COMMISSIE VAN DE EUROPESE GEMEENSCHAPPEN

Brussel, 20.10.2004
COM(2004) 702 definitief

MEDEDELING VAN DE COMMISSIE AAN DE RAAD EN HET EUROPEES PARLEMENT

Terrorismebestrijding: bescherming van kritieke infrastructuur

INHOUD

1. INLEIDING 3

2. DE DREIGING 3

3. DE KRITIEKE INFRASTRUCTUUR IN EUROPA 4

3.1. Wat is kritieke infrastructuur? 4

3.2. Veiligheidsmanagement 6

4. VOORUITGANG DIE TOT OP HEDEN OP HET NIVEAU VAN DE GEMEENSCHAP BIJ DE BEVEILIGING VAN KRITIEKE INFRASTRUCTUREN IS GEBOEKT 7

5. VERSTERKING VAN DE CAPACITEIT VOOR DE BESCHERMING VAN DE KRITIEKE INFRASTRUCTUUR IN DE EU 8

5.1. Een Europees programma voor de bescherming van de kritieke infrastructuur 8

5.2. Uitvoering van het EPCIP 9

5.3. Doelstellingen van het EPCIP en voortgangsindicatoren 10

TECHNISCHE BIJLAGE 12

1. INLEIDING

De Europese Raad van juni 2004 verzocht de Commissie en de Hoge Vertegenwoordiger een algemene strategie voor de bescherming van kritieke infrastructuur uit te stippelen.

In deze mededeling wordt een overzicht gegeven van de maatregelen die momenteel door de Commissie inzake de bescherming van kritieke infrastructuur worden genomen en worden aanvullende maatregelen voorgesteld om de bestaande instrumenten te versterken en de door de Europese Raad gegeven opdrachten te volbrengen.

2. DE DREIGING

Het risico dat catastrofale terroristische aanslagen worden gepleegd waardoor kritieke infrastructuur wordt beschadigd, neemt toe. De gevolgen van een aanval op de industriële besturingssystemen van kritieke infrastructuur kunnen zeer uiteenlopend zijn. Algemeen wordt aangenomen dat bij een geslaagde cyberaanval weinig of zelfs geen slachtoffers zouden vallen, maar dat vitale infrastructurele diensten zouden uitvallen. Door een geslaagde cyberaanval op het openbare telefoonnet zou de cliënten bijvoorbeeld de mogelijkheid worden ontnomen om te telefoneren terwijl technici het netwerk herstellen. Een aanval op het besturingssysteem van een chemische installatie of van een aardgasinstallatie zou tot een groter verlies aan mensenlevens en tot aanzienlijke materiële schade kunnen leiden.

Een ander soort catastrofale storing waardoor de infrastructuur uitvalt, kan zich voordoen wanneer een verstoring van een deel van de infrastructuur naar andere delen overslaat en een grootschalig domino-effect veroorzaakt. Een dergelijke storing zou het gevolg kunnen zijn van de onderlinge verwevenheid van de infrastructuurvoorzieningen. Een eenvoudig voorbeeld hiervan is bijvoorbeeld een aanval op een stroomvoorzieningsinstallatie, waardoor de stroomvoorziening uitvalt; als gevolg daarvan zouden ook waterzuiveringsinstallaties en watervoorzieningsbedrijven kunnen uitvallen, omdat de turbines en andere elektrische systemen zouden stilvallen.

