ieee.es
Instituto Español de Estudios Estratégicos

Documento
Análisis

021/2011 27 de julio de 2011

María José Caro Bejarano

LA PROTECCIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS

LA PROTECCIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS

Resumen:

La protección de las infraestructuras críticas es una preocupación de los Estados desarrollados. El alto nivel de desarrollo de las sociedades occidentales descansa en su mayor parte en una serie de servicios básicos y esenciales cuya prestación radica mayoritariamente en el sector privado. Garantizar la seguridad de los suministros de estos servicios básicos ante nuevas amenazas es una responsabilidad no sólo de las administraciones públicas sino que es necesaria la concienciación y colaboración de los operadores privados. En este documento se presenta el concