COMISIÓN DE LAS COMUNIDADES EUROPEAS

Bruselas, 20.10.2004
COM(2004) 702 final

COMUNICACIÓN DE LA COMISIÓN AL CONSEJO Y AL PARLAMENTO EUROPEO

Protección de las infraestructuras críticas en la lucha contra el terrorismo

ÍNDICE

1. INTRODUCCIÓN

El Consejo Europeo de junio de 2004 pidió a la Comisión y al Alto Representante que prepararan una estrategia global para proteger las infraestructuras críticas.

La presente Comunicación describe las acciones que la Comisión adopta actualmente para proteger las infraestructuras críticas y propone medidas adicionales para consolidar los instrumentos existentes y cumplir los mandatos del Consejo Europeo.

2. LA AMENAZA

El potencial de ataques terroristas catastróficos contra infraestructuras críticas está en aumento. Las consecuencias de un ataque contra los sistemas industriales de control de las infraestructuras críticas podrían ser muy variadas. Se da por supuesto que un ataque cibernético causaría pocas víctimas o ninguna, pero que podría acarrear la pérdida de servicios de infraestructura vitales. Por ejemplo, un ciberataque contra la red de conmutación telefónica pública podría dejar a los clientes sin servicio telefónico mientras los técnicos reajustan y reparan la red. Un ataque contra los sistemas de control de una planta química o de gas natural licuado podría causar más víctimas humanas junto con daños físicos significativos.

Otro tipo de fallo catastrófico de infraestructuras se produciría cuando una parte de la infraestructura indujera el fallo de otras partes, en un amplio efecto de cascada. Estos fallos podrían darse por un efecto sinérgico entre industrias de infraestructura. Un ejemplo simple sería un ataque contra centrales eléctricas que interrumpiera la distribución de electricidad: podrían pararse también las depuradoras y las centrales de suministro de agua, ya que podrían caerse las turbinas y demás maquinaria eléctrica de estas instalaciones.

Los efectos en cascada pueden ser muy dañinos, provocando grandes caídas de los servicios públicos. Los cortes de electricidad ocurridos en Norteamérica y en Europa en los últimos dos años demuestran la vulnerabilidad de las infraestructuras energéticas, y con ello la necesidad de encontrar medidas eficaces de prevención o atenuación de las consecuencias de una masiva interrupción del suministro. Este ciberterrorismo podría además amplificar los efectos de un ataque físico. Un ejemplo sería un ataque convencional contra un edificio, combinado con un corte temporal del servicio eléctrico o telefónico. El consiguiente retraso de la respuesta de urgencia, en tanto llegan y se ponen en marcha los sistemas de reserva, aumentaría el número de víctimas y el pánico de la población.

3. LAS INFRAESTRUCTURAS CRÍTICAS EN EUROPA

3.1. ¿Qué se entiende por infraestructura crítica?

Las infraestructuras críticas son aquellas instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya interrupción o destrucción tendría un impacto mayor en la salud, la seguridad o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de los gobiernos de los Estados miembros. Las infraestructuras críticas están presentes en numerosos sectores de la economía: actividades bancarias y financieras, transporte y distribución, energía, servicios, salud, abastecimiento de alimentos, comunicaciones, administraciones públicas clave. Algunos elementos críticos de estos sectores no son

"infraestructuras" en sentido estricto, sino que son redes o cadenas de suministro que contribuyen a la entrega de un producto o servicio esenciales. Así, por ejemplo, el suministro de alimentos y agua a las grandes zonas urbanas depende de algunas instalaciones clave, pero también de una compleja red de productores, procesadores, fabricantes, distribuidores y minoristas.

