Commissie van 4 juli 2003 tot vaststelling van gemeenschappelijke specificaties voor nationale programma's voor de kwaliteitscontrole van de beveiliging van de burgerluchtvaart;

(g) Verordening (EG) nr. 1486/2003 van de Commissie van 22 augustus 2003 tot vaststelling van procedures voor de inspecties van de Commissie op het gebied van de beveiliging van de burgerluchtvaart;

(h) Verordening (EG) nr. 68/2004 van de Commissie van 15 januari 2004 tot wijziging van Verordening (EG) nr. 622/2003 van de Commissie tot vaststelling van maatregelen voor de tenuitvoerlegging van de gemeenschappelijke basisnormen op het gebied van de beveiliging van de luchtvaart;

(i) Verordening (EG) nr. 849/2004 van het Europees Parlement en de Raad van 29 april 2004 houdende wijziging van Verordening (EG) nr. 2320/2002 tot vaststelling van gemeenschappelijke regels op het gebied van de beveiliging van de burgerluchtvaart;

(j) Verordening (EG) nr. 1138/2004 van de Commissie van 21 juni 2004 tot vaststelling van een gemeenschappelijke definitie van de meest kwetsbare sectoren van de om beveiligingsredenen beperkt toegankelijke zones van luchthavens;

(k) Verordening (EG) nr. 781/2005 van de Commissie van 24 mei 2005 tot wijziging van Verordening (EG) nr. 622/2003 tot vaststelling van maatregelen voor de tenuitvoerlegging van de gemeenschappelijke basisnormen op het gebied van de beveiliging van de luchtvaart;

(l) Verordening (EG) nr. 857/2005 van de Commissie van 6.juni.2005 tot wijziging van Verordening (EG) nr. 622/2003 tot vaststelling van maatregelen voor de tenuitvoerlegging van de gemeenschappelijke basisnormen op het gebied van de beveiliging van de luchtvaart;

(m) Richtlijn 2001/14/EG inzake de toewijzing van spoorweginfrastructuurcapaciteit;

(n) Het vervoer van gevaarlijke goederen per spoor valt onder Richtlijn 96/49/EG (gewijzigd bij Richtlijn 2004/110, tot goedkeuring van het RID 2005 (Reglement betreffende het spoorwegvervoer van gevaarlijke goederen);

(o) Verdrag inzake de fysieke beveiliging van kernmateriaal en nucleaire faciliteiten (ondertekening van het Verdrag in 1980, toetreding tot het Verdrag in 1981 en inwerkingtreding van het Verdrag in 1987).

- in de chemische sector:

    (a) Gevaarlijke installaties onder de Seveso II-richtlijn (Richtlijn 96/82/EG van de Raad van 9 december 1996 betreffende de beheersing van de gevaren van zware ongevallen waarbij gevaarlijke stoffen zijn betrokken ("Seveso II-richtlijn"), gewijzigd bij Richtlijn 2003/105/EG van het Europees Parlement en de Raad van 16 december 2003.

- in de nucleaire sector:

    (a) Richtlijn 89/618/Euratom van de Raad van 27 november 1989 betreffende de informatie van de bevolking over de bij stralingsgevaar toepasselijke maatregelen ter bescherming van de gezondheid en over de alsdan te volgen gedragslijn;

    (b) Beschikking 87/600/Euratom van de Raad van 14 december 1987 inzake communautaire regelingen voor snelle uitwisseling van informatie in geval van stralingsgevaar.

- **Samenhang met andere beleidsgebieden en doelstellingen van de EU**

Dit voorstel is volledig in overeenstemming met de doelstellingen van de Unie en meer bepaald met het doel de Unie te handhaven en te ontwikkelen "als een ruimte van vrijheid, veiligheid en rechtvaardigheid waarin het vrije verkeer van personen gewaarborgd is in combinatie met passende maatregelen met betrekking tot controles aan de buitengrenzen, asiel, immigratie, en voorkoming en bestrijding van criminaliteit".

Dit voorstel is verenigbaar met andere beleidsmaatregelen, aangezien het niet de bedoeling is bestaande maatregelen te vervangen, maar wel deze aan te vullen teneinde de bescherming van ECI te verbeteren.

2) RAADPLEGING VAN DE BELANGHEBBENDE PARTIJEN EN EFFECTBEOORDELING

- **Raadpleging van de belanghebbende partijen**

Alle belanghebbende partijen zijn geraadpleegd over de uitwerking van het EPCIP. Dit is gebeurd door middel van:

- het groenboek betreffende een EPCIP, dat op 17 november 2005 werd goedgekeurd en waarvoor de raadplegingstermijn op 15 januari 2006 verstreek. 22 lidstaten hebben officieel op de raadpleging gereageerd. Ongeveer 100 vertegenwoordigers van de particuliere sector hebben eveneens opmerkingen gemaakt bij het groenboek. In het algemeen werd positief gereageerd op de idee om een EPCIP uit te werken;

- drie seminars over de bescherming van kritieke infrastructuur onder auspiciën van de Commissie (in juni 2005, september 2005 en maart 2006). Op elk van deze drie seminars kwamen vertegenwoordigers van de lidstaten bijeen. De particuliere

sector werd uitgenodigd op de seminars die in september 2005 en maart 2006 werden gehouden;

- informele bijeenkomsten van contactpunten voor aangelegenheden in verband met de bescherming van kritieke infrastructuur (CIP-contactpunten). Er werden door de Commissie twee bijeenkomsten van de CIP-contactpunten van de lidstaten belegd (december 2005 en februari 2006);

- informele bijeenkomsten met vertegenwoordigers van de particuliere sector. Er werden talrijke informele bijeenkomsten met vertegenwoordigers van bepaalde particuliere ondernemingen en met bedrijfsorganisaties gehouden;

- intern, binnen de Commissie, werden de werkzaamheden ter ontwikkeling van het EPCIP voortgezet tijdens regelmatig gehouden bijeenkomsten van de subgroep inzake de bescherming van kritieke infrastructuur en de interdienstengroep inzake de interne aspecten van terrorisme.

- **Bijeenbrengen en benutten van deskundigheid**

De beschikbare deskundigheid werd bijeengebracht via talrijke in 2005 en 2006 gehouden bijeenkomsten en seminars en via het raadplegingsproces naar aanleiding van het groenboek betreffende een EPCIP. Er werd informatie vergaard bij alle belanghebbende partijen.

- **Effectbeoordeling**

Een kopie van de effectbeoordeling van het EPCIP is bijgevoegd.

3) JURIDISCHE ELEMENTEN VAN HET VOORSTEL

- **Samenvatting van de voorgestelde maatregel**

Met de voorgestelde maatregel wordt een horizontaal kader gecreëerd voor het in kaart brengen van Europese kritieke infrastructuur, voor de aanmerking van infrastructuur als Europese kritieke infrastructuur en voor de beoordeling van de noodzaak de bescherming van deze infrastructuur te verbeteren.

- **Rechtsgrondslag**

De rechtsgrondslag voor het voorstel is artikel 308 van het Verdrag tot oprichting van de Europese Gemeenschap.

- **Subsidiariteitsbeginsel**

Het subsidiariteitsbeginsel is nageleefd, aangezien de maatregelen die door middel van dit voorstel worden genomen niet door enige afzonderlijke EU-lidstaat kunnen worden uitgevoerd en daarom op EU-niveau moeten worden vastgesteld. Hoewel het de verantwoordelijkheid van elke lidstaat is de kritieke infrastructuur binnen zijn bevoegdheidsgebied te beschermen, is het voor de veiligheid van de Europese Unie van cruciaal belang dat ervoor wordt gezorgd dat infrastructuur die een impact heeft op twee of meer lidstaten of op een enkele lidstaat, indien dit een andere lidstaat is dan die waar de kritieke infrastructuur zich bevindt, voldoende wordt beschermd en dat een of meer lidstaten

niet kwetsbaar worden gemaakt door zwakke punten of lagere veiligheidsnormen in een andere lidstaat. Soortgelijke regels inzake veiligheid in de verschillende lidstaten zouden er ook voor helpen zorgen dat geen afbreuk wordt gedaan aan de mededingingsregels binnen de interne markt.

- **Evenredigheidsbeginsel**

Dit voorstel gaat niet verder dan nodig is om de onderliggende doelstelling van verbetering van de bescherming van Europese kritieke infrastructuur te verwezenlijken. De belangrijkste in het voorstel geformuleerde ideeën betreffen de invoering van een basismechanisme voor coördinatie op EU-niveau, de verplichting voor de lidstaten hun kritieke infrastructuur te inventariseren, de tenuitvoerlegging van een reeks basisveiligheidsmaatregelen voor kritieke infrastructuur en ten slotte de inventarisatie van Europese kritieke infrastructuur en de aanmerking van infrastructuur als Europese kritieke infrastructuur. In dit voorstel worden daarom de voorwaarden vastgelegd waaraan minimaal moet zijn voldaan om te beginnen met de werkzaamheden ter verbetering van de bescherming van kritieke infrastructuur. Dit doel kan niet voldoende worden verwezenlijkt door andere maatregelen, zoals de vaststelling van richtsnoeren voor het EPCIP, omdat hierdoor niet de verbetering van de beschermingsniveaus in de hele EU en de volledige deelname van alle betrokken partijen zouden worden gegarandeerd.

- **Keuze van instrumenten**

De lidstaten pakken de bescherming van kritieke infrastructuur op uiteenlopende wijzen aan en ook hun rechtsstelsels zijn verschillend. Een richtlijn is daarom het meest geschikte instrument om een gemeenschappelijke procedure voor de inventarisatie van Europese kritieke infrastructuur en voor de aanmerking van infrastructuur als ECI uit te werken en om te komen tot een gemeenschappelijke aanpak voor de beoordeling van de noodzaak de bescherming van dergelijke infrastructuur te verbeteren.

4) GEVOLGEN VOOR DE BEGROTING

De gevolgen voor de begroting worden geraamd in het begeleidende financieel memorandum.

Het programma "Terrorisme en andere aan veiligheid gerelateerde risico's: preventie, paraatheid en beheersing van de gevolgen" voor de periode 2007-2013 zal bijdragen tot de tenuitvoerlegging van deze richtlijn bij de bescherming van personen tegen veiligheidsrisico's en die materiële middelen, diensten en informatietechnologische voorzieningen, netwerken en infrastructuuractiva waarvan de ontwrichting of vernietiging een groot effect zou hebben op de kritieke maatschappelijke functies, als onderdeel van het algemene programma "Veiligheid en bescherming van de vrijheden".

Dit programma is niet van toepassing op aangelegenheden die onder andere financiële instrumenten, en in het bijzonder onder het instrument voor snelle respons bij ernstige noodsituaties en het Solidariteitsfonds van de EU, vallen.

5) AANVULLENDE INFORMATIE

- **Intrekking van bestaande wetgeving**

Er hoeft geen bestaande wetgeving te worden ingetrokken.

- **Nadere uitleg van het voorstel**

Artikel 1 – Omschrijving van het voorwerp van de richtlijn. Bij de richtlijn wordt een gemeenschappelijke procedure ingesteld voor de inventarisatie van Europese kritieke infrastructuur en voor de aanmerking van infrastructuur als Europese kritieke infrastructuur, waarmee die infrastructuur wordt bedoeld waarvan de vernietiging of verstoring invloed heeft in twee of meer lidstaten, of in een enkele lidstaat, indien dit een andere lidstaat is dan die waar de kritieke infrastructuur zich bevindt. Bij de richtlijn wordt een gemeenschappelijke aanpak vastgesteld om te beoordelen of het nodig is de bescherming van Europese kritieke infrastructuur te verbeteren. Deze beoordeling zal een bijdrage leveren aan de voorbereiding van specifieke beschermingsmaatregelen in de afzonderlijke CI-sectoren.

Artikel 2 – Vaststelling van een lijst van voor de richtlijn dienstige basisdefinities.

Artikel 3 – Vaststelling van de procedure voor de inventarisatie van ECI. Onder ECI wordt die kritieke (ook wel: vitale) infrastructuur verstaan waarvan de verstoring of vernietiging een ernstige invloed zou hebben op twee of meer lidstaten, of op een enkele lidstaat, indien dit een andere lidstaat is dan die waar de kritieke infrastructuur zich bevindt. Deze procedure is gebaseerd op een driestappenaanpak. Eerst ontwikkelt de Commissie samen met de lidstaten en de belanghebbende partijen sectoroverstijgende en sectorspecifieke criteria voor de inventarisatie van ECI, die dan via de comitéprocedure worden aangenomen. De sectoroverstijgende criteria worden vastgesteld op grond van de ernst van de verstoring of vernietiging van de CI. De ernst van de gevolgen van de verstoring of vernietiging van een bepaalde infrastructuurvoorziening zou, waar mogelijk, moeten worden beoordeeld op basis van:

- de gevolgen voor het publiek (aantal getroffen personen);
- de economische gevolgen (omvang van het economisch verlies en/of de kwaliteitsvermindering van producten of diensten);
- de gevolgen voor het milieu;
- de politieke gevolgen;
- de psychologische gevolgen;
- de gevolgen voor de volksgezondheid.

Elke lidstaat stelt dan een inventaris op van die infrastructuurvoorzieningen die aan de criteria voldoen. Ten slotte stelt elke lidstaat de Commissie in kennis van de kritieke infrastructuurvoorzieningen die aan de vastgestelde criteria voldoen. De nodige werkzaamheden worden verricht in het kader van de prioritaire CI-sectoren die door de Commissie op jaarbasis worden geselecteerd uit die welke in bijlage I zijn opgenomen. De in

bijlage I opgenomen lijst kan via de comitéprocedure worden gewijzigd voor zover het toepassingsgebied van de richtlijn er niet door wordt uitgebreid. Dat zou in het bijzonder betekenen dat wijzigingen in de lijst worden aangebracht om de inhoud ervan te verduidelijken. De Commissie beschouwt de transport- en de energiesector als sectoren waarin onmiddellijk actie moet worden ondernomen.

Artikel 4 – Beschrijving van de procedure voor de aanmerking als ECI. In aansluiting op de overeenkomstig artikel 3 uitgevoerde inventarisatieprocedure, stelt de Commissie een ontwerplijst van ECI op. De ontwerplijst is gebaseerd op de van de lidstaten ontvangen kennisgevingen en op andere relevante informatie van de Commissie. Vervolgens wordt de lijst aangenomen via de comitéprocedure.

Artikel 5 – Beveiligingsplannen van de exploitanten (Operator Security Plans - OSP). Overeenkomstig artikel 5 dienen alle eigenaren/exploitanten van als ECI aangemerkte infrastructuur een OSP op te stellen waarin de Europese kritieke infrastructuur van de eigenaren en exploitanten wordt geïnventariseerd en passende beveiligingsoplossingen voor de bescherming ervan worden voorgesteld. In bijlage II wordt vastgesteld wat een dergelijk OSP op zijn minst moet omvatten, namelijk:

- een inventaris van belangrijke infrastructuurvoorzieningen;
- een risicoanalyse verricht op basis van de belangrijkste dreigingen, de kwetsbaarheden van elke infrastructuurvoorziening en de potentiële impact;
- de vastgestelde, geselecteerde en als prioritair beschouwde tegenmaatregelen en procedures, waarbij een onderscheid moet worden gemaakt tussen:
    - **permanente beveiligingsmaatregelen:** hieronder vallen absoluut noodzakelijke investeringen in beveiliging en middelen die door de eigenaar/exploitant niet op korte termijn kunnen worden opgebracht. Dit onderdeel moet informatie bevatten over algemene maatregelen, technische maatregelen (waaronder de installatie van detectie-, toegangscontrole-, beschermings- en preventieapparatuur), organisatorische maatregelen (waaronder alerterings- en crisisbeheersingsprocedures), controle- en verificatiemaatregelen, Communicatie, bewustmaking en opleiding, en beveiliging van informatiesystemen.
    - **graduele beveiligingsmaatregelen:** beveiligingsmaatregelen die worden aangepast aan het risico- en dreigingsniveau.