Ook domino-effecten kunnen tot enorme schade leiden, omdat zij belangrijke onderbrekingen van de nutsvoorzieningen veroorzaken. Door de stroomonderbrekingen in Noord-Amerika en Europa de voorbije twee jaar is duidelijk geworden hoe kwetsbaar de infrastructuur voor de energievoorziening is en hoe noodzakelijk het bijgevolg is dat doeltreffende oplossingen worden gevonden om de gevolgen van belangrijke onderbrekingen in de energievoorziening te voorkomen of te beperken. Dit soort cyberterrorisme zou ook een aanzienlijke materiële schade tot gevolg kunnen hebben. Als voorbeeld daarvan kan een conventionele bomaanval op een gebouw worden gegeven, die zou gepaard gaan met een tijdelijk uitvallen van de stroomvoorziening of het telefoonnet. Aangezien de noodhulp hierdoor zou worden bemoeilijkt tot noodsystemen voor de stroomvoorziening en de communicatie gebruiksklaar zijn en kunnen worden opgestart, zou dit kunnen leiden tot een verhoging van het aantal slachtoffers en paniek onder de bevolking.

3. DE KRITIEKE INFRASTRUCTUUR IN EUROPA

3.1. Wat is kritieke infrastructuur?

Met kritieke infrastructuur worden materiële en informatietechnologische voorzieningen, netwerken, diensten en activa bedoeld waarvan de verstoring of vernietiging ernstige gevolgen zou hebben voor de gezondheid, de veiligheid, de bescherming of het economische welzijn van de burgers alsmede voor het doeltreffend functioneren van de regeringen in de lidstaten. Kritieke infrastructuur is te vinden in talrijke economische sectoren, met name het bank- en financiewezen, de transport- en distributiesector, de energiesector, de nutsvoorzieningen, de gezondheidssector, de voedselvoorziening en de communicatiesector, alsmede bij belangrijke overheidsdiensten. Bij een aantal kritieke elementen in deze sectoren gaat het strikt genomen niet om "infrastructuur", maar eigenlijk om netwerken of aanvoerketens voor de continue levering van een belangrijke producten of essentiële dienstverlening. Voor de bevoorrading van onze dichtstbevolkte gebieden met levensmiddelen of water zijn bijvoorbeeld niet alleen een aantal belangrijke voorzieningen nodig, maar is ook een complex netwerk van producenten, be- en verwerkingsbedrijven, fabrikanten, distributeurs en detailhandelaars vereist.

Kritieke infrastructuren zijn:

- energievoorzieningsinstallaties en –netwerken (bijvoorbeeld voor de productie van elektriciteit, olie en gas, opslaginstallaties en raffinaderijen, systemen voor het transport en de distributie van energie)

- communicatie- en informatietechnologie (bijvoorbeeld telecommunicatiesystemen, omroepsystemen, software, hardware en netwerken zoals internet)

- het financiewezen (bijvoorbeeld de bank-, effecten- en investeringssector)

- de gezondheidszorg (bijvoorbeeld ziekenhuizen, instellingen voor gezondheidszorg en bloedbanken, laboratoria en de geneesmiddelensector, opsporings- en reddingsdiensten, hulpdiensten)

- de levensmiddelensector (bijvoorbeeld veiligheid, productiemiddelen, groothandel en levensmiddelenindustrie)

- de watervoorziening (bijvoorbeeld stuwdammen, spaarbekkens, zuiveringsinstallaties en netwerken)

- de transportsector (bijvoorbeeld luchthavens, havens, intermodale vervoerssystemen, spoorwegnetwerken en openbare vervoersnetwerken, verkeersleidingssystemen)

- de productie, opslag en het vervoer van gevaarlijke goederen (bijvoorbeeld chemisch, biologisch, radiologisch en nucleair materiaal)

- het overheidsapparaat (bijvoorbeeld essentiële diensten, installaties, informatienetwerken, activa en belangrijke nationale sites en monumenten).

Deze infrastructuren zijn eigendom van of worden geëxploiteerd door de openbare en de particuliere sector. In haar mededeling 574/2001 van 10 oktober 2001 verklaarde de

Commissie: "Worden sommige van deze veiligheidsmaatregelen, naar aanleiding van tegen de samenleving in haar geheel gerichte aanslagen, door de overheid en dus niet door de betrokkenen in de luchtvaartindustrie aangescherpt, dan moeten, volgens de Commissie, de kosten hiervan door die overheid zelf gedragen worden". De openbare sector speelt bijgevolg een belangrijke rol.

Er moet op het niveau van de lidstaten en op Europees niveau worden bepaald wat kritieke infrastructuren zijn en tegen het einde van 2005 zouden lijsten van dergelijke infrastructuren moeten worden opgesteld.

De kritieke infrastructuren in Europa zijn nauw met elkaar verweven en in belangrijke mate van elkaar afhankelijk. Dat is met name het gevolg van het samengaan van ondernemingen, de rationalisatie van de industrie, doeltreffender handelspraktijken zoals bijvoorbeeld "just-in-time"-productie en de concentratie van de bevolking in stedelijke gebieden. De kritieke infrastructuren in Europa zijn afhankelijker geworden van gemeenschappelijke informatietechnologieën zoals internet en satellietradionavigatie- en communicatiesystemen. Omdat deze infrastructuren onderling van elkaar afhankelijk zijn, kunnen problemen een kettingreactie veroorzaken en onverwachte en steeds ernstigere stoornissen van essentiële diensten tot gevolg hebben. Door hun verwevenheid en hun onderlinge afhankelijkheid zijn deze infrastructuursystemen kwetsbaarder en kunnen zij gemakkelijker worden verstoord of vernietigd.

De criteria voor de vaststelling van de factoren op grond waarvan infrastructuren of een onderdeel daarvan als kritiek worden beschouwd, moeten worden onderzocht. Deze selectiecriteria zouden ook op sectorspecifieke deskundigheid en de collectieve expertise van deskundigen moeten zijn gebaseerd. Om vast te stellen welke infrastructuur als potentieel kritieke infrastructuur kan worden beschouwd, kan gebruik worden gemaakt van drie factoren:

- Het bereik – het wegvallen van een kritiek infrastructuurelement wordt beoordeeld op grond van de omvang van het geografische gebied dat door het uitvallen of de onbeschikbaarheid van infrastructuur wordt getroffen – op internationaal, nationaal, provinciaal/territoriaal of lokaal niveau.

- De omvang – de gevolgen of het uitvallen van infrastructuur kunnen worden ingeschat als gelijk aan nul, minimaal, bescheiden of belangrijk. Ter beoordeling van de potentiële omvang zou gebruik kunnen worden gemaakt van de volgende criteria:

    (a) gevolgen voor het publiek (aantal getroffen personen, aantal dodelijke slachtoffers, ziekten, zware letsels, evacuatie);

    (b) economische gevolgen (gevolgen voor het BBP, omvang van het economisch verlies en/of daling van de kwaliteit van producten of diensten);

    (c) gevolgen voor het milieu (impact op het publiek en de omgeving);

    (d) onderlinge afhankelijkheid (van andere kritieke infrastructuurelementen);

    (e) politieke gevolgen (vertrouwen in de bekwaamheid van de overheid).

- Gevolgen in de tijd – op grond van dit criterium wordt vastgesteld op welk ogenblik het uitvallen van een infrastructuurelement ernstige gevolgen kan hebben (bv. onmiddellijk, binnen 24-48 uur, na een week, op een ander ogenblik).

In vele gevallen echter kunnen psychologische factoren ertoe bijdragen dat minder belangrijke gebeurtenissen worden gedramatiseerd.

In technische bijlage worden de ontwikkelingen op het gebied van de bescherming van kritieke infrastructuur geschetst en wordt een overzicht per sector gegeven van de verwezenlijkingen van de Commissie tot op heden, waaruit blijkt dat zij een ruime ervaring op dit gebied heeft opgedaan.

3.2. Veiligheidsmanagement

Om de dreiging, de incidenten en de kwetsbaarheid van de kritieke infrastructuren van de lidstaten en hun onderlinge afhankelijkheid te kunnen beoordelen, is informatie uit verschillende bronnen vereist. Alle sectoren en lidstaten dienen binnen hun bevoegdheidsgebied volgens een op EU-niveau geharmoniseerde formule en de organisaties of personen die verantwoordelijk zijn voor de veiligheid zij als kritiek beschouwen.

Niet alle infrastructuren kunnen tegen alle dreigingen worden beschermd. Stroomvoorzieningsnetwerken bijvoorbeeld zijn te omvangrijk om te worden omheind of bewaakt. De toepassing van risicomanagementtechnieken maakt het mogelijk de aandacht te toe te spitsen op de gebieden waar het risico het grootst is, rekening houdend met de dreiging, de mate waarin infrastructuur als kritieke infrastructuur wordt beschouwd, het bestaande beschermingsniveau en de doeltreffendheid van de beschikbare strategieën om de gevolgen op te vangen en de continuïteit van de bedrijvigheid te garanderen.

Veiligheidsmanagement is een weloverwogen proces dat ten doel heeft inzicht te verkrijgen in de risico's en in de loop waarvan wordt besloten welke maatregelen zullen worden genomen en ten uitvoer gelegd om het risico tegen een aanvaardbare prijs tot een bepaald niveau te reduceren. Het doel van deze benadering is de risico's te onderkennen, in te schatten en tot een bepaald niveau te beperken.

Voor de beveiliging van kritieke infrastructuur (CIP - critical infrastructure protection) is een coherent, op samenwerking gebaseerd partnerschap tussen de eigenaars en exploitanten van kritieke infrastructuur en de autoriteiten van de lidstaten vereist. De verantwoordelijkheid voor het risicomanagement in de installaties, de bevoorradingsketens, de informatietechnologie- en communicatienetwerken berust in de eerste plaats bij de eigenaars en exploitanten.

Waarschuwingen, adviezen en informatie moeten belanghebbenden uit de openbare en de particuliere sector helpen bij de beveiliging van belangrijke infrastructuursystemen. Af en toe kan er sprake zijn van specifieke gevaren of dreigende terroristische aanslagen waarop een onmiddellijke reactie vereist is. In dat geval dienen de regeringen van de lidstaten en het bedrijfsleven gecoördineerd en doelgericht te reageren. In dergelijke omstandigheden zou de EU de vereiste politieke reacties moeten coördineren en op grond daarvan zullen per geval ondersteunende maatregelen met de belanghebbenden worden overeengekomen.

Zelfs de beste programma's inzake veiligheidsmanagement en de beste wetgeving inzake verplichte toepassing van deze programma's zijn waardeloos wanneer zij niet ten uitvoer worden gelegd. De ervaring leert dat onafhankelijke inspecties van de Commissie om op de uitvoering ervan toe te zien, het enige doeltreffende instrument zijn om te waarborgen dat de veiligheidsvoorschriften correct ten uitvoer worden gelegd.

4. VOORUITGANG DIE TOT OP HEDEN OP HET NIVEAU VAN DE GEMEENSCHAP BIJ DE BEVEILIGING VAN KRITIEKE INFRASTRUCTUREN IS GEBOEKT

De Europese burgers verwachten dat kritieke infrastructuren blijven functioneren, ongeacht de organisaties die eigenaar van de verschillende componenten ervan zijn of die deze exploiteren. Zij rekenen erop dat in de eerste plaats de regeringen van de lidstaten en de EU ervoor zorgen dat dit ook het geval is. Zij verwachten dat de eigenaars en exploitanten op alle niveaus van de openbare en de particuliere sector samenwerken om de continuïteit te waarborgen van de dienstverlening waarvan de Europese burgers afhankelijk zijn.

Ter aanvulling van de maatregelen op nationaal niveau heeft de Europese Unie in het kader van haar beleid op verschillende gebieden, reeds een aantal wetgevingsmaatregelen genomen tot vaststelling van minimumnormen voor de beveiliging van infrastructuur. Dat geldt met name voor de sectoren transport, communicatie, energie, veiligheid en gezondheid op het werk, en volksgezondheid. Na de recente aanslagen in Amerika en Europa zijn de activiteiten opgevoerd, hetgeen tot een verdere verbetering of uitbreiding van de bestaande maatregelen zal leiden.

Decennialang zijn in het kader van het Euratom-Verdrag inspecties verricht om te controleren of kernmateriaal correct werd gebruikt. In verband met stralingsbescherming bestaat er een omvangrijke wetgeving betreffende de risico's die verbonden zijn aan de exploitatie van nucleaire installaties en het gebruik van radioactieve stoffen als energiebron.

Op het gebied van het internationale transport heeft de Europese Unie wetgeving aangenomen ter uitvoering of bevestiging van overeenkomsten die door internationale regelgevingsorganen in de luchtvaartsector en de maritieme sector werden gesloten. De Europese Unie zal de werkzaamheden van deze organen op internationaal niveau blijven bevorderen en er actief aan deelnemen. Zij zal derde landen die economische betrekkingen met de EU hebben, ertoe aanmoedigen deze overeenkomsten ten uitvoer te leggen. Zij heeft enige van deze landen bijstand verleend teneinde binnen en buiten de grenzen van de EU een homogeen en constant veiligheidsniveau tot stand te brengen.

Een verdere stap vormt de oprichting van organen ter beveiliging van de communicatie zoals het Europees Agentschap voor netwerk- en informatiebeveiliging (ENISA). Daarnaast zijn in sectoren zoals de veiligheid van de luchtvaart en de zeevaart, binnen de Commissie inspectiediensten in het leven geroepen die erop moeten toezien dat de veiligheidswetgeving door de lidstaten wordt uitgevoerd. Dankzij deze inspecties kunnen de nodige vergelijkingsmaatstaven worden vastgesteld om in de Unie een uniform niveau van uitvoering van de wetgeving te waarborgen.

In technische bijlage worden de ontwikkelingen op het gebied van de bescherming van kritieke infrastructuur geschetst en wordt een overzicht per sector gegeven van de

verwezenlijkingen van de Commissie tot op heden, waaruit blijkt dat zij op dit gebied een ruime ervaring heeft opgedaan.

5. VERSTERKING VAN DE CAPACITEIT VOOR DE BESCHERMING VAN DE KRITIEKE INFRASTRUCTUUR IN DE EU

5.1. Een Europees programma voor de bescherming van de kritieke infrastructuur

Gezien het grote aantal potentiële kritieke infrastructuren, die ieder hun eigen kenmerken hebben, is het onmogelijk deze alle door maatregelen op Europees niveau te beschermen. Als gevolg van de toepassing van het subsidiariteitsbeginsel moet Europa zijn inspanningen vooral concentreren op de bescherming van grensoverschrijdende infrastructuren en andere infrastructuren aan de uitsluitende verantwoordelijkheid van de lidstaten overlaten, zij het binnen een gemeenschappelijk kader.

Er zijn reeds talrijke richtlijnen en verordeningen voorhanden overeenkomstig welke instrumenten voor het opsporen van incidenten vereist zijn, interventieplannen moeten worden opgesteld in samenwerking met de civiele bescherming, geregeld oefeningen moeten worden gehouden en duidelijke banden moeten bestaan tussen de verschillende interventieniveaus, de overheidsdiensten, de centrale organisaties en de hulpdiensten. Anderzijds is op het gebied van de bescherming van andere dan kerninstallaties nog een belangrijke inspanning vereist. Zoals blijkt uit technische bijlage, is het ontwikkelingsniveau van de regelgeving van het communautair acquis op het gebied van de bescherming van kritieke infrastructuren zeer ongelijk.

Op de meeste van bovengenoemde gebieden worden de werkzaamheden voortgezet en wordt samengewerkt met de deskundigen van de lidstaten en de betrokken economische sectoren om mogelijke tekortkomingen op te sporen en vast te stellen welke corrigerende (wettelijke of andere) maatregelen moeten worden genomen. Er zijn talrijke netwerken opgezet en vele veiligheidscomités opgericht.

De Commissie zal de andere instellingen elk kalenderjaar in een mededeling op de hoogte brengen van de geboekte vooruitgang. Met het oog op het advies van deze instellingen zal zij voor iedere sector een analyse maken van de ontwikkelingen van de communautaire werkzaamheden op het gebied van de risico-evaluatie, de ontwikkeling van beschermingstechnieken of lopende/overwogen juridische acties. Voorts zal de Commissie in deze mededeling zo nodig updates en horizontale organisatorische maatregelen voorstellen, die moeten worden geharmoniseerd of gecoördineerd dan wel waarvoor samenwerking vereist is. Deze mededeling, waarin alle sectoranalyses en maatregelen zullen worden opgenomen, zal de grondslag vormen voor een Europees programma voor de bescherming van de kritieke infrastructuur (EPCIP - European Programma for Critical Infrastructure Protection).

Een dergelijk programma heeft ten doel het bedrijfsleven en de regeringen van de lidstaten op alle niveaus in de EU bij te staan, zonder dat evenwel wordt geraakt aan individuele bevoegdheden en verantwoordelijkheden. De Commissie is van mening dat een netwerk van deskundigen uit de EU-lidstaten op het gebied van de bescherming van kritieke infrastructuur de Commissie zou kunnen bijstaan bij het opstellen van het programma – dit waarschuwings- en informatienetwerk kritische infrastructuur (CINWIN – Critical Infrastructure Warning Information Network) zou zo snel mogelijk in 2005 moeten worden opgezet.

Met het opzetten van dit netwerk wordt er in hoofdzaak naar gestreefd de uitwisseling van informatie over gemeenschappelijke dreigingen en zwakke punten alsmede over passende maatregelen en strategieën ter beperking van de risico's te stimuleren om de bescherming van kritieke infrastructuur te verbeteren. De lidstaten moeten er zich daarom op hun beurt van vergewissen dat de relevante informatie ter kennis wordt gebracht van alle bevoegde overheidsdiensten en instanties, zoals bijvoorbeeld hulporganisaties, en dat de bevoegde instanties van het bedrijfsleven op de hoogte worden gebracht, zodat zij op hun beurt de getroffen eigenaars en exploitanten van kritieke infrastructuur via een netwerk van contacten in de lidstaten kunnen inlichten.

Het EPCIP zou het mogelijk maken een permanent forum op te zetten, in het kader waarvan de concurrentiedruk, de verantwoordelijkheid, en de gevoeligheid van informatie kunnen worden afgewogen tegen de voordelen die een veiligere kritieke infrastructuur biedt. Het bedrijfsleven zal nauw bij dit proces worden betrokken. Het programma zal ertoe bijdragen dat aan de partners meer informatie kan worden verschaft over specifieke dreigingen, die het hen mogelijk zal maken maatregelen te nemen om het hoofd te bieden aan de mogelijke gevolgen daarvan. Dat zou niets veranderen aan het feit dat de eigenaars en exploitanten verantwoordelijk zijn voor hun eigen beslissingen en plannen om hun activa te beschermen.

Wanneer voor een sector geen normen bestaan of nog geen internationale normen zijn vastgelegd, zouden het Europees comité voor normalisatie (CEN) en andere bevoegde normalisatieorganisaties het netwerk kunnen bijstaan en uniforme, sectorspecifieke veiligheidsnormen en aangepaste normen voor de verschillende betrokken bedrijfstakken en sectoren voorstellen. Dergelijke normen zouden ook op internationaal niveau via de ISO kunnen worden voorgesteld teneinde voor iedereen gelijke voorwaarden te scheppen.

Omzichtigheid is geboden wanneer melding wordt gemaakt van nationale veiligheidsbedreigingen voor de kritieke infrastructuur, zoals terrorisme, teneinde binnen de EU zelf alsmede bij potentiële toeristen en investeerders geen overmatige bezorgdheid te wekken. Terrorisme vormt een constante bedreiging, maar het is de taak van de beleidsmakers iedereen ertoe aan te moedigen hun leven daardoor zo weinig mogelijk te laten beïnvloeden. Tevens moet erop worden toegezien dat het recht op privacy, zowel binnen als buiten de Unie, wordt geëerbiedigd. De consumenten en exploitanten moeten erop kunnen vertrouwen dat informatie zorgvuldig, vertrouwelijk en correct zal worden behandeld. Er moet een passend kader voorhanden zijn om te garanderen dat geclassificeerde informatie correct wordt beheerd en wordt beschermd tegen ongeoorloofd gebruik of openbaarmaking zonder machtiging.

Een aanzienlijk deel van de kritieke infrastructuur van de EU en van de lidstaten overschrijdt de grenzen van de EU. Pijpleidingen doorkruisen hele continenten, kabels die van essentieel belang zijn voor informatietechnologiediensten liggen op grote diepte op de oceaanbodem, enz. Dat betekent dat internationale samenwerking een belangrijke component is bij de vorming van permanente, dynamische, nationale en internationale partnerschappen tussen de eigenaars en exploitanten van kritieke infrastructuur en de regeringen van derde landen, in het bijzonder die welke rechtstreeks energieproducten aan de Unie leveren.

5.2. Uitvoering van het EPCIP

Voor de bescherming van kritieke infrastructuur is de actieve deelneming van de eigenaars en exploitanten van de infrastructuur, de regelgevende instanties, de beroepsorganisaties en de industriële organisaties, alsmede van de lidstaten en de Commissie vereist. Het EPCIP heeft ten doel op grond van de informatie die door de contactpunten van de lidstaten en het netwerk

wordt verschaft, te blijven nagaan welke infrastructuur kritieke infrastructuur is, de kwetsbaarheid en de onderlinge afhankelijkheid van deze infrastructuur te analyseren en oplossingen aan te bieden om deze op alle mogelijke gevaren voor te bereiden en deze tegen die gevaren te beschermen. Daartoe zouden de industriesectoren moeten worden geholpen om een beter inzicht te krijgen in de variabelen dreiging en de gevolgen daarvan in hun risicobeoordelingen. De rechtshandhavingsdiensten en de civiele-beschermingsmechanismen van de lidstaten zouden ervoor moeten zorgen dat het EPCIP een integrerend deel uitmaakt van hun planning en hun bewustmakingsactiviteiten.

De diensten van de Commissie zullen in nauwe samenwerking met het netwerk verdere maatregelen, in de vorm van de goedkeuring van wetgeving en/of de verspreiding van informatie, nemen. De Task Force van hoofden van politie en Europol kunnen een rol spelen bij het verstrekken van informatie over de veiligheidsniveaus en van onderzoeksinformatie aan de rechtshandhavingsinstanties van de lidstaten, die op hun beurt contact zouden moeten opnemen met de eigenaars en exploitanten van kritieke infrastructuur om hen op de hoogte te brengen van gevaren en advies te geven over veiligheidsmaatregelen en de ontwikkeling van veiligheidsstrategieën om terrorisme te bestrijden.

De regeringen van de lidstaten zullen databanken van nationale belangrijke kritieke infrastructuur voortzetten en/of ontwikkelen en up-to-date houden. Zij zouden verantwoordelijk zijn voor de ontwikkeling, de validatie en de audit van relevante plannen en aldus de continuïteit van de diensten in hun bevoegdheidsgebied waarborgen. Bij het opstellen van het EPCIP zal de Commissie voorstellen doen over de minimuminhoud en de opzet van dergelijke databanken en over de wijze waarop zij onderling zouden moeten worden gekoppeld.