Serían infraestructuras críticas las siguientes:

- Centrales y redes de energía (por ejemplo electricidad, producción de petróleo y gas, instalaciones de almacenamiento y refinerías, sistemas de transmisión y distribución)

- Tecnologías de las comunicaciones y la información (por ejemplo telecomunicaciones, sistemas de radiodifusión, programas informáticos, soporte físico y redes, incluido Internet)

- Finanzas (por ejemplo banca, valores e inversión)

- Salud (por ejemplo hospitales, centros de atención sanitaria y de suministro de sangre, laboratorios y empresas farmacéuticas, búsqueda y rescate, servicios de urgencia)

- Alimentación (por ejemplo seguridad alimentaria, medios de producción, mayoristas, industria alimentaria)

- Agua (por ejemplo embalses, almacenamiento, tratamiento, redes)

- Transporte (por ejemplo aeropuertos, puertos, instalaciones intermodales, ferrocarril, redes de transporte público, sistemas de control de tráfico)

- Producción, almacenamiento y transporte de mercancías peligrosas (por ejemplo materiales químicos, biológicos, radiológicos y nucleares)

- Estado (por ejemplo servicios críticos, instalaciones, redes de información, activos, sitios y monumentos principales)

Estas infraestructuras pueden ser de propiedad o gestión tanto del sector público como del sector privado. Sin embargo, en su Comunicación 574/2001, de 10 de octubre de 2001, la Comisión ha declarado que el refuerzo de determinadas medidas de seguridad por los poderes públicos como consecuencia de los ataques dirigidos contra la sociedad en su conjunto y no contra las empresas debe correr a cargo del Estado. El sector público tiene, por tanto, un papel fundamental.

Las infraestructuras críticas deberán ser definidas a nivel de los Estados miembros y a nivel europeo y las listas correspondientes deberán quedar establecidas para finales de 2005.

Las infraestructuras críticas europeas están muy interconectadas y son sumamente interdependientes. A esta situación han contribuido la consolidación corporativa, la racionalización industrial, prácticas de eficiencia empresarial como la fabricación *just-in-time*, y la concentración de la población en las zonas urbanas. Estas infraestructuras críticas dependen cada vez más de tecnologías de la información como Internet y la radionavegación y la comunicación por satélite. Los problemas pueden desencadenarse en cascada a través de estas infraestructuras interdependientes, ocasionando fallos inesperados y cada vez más

graves de los servicios esenciales. La interconexidad y la interdependencia las hacen más vulnerables a la interrupción o a la destrucción.

Será preciso estudiar los criterios que permitan determinar qué factores confieren carácter crítico a una infraestructura o elemento de infraestructura particular. Estos criterios de selección deberían basarse en conocimientos sectoriales y generales. Pueden adelantarse tres factores de identificación de una infraestructura crítica potencial:

- Alcance - la pérdida de un elemento de infraestructura crítico se mide por el tamaño del área geográfica que pudiera verse afectada por su pérdida o indisponibilidad - internacional, nacional, provincial/territorial o local.
- Magnitud - el grado del impacto o de la pérdida puede evaluarse como nulo, mínimo, moderado o principal. Entre los criterios que podrían utilizarse para evaluar la magnitud potencial se encuentran los siguientes:
    (a) Impacto público (cantidad de población afectada, pérdidas de vidas, enfermedades, lesiones graves, evacuación);
    (b) Económico (efecto PIB, volumen de pérdida económica y/o degradación de productos o servicios);
    (c) Ambiental (impacto en el lugar y sus alrededores);
    (d) Interdependencia (con otros elementos de infraestructura críticos).
    (e) Político (confianza en la capacidad de las administraciones públicas);
- Efectos en el tiempo - estos criterios determinan en qué plazo la pérdida de un elemento podría tener un impacto importante (inmediato, 24-48 horas, una semana, otros).

Sin embargo, en muchos casos los efectos psicológicos pueden potenciar hechos en sí mismo menores.

El estado actual de los avances en materia de protección de infraestructuras críticas figura en el anexo técnico, que resume, por sectores, las realizaciones de la Comisión. Como se puede observar, la Comisión ha adquirido una experiencia considerable en la materia.

3.2. Gestión de la seguridad

Para efectuar el análisis de las amenazas, incidencia y vulnerabilidad de los elementos de infraestructura críticos de los Estados miembros y sus dependencias es necesaria una información procedente de fuentes diversas. Cada sector y cada Estado miembro deberán identificar las infraestructuras que les son críticas en sus territorios respectivos, según una fórmula armonizada a nivel UE, así como los organismos o personas responsables de su seguridad.

No es posible proteger todas las infraestructuras contra todas las amenazas. Por ejemplo, las redes de transmisión de electricidad son tan extensas que no resulta posible vallarlas o vigilarlas. Sin embargo, mediante técnicas de gestión de riesgos se puede focalizar la atención en los puntos de máximo riesgo, teniendo en cuenta la amenaza, el carácter crítico relativo, el nivel actual de seguridad y la eficacia de las estrategias disponibles de reducción de daños para asegurar la continuidad de los servicios.

