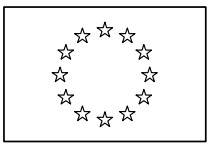

COMISIÓN DE LAS COMUNIDADES EUROPEAS

Bruselas, 17.11.2005
COM(2005) 576 final

LIBRO VERDE

SOBRE UN PROGRAMA EUROPEO PARA LA PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS

(presentado por la Comisión)

LIBRO VERDE

SOBRE UN PROGRAMA EUROPEO PARA LA PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS

1. ANTECEDENTES

Las infraestructuras críticas pueden ser destruidas o sufrir daños o interrupciones debido a acciones terroristas deliberadas, catástrofes naturales, accidentes o actos de piratería informática, actividades delictivas o comportamientos malintencionados. Para preservar las vidas y los bienes de las personas de la UE expuestas al terrorismo, las catástrofes naturales y los accidentes, toda interrupción o manipulación de infraestructuras críticas debe, en la medida de lo posible, ser breve, infrecuente, gestionable, geográficamente aislada y lo menos perjudicial posible para el bienestar de los Estados miembros, sus ciudadanos y la Unión Europea. Los recientes atentados terroristas en Madrid y Londres han puesto de manifiesto el riesgo de atentado terrorista contra las infraestructuras europeas. La respuesta de la UE debe ser rápida, coordinada y eficaz.

El Consejo Europeo de junio de 2004 instó a la Comisión a elaborar una estrategia global sobre protección de infraestructuras críticas. En respuesta, la Comisión adoptó el 20 de octubre de 2004 una Comunicación sobre protección de las infraestructuras críticas en la lucha contra el terrorismo, donde se formulan propuestas claras a fin de mejorar la prevención, preparación y respuesta de Europa frente a atentados terroristas que afecten a infraestructuras críticas.

En las conclusiones del Consejo sobre prevención, preparación y respuesta a los ataques terroristas y en el Programa de solidaridad de la UE sobre las consecuencias de las amenazas y ataques terroristas, adoptado por el Consejo en diciembre de 2004, se respalda el propósito de la Comisión de lanzar un Programa europeo de protección de infraestructuras críticas (PEPIC) y se aprueba la creación por la Comisión de una Red de información sobre alertas en infraestructuras críticas (CIWIN).

La Comisión ha organizado dos seminarios y solicitado ideas y observaciones a los Estados miembros. El primer Seminario sobre protección de infraestructuras críticas de la UE se celebró los días 6 y 7 de junio de 2005 con la participación de los Estados miembros. Después del seminario, los Estados miembros remitieron a la Comisión documentación sobre su planteamiento en materia de protección de infraestructuras críticas (PIC) y observaciones sobre los conceptos debatidos en el seminario. Toda esta documentación se recibió en junio y julio y constituyó la base para los posteriores trabajos en este ámbito. El segundo Seminario de la UE sobre protección de infraestructuras críticas tuvo lugar los días 12 y 13 de septiembre con el objetivo de profundizar en el debate. Este segundo Seminario contó con la participación de los Estados miembros y las asociaciones del sector. Concluidos los seminarios, la Comisión ha decidido presentar el presente Libro Verde, en el que se exponen las diferentes opciones para el PEPIC.

2. OBJETIVO DEL LIBRO VERDE

El principal objetivo del Libro Verde es recabar puntos de vista en torno a las posibles opciones para el PEPIC gracias a una amplia participación de los agentes interesados. Una protección eficaz de las infraestructuras críticas requiere la comunicación, coordinación y cooperación, en el ámbito tanto nacional como de la UE, entre todas las partes interesadas: propietarios y operadores de infraestructuras, reguladores, asociaciones profesionales y empresariales en cooperación con todos los niveles de la administración y el público en general.

El Libro Verde presenta las opciones para una respuesta de la Comisión a la solicitud del Consejo de establecer el PEPIC y la CIWIN y constituye la segunda fase del proceso de consulta con vistas al Programa europeo de protección de infraestructuras críticas. Una vez presentado el Libro Verde, la Comisión espera recibir propuestas concretas sobre las opciones que en él se exponen. En función del resultado del proceso de consulta, el conjunto de medidas que integren el Programa podría presentarse en 2006.

3. OBJETIVO Y ÁMBITO DEL PEPIC

3.1. Objetivo global del PEPIC

El objetivo del PECIP sería asegurar niveles adecuados y equivalentes de seguridad en las infraestructuras críticas, minimizar los puntos de fallo y proponer mecanismos rápidos y probados de recuperación de infraestructuras para toda la Unión. El nivel de protección puede no ser el mismo para todas las infraestructuras críticas, sino depender de las repercusiones que ocasionara su fallo. El PEPIC sería un proceso permanente, que requeriría revisiones periódicas en vista de los problemas y preocupaciones que fueran surgiendo.

EL PEPIC debe reducir al mínimo cualquier impacto negativo que sobre la competitividad de un determinado sector pudiera tener una mayor inversión en seguridad. Al calcular la proporcionalidad de los costes, no debe perderse de vista la necesidad de mantener la estabilidad de los mercados, aspecto crucial para la inversión a largo plazo, así como la influencia de la seguridad en la evolución de los mercados de valores y de la macroeconomía.

Pregunta

¿Es éste un objetivo adecuado para el PEPIC? En caso contrario, ¿cuál debiera ser?

3.2. ¿Frente a qué debe proteger el PEPIC?

Así como, en la mayoría de los incidentes, las medidas de gestión de las consecuencias son idénticas o similares, las medidas de protección pueden presentar diferencias en función del carácter de la amenaza. Los ataques intencionados y las catástrofes naturales figuran entre las amenazas que podrían reducir de forma significativa la capacidad de satisfacer las necesidades fundamentales y garantizar la seguridad de la población, mantener el orden, prestar los servicios públicos mínimos e indispensables y garantizar un ordenado funcionamiento de la economía. Las opciones son las siguientes:

a) **un planteamiento global frente a todos los peligros**: se trataría de un planteamiento amplio que atendiera a las amenazas debidas tanto a ataques intencionados como a catástrofes naturales. Garantizaría un máximo aprovechamiento de las sinergias entre las medidas de protección, pero no haría especial hincapié en el terrorismo;

b) **un planteamiento global con prioridad sobre el terrorismo**: un planteamiento flexible, que atendiera a otros tipos de peligros, tales como ataques intencionados o catástrofes naturales, pero con el terrorismo como prioridad. Si el nivel de las medidas de protección en un determinado sector se considerase adecuado, los agentes interesados podrían entonces concentrarse en aquellas amenazas a las cuales fueran aún vulnerables.

c) **un planteamiento centrado en la amenaza del terrorismo**: un planteamiento específico sobre terrorismo, que no prestaría especial atención a las amenazas más comunes.

Pregunta

¿Qué planteamiento debe adoptar el PEPIC? ¿Por qué?

4. PROPUESTA DE PRINCIPIOS BÁSICOS

Se proponen los siguientes principios básicos como fundamento para el PEPIC:

- **Subsidiariedad:** el principio de subsidiariedad estaría en el núcleo mismo del PEPIC; la protección de las infraestructuras críticas sería, ante todo, responsabilidad nacional. Las responsabilidades primordiales en cuanto a protección de estructuras críticas incumbirían a los Estados miembros y a los propietarios/operadores, actuando bajo un marco común. La Comisión, por su parte, se concentraría en los aspectos relacionados con la protección de infraestructuras críticas con repercusiones transfronterizas dentro de la UE. Lo que no cambiaría es la responsabilidad de los propietarios y operadores, los cuales habrían de adoptar sus propias decisiones y planes para proteger sus activos.

- **Complementariedad**: el marco común del PEPIC sería complementario con respecto a medidas ya vigentes. En caso de que ya existan mecanismos comunitarios, deben seguir utilizándose y contribuir a garantizar la aplicación global del PEPIC.

- **Confidencialidad**: el intercambio de información sobre protección de infraestructuras críticas tendría lugar en un entorno de confianza y confidencialidad. Se trata de una necesidad, pues los datos específicos de una infraestructura critica pueden utilizarse para ocasionar fallos o consecuencias inaceptables en las instalaciones que la componen. Tanto en el ámbito de la UE como en el de los Estados miembros, la información sobre PIC debe ser clasificada, y el acceso a la misma, concedido únicamente en caso necesario.

- **Cooperación de los agentes interesados**: todos los agentes interesados, incluidos los Estados miembros, la Comisión, las asociaciones sectoriales o profesionales, los organismos de normalización y los propietarios, operadores y usuarios (entendiéndose por «usuarios» las organizaciones que explotan y utilizan la infraestructura para fines comerciales y de prestación de servicios) deben desempeñar un papel en la protección de las infraestructuras críticas. Todos los agentes interesados, según sus funciones y responsabilidades propias, deben cooperar y contribuir al desarrollo y aplicación del PEPIC. Las autoridades de los Estados miembros dirigirían y coordinarían la elaboración y

puesta en práctica de un planteamiento coherente en el ámbito nacional para la protección de las infraestructuras críticas bajo su competencia. Los propietarios, operadores y usuarios participarían activamente, tanto en el ámbito nacional como en el de la UE. En caso de no existir normas sectoriales o no haberse establecido aún normas internacionales, los organismos de normalización podrían, en su caso, adoptar normas comunes.

- **Proporcionalidad**: las estrategias y medidas de protección serían proporcionales al grado de riesgo en cuestión, pues no todas las infraestructuras pueden protegerse frente a todas las amenazas (por ejemplo, las redes de transporte de electricidad son demasiado extensas para protegerlas con vallas u otro tipo de dispositivo de protección). Sin embargo, mediante las técnicas adecuadas de gestión de riesgos, podría centrarse la atención en los puntos de máximo riesgo según la amenaza de que se trate, el carácter crítico relativo de la infraestructura en cuestión, la relación entre costes y beneficios, el nivel de seguridad existente y la eficacia de las estrategias disponibles de reducción de riesgo.

Pregunta

¿Son aceptables estos principios básicos? ¿Hay alguno superfluo? ¿Cabe introducir algún otro?

¿Están de acuerdo en que las medidas de protección deben ser proporcionadas al nivel del riesgo concreto, pues no todas las infraestructuras pueden protegerse frente a todas las amenazas?

5. UN MARCO COMÚN PARA EL PEPIC

El daño o pérdida de un elemento de infraestructura en un Estado miembro puede tener efectos negativos en otros, y aun en el conjunto de la economía europea. Tales efectos son cada vez más probables, pues las nuevas tecnologías (por ejemplo, Internet) y la liberalización de los mercados (por ejemplo, los del suministro de electricidad y gas) suponen la integración de gran parte de las infraestructuras en redes más amplias. En esta situación, las medidas de protección son tan fuertes como su eslabón más débil. Ello puede hacer necesario establecer un nivel de protección común.

Una protección eficaz requiere la comunicación, coordinación y cooperación de todos los agentes interesados en el ámbito nacional, internacional y, en su caso, de la UE. Podría establecerse un marco comunitario común para la protección de infraestructuras críticas en Europa que garantizara que cada Estado miembro ofreciera niveles adecuados y equivalentes de protección de sus infraestructuras críticas, sin falseamiento de las normas de competencia en el mercado interior. Como apoyo a las actividades de los Estados miembros, la Comisión podría facilitar la definición, intercambio y difusión de las mejores prácticas en materia de PIC estableciendo un marco común en este ámbito. Cuál sería el campo de aplicación de este marco general es asunto que requiere consideración.

El marco general del PEPIC contemplaría una serie de medidas horizontales que definirían las competencias y responsabilidades de todos los agentes interesados en el ámbito de la PIC y establecerían los fundamentos para los planteamientos sectoriales específicos. El marco común serviría de complemento a las medidas sectoriales ya existentes, en el ámbito comunitario y en los Estados miembros, a fin de garantizar el máximo de seguridad de las

infraestructuras críticas presentes en la Unión Europea. Es prioritario alcanzar el acuerdo en torno a una lista común de definiciones y sectores de infraestructuras críticas.