In elke CI-sector kunnen sectorspecifieke beveiligingsplannen worden opgesteld, die op de minimumvereisten van bijlage II zijn gebaseerd. Zulke sectorspecifieke beveiligingsplannen kunnen via de comitéprocedure worden aangenomen.

Voor die sectoren waarin soortgelijke verplichtingen reeds bestaan, voorziet artikel 5, lid 2, in de mogelijkheid van vrijstelling van de OSP-verplichtingen op grond van een via de comitéprocedure genomen beslissing. Er wordt erkend dat Richtlijn 2005/65/EG van het Europees Parlement en de Raad van 26 oktober 2005 betreffende het verhogen van de veiligheid van havens reeds voldoet aan de voorwaarde dat een beveiligingsplan van de exploitant moet worden opgesteld.

Zodra een OSP is opgesteld, zou elke eigenaar/exploitant van ECI dit aan de bevoegde autoriteit van de lidstaat moeten voorleggen. Elke lidstaat zet een systeem voor toezicht op de beveiligingsplannen op, dat garandeert dat de eigenaar/exploitant van ECI voldoende feedback krijgt over de kwaliteit van de beveiligingsplannen en in het bijzonder over de doeltreffendheid van de risico- en dreigingsanalyse.

Artikel 6 – De veiligheidsverbindingsfunctionaris (Security Liaison Officer - SLO). In artikel 6 wordt bepaald dat alle eigenaren/exploitanten van als ECI aangemerkte infrastructuur een SLO moeten aanstellen. Deze veiligheidsverbindingsfunctionaris zou fungeren als contactpunt voor aangelegenheden in verband met veiligheid tussen de ECI en de voor de bescherming van kritieke infrastructuur bevoegde autoriteiten in de lidstaten. De SLO zou daartoe alle relevante informatie in verband met de bescherming van kritieke infrastructuur ontvangen van de autoriteiten van de lidstaten en verantwoordelijk zijn voor de verstrekking van relevante informatie over de ECI aan de lidstaat.

Artikel 7 – Verslagen. Bij artikel 7 wordt een reeks rapportageregels ingevoerd. Elke lidstaat is verplicht om ECI aan een risico- en dreigingsanalyse te onderwerpen. Deze informatie zal de basis vormen voor de dialoog over veiligheidsaangelegenheden (toezicht) van de lidstaten met de ECI, zoals aangegeven in artikel 5. Aangezien eigenaren/exploitanten van ECI overeenkomstig artikel 5 beveiligingsplannen dienen op te stellen en deze aan de autoriteiten van de lidstaten dienen voor te leggen, wordt elke lidstaat verzocht een algemeen overzicht op de stellen van de soorten kwetsbare plekken, dreigingen en risico's die in elke CI-sector worden vastgesteld, en deze informatie aan de Commissie te verstrekken. Deze informatie zal voor de Commissie de basis vormen om te beoordelen of aanvullende beschermingsmaatregelen nodig zijn. De informatie zou later kunnen worden gebruikt voor de uitwerking van effectbeoordelingen, die bij toekomstige voorstellen op dit gebied zouden worden gevoegd.

Overeenkomstig dit artikel kunnen ook gemeenschappelijke methoden voor risico-, dreigings- en kwetsbaarheidsanalyses met betrekking tot ECI worden uitgewerkt. Dergelijke gemeenschappelijke methoden zouden via de comitéprocedure worden aangenomen.

Artikel 8 – Steun van de Commissie voor ECI. De Commissie zal de eigenaren/exploitanten van ECI helpen door toegang te verlenen tot beproefde methoden in verband met de bescherming van CI. De Commissie zal dergelijke informatie uit verschillende bronnen (bijv. de lidstaten, eigen bronnen) bijeenbrengen en ter beschikking stellen van alle betrokkenen.

Artikel 9 – Contactpunten voor aangelegenheden in verband met de bescherming van kritieke infrastructuur (CIP-contactpunten). Teneinde de samenwerking en coördinatie inzake aangelegenheden in verband met de bescherming van kritieke infrastructuur te waarborgen, dient elke lidstaat een contactpunt voor aangelegenheden in verband met de bescherming van kritieke infrastructuur aan te wijzen. Het contactpunt zou aangelegenheden in verband met de bescherming van kritieke infrastructuur coördineren binnen de lidstaat, met andere lidstaten en met de Commissie.

Artikel 10 – Vertrouwelijkheid en uitwisseling van informatie over de bescherming van kritieke infrastructuur. Vertrouwelijkheid en de uitwisseling van informatie over de bescherming van kritieke infrastructuur vormen een cruciaal en delicaat bestanddeel van de werkzaamheden met betrekking tot de bescherming van kritieke infrastructuur. Daarom bepaalt de richtlijn dat de Commissie en de lidstaten passende maatregelen moeten nemen om informatie te beschermen. Elk personeelslid dat vertrouwelijke informatie over de

bescherming van kritieke infrastructuur hanteert, zou aan het vereiste, door de autoriteiten van de lidstaat verrichte veiligheidsonderzoek moeten worden onderworpen.

Artikel 11 – Comité. Bepaalde onderdelen van de richtlijn zullen via de comitéprocedure ten uitvoer worden gelegd. Het comité zal zijn samengesteld uit de CIP-contactpunten. Voor de doelstelling van artikel 5, lid 2, namelijk de vrijstelling van bepaalde sectoren van de verplichting een beveiligingsplan op te stellen, zal gebruik worden gemaakt van de raadplegingsprocedure.

Voor de volgende aangelegenheden wordt de regelgevingsprocedure overwogen:

- artikel 3, lid 1 – aanneming van de sectoroverstijgende en sectorspecifieke criteria om ECI te inventariseren;
- artikel 3, lid 2 – wijziging van de lijst van CI-sectoren van bijlage I;
- Artikel 4, lid 2 - aanneming van de ontwerplijst van ECI;
- artikel 5, lid 2 – ontwikkeling van sectorspecifieke vereisten voor de OSP;
- artikel 7, lid 2 – ontwikkeling van een gemeenschappelijk rapportagemodel voor algemene verslagen over vastgestelde risico's, dreigingen en kwetsbaarheden;
- artikel 7, lid 4 – ontwikkeling van gemeenschappelijke methoden voor de uitvoering van risico-, dreigings- en kwetsbaarheidsanalyses.

2006/0276 (CNS)

Voorstel voor een

RICHTLIJN VAN DE RAAD

inzake de inventarisatie van Europese kritieke infrastructuur, de aanmerking van infrastructuur als Europese kritieke infrastructuur en de beoordeling van de noodzaak de bescherming van dergelijke infrastructuur te verbeteren

(Voor de EER relevante tekst)

DE RAAD VAN DE EUROPESE UNIE,

Gelet op het Verdrag tot oprichting van de Europese Gemeenschap, en met name op artikel 308,

Gelet op het Verdrag tot oprichting van de Europese Gemeenschap voor Atoomenergie, en met name op artikel 203,

Gezien het voorstel van de Commissie[1],

Gezien het advies van het Europees Parlement[2],

Gezien het advies van de Europese Centrale Bank[3],

Overwegende hetgeen volgt:

(1) In juni 2004 verzocht de Europese Raad een algemene strategie voor de bescherming van kritieke infrastructuur voor te bereiden[4]. Naar aanleiding van dit verzoek heeft de Commissie op 20 oktober 2004 een mededeling over "Terrorismebestrijding: bescherming van kritieke infrastructuur"[5] aangenomen, waarin 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.