La gestión de la seguridad es un proceso deliberado de análisis del riesgo y de decisión y ejecución de acciones con objeto de reducir el riesgo a un nivel definido, es decir, un nivel de riesgo aceptable a un coste aceptable. Este planteamiento se caracteriza por la identificación, la medición y el control de los riesgos a un nivel equivalente a un nivel predeterminado.

La protección de infraestructuras críticas (PIC) requiere un partenariado firme y cooperativo entre los propietarios y gestores de infraestructuras críticas y las autoridades de los Estados miembros. La responsabilidad principal de la gestión del riesgo en las instalaciones físicas, cadenas de suministro, tecnologías de la información y redes de comunicaciones corresponde a sus propietarios y gestores.

Deberán publicarse alertas, avisos y notas de información que ayuden a los responsables de los sectores público y privado a proteger los principales sistemas de infraestructuras. En ocasiones aparecerán riesgos o amenazas específicos de ataques terroristas que exigirán respuesta inmediata. Los gobiernos y las empresas de los Estados miembros deberán dar entonces una respuesta operativa precisa y bien coordinada. En tales circunstancias, la UE debería coordinar las respuestas políticas necesarias, y sobre esa base se acordarán con las partes interesadas mecanismos detallados de apoyo caso por caso.

Pero sin una buena aplicación, los mejores planes y leyes de gestión de la seguridad no sirven para nada. La experiencia demuestra que el único instrumento eficaz para garantizar la aplicación correcta de los requisitos de seguridad son las inspecciones independientes realizadas por la Comisión.

4. AVANCES EN LA PROTECCIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS A NIVEL COMUNITARIO

Los europeos esperan que las infraestructuras críticas sigan funcionando independientemente de quiénes sean sus propietarios o gestores. Esperan que los Gobiernos y la UE asuman el liderazgo y aseguren que así sea. Esperan que las administraciones en todos sus niveles y los propietarios y gestores privados cooperen para garantizar la continuidad de los servicios en los que confían.

Como complemento a las medidas adoptadas a nivel nacional, la Unión Europea ha adoptado ya medidas legislativas que establecen normas mínimas de protección de las infraestructuras en el marco de sus políticas. Se trata, en particular, del transporte, las comunicaciones, la energía, la medicina y la seguridad del trabajo, y la salud pública. Estas actuaciones han recibido nuevo impulso tras los recientes atentados en América y Europa. Con ello se mejoran o amplían medidas ya existentes.

Desde hace décadas, en el marco del Tratado Euratom, se realizan inspecciones para vigilar el buen uso de los materiales nucleares. En materia de protección contra la radiación existe todo un corpus de legislación aplicable a los riesgos relacionados con el funcionamiento de las instalaciones y el uso de fuentes en las que estén presentes sustancias radiactivas.

En materia de transporte internacional, la Unión Europea ha adoptado disposiciones legislativas que aplican o refuerzan los acuerdos alcanzados por los organismos internacionales de aviación y transporte marítimo. La Unión Europea seguirá promoviendo estas actividades a nivel internacional y participando activamente en ellas, y procurará que los países terceros que mantienen relaciones económicas con la UE apliquen dichos acuerdos. A

algunos de estos países se les ha proporcionado ayuda con el fin de alcanzar un nivel homogéneo y coherente de seguridad dentro y fuera de las fronteras de la UE.

Un nuevo paso es la creación de entidades como la Agencia Europea de Seguridad de las Redes y de la Información (ENISA) en materia de seguridad de las comunicaciones. Además, en sectores como la aviación y la seguridad marítima, la Comisión ha creado servicios de inspección para supervisar la aplicación de la legislación de seguridad en los Estados miembros. Estas inspecciones están generando los instrumentos de evaluación necesarios para garantizar un mismo nivel de aplicación en toda la Unión.

Es estado actual de la protección de las infraestructuras críticas figura en el anexo técnico, que describe, por sectores, las realizaciones de la Comisión. Como se puede observar, la Comisión ha adquirido una considerable experiencia en la materia.