Dada la diversidad de sectores en los que existen infraestructuras críticas, sería arduo establecer criterios detallados para su identificación y total protección a través de un marco horizontal; se trata de una labor que debe llevarse a cabo sector por sector. No obstante, es preciso hallar un entendimiento común sobre una serie de aspectos generales.

En consecuencia, se propone fortalecer las infraestructuras críticas de la UE mediante el establecimiento de un marco común para el PEPIC (que incluya objetivos y metodologías comunes a efectos, por ejemplo, de comparación e interdependencia), el intercambio de mejores prácticas y la utilización de mecanismos de control. Entre los elementos que podrían formar parte del marco común cabe incluir:

- principios comunes en materia de PIC;
- códigos/normas acordadas de común acuerdo;
- definiciones comunes a partir de las cuales puedan acordarse definiciones específicas para cada sector (en el Anexo 1 figura una lista indicativa de dichas definiciones);
- una lista común de sectores de infraestructuras críticas (en el Anexo 2 figura una lista indicativa de dichos sectores);
- ámbitos prioritarios para la PIC;
- descripción de las responsabilidades de los agentes interesados;
- instrumentos de evaluación acordados;
- metodologías para la comparación y el establecimiento de prioridades entre infraestructuras de diferentes sectores.

Este marco común reduciría, además, los posibles efectos de falseamiento en el mercado interior.

El marco común para el PEPIC podría ser de carácter voluntario, obligatorio… o bien, según el tema, una combinación de ambos. Los dos tipos de marco pueden complementar las medidas sectoriales y horizontales ya vigentes en los ámbitos comunitario y nacional; pero sólo un marco de carácter jurídico puede sentar fundamentos sólidos y aplicables, que permitan una ejecución coherente y uniforme de las medidas de protección de las infraestructuras críticas europeas y delimitar con claridad las responsabilidades respectivas de los Estados miembros y la Comisión. Las medidas voluntarias y no vinculantes, pese a su flexibilidad, no permiten establecer con claridad suficiente los respectivos cometidos.

En función de los resultados de un minucioso análisis y con la debida atención a la proporcionalidad de las medidas propuestas, la Comisión podrá hacer uso de toda una serie de instrumentos, incluidos los legislativos, en su propuesta de PEPIC. Cuando corresponda, las medidas específicas irán acompañadas de evaluaciones de impacto.

Preguntas

Para el fortalecimiento de la PIC ¿sería eficaz un marco común?

En caso de que sea necesario un marco legislativo ¿de qué elementos debe constar?

¿Están de acuerdo en que los criterios para determinar los diferentes tipos de infraestructura crítica de la Unión Europea (ICE) y las medidas de protección que se consideren necesarias deben establecerse sector por sector?

¿Contribuiría el marco común a delimitar las responsabilidades de los respectivos agentes interesados? ¿En qué medida debe este marco común ser obligatorio y en qué medida voluntario?

¿Cuál debe ser el ámbito de aplicación del marco común? ¿Están de acuerdo con la lista de términos y definiciones indicativos (Anexo I) a partir de la cual podrían crearse, en su caso, definiciones específicas para cada sector? ¿Están de acuerdo con la lista indicativa de sectores de infraestructuras críticas (Anexo II)?

6. INFRAESTRUCTURAS CRÍTICAS DE LA UE (ICE)

6.1. Definición de infraestructura crítica de la UE

La definición de lo que constituye una infraestructura crítica de la UE depende de sus efectos transfronterizos, los cuales determinan si un incidente puede tener graves repercusiones fuera del territorio del Estado miembro en el cual esté situada la instalación. A este respecto, deben también tomarse en consideración los regímenes bilaterales de cooperación en materia de PIC, que constituyen un medio bien establecido y eficaz de atender a las infraestructuras críticas entre las fronteras de dos Estados miembros. Este tipo de cooperación sería complementaria con el PEPIC.

Entre las ICE figurarían los recursos físicos, servicios y sistemas de tecnologías de la información, redes y elementos de infraestructura cuya interrupción o destrucción tuviera grave impacto en la salud, la seguridad o el bienestar económico o social:

a) de dos o más Estados miembros: **esto incluiría determinadas infraestructuras críticas bilaterales (en su caso);** o bien

b) de tres o más Estados miembros: **esto excluiría todas las infraestructuras críticas bilaterales.**

A la hora de estudiar los méritos respectivos de ambas opciones, cabe tener presentes las siguientes consideraciones:

– el hecho de que un elemento de infraestructura se clasifique como ICE no implica que requiera medidas de protección adicionales; las medidas de protección vigentes, incluidos los acuerdos bilaterales entre Estados miembros, pueden ser perfectamente suficientes y, en consecuencia, no verse afectadas por la designación de una infraestructura como ICE;

– la opción a) podría dar lugar a la clasificación como ICE de un número mayor de infraestructuras;

– la opción b), en el caso de las infraestructuras que tan sólo interesen a dos Estados miembros, podría implicar que la Comunidad no desempeñara papel alguno, y ello aún en caso de que uno de los dos Estados miembros considerara insuficiente la protección y el otro se negara a tomar medidas; además, esta opción podría dar lugar a una multitud de acuerdos bilaterales, o a desacuerdos entre los Estados miembros; y las empresas, que a

menudo operan en el ámbito paneuropeo, podrían verse inmersas en un rompecabezas de acuerdos que acarreara costes adicionales.

Por otra parte, debe reconocerse la necesidad de atender a las infraestructuras críticas originadas o existentes fuera de la UE, pero con interconexiones o efectos directos potenciales en los Estados miembros.

Pregunta

¿Deben clasificarse como ICE las infraestructuras que puedan tener un impacto transfronterizo potencialmente grave en dos o más Estados miembros, o bien las que puedan tenerlo en tres o más Estados miembros? ¿Por qué?

6.2. Interdependencias

Se propone que la clasificación gradual de todas las ICE atienda a las interdependencias. Los estudios sobre las interdependencias contribuirían a evaluar el impacto potencial de las amenazas a infraestructuras críticas concretas y, más concretamente, a determinar qué Estados miembros se verían afectados en caso de incidente grave que afectara a infraestructuras críticas.

Deben tomarse plenamente en consideración las interdependencias existentes entre y dentro de las empresas, los sectores industriales, las instancias territoriales competentes y las autoridades de los Estados miembros; en particular, las interdependencias debidas a las tecnologías de la información y la comunicación (TIC). La Comisión, los Estados miembros y los propietarios/operadores de infraestructuras críticas colaborarían para determinar las interdependencias y aplicar estrategias adecuadas a fin de reducir los riesgos en la medida de lo posible.

Preguntas

¿Cómo pueden tomarse en consideración las interdependencias?

¿Conocen alguna metodología adecuada para el análisis de las interdependencias?

¿En qué nivel deben identificarse las interdependencias: el de la UE, el de los Estados miembros o ambos?

6.3. Etapas de aplicación de las medidas en materia de ICE

La Comisión propone las siguientes etapas de aplicación de las medidas en materia de ICE:

(1) La Comisión, conjuntamente con los Estados miembros, elaborará los criterios específicos que se emplearán a fin de identificar las ICE de cada sector.

(2) Identificación y verificación gradual por los Estados miembros y la Comisión de las ICE presentes en cada sector. La decisión de designar una determinada infraestructura crítica como ICE se tomará a nivel europeo[1] habida cuenta del carácter transfronterizo de este tipo de infraestructuras.

(3) Los Estados miembros y la Comisión analizarán sector por sector las deficiencias en materia de seguridad que afecten a las ICE.

(4) Los Estados miembros y la Comisión determinarán de común acuerdo los sectores/infraestructuras prioritarios teniendo en cuenta las interdependencias.

(5) Cuando proceda, la Comisión y los principales agentes interesados de los Estados miembros acordarán para cada sector propuestas de medidas de protección mínima, que podrán incluir normas.

(6) Una vez adoptadas las propuestas por el Consejo, las medidas entrarán en vigor.

(7) Los Estados miembros y la Comisión serán responsables de la supervisión periódica. Las revisiones (de las medidas y de la identificación de las ICE) se efectuarán cuando corresponda.

Preguntas

¿Es aceptable esta lista de etapas para la aplicación de las medidas en materia de ICE?

¿Cómo deben cooperar, a su juicio, la Comisión y los Estados miembros para designar las ICE? ¿Ofrecerán los Estados miembros los conocimientos especializados, mientras que la Comisión velará por el interés europeo? ¿Debe esto ser objeto de decisión jurídica?

¿Es necesario un mecanismo de arbitraje en caso de que un determinado Estado miembro no acceda a designar como ICE una infraestructura bajo su competencia?

¿Deben verificarse las designaciones? ¿Quién sería responsable de hacerlo?

¿Deben los Estados miembros tener la posibilidad de designar como críticas las infraestructuras situadas en otros Estados miembros o en terceros países? ¿Qué ocurriría si un Estado miembro, un tercer país o un sector considerarse crítico un elemento de infraestructura situado en otro Estado miembro?

Y ¿qué ocurriría si el Estado miembro en cuestión no lo considerase como tal? ¿Será necesario un mecanismo de recurso? En caso afirmativo, ¿cuál?

¿Deben los operadores tener vías de recurso en caso de no aceptar la designación o no designación de sus infraestructuras como críticas? En caso afirmativo, ¿ante qué instancia?

[1] Con excepción de las infraestructuras relacionadas con la defensa.

¿Qué metodologías deben desarrollarse para determinar los sectores/infraestructuras que deben ser objeto de medidas prioritarias? ¿Existen ya en la actualidad metodologías adecuadas que puedan adaptarse al ámbito europeo?

¿De qué modo puede participar la Comisión en el análisis de las deficiencias en materia de seguridad que afecten a ICE?

7 . INFRAESTRUCTURAS CRÍTICAS NACIONALES (ICN)

7.1. Papel de las ICN en el PEPIC

Numerosas empresas europeas operan a través de las fronteras y por ello se encuentran sometidas a obligaciones diferentes en materia de ICN. En consecuencia se propone, en interés de los Estados miembros y del conjunto de la UE, que cada Estado miembro proteja sus infraestructuras críticas nacionales con arreglo a un marco común, de modo que los propietarios y operadores de toda Europa no se vean sujetos a un rompecabezas de marcos diferentes que den lugar a multitud de metodologías y acarreen costes adicionales. Por tal motivo, la Comisión considera que el PEPIC, pese a centrarse ante todo en las infraestructuras críticas para la UE, no puede desatender completamente las infraestructuras críticas nacionales. Ahora bien, cabe plantearse tres opciones:

a) Plena integración de las ICN en el PEPIC

b) Exclusión de las ICN del PEPIC

c) Aplicación por los Estados miembros, de manera voluntaria y sin obligación alguna, de determinadas partes del PEPIC a las ICN

Preguntas

Para una eficaz protección de las infraestructuras críticas en la Unión Europea sería necesario identificar tanto las ICE como las ICN. ¿Están de acuerdo en que, si bien el PEPIC debe centrarse en las ICE, no puede desatender completamente las ICN?

¿Cuál de las opciones precedentes considera más adecuada para el PEPIC?

7.2. Programas nacionales de PIC

A partir del marco común del PEPIC, los Estados miembros podrían elaborar programas nacionales de PIC para sus ICN. Los Estados miembros tendrían la posibilidad de aplicar medidas más estrictas que las contempladas en el PEPIC.

Pregunta

¿Es conveniente que cada Estado miembro adopte un programa nacional de PIC basado en el PEPIC?