(2) Op 17 november 2005 hechtte de Commissie haar goedkeuring aan een Groenboek betreffende een Europees programma voor de bescherming van kritieke infrastructuur[6], waarin beleidsopties voor het opzetten van het programma en van het netwerk voor waarschuwing en informatie inzake kritieke infrastructuur (CIWIN) zijn opgenomen. Uit de op het Groenboek ontvangen reacties blijkt duidelijk dat het noodzakelijk is dat een gemeenschappelijk kader voor de bescherming van kritieke

---

1 PB C […] van […], blz. […].
2 PB C […] van […], blz. […].
3 PB C […] van […], blz. […].
4 Document 10679/2/04, rev 2, van de Raad.
5 COM(2004) 702.
6 COM(2005) 576.

infrastructuur wordt opgezet. Er werd erkend dat het nodig is de capaciteit voor de bescherming van kritieke infrastructuur in Europa op te voeren en deze infrastructuur minder kwetsbaar te maken. De nadruk werd gelegd op het belang van het subsidiariteitsbeginsel en van overleg met de belanghebbende partijen.

(3) In december 2005 heeft de Raad Justitie en Binnenlandse Zaken de Commissie verzocht een voorstel voor een Europees programma voor de bescherming van kritieke infrastructuur (EPCIP) in te dienen en besloten dat dit gebaseerd moet zijn op een alle risico's omvattende aanpak, waarbij de bestrijding van terroristische dreigingen als prioriteit zou gelden. Bij een dergelijke aanpak dient in het proces ter bescherming van kritieke infrastructuur rekening te worden gehouden met van de mens uitgaande, technologische dreigingen en natuurrampen, maar dient voorrang te worden gegeven aan terroristische dreigingen. Indien het niveau van de beschermingsmaatregelen tegen een bijzonder grote dreiging in een bepaalde sector met kritieke infrastructuur toereikend wordt geacht, moeten de betrokken partijen zich concentreren op andere dreigingen waarvoor zij nog gevoelig zijn.

(4) De hoofdverantwoordelijkheid voor de bescherming van kritieke infrastructuur ligt momenteel bij de lidstaten en de eigenaren/exploitanten van dergelijke infrastructuur. Dat dient zo te blijven.

(5) Er zijn een aantal kritieke infrastructuurvoorzieningen in de Gemeenschap waarvan de ontwrichting of vernietiging invloed zou kunnen hebben in twee of meer lidstaten of in een andere lidstaat dan die waarin de kritieke infrastructuur zich bevindt. Het kan daarbij met name gaan om grensoverschrijdende, sectoroverstijgende effecten die het gevolg zijn van interdependenties tussen onderling gekoppelde infrastructuurvoorzieningen. Om dergelijke Europese kritieke infrastructuur in kaart te brengen en om infrastructuur als Europese kritieke infrastructuur aan te merken, dient gebruik te worden gemaakt van een gemeenschappelijke procedure. De vraag of het nodig is de bescherming van dergelijke kritieke infrastructuur te verbeteren, moet op grond van een gemeenschappelijke regeling worden beoordeeld. Bilaterale programma's voor samenwerking tussen de lidstaten op het gebied van de bescherming van kritieke infrastructuur hebben hun nut en doeltreffendheid bewezen in geval van grensoverschrijdende kritieke infrastructuur. Het Europees programma voor de bescherming van kritieke infrastructuur moet op een dergelijke samenwerking worden gebaseerd.

(6) Aangezien de verschillende sectoren beschikken over specifieke ervaring en deskundigheid op het gebied van de bescherming van kritieke infrastructuur en specifieke behoeften op dat gebied hebben, moet een communautaire aanpak van de bescherming van kritieke infrastructuur worden ontwikkeld en ten uitvoer gelegd met inachtneming van de specifieke kenmerken van elke sector en van de in elke sector bestaande maatregelen, waaronder die welke reeds op EU-niveau en op nationaal en regionaal niveau bestaan, alsmede eventueel reeds bestaande grensoverschrijdende overeenkomsten inzake wederzijdse bijstandsverlening tussen eigenaren/exploitanten van kritieke infrastructuur. Gezien de zeer grote betrokkenheid van de particuliere sector bij het risicotoezicht, het risicobeheer, de bedrijfscontinuïteitsplanning en het herstel na rampen moet een communautaire aanpak de volledige betrokkenheid van de particuliere sector aanmoedigen. Om deze sectorale aanpak van de bescherming van kritieke infrastructuur te vergemakkelijken, dient een gemeenschappelijke lijst van sectoren met kritieke infrastructuur te worden opgesteld.

(7) Elke eigenaar/exploitant van Europese kritieke infrastructuur dient een beveiligingsplan op te stellen, waarin de kritieke infrastructuur wordt geïnventariseerd en waarin passende beveiligingsmaatregelen voor de bescherming ervan worden aangereikt. In het beveiligingsplan van de exploitant moet rekening worden gehouden met de kwetsbaarheids-, dreigings- en risicoanalyses alsmede met andere, door de autoriteiten van de lidstaat verstrekte relevante informatie.

(8) Elke eigenaar/exploitant van Europese kritieke infrastructuur dient een veiligheidsverbindingsfunctionaris aan te wijzen teneinde de samenwerking en de communicatie met de nationale autoriteiten voor de bescherming van kritieke infrastructuur te vergemakkelijken.

(9) Teneinde risico's, dreigingen en kwetsbaarheden in specifieke sectoren te inventariseren, is communicatie zowel tussen de eigenaren/exploitanten van Europese kritieke infrastructuur en de lidstaten als tussen de lidstaten en de Commissie nodig. Elke lidstaat dient informatie te verzamelen over Europese kritieke infrastructuur die zich op zijn grondgebied bevindt. De Commissie dient van de lidstaten algemene informatie over kwetsbaarheden, dreigingen en risico's te ontvangen, waaronder eventueel relevante informatie over mogelijke leemten en sectoroverstijgende afhankelijkheden. Waar nodig, moet deze informatie de basis moeten vormen voor de uitwerking van specifieke voorstellen over de verbetering van de bescherming van Europese kritieke infrastructuur.

(10) Teneinde het gemakkelijker te maken de bescherming van Europese kritieke infrastructuur te verbeteren, dienen gemeenschappelijke methoden voor de inventarisatie en classificatie van met betrekking tot infrastructuurvoorzieningen bestaande kwetsbaarheden, dreigingen en risico's te worden uitgewerkt.

(11) Alleen een gemeenschappelijk kader kan de vereiste basis voor een coherente uitvoering van maatregelen ter bescherming van Europese kritieke infrastructuur en een duidelijke afbakening van de respectieve bevoegdheden van alle belanghebbenden verschaffen. De eigenaren/exploitanten van Europese kritieke infrastructuur dienen toegang te krijgen tot beproefde methoden ter bescherming van kritieke infrastructuur.

(12) Voor een doeltreffende bescherming van kritieke infrastructuur is communicatie, coördinatie en samenwerking op nationaal niveau en op EU-niveau vereist. Deze wordt het best verwezenlijkt door de aanwijzing in elke lidstaat van contactpunten voor aangelegenheden in verband met de bescherming van kritieke infrastructuur, die kwesties die de bescherming van kritieke infrastructuur betreffen zowel intern als met andere lidstaten en de Commissie moeten coördineren.

(13) Teneinde op gebieden die tot een zekere mate van vertrouwelijkheid nopen activiteiten te ontwikkelen die de bescherming van kritieke infrastructuur betreffen, moet in het kader van deze richtlijn voor een coherente en veilige uitwisseling van informatie worden gezorgd. Bepaalde inlichtingen over de bescherming van kritieke infrastructuur zijn van die aard dat openbaarmaking ervan zou leiden tot ondermijning van de bescherming van het openbaar belang waar dit de openbare veiligheid betreft. Bepaalde gegevens over kritieke infrastructuur die zouden kunnen worden gebruikt om plannen te maken en feiten te plegen die onaanvaardbare gevolgen zouden hebben voor deze installaties, dienen als vertrouwelijk te worden behandeld en zowel op het

niveau van de Gemeenschap als van de lidstaten slechts op een "need-to-know"-basis te worden verstrekt.