5. MEJORA DE LA CAPACIDAD DE PROTECCIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS DE LA UE

5.1. Un programa europeo para la protección de infraestructuras críticas

Dado el gran número de infraestructuras críticas potenciales y sus propias particularidades, es imposible protegerlas todas a través de medidas europeas. Aplicando el principio de subsidiariedad, Europa debe centrar sus esfuerzos en la protección de aquellas infraestructuras que tienen efectos transfronterizos y dejar las demás a la entera responsabilidad de los Estados miembros, aunque en un marco común.

Existen ya numerosos reglamentos y directivas que obligan a dotarse de medios de detección de accidentes, a establecer planes de intervención en cooperación con la defensa civil, a efectuar ejercicios periódicos y a crear vinculaciones claras entre los diversos niveles de intervención: poderes públicos, organismos centrales y servicios de urgencia. Pero queda mucho por hacer en materia de protección de instalaciones energéticas que no sean las nucleares. Según se observa en el anexo técnico, existe un acervo comunitario para la protección de las infraestructuras críticas, en fases de desarrollo variables.

En la mayoría de los ámbitos arriba mencionados se sigue trabajando; se ha establecido una cooperación con los expertos de los Estados miembros y con los sectores económicos concernidos a fin de identificar posibles fallos y medidas de corrección (legislativas u otras). Se han establecido numerosas redes y comités de seguridad.

La Comisión informará anualmente a las demás instituciones por medio de una Comunicación. Analizará sector por sector los avances de los trabajos comunitarios en materia de evaluación de riesgos, desarrollo de técnicas de protección, normativa en curso o prevista, con objeto de recoger sus opiniones. La Comisión propondrá en esta Comunicación, cuando proceda, las actualizaciones y medidas organizativas horizontales necesitadas de armonización, coordinación o cooperación. La Comunicación, que integrará todos los análisis y medidas sectoriales, servirá de base para un programa europeo de protección de las infraestructuras críticas (PEPIC).

Este programa ayudará a las empresas y a las administraciones públicas de los Estados miembros, respetando al mismo tiempo sus mandatos y responsabilidades individuales. La Comisión considera que es preciso crear lo antes posible, en 2005, una red que agrupe a los especialistas PIC de los Estados miembros y que colabore con la Comisión en la elaboración

del programa: la red de información sobre alertas en infraestructuras críticas (Critical Infrastructure Warning Information Network, CIWIN).

La creación de esta red contribuiría ante todo a fomentar el intercambio de información sobre amenazas y vulnerabilidades compartidas, y sobre medidas y estrategias para atenuar los riesgos. Los Estados miembros, a su vez, asegurarían el traslado de la información pertinente a todos los departamentos y organismos gubernamentales concernidos, en particular a las organizaciones de servicios de emergencia, e informarían a los organismos correspondientes del sector privado, lo cuales informarían a los propietarios y gestores de las infraestructuras críticas a través de una red de contactos establecida en cada Estado miembro.

El programa PEPIC promovería un foro permanente en el que los problemas de competencia, responsabilidad y sensibilidad de las informaciones quedarían compensados con las ventajas de una infraestructura crítica más segura. En este proceso, las empresas serían atentamente escuchadas. Contribuiría a mejorar la información de las partes sobre situaciones de amenaza específicas, permitiéndoles así tomar medidas frente a sus consecuencias potenciales. Lo que no cambiaría es la responsabilidad de los propietarios y gestores, los cuales deberán adoptar sus propias decisiones y planes para proteger sus activos.

Donde no existan normas sectoriales o no se hayan establecido aún normas internacionales, el Comité Europeo de Normalización (CEN) y otras entidades de normalización podrían ayudar a la red y proponer normas uniformes de seguridad a nivel sectorial así como estándares adecuados para las ramas y sectores en cuestión. Normas que deberían proponerse también a nivel internacional a través de la ISO, con objeto de establecer condiciones de competencia equitativas.

Toda referencia a amenazas de seguridad a las infraestructuras críticas, incluido el terrorismo, debe ser cautelosa para evitar alarmas innecesarias tanto en la propia UE como entre turistas e inversores potenciales. El terrorismo es una amenaza constante, pero es obligación de los dirigentes políticos animar a todos los ciudadanos a seguir viviendo lo más tranquilamente posible. Es preciso asimismo asegurar el respeto del derecho a la intimidad, tanto dentro como fuera de la Unión. Los consumidores y los operadores deben tener garantías de que la información será manejada de forma exacta, confidencial y segura. Se necesita un marco adecuado para asegurar que la información clasificada sea correctamente gestionada y protegida contra usos o revelaciones no autorizados.