7.3. Organismo de supervisión único

Por motivos de eficacia y coherencia, cada uno de los Estados miembros habría de designar a un organismo de supervisión único que fuera responsable de la aplicación global del PEPIC. Podrían plantearse dos opciones:

a) Un organismo de supervisión único en materia de PIC, o bien

b) Un punto de contacto nacional sin autoridad alguna y cuya organización quedaría a discreción de los Estados miembros.

Este organismo coordinaría, supervisaría y controlaría la aplicación del PEPIC en su territorio de competencia y podría servir como principal punto de contacto institucional en materia de PIC para la Comisión, los demás Estados miembros y los propietarios y operadores de infraestructuras críticas. El organismo podría servir de base para la representación de los Estados miembros en los grupos de expertos sobre asuntos de PIC y estar vinculado a la Red de información sobre alertas en infraestructuras críticas (CIWIN). El Organismo de coordinación nacional de la PIC (OCNP) se ocuparía de coordinar todo lo relativo a la PIC, sin perjuicio de otros organismos y entidades con responsabilidades en este ámbito que puedan existir en los Estados miembros.

La gradual identificación de las ICN podría llevarse a cabo a través de la obligación de los propietarios y operadores de infraestructuras de comunicar al OCNP toda actividad de interés para la PIC.

El OCNP podría ser responsable de la decisión jurídica por la cual una infraestructura bajo su competencia se clasificara como ICN. Esta información estaría a disposición exclusiva del Estado miembro interesado.

Entre sus competencias específicas figurarían:

a) La coordinación, control y supervisión de la aplicación general del PEPIC en un Estado miembro;

b) Actuar como principal punto de contacto institucional en materia de PIC con:

   i. la Comisión

   ii. los demás Estados miembros

   iii. los propietarios y operadores de PIC

c) Participar en la designación de infraestructuras críticas de la UE (ICE);

d) Adoptar la decisión jurídica por la cual una infraestructura bajo su competencia se designe Infraestructura crítica nacional;

e) Actuar como instancia de recurso legal para los propietarios/operadores que no estén de acuerdo con la designación de su infraestructura como «infraestructura crítica»;

f) Participar en la elaboración del Programa nacional de protección de infraestructuras críticas y de los programas sectoriales de PIC;

g) Determinar las interdependencias existentes entre sectores específicos de infraestructuras críticas;

h) Contribuir a elaborar planteamientos en materia de PIC aplicables a sectores específicos mediante la participación en grupos de expertos; podría invitarse a participar en los debates a representantes de propietarios y operadores; se celebrarían reuniones periódicas.

i) Supervisar el proceso de elaboración de planes de intervención en materia de infraestructuras críticas;

Preguntas

¿Están de acuerdo en que los Estados miembros sean responsables únicos de la designación y gestión de las ICN dentro del marco común del PEPIC?

¿Es conveniente designar en cada Estado miembro un Organismo de coordinación de PIC que sea responsable de la coordinación general de las medidas en este ámbito, sin perjuicio de las responsabilidades ya existentes en cada sector (autoridades de aviación civil, Directiva Seveso, etc.)?

¿Son adecuadas las competencias que se proponen para este organismo de coordinación? ¿Son necesarias otras?

7.4. Etapas de aplicación de las medidas en materia de ICN

La Comisión propone las siguientes etapas de aplicación de las medidas en materia de ICN:

(1) Los Estados miembros, a partir del PEPIC, elaborarán los criterios específicos que permitan identificar a las ICN.

(2) Determinación y verificación gradual por los Estados miembros de las ICN presentes en cada sector.

(3) Los Estados miembros analizarán sector por sector las deficiencias en materia de seguridad que afecten a las ICN.

(4) Los Estados miembros determinarán los sectores/infraestructuras prioritarios teniendo en cuenta las interdependencias y, en su caso, las prioridades acordadas en el ámbito de la UE.

(5) Cuando proceda, los Estados miembros acordarán medidas de protección mínima para cada sector.

(6) Los Estados miembros serán responsables de velar por que los propietarios/operadores de su territorio de competencia apliquen las medidas de ejecución oportunas.

(7) Los Estados miembros serán responsables de una supervisión periódica. Las revisiones (de las medidas y de la identificación de las infraestructuras críticas) se efectuarán cuando corresponda.

Pregunta

¿Es aceptable la lista de etapas para la aplicación de las medidas en materia de ICN? ¿Sobra alguna? ¿Deben añadirse otras?

8. PAPEL DE LOS PROPIETARIOS, OPERADORES Y USUARIOS DE INFRAESTRUCTURAS CRÍTICAS

8.1. Responsabilidades de los propietarios, operadores y usuarios de infraestructuras críticas

La designación de una infraestructura como crítica comporta para sus propietarios y operadores una serie de responsabilidades. Para los propietarios y operadores de infraestructuras clasificadas como ICN o ICE cabe contemplar cuatro responsabilidades:

(1) **La comunicación del posible carácter crítico de una infraestructura al organismo competente en materia de PIC del Estado miembro**.

(2) **La designación de uno o varios representantes de alto nivel como funcionarios de enlace para la seguridad (FES) de común acuerdo entre el propietario/operador y la autoridad competente en materia de PIC del Estado miembro.** El FES participaría en el desarrollo de los planes de seguridad y de intervención. Sería el principal funcionario de enlace con el organismo sectorial competente en materia de de PIC en los Estados miembros, así como, en su caso, con las autoridades represivas.

(3) **El establecimiento, ejecución y actualización de un Plan de seguridad para los operadores (PSO).** En el Anexo 3 figura una propuesta de modelo de PSO.

(4) **La participación en la elaboración de un plan de intervención** relativo a las infraestructuras críticas, conjuntamente con las autoridades competentes en materia de protección civil de los Estados miembros, así como las autoridades represivas.