(14) Informatie over de bescherming van kritieke infrastructuur moet worden uitgewisseld op basis van vertrouwen en vertrouwelijkheid. De uitwisseling van informatie vereist een zodanige vertrouwensrelatie dat ondernemingen en organisaties weten dat hun gevoelige gegevens voldoende beschermd zijn. Teneinde de uitwisseling van informatie aan te moedigen, dient het voor het bedrijfsleven duidelijk te zijn dat de voordelen van de uitwisseling van informatie over kritieke infrastructuur opwegen tegen de kosten ervan voor het bedrijfsleven en de samenleving in het algemeen. De uitwisseling van informatie over de bescherming van kritieke infrastructuur moet derhalve worden aangemoedigd.

(15) Deze richtlijn vult op het niveau van de Gemeenschap en in de lidstaten bestaande sectorspecifieke maatregelen aan. Waar op het niveau van de Gemeenschap reeds mechanismen bestaan, moeten deze verder worden gebruikt en zullen deze tot de volledige uitvoering van deze richtlijn bijdragen.

(16) De voor de uitvoering van deze richtlijn vereiste maatregelen dienen te worden vastgesteld overeenkomstig Besluit 1999/468/EG van de Raad van 28 juni 1999 tot vaststelling van de voorwaarden voor de uitoefening van de aan de Commissie verleende uitvoeringsbevoegdheden[7].

(17) Daar de doelstellingen van deze richtlijn, namelijk de instelling van een procedure voor de inventarisatie van Europese kritieke infrastructuur en voor de aanmerking van infrastructuur als Europese kritieke infrastructuur, alsmede de uitwerking van een gemeenschappelijke aanpak om te beoordelen of het nodig is de bescherming van dergelijke infrastructuur te verbeteren, niet voldoende door de lidstaten kunnen worden verwezenlijkt en derhalve wegens de omvang van het optreden beter door de Gemeenschap kunnen worden verwezenlijkt, kan de Gemeenschap, overeenkomstig het in artikel 5 van het Verdrag neergelegde subsidiariteitsbeginsel, maatregelen nemen. Overeenkomstig het in hetzelfde artikel neergelegde evenredigheidsbeginsel gaat deze richtlijn niet verder dan nodig is om deze doelstellingen te verwezenlijken.

(18) Deze richtlijn eerbiedigt de grondrechten en neemt de beginselen in acht die met name zijn erkend in het Handvest van de grondrechten van de Europese Unie,

HEEFT DE VOLGENDE RICHTLIJN VASTGESTELD:

Artikel 1
Onderwerp

Bij deze richtlijn wordt een procedure ingesteld voor de inventarisatie van Europese kritieke infrastructuur en voor de aanmerking van infrastructuur als Europese kritieke infrastructuur, alsmede een gemeenschappelijke aanpak om te beoordelen of het nodig is de bescherming van dergelijke infrastructuur te verbeteren.

[7] PB L 184 van 17.7.1999, blz. 23.

Artikel 2
Definities

Voor de toepassing van deze richtlijn wordt verstaan onder:

a) "kritieke (ook wel: "vitale") infrastructuur": die infrastructuur of delen daarvan die van essentieel belang zijn voor het behoud van kritieke maatschappelijke functies, waaronder de bevoorradingsketen, de gezondheid, de veiligheid en de beveiliging, de economische welvaart en het maatschappelijk welzijn;

b) "Europese kritieke (ook wel: "vitale") infrastructuur": die kritieke infrastructuur waarvan de verstoring of vernietiging een belangrijke invloed zou hebben in twee of meer lidstaten, of in een enkele lidstaat, indien dit een andere lidstaat is dan die waar de kritieke infrastructuur zich bevindt. Het betreft bijvoorbeeld effecten die het gevolg zijn van sectoroverstijgende afhankelijkheden van andere soorten infrastructuur;

c) "ernst": de impact van de verstoring of vernietiging van een bepaalde infrastructuurvoorziening, rekening houdend met:

- de gevolgen voor het publiek (aantal getroffen personen);
- de economische gevolgen (omvang van het economisch verlies en/of de kwaliteitsvermindering van producten of diensten);
- de gevolgen voor het milieu;
- de politieke gevolgen;
- de psychologische gevolgen;
- de gevolgen voor de volksgezondheid;

d) "kwetsbaarheid": een kenmerk van een onderdeel van het ontwerp, de uitvoering of het functioneren van kritieke infrastructuur dat deze vatbaar maakt voor verstoring of vernietiging door een dreiging, waaronder afhankelijkheid van andere soorten infrastructuur;

e) "dreiging": elke omstandigheid of gebeurtenis die kritieke infrastructuur, of welk onderdeel daarvan ook, kan verstoren of vernietigen, en elke aanwijzing dat dit zou kunnen gebeuren;

f) "risico": de mogelijkheid van verlies, schade of nadeel wat de waarde betreft die door de eigenaar/exploitant aan de infrastructuur wordt toegekend, het gevolg van het verlies of de wijziging van de infrastructuur en de waarschijnlijkheid dat een specifieke kwetsbaarheid voor een specifieke dreiging wordt benut;

g) "informatie over de bescherming van kritieke infrastructuur": bepaalde gegevens over kritieke infrastructuur die, wanneer zij openbaar worden gemaakt, zouden kunnen worden gebruikt om plannen te maken en feiten te plegen die het

functioneren van kritieke-infrastructuurinstallaties verstoren of onaanvaardbare gevolgen hebben voor deze installaties.

Artikel 3
Inventarisatie van Europese kritieke infrastructuur

1. De voor de inventarisatie van Europese kritieke infrastructuur te gebruiken sectoroverstijgende en sectorspecifieke criteria worden vastgesteld overeenkomstig de in artikel 11, lid 3, bedoelde procedure. Zij kunnen worden gewijzigd overeenkomstig de in artikel 11, lid 3, bedoelde procedure.

   De sectoroverstijgende criteria die horizontaal van toepassing zijn op alle sectoren met kritieke infrastructuur worden uitgewerkt met inachtneming van de ernst van het effect van de verstoring of vernietiging van een bepaalde infrastructuurvoorziening. Zij worden uiterlijk [*een jaar na de inwerkingtreding van deze richtlijn*] vastgesteld.

   De sectorspecifieke criteria worden voor prioritaire sectoren uitgewerkt met inachtneming van de kenmerken van de afzonderlijke sectoren met kritieke infrastructuur en, waar nodig, worden de relevante belanghebbende partijen daarbij betrokken. Deze criteria worden voor elke prioritaire sector uiterlijk één jaar na de aanmerking ervan als prioritaire sector vastgesteld.

2. Jaarlijks kiest de Commissie de in bijlage I vermelde prioritaire sectoren waarvoor de in lid 1 bedoelde criteria moeten worden uitgewerkt.

   Bijlage I kan overeenkomstig de in artikel 11, lid 3, bedoelde procedure worden gewijzigd voor zover het toepassingsgebied van deze richtlijn daardoor niet wordt uitgebreid.

3. Elke lidstaat stelt een inventaris op van de kritieke infrastructuur die zich op zijn grondgebied bevindt en van de kritieke infrastructuur buiten zijn grondgebied die invloed kan hebben op zijn grondgebied en die voldoet aan de overeenkomstig de leden 1 en 2 vastgestelde criteria.

   Elke lidstaat stelt de Commissie uiterlijk één jaar na de vaststelling van de relevante criteria en vervolgens doorlopend in kennis van de kritieke infrastructuur die aldus is geïnventariseerd.