Son numerosas las infraestructuras críticas de la UE y de los Estados miembros que desbordan las fronteras de la UE. Los oleoductos atraviesan los continentes, y cables vitales para los servicios de tecnología de la información se hallan profundamente enterrados en el fondo de los océanos... Por tanto, la cooperación internacional es un componente importante para el establecimiento de partenariados nacionales e internacionales permanentes y dinámicos entre los propietarios y gestores de infraestructuras críticas y los Gobiernos de terceros países, especialmente aquellos que son proveedores directos de productos energéticos a la Unión.

5.2. Implementación del PEPIC

La protección de las infraestructuras críticas exige la participación activa de los propietarios y gestores de infraestructuras, los reguladores, las asociaciones profesionales y empresariales, los Estados miembros y la Comisión. Basándose en la información suministrada por los corresponsales de los Estados miembros y la red, los objetivos del PEPIC serán los siguientes:

continuar la identificación de las infraestructuras críticas, analizar su vulnerabilidad e interdependencia, y presentar soluciones que protejan y preparen para todo tipo de peligros. Deberá ayudar a las empresas a integrar las variables de la amenaza y sus consecuencias en sus evaluaciones del riesgo. Las fuerzas del orden y de protección civil de los Estados miembros deberían integrar el PEPIC en sus tareas de planificación e información.

En estrecha coordinación con la red, los servicios de la Comisión desarrollarán nuevas medidas consistentes en la adopción de legislación y/o la difusión de información. El Grupo de Trabajo de los jefes de policía y Europol tendría un papel decisivo en la difusión de los niveles de seguridad y de los datos de inteligencia a las fuerzas del orden de los Estados miembros, las que a su vez deberán asesorar y coordinar a los propietarios y gestores de infraestructuras críticas facilitándoles adecuada información sobre las amenazas, y proporcionándoles aseroramiento sobre medidas y estrategias de prevención del terrorismo.

Los Gobiernos de los Estados miembros deberán seguir desarrollando y manteniendo bases de datos sobre las infraestructuras críticas significativas en el plano nacional y serían responsables de la elaboración, validación y auditoría de los planes correspondientes, asegurando así la continuidad de los servicios bajo su mando. En la formulación del PEPIC, la Comisión presentará indicaciones sobre el contenido y el formato mínimos de estas bases y su interconexión.

Los Gobiernos de los Estados miembros, a su vez, seguirán informando a los propietarios y gestores (y, cuando proceda, a otros Estados miembros) sobre inteligencia y alertas, así como del tipo de respuesta que se espera de cada instancia según los niveles de amenaza o de alerta.

Los propietarios y gestores de infraestructuras críticas deberán hacerse cargo de la adecuada seguridad de sus activos aplicando activamente sus planes de seguridad y efectuando de forma periódica inspecciones, ejercicios, evaluaciones y planes. Los Estados miembros deberán supervisar el proceso global, mientras que la Comisión garantizaría, mediante sistemas de inspección adecuados, la uniformidad de la aplicación en toda la Unión.

5.3. Objetivos e indicadores de resultados del PEPIC

El objetivo del PECIP y el deber de la Comisión serían asegurar niveles adecuados e iguales 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 PEPIC sería un proceso permanente que requerirá revisiones periódicas para anticipar los problemas y preocupaciones de la sociedad.

Los indicadores de éxito serían los siguientes:

- Identificación y establecimiento, por parte de los Gobiernos de los Estados miembros, de listas de las infraestructuras críticas de sus territorios, según las prioridades elaboradas por el PEPIC;

- Colaboración de las empresas por sectores y con las administraciones públicas para compartir información y reducir la probabilidad de incidentes que ocasionen caídas muy amplias o prolongadas de las infraestructuras críticas;

- La Comunidad Europea se dota de un planteamiento común para la seguridad de las infraestructuras críticas mediante la cooperación de todos los actores, tanto públicos como privados.

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.