El PSO podría remitirse para su aprobación a la autoridad competente del Estado miembro en materia de protección de infraestructuras críticas, bajo la supervisión general del OCNP, con independencia de que se trate de una ICN o de una ICE; esto garantizaría la coherencia de las medidas de seguridad adoptadas por cada propietario u operador y los sectores interesados en general. A cambio, los propietarios y operadores podrían obtener del OCNP y, en su caso, de la Comisión información y asistencia sobre determinadas amenazas y sobre la elaboración de mejores prácticas así como, en su caso, ayuda a fin de evaluar las interdependencias y puntos vulnerables.

Cada uno de los Estados miembros podría fijar plazos límite para la elaboración de PSO por los propietarios y operadores de ICN e ICE (en este último caso, con la participación de la Comisión) e imponer multas administrativas en caso de no cumplirse.

Se propone que el PSO determine los activos de infraestructuras críticas del propietario/operador y establezca las correspondientes soluciones de seguridad para su protección. El PSO describiría los métodos y procedimientos que deben seguirse para garantizar el cumplimiento del PEPIC, de los programas nacionales y de los programas sectoriales específicos de PIC. El PSO podría servir de vehículo para un planteamiento «de

arriba a abajo» en materia de regulación de la PIC que contemple una mayor participación (pero también una mayor responsabilidad) del sector privado.

En particular, en situaciones que afecten a determinadas infraestructuras tales como las redes de distribución eléctrica o las redes de información, no sería realista (desde un punto de vista práctico y financiero) esperar de los propietarios y los operadores que ofrezcan los mismos niveles de seguridad para todas sus infraestructuras. En este tipo de casos, se propone que los propietarios y los operadores, junto con las autoridades competentes, determinen los puntos críticos (nodos) de la red física o informática en la cual podrían concentrarse las medidas de protección de la seguridad.

El PSO podría contemplar medidas de seguridad centradas en dos ejes:

- **medidas de seguridad permanentes**, que requerirían una serie de inversiones y medios imprescindibles para la seguridad que los propietarios/operadores no pudieran contemplar a corto plazo. Los propietarios/operadores mantendrían un estado de alerta continua frente a posibles amenazas, la cual no interferiría con sus actividades normales económicas, administrativas y sociales.

- **medidas de seguridad graduadas**, que podrían activarse en función de los diferentes niveles de amenaza. Así, el PSO contemplaría varios regímenes de seguridad en función de los posibles niveles de amenaza existentes en los Estados miembros en los que estuvieran situadas las infraestructuras.

En caso de incumplimiento por parte de un propietario u operador de infraestructuras críticas de la obligación de elaborar un PSO, contribuir a la elaboración de los planes de intervención y designar a un FES, se propone contemplar la posibilidad de sanciones financieras.

Preguntas

¿Son aceptables las posibles responsabilidades de los propietarios/operadores de infraestructuras críticas en el sentido de aumentar la seguridad de dichas infraestructuras? ¿Cuál sería su coste probable?

¿Debe obligarse a los propietarios y operadores a informar del posible carácter crítico de sus infraestructuras? ¿Consideran útil la idea del PSO? ¿Por qué?

¿Son las obligaciones propuestas proporcionales a los costes que acarrearían?

¿Qué derechos podrían reconocer las autoridades de los Estados miembros y la Comisión a los propietarios y operadores de infraestructuras críticas?

8.2. Diálogo con los propietarios, operadores y usuarios de infraestructuras críticas

El PEPIC podría fomentar el establecimiento de estructuras de asociación con los propietarios y operadores. El éxito de todo programa de protección depende de la cooperación y el nivel de participación que pueda establecerse con los propietarios y operadores. En los Estados miembros, los propietarios y operadores de infraestructuras críticas podrían participar estrechamente en su protección mediante contactos periódicos con el OCNP.

En el ámbito de la UE, podrían crearse foros que facilitaran los intercambios de puntos de vista sobre asuntos generales y específicos en materia de protección de infraestructuras críticas. Un planteamiento común sobre la participación del sector privado en asuntos de protección de infraestructuras críticas que reuniera a todos los agentes interesados del ámbito público y privado ofrecería a los Estados miembros, la Comisión y las empresas una plataforma para la comunicación sobre cualquier novedad relacionada con la PIC. Los propietarios, operadores y usuarios de infraestructuras críticas contribuirían a la elaboración de directrices comunes, al establecimiento de normas sobre mejores prácticas y, en su caso, al intercambio de información. Un diálogo de este tipo sería de ayuda para configurar futuras versiones del PEPIC.

En su caso, la Comisión podría impulsar la creación de asociaciones industriales o profesionales en materia de PIC en la Unión Europea. El objetivo último sería doble: garantizar que la industria europea conserve su competitividad y mejorar la seguridad de los ciudadanos de la UE.

Pregunta

¿Cómo debe estructurarse el diálogo con los propietarios, operadores y usuarios de infraestructuras críticas?

¿Quién debe representar a los propietarios, operadores y usuarios en el diálogo entre los sectores público y privado?

9. MEDIDAS DE APOYO AL PEPIC

9.1. Red de información sobre alertas en infraestructuras críticas (CIWIN)

La Comisión ha desarrollado una serie de sistemas de alerta rápida que permiten una respuesta concreta, coordinada y eficaz en caso de urgencia, incluso de origen terrorista. El 20 de octubre de 2004, la Comisión anunció la creación de una red central de la Comisión que garantizará un flujo de información rápido entre todos sus sistemas de alerta rápida y sus departamentos responsables (ARGUS).

La Comisión propone crear la red CIWIN, la cual podría estimular el desarrollo de medidas de protección adecuadas por facilitar un intercambio de mejores prácticas realizado de manera segura, además de actuar como vehículo de comunicación sobre amenazas y alertas inmediatas. El sistema garantizaría que las personas adecuadas recibieran la información adecuada en el momento adecuado.

Para el desarrollo de la CIWIN se plantean las tres opciones siguientes:

(1) **CIWIN como foro limitado al intercambio de ideas y mejores prácticas en materia de PIC** en apoyo a los propietarios y operadores de infraestructuras críticas. Este foro consistiría en una red de expertos y una plataforma electrónica para el intercambio de información en un entorno seguro. La Comisión desempeñaría un papel importante en la recopilación y divulgación de todos estos datos. Esta opción no permitiría transmitir las necesarias alertas rápidas sobre amenazas inminentes. Ahora bien, siempre existiría la posibilidad de ampliar la red más adelante.