Artikel 4
Aanmerking als Europese kritieke infrastructuur

1. Op grond van de overeenkomstig artikel 3, lid 3, tweede alinea, gedane kennisgevingen en van andere informatie waarover zij beschikt, stelt de Commissie een lijst voor van als Europese kritieke infrastructuur aan te merken kritieke infrastructuur.

2. De lijst van als Europese kritieke infrastructuur aangemerkte kritieke infrastructuur wordt vastgesteld overeenkomstig de in artikel 11, lid 3, bedoelde procedure.

De lijst kan worden gewijzigd overeenkomstig de in artikel 11, lid 3, bedoelde procedure.

Artikel 5
Beveiligingsplannen van de exploitanten

1. Elke lidstaat verlangt van de eigenaren/exploitanten van zich op zijn grondgebied bevindende Europese kritieke infrastructuur dat zij een beveiligingsplan opstellen en dat zij dit ten minste om de twee jaar herzien.

2. In het beveiligingsplan van de exploitant wordt de Europese kritieke infrastructuur geïnventariseerd en worden passende beveiligingsoplossingen voor de bescherming ervan voorgesteld overeenkomstig bijlage II. Sectorspecifieke vereisten voor het beveiligingsplan van de exploitant waarin bestaande communautaire maatregelen in aanmerking worden genomen, kunnen overeenkomstig de in artikel 11, lid 3, bedoelde procedure worden vastgesteld.

   De Commissie kan overeenkomstig de in artikel 11, lid 2, bedoelde procedure beslissen dat aan de voorwaarde dat een beveiligingsplan van de exploitant moet worden opgesteld en herzien, is voldaan wanneer de maatregelen in acht zijn genomen die van toepassing zijn op specifieke sectoren die in bijlage I zijn vermeld.

3. De eigenaar/exploitant van Europese kritieke infrastructuur legt het beveiligingsplan binnen één jaar na de aanmerking van kritieke infrastructuur als Europese kritieke infrastructuur voor aan de bevoegde autoriteit van de lidstaat.

   Wanneer op grond van lid 2 sectorspecifieke vereisten voor het beveiligingsplan van de exploitant worden vastgesteld, wordt het beveiligingsplan van de exploitant pas binnen één jaar na de vaststelling van de sectorspecifieke vereisten aan de bevoegde autoriteit van de lidstaat voorgelegd.

4. Elke lidstaat zet een systeem op dat een adequaat en regelmatig toezicht op de beveiligingsplannen van de exploitanten en op de uitvoering daarvan waarborgt en dat is gebaseerd op de overeenkomstig artikel 7, lid 1, verrichte risico- en dreigingsanalyses.

5. Wanneer Richtlijn 2005/65/EG van het Europees Parlement en de Raad van 26 oktober 2005 betreffende het verhogen van de veiligheid van havens in acht is genomen, is voldaan aan de voorwaarde dat een beveiligingsplan van de exploitant moet worden opgesteld.

Artikel 6
Veiligheidsverbindingsfunctionarissen

1. Elke lidstaat verlangt van de eigenaren/exploitanten van Europese kritieke infrastructuur op zijn grondgebied dat zij een veiligheidsverbindingsfuctionaris aanwijzen als contactpunt voor veiligheidsaangelegenheden tussen de eigenaar/exploitant van de infrastructuur en de voor de bescherming van kritieke infrastructuur bevoegde autoriteiten in de lidstaat. De

veiligheidsverbindingsfunctionaris wordt aangewezen binnen één jaar na de aanmerking van de kritieke infrastructuur als Europese kritieke infrastructuur.

2. Elke lidstaat deelt alle relevante informatie over vastgestelde risico's en dreigingen mee aan de voor de betrokken Europese kritieke infrastructuur bevoegde veiligheidsverbindingsfunctionarissen.

Artikel 7
Verslagen

1. Elke lidstaat verricht binnen één jaar na de aanmerking van kritieke infrastructuur als Europese kritieke infrastructuur een risico- en dreigingsanalyse in verband met zich op zijn grondgebied bevindende Europese kritieke infrastructuur.

2. Elke lidstaat brengt binnen 18 maanden na de vaststelling van de in artikel 4, lid 2, bedoelde lijst en vervolgens om de twee jaar een beknopt verslag uit over de kwetsbaarheden, dreigingen en risico's die zijn vastgesteld in elke in bijlage I genoemde sector.

   Er zal een gemeenschappelijk model voor deze verslagen worden uitgewerkt overeenkomstig de in artikel 11, lid 3, bedoelde procedure.

3. De Commissie beoordeelt per sector of specifieke beschermingsmaatregelen vereist zijn voor Europese kritieke infrastructuur.

4. Er kunnen per sector gemeenschappelijke methoden voor kwetsbaarheids-, dreigings- en risicoanalyses voor Europese kritieke infrastructuur worden vastgesteld overeenkomstig de in artikel 11, lid 3, bedoelde procedure.

Artikel 8
Steun van de Commissie voor Europese kritieke infrastructuur

De Commissie staat de eigenaren/exploitanten van als Europese kritieke infrastructuur aangemerkte infrastructuur bij door toegang te verlenen tot beproefde methoden voor de bescherming van kritieke infrastructuur.

Artikel 9
Contactpunten voor aangelegenheden in verband met de bescherming van kritieke infrastructuur

1. Elke lidstaat wijst een contactpunt voor aangelegenheden in verband met de bescherming van kritieke infrastructuur (CIP-contactpunt) aan.

2. Het contactpunt coördineert aangelegenheden in verband met de bescherming van kritieke infrastructuur binnen de lidstaat, met andere lidstaten en met de Commissie.

Artikel 10
Vertrouwelijkheid en uitwisseling van informatie over de bescherming van kritieke infrastructuur

1. Voor de tenuitvoerlegging van deze richtlijn neemt de Commissie overeenkomstig Besluit 2001/844/EG, EGKS, Euratom, passende maatregelen voor de bescherming van vertrouwelijke informatie die voor haar toegankelijk is of haar door de lidstaten wordt meegedeeld. De lidstaten nemen vergelijkbare maatregelen overeenkomstig de betrokken nationale wetgeving. Hierbij wordt rekening gehouden met de ernst van de aan de wezenlijke belangen van de Gemeenschap of van een of meer van haar lidstaten toegebrachte potentiële schade.

2. Personen die namens een lidstaat vertrouwelijke informatie behandelen uit hoofde van deze richtlijn, moeten een passend veiligheidsniveau hebben dat door de betrokken lidstaat wordt gecontroleerd.

3. De lidstaten zien erop toe dat de aan de lidstaten of aan de Commissie verstrekte informatie over de bescherming van kritieke infrastructuur niet voor enig ander doel dan de bescherming van kritieke infrastructuur wordt gebruikt.

Artikel 11
Comité

1. De Commissie wordt bijgestaan door een comité dat is samengesteld uit een vertegenwoordiger van elk contactpunt voor aangelegenheden in verband met de bescherming van kritieke infrastructuur.

2. Wanneer naar dit lid wordt verwezen, zijn de artikelen 3 en 7 van Besluit 1999/468/EG van toepassing, met inachtneming van artikel 8 van dat besluit.

3. Wanneer naar dit lid wordt verwezen, zijn de artikelen 5 en 7 van Besluit 1999/468/EG van toepassing, met inachtneming van artikel 8 van dat besluit.

   De in artikel 5, lid 6, van Besluit 1999/468/EG bedoelde termijn wordt vastgesteld op één maand.

4. Het comité stelt zijn reglement van orde vast.

Artikel 12
Uitvoering

1. De lidstaten doen de nodige wettelijke en bestuursrechtelijke bepalingen in werking treden om uiterlijk op 31 december 2007 aan deze richtlijn te voldoen. Zij delen de Commissie de tekst van die bepalingen onverwijld mede, alsmede een tabel ter weergave van het verband tussen die bepalingen en deze richtlijn.

   Wanneer de lidstaten die bepalingen aannemen, wordt in de bepalingen zelf of bij de officiële bekendmaking daarvan naar deze richtlijn verwezen. De regels voor die verwijzing worden vastgesteld door de lidstaten.

2. De lidstaten delen de Commissie de tekst van de belangrijkste bepalingen van intern recht mee die zij op het onder deze richtlijn vallende gebied vaststellen.

Artikel 13
Inwerkingtreding

Deze richtlijn treedt in werking op de twintigste dag volgende op die van haar bekendmaking in het *Publicatieblad van de Europese Unie*.

Artikel 14
Adressaten

Deze richtlijn is gericht tot alle lidstaten.

Gedaan te Brussel,

Voor de Raad

BIJLAGE I

LIJST VAN SECTOREN MET KRITIEKE INFRASTRUCTUUR

Sector		Deelsector	
I	Energie	1	Aardolie- en gasproductie, -raffinage, -behandeling, -opslag en -distributie via pijpleidingen
		2	Elektriciteitsproductie en -transmissie
II	Nucleaire industrie	3	Productie en opslag/verwerking van nucleaire stoffen
III	Informatie- en communicatietechnologieën, ICT	4	Bescherming van informatiesystemen en -netwerken
		5	Instrumentatie-, automatiserings- en controlesystemen (SCADA enz.)
		6	Internet
		7	Vaste telecommunicatievoorziening
		8	Mobiele telecommunicatievoorziening
		9	Radiocommunicatie en navigatie
		10	Satellietcommunicatie
		11	Omroep
IV	Water	12	Drinkwatervoorziening
		13	Controle van de waterkwaliteit
		14	Keren en beheren van de waterkwantiteit
V	Voedsel	15	Voedselvoorziening en waarborging van voedselveiligheid en voedselzekerheid
VI	Gezondheid	16	Medische verzorging en ziekenhuisverpleging
		17	Geneesmiddelen, sera, vaccins en farmaceutica
		18	Biolaboratoria en bio-agentia
VII	Financieel	19	Betalingsinfrastructuur en –systemen en infrastructuur en systemen voor de clearing en afwikkeling van effecten
		20	Gereglementeerde markten
VIII.	Transport	21	Wegvervoer
		22	Spoorvervoer
		23	Luchtvervoer
		24	Vervoer over de binnenwateren
		25	Zeevervoer (kustvaart en grote vaart)
IX	Chemische industrie	26	Productie en opslag/verwerking van chemische stoffen
		27	Pijpleidingen voor gevaarlijke stoffen (chemische stoffen)
X	Ruimte	28	Ruimtevaart
XI	Researchfaciliteiten	29	Onderzoeksinstallaties

BIJLAGE II

BEVEILIGINGSPLAN VAN DE EXPLOITANT (OPERATOR SECURITY PLAN - OSP)

In het OSP wordt een overzicht gegeven van de kritieke infrastructuur van de eigenaren en exploitanten en worden passende beveiligingsoplossingen voor de bescherming ervan voorgesteld. Het OSP omvat ten minste:

– een inventaris van belangrijke kritieke infrastructuur;

– een risicoanalyse op basis van de belangrijkste dreigingen, de kwetsbaarheden van elke infrastructuurvoorziening en de potentiële impact;

– de vastgestelde, geselecteerde en als prioritair beschouwde tegenmaatregelen en procedures, waarbij een onderscheid moet worden gemaakt tussen:

- **permanente beveiligingsmaatregelen:** hieronder vallen absoluut noodzakelijke investeringen in beveiliging en middelen die door de eigenaar/exploitant niet op korte termijn kunnen worden opgebracht. Dit onderdeel moet informatie bevatten over algemene maatregelen, technische maatregelen (waaronder de installatie van detectie-, toegangscontrole-, beschermings- en preventieapparatuur), organisatorische maatregelen (waaronder alerterings- en crisisbeheersingsprocedures), controle- en verificatiemaatregelen, communicatie, bewustmaking en opleiding, en beveiliging van informatiesystemen.

- **graduele beveiligingsmaatregelen:** beveiligingsmaatregelen die worden aangepast aan het risico- en dreigingsniveau.

FINANCIEEL MEMORANDUM

Beleidsgebied(en): justitie en binnenlandse zaken

Activiteit: bescherming van kritieke infrastructuur

BENAMING VAN DE ACTIE: Richtlijn van de Raad inzake de inventarisatie van Europese kritieke infrastructuur, de aanmerking van infrastructuur als Europese kritieke infrastructuur en de beoordeling van de noodzaak de bescherming van dergelijke infrastructuur te verbeteren

1. BEGROTINGSONDERDEEL + OMSCHRIJVING

Nvt

2. ALGEMENE CIJFERS

2.1. Totale toewijzing voor de actie (deel B): miljoen € voor vastleggingen

Nvt

2.2. Duur:

Beginjaar 2006

2.3. Meerjarenraming van de uitgaven:

a) Overzicht van de vastleggingskredieten en betalingskredieten (financiering uit de begroting) (*zie punt 6.1.1*)

miljoen euro (*tot drie cijfers na de komma*)

	[2006]	[2007]	[2008]	[2009]	[2010]	[2011]	Totaal
Vastleggingen	-	-	-	-	-	-	-
Betalingen	-	-	-	-	-	-	-

b) Technische en administratieve bijstand en ondersteuningsuitgaven (*zie punt 6.1.2*)

Vastleggingen	-	-	-	-	-	-	-
Betalingen	-	-	-	-	-	-	-

Subtotaal a+b	-	-	-	-	-	-	-
Vastleggingen	-	-	-	-	-	-	-
Betalingen	-	-	-	-	-	-	-

c) Financiële gevolgen van het personeel en andere administratieve uitgaven*(zie punten 7.2 en 7.3)*

Vastleggingen / betalingen	1.280.000	1.280.000	1.280.000	1.280.000	1.280.000	1.280.000	1.280.000

TOTAAL a+b+c	1.280.000	1.280.000	1.280.000	1.280.000	1.280.000	1.280.000	1.280.000
Vastleggingen	1.280.000	1.280.000	1.280.000	1.280.000	1.280.000	1.280.000	1.280.000
Betalingen	1.280.000	1.280.000	1.280.000	1.280.000	1.280.000	1.280.000	1.280.000

2.4. Verenigbaarheid met de financiële programmering en de financiële vooruitzichten

De richtlijn is verenigbaar met het programma "Terrorisme en andere aan veiligheid gerelateerde risico's: preventie, paraatheid en beheersing van de gevolgen" voor de periode 2007-2013.

2.5. Financiële gevolgen voor de ontvangsten:

Het onlangs aangenomen programma "Terrorisme en andere aan veiligheid gerelateerde risico's: preventie, paraatheid en beheersing van de gevolgen" voor de periode 2007-2013 (137,5 miljoen EUR) zal als onderdeel van het algemene programma "Veiligheid en bescherming van de vrijheden", bijdragen aan de tenuitvoerlegging van het EPCIP bij de bescherming tegen veiligheidsrisico's en bij de bescherming van die materiële middelen, diensten en informatietechnologische voorzieningen, netwerken en infrastructuurvoorzieningen waarvan de ontwrichting of vernietiging een belangrijk effect zou hebben op de kritieke maatschappelijke functies. Het toepassingsgebied van het programma is echter beperkt, aangezien het geen betrekking heeft op de investeringen in hardware of software. Dit programma is niet van toepassing op aangelegenheden die onder andere financiële instrumenten, en in het bijzonder onder het instrument voor snelle respons bij ernstige noodsituaties, vallen.

Op het gebied van preventie en paraatheid is het programma erop gericht:

a) de beoordeling van de risico's en dreigingen ten aanzien van kritieke infrastructuur, inclusief evaluaties ter plaatse om dreigingen en kwetsbaarheden in kaart te brengen en na te gaan of er behoefte is aan verbetering van de beveiliging ervan, aan te moedigen, te bevorderen en te ondersteunen;

b) gemeenschappelijke operationele maatregelen te bevorderen en te ondersteunen met het oog op een betere continuïteit van grensoverschrijdende bevoorradingsketens, mits geen afbreuk wordt gedaan aan de mededingingsregels op de interne markt;

c) de ontwikkeling van minimumveiligheidsnormen, de uitwisseling van beproefde methoden, instrumenten voor de risicobeoordeling, methoden om infrastructuur in verschillende sectoren te vergelijken en vast te stellen welke

ervan prioritair is, de analyse van kwetsbaarheden en interdependenties bij de bescherming van kritieke infrastructuur te bevorderen en te ondersteunen;

d) de coördinatie en de samenwerking op het gebied van de bescherming van kritieke infrastructuur op het niveau van de Gemeenschap te bevorderen en te ondersteunen, en eventueel voorstellen voor minimumbeschermingsmaatregelen en gemeenschappelijke richtsnoeren uit te werken.

Op het gebied van de gevolgenbeheersing is het programma erop gericht:

a) de uitwisseling van knowhow, ervaring en technologie aan te moedigen, te bevorderen en te ondersteunen;

b) de ontwikkeling van een passende methodiek en passende rampenplannen aan te moedigen, te bevorderen en te ondersteunen;

c) te zorgen voor een real-time input van specifieke kennis inzake beveiliging in het kader van de algemene crisisbeheersing en de mechanismen voor snelle waarschuwing en civiele bescherming.

Het voorstel heeft geen financiële gevolgen voor de ontvangsten.

3. BEGROTINGSKENMERKEN

Soort uitgave		**Nieuw**	**Bijdrage EVA**	**Bijdragen kandidaat-lidstaten**	**Rubriek financiële vooruitzich-ten**
NVU	NGK	Nvt	Nvt	Nvt	**Neen** Nvt

4. RECHTSGRONDSLAG

De rechtsgrondslag voor het voorstel is artikel 308 van het Verdrag tot oprichting van de Europese Gemeenschap.

5. OMSCHRIJVING EN MOTIVERING

5.1. Doel van het communautaire optreden

5.1.1. Nagestreefde doelstellingen

Een richtlijn is het meest geschikte instrument om het gemeenschappelijke EPCIP-kader tot stand te brengen, aangezien de lidstaten de bescherming van kritieke infrastructuur op uiteenlopende wijzen aanpakken en ook hun rechtsstelsels verschillend zijn. Door de formulering van een aantal belangrijke ideeën en door het de lidstaten mogelijk te maken gebruik te maken van de methoden die het best voldoen aan hun behoeften, kunnen de doelstellingen van het EPCIP volledig worden gerealiseerd door voort te bouwen op wat reeds is verwezenlijkt.

5.1.2. Maatregelen die in verband met de evaluatie vooraf zijn getroffen

Alle belanghebbende partijen zijn geraadpleegd over de uitwerking van het EPCIP. Dit is gebeurd door middel van:

- het groenboek betreffende een EPCIP, dat op 17 november 2005 werd goedgekeurd en waarvoor de raadplegingstermijn op 15 januari 2006 verstreek. 22 lidstaten hebben officieel op de raadpleging gereageerd. Ongeveer 100 vertegenwoordigers van de particuliere sector hebben eveneens opmerkingen gemaakt bij het groenboek. In het algemeen werd positief gereageerd op de idee om een EPCIP uit te werken;

- drie seminars over de bescherming van kritieke infrastructuur onder auspiciën van de Commissie (in juni 2005, september 2005 en maart 2006). Op elk van deze drie seminars kwamen vertegenwoordigers van de lidstaten bijeen. De particuliere sector werd uitgenodigd op de seminars die in september 2005 en maart 2006 werden gehouden;

- informele bijeenkomsten van contactpunten voor aangelegenheden in verband met de bescherming van kritieke infrastructuur (CIP-contactpunten). Er werden door de Commissie twee bijeenkomsten van de CIP-contactpunten van de lidstaten belegd (december 2005 en februari 2006);

- informele bijeenkomsten met vertegenwoordigers van de particuliere sector. Er werden talrijke informele bijeenkomsten met vertegenwoordigers van bepaalde particuliere ondernemingen en met bedrijfsorganisaties gehouden;

- intern, binnen de Commissie, werden de werkzaamheden ter ontwikkeling van het EPCIP voortgezet tijdens regelmatig gehouden bijeenkomsten van de subgroep inzake de bescherming van kritieke infrastructuur en de interdienstengroep inzake de interne aspecten van terrorisme.

5.2. Voorgenomen actie en wijze van financiering uit de begroting

De gevolgen voor de begroting worden geraamd in het begeleidende financieel memorandum.

5.3. Uitvoering

Aangezien het om een richtlijn gaat, is geen methode tot uitvoering van de begroting nodig.

6. FINANCIËLE GEVOLGEN

6.1. Totale financiële gevolgen voor deel B — (voor de hele programmeringsperiode)

6.1.1. Financiering

Nvt

6.1.2. Technische en administratieve bijstand, ondersteuningsuitgaven en IT-uitgaven (vastleggingskredieten)

Nvt

6.2. Berekening van de kosten per overwogen maatregel in deel B (voor de gehele programmeringsperiode)

Nvt

7. GEVOLGEN VOOR HET PERSONEELSBESTAND EN DE ADMINISTRATIEVE UITGAVEN

7.1. Gevolgen voor de personele middelen

Soort post		Personeel voor het beheer van de actie		Totaal	Omschrijving van de taken die uit de actie voortvloeien
		Vast	Tijdelijk		
Ambtenaren of tijdelijk personeel	A B C	8 A 1 B	1 C	10	Verzameling en verwerking van gegevens, voorbereiding van de bijeenkomsten van het comité
Ander personeel					
Totaal		9	1	10	

De behoeften aan personele en administratieve middelen zullen worden gefinancierd uit de toewijzing die het beherende DG in het kader van de jaarlijkse toewijzingsprocedure ontvangt.

7.2. Financiële gevolgen in verband met de personele middelen

Soort personeel	Bedrag in euro	Wijze van berekening *
Ambtenaren Tijdelijk personeel	1.080.000 48.000	(108.000x10=1.080.000 4.000 x 12 = 48.000
Ander personeel (vermeld begrotingsonderdeel)		
Totaal	1.128.000	

De bedragen stemmen overeen met de totale uitgaven gedurende twaalf maanden.

7.3. Andere huishoudelijke uitgaven die uit de actie voortvloeien

Begrotingsonderdeel (nummer en omschrijving)	Bedrag in euro	Wijze van berekening
Totale toewijzing (Titel A7)		
A0701 – Dienstreizen	24.000	2000x12 maanden=24.000
A07030 – Vergaderingen	-	-
A07031 – Comités die moeten worden geraadpleegd	128.000	32.000 x 4 vergaderingen per jaar=128.000
A07032 – Comités die niet hoeven te worden geraadpleegd	-	-
A07040 – Conferenties	-	-
A0705 – Studies en adviezen		-
Overige uitgaven (specificeer)		
Informatiesystemen (A-5001/A-4300)	-	-
Overige uitgaven - Deel A (specificeren)		
Totaal	152.000	

De bedragen stemmen overeen met de totale uitgaven gedurende twaalf maanden.

Vermeld het soort comité en de groep waartoe het behoort.

I.	Jaartotaal (7.2 + 7.3)	1.280.000
II.	II. Duur van de actie	Aan de gang
III.	Totale kosten van de actie (I × II)	

8. FOLLOW-UP EN EVALUATIE

8.1. Follow-upsysteem

Nvt

8.2. Procedure en tijdschema van de voorgeschreven evaluatie

Nvt

9. FRAUDEBESTRIJDINGSMAATREGELEN

Nvt