De regeringen van de lidstaten zouden op hun beurt de eigenaars en exploitanten van kritieke infrastructuur (alsmede zo nodig andere lidstaten) op de hoogte blijven houden van relevante onderzoeksinformatie en waarschuwingen, alsmede van het soort reactie dat voor elk gevaren- of waarschuwingsniveau is overeengekomen.

De eigenaars en exploitanten van kritieke infrastructuur zorgen voor een adequate beveiliging van hun activa door hun veiligheidsplannen actief uit te voeren en geregeld inspecties te verrichten, oefeningen te houden, tot evaluaties over te gaan en plannen uit te voeren. De lidstaten zouden moeten toezien op het proces in zijn geheel, terwijl de Commissie door middel van adequate inspectiesystemen voor een uniforme tenuitvoerlegging in de hele Unie zou moeten zorgen.

5.3. Doelstellingen van het EPCIP en voortgangsindicatoren

Het doel van het EPCIP en de taak van de Commissie zou zijn, te zorgen voor adequate en uniforme veiligheidsniveaus voor kritieke infrastructuur, een zo gering mogelijk aantal individuele zwakke punten (single points of failure) en snelle, beproefde hulpverleningsvoorzieningen in de hele Unie. Het EPCIP zou continu verder moeten worden ontwikkeld en een geregelde herziening zal nodig zijn om gelijke tred te houden met de problemen en bezorgdheid in de Gemeenschap.

In hoeverre het programma een succes is, zal worden afgemeten aan:

- het feit of en in hoeverre de lidstaten infrastructuren op hun grondgebied als kritieke infrastructuren hebben geïdentificeerd en een inventaris ervan hebben

opgemaakt overeenkomstig de in het kader van het EPCIP vastgelegde prioriteiten;

- de samenwerking binnen de sectoren en met de regering met het oog op de uitwisseling van informatie, en de beperking van de waarschijnlijkheid dat zich incidenten voordoen die verstrekkende of langdurige verstoringen van kritieke infrastructuur ten gevolge hebben;

- de vastberadenheid van de Europese Gemeenschap om een gemeenschappelijke methode te ontwikkelen om de veiligheid van kritieke infrastructuren te waarborgen via samenwerking tussen alle actoren uit de openbare en de particuliere sector.

TECHNICAL ANNEX

GLOSSARY

Critical Infrastructure (CI)

Those physical resources; services; and information technology facilities, networks and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of Europeans or the effective functioning of the EU or its Member States governments.

Critical infrastructure Warning Information Network (CIWIN)

A EU network to assist Member States, EU Institutions, owners and operators of critical infrastructure to exchange information on shared threats, vulnerabilities and appropriate measures and strategies to mitigate risk in support of critical infrastructure protection.

Critical Infrastructure Protection (CIP)

The programs, activities and interactions used by owners and operators to protect their critical infrastructure.

CIP capability

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

European programme for Critical Infrastructure Protection (EPCIP)

A programme to provide enhanced security for critical infrastructure as an ongoing, dynamic, national partnership among EU institutions, critical infrastructure owner/operators and EU Member States to assure the continued functioning of Europe's critical infrastructure

Infrastructure

The framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services, the smooth functioning of governments at all levels, and society as a whole.

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.

Risk Assessment

A process of evaluating threats to the vulnerabilities of an asset to give an expert opinion on the probability of loss or damage and its impact, as a guide to taking action.

Risk Management

A deliberate process of understanding risk and deciding upon and implementing actions to reduce risk to a defined level, which is an acceptable level of risk at an acceptable cost. This approach is characterized by identifying, measuring, and controlling risks to a level commensurate with an assigned level.

Threat

Any event that has 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.

Threat Assessment

A standardized and reliable manner to evaluate threats to infrastructure.

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.