(2) **CIWIN como sistema de alerta rápida entre los Estados miembros y la Comisión.** Se trata de una opción que incrementaría la seguridad de las infraestructuras críticas al limitar las alertas a las amenazas de carácter inmediato. El objetivo sería facilitar el intercambio rápido de información a los propietarios y operadores de infraestructuras críticas sobre amenazas potenciales. El sistema de alerta rápida no implicaría compartir datos de inteligencia a largo plazo. Se emplearía para una rápida puesta en común de información sobre amenazas inminentes contra infraestructuras específicas.

(3) **CIWIN como sistema de comunicación/alerta en niveles múltiples y con dos funciones diferentes:** a) como sistema de alerta rápida que vinculara a los Estados miembros con la Comisión y b) como foro de intercambio de ideas sobre protección de infraestructuras críticas y mejores prácticas que sirviera de ayuda para los propietarios y operadores; estaría compuesto por una red de expertos y una plataforma de intercambio electrónico de datos.

Con independencia de la opción que se elija, la red CIWIN sería complementaria respecto de las redes existentes, y se pondría especial precaución en evitar la duplicación de cometidos. A largo plazo, CIWIN podría conectarse con todos los propietarios y operadores de infraestructuras críticas de cada Estado miembro; por ejemplo, a través del OCNP. Las alertas y las mejores prácticas podrían trasmitirse a través de este organismo, que sería el único servicio directamente conectado con la Comisión y, por ende, a los demás Estados miembros. Los Estados miembros podrían utilizar sus sistemas de información ya existentes para establecer dentro de la CIWIN sus respectivas capacidades nacionales, que vincularían a las autoridades con cada propietario u operador. Es importante señalar que estas redes nacionales podrían servir como sistema de comunicación bidireccional entre los organismos competentes en materia de PIC de los Estados miembros.

Se emprenderá un estudio a fin de determinar la extensión y las especificaciones técnicas de la futura interfaz de CIWIN con los Estados miembros.

Preguntas

¿Qué forma debe adoptar la red CIWIN para contribuir a los objetivos del PEPIC?

¿Deben los usuarios y operadores de infraestructuras críticas estar conectados a la CIWIN?

9.2. Metodologías comunes

Los distintos Estados miembros poseen niveles de alarma distintos, que responden a situaciones distintas. Hoy por hoy, no existe modo de saber, por ejemplo, si un nivel de alerta «alto» en un Estado miembro corresponde al mismo nivel en otro. Esto puede dificultar a las empresas trasnacionales el establecimiento de prioridades a la hora de calcular gastos en medidas de protección. Por ello, podría ser de provecho intentar armonizar o calibrar los distintos niveles.

A cada nivel de amenaza le correspondería un nivel de preparación, que requeriría, en general, la adopción de medidas de seguridad comunes y, en su caso, de medidas de seguridad graduadas. Los Estados miembros que no desearan aplicar una determinada medida podrían reaccionar ante una amenaza específica mediante medidas de seguridad alternativas.

Podría estudiarse la elaboración de una metodología común que permita identificar y clasificar las amenazas, capacidades, riesgos y puntos vulnerables y sacar conclusiones sobre la posibilidad, probabilidad y gravedad de cualquier amenaza contra instalaciones de infraestructura. Esta metodología clasificaría los riesgos y prioridades de modo tal que todo acontecimiento de riesgo quedara definido en términos de su probabilidad, impacto y relación con otras áreas o procesos de riesgo.

Preguntas

¿En qué medida es deseable y factible armonizar o calibrar los distintos niveles de alerta?

¿Debe existir una metodología común a fin de identificar y clasificar las amenazas, capacidades, riesgos y puntos vulnerables y que permita sacar conclusiones sobre la posibilidad, probabilidad y gravedad de toda amenaza a instalaciones de infraestructura.

9.3. Financiación

El 15 de septiembre, y tras una iniciativa del Parlamento Europeo (creación de una nueva línea presupuestaria, correspondiente al proyecto piloto «Lucha contra el terrorismo», en el presupuesto de 2005), la Comisión decidió destinar 7 millones de euros a la financiación de un conjunto de medidas que mejorarán la prevención, preparación y respuesta de Europa a los atentados terroristas, incluida la gestión de las competencias, la protección de infraestructuras críticas y medidas en materia de financiación del terrorismo, explosivos y radicalización violenta. Más de dos tercios de este presupuesto se destinan a la preparación del futuro Programa europeo de protección de infraestructuras críticas, a la integración y desarrollo de las capacidades necesarias para la gestión de crisis de importancia transnacional derivadas de posibles atentados terroristas y a medidas de urgencia que puedan ser necesarias en respuesta a amenazas significativas o atentados de este tipo. Se prevé mantener esta dotación en 2006.

De 2007 a 2013, la financiación pasará al Programa marco de seguridad y defensa de las libertades. Se incluirá un programa específico sobre «Prevención, preparación y gestión de las consecuencias del terrorismo»; la propuesta de la Comisión destina un importe de 137,4 millones de euros a la determinación de las necesidades en este ámbito y la elaboración de normas técnicas comunes para la protección de infraestructuras críticas.

El programa contempla la financiación comunitaria de proyectos presentados por las autoridades nacionales, regionales y locales para la protección de infraestructuras críticas. El programa se centra en la determinación de las necesidades de protección y el suministro de información para el desarrollo de normas y evaluaciones comunes de las amenazas y riesgos, con el objetivo de proteger las infraestructuras críticas o elaborar planes de intervención específicos. La Comisión ofrecería su experiencia en este ámbito o podría contribuir a la financiación de estudios sobre interdependencias en sectores específicos. A continuación, será ante todo responsabilidad de los Estados miembros o de los propietarios y operadores actualizar la seguridad de sus infraestructuras en función de las necesidades que se hayan determinado. El programa en sí no financia la mejora de la protección de infraestructuras críticas. Los préstamos de las instituciones financieras podrían emplearse a fin de mejorar la seguridad de las infraestructuras en los Estados miembros, a partir de las necesidades determinadas mediante el programa, y a aplicar normas comunes. La Comisión estaría dispuesta a apoyar estudios sectoriales que permitan evaluar los posibles costes financieros para la industria de la mejora de la seguridad de las infraestructuras.

La Comisión financia proyectos de investigación que contribuyan a la protección de las infraestructuras críticas a través de la Acción preparatoria relativa a la investigación sobre seguridad (2004-2006)[2] y contempla actividades más sustanciales en el ámbito de la investigación sobre seguridad a través de su Propuesta de Decisión del Parlamento Europeo y del Consejo relativa al 7º Programa Marco de Investigación (COM(2005) 119 final)[3] y su Propuesta de Decisión del Consejo relativa al Programa Específico «Cooperación» por el que se ejecuta el Séptimo Programa Marco (COM(2005) 440 final). Una investigación específicamente destinada a elaborar estrategias prácticas o instrumentos de reducción del riesgo es de importancia primordial para la seguridad de las infraestructuras críticas de la UE a medio y largo plazo. Toda la investigación sobre seguridad, incluida la efectuada en este ámbito, se someterá a revisión ética a fin de garantizar su compatibilidad con la Carta de Derechos Fundamentales. La demanda de investigación sólo puede ir en aumento a medida que crezcan las interdependencias entre infraestructuras.

Preguntas

¿Cuál sería su estimación sobre el coste y las repercusiones de la aplicación de las medidas propuestas en este Libro Verde para las administraciones y las empresas? ¿Son, a su juicio, proporcionados?

9.4. Evaluación y control

La evolución y el control de la aplicación del PEPIC conduce a un proceso en múltiples niveles que requerirá la participación de todos los agentes interesados:

- **en el ámbito de la UE, podría establecerse un mecanismo de evaluación paritaria** que permitiera a los Estados miembros y la Comisión colaborar a la hora de evaluar el grado global de aplicación del PEPIC en cada Estado miembro. Podrían elaborarse informes anuales de la Comisión sobre la aplicación del PEPIC.

- **la Comisión informaría anualmente a los Estados miembros y a las demás instituciones** por medio de un documento de trabajo de sus servicios.

- **en el ámbito de los Estados miembros, el OCNP de cada uno podría supervisar la aplicación global del PEPIC en su ámbito competencial y garantizar el cumplimiento de los programas nacionales y los programas específicos sectoriales de PIC**, a fin de garantizar su aplicación efectiva, mediante informes anuales al Consejo y la Comisión.

La aplicación del PEPIC sería un proceso dinámico, en constante evolución y sometido a evaluación a fin de mantenerlo actualizado y aprovechar las experiencias que de él se obtengan. Las evaluaciones paritarias y los informes de supervisión de los Estados miembros podrían formar parte de los instrumentos empleados a fin de revisar el PEPIC y proponer nuevas medidas para una mejor protección de las infraestructuras críticas.

---

2 La propuesta presupuestaria de la Comisión para actividades relativas a la seguridad y el espacio dentro del 7º Programa Marco de IDT asciende a 570 millones de euros (COM(2005)119 final).

3 El importe total de los créditos inscritos en los presupuestos 2004 y 2005 ascendió a 30 millones de euros. Para 2006, la Comisión ha propuesto un importe de 24 millones de euros, actualmente sometido a examen por la autoridad presupuestaria.

Los Estados miembros facilitarían a la Comisión datos sobre las ICE con vistas a la elaboración de evaluaciones conjuntas de la vulnerabilidad, planes de gestión de las consecuencias, normas comunes para la protección de las infraestructuras críticas, prioridades en materia de investigación y, en su caso, reglamentación y armonización. Los datos serían clasificados y tratados de manera estrictamente confidencial.

La Comisión podría supervisar las diversas iniciativas de los Estados miembros y, en particular, las que contemplen consecuencias financieras para aquellos propietarios y operadores que no sean capaces de restablecer servicios fundamentales para los ciudadanos en un plazo máximo determinado.

Pregunta

¿Qué tipo de mecanismo de evaluación sería necesario para el PEPIC? ¿Bastaría con este mecanismo?

Las respuestas deben enviarse a más tardar el 15 de enero de 2006 a la siguiente dirección de correo electrónico: **JLS-EPCIP@cec.eu.int**. Las respuestas se considerarán confidenciales, salvo en caso de que el remitente declare explícitamente que desea hacerlas públicas, en cuya circunstancia la Comisión las publicará en su sitio de Internet.

ANNEXES

ANNEX 1

CIP TERMS AND DEFINITIONS

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

Alert

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

Critical infrastructure protection (CIP)

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

Critical Information Infrastructure (CII):

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

Critical Information Infrastructure Protection (CIIP)

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

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

Contingency plan

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

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

Critical Information

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

Critical Infrastructure (CI)

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

There are three types of infrastructure assets:

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

Essential service

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

European critical infrastructure (ECI)

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

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

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

Impact

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

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

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

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

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

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

  – Interdependency (between other critical infrastructure elements).

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

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

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

Interdependency

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

Occurrence

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

Operator Security Plan

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

Prevention

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

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

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

Response

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

Risk

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

Threat

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

Vulnerability

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

ANNEX 2

INDICATIVE LIST OF CRITICAL INFRASTRUCTURE SECTORS

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

ANNEX 3

OPERATOR SECURITY PLAN

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

Introduction)

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

Detailed part *(classified)*

– **Presentation of the operator**

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

– **Legal context**

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

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

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

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

– **Formalisation of security requirements**

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

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

– **Risk analysis and management**

The operator conducts and risk analysis concerning each critical point.

– **Security measures**

The operator presents the security measures arranged around two headings:

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

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

– **Presentation and application**

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

– **Monitoring and updating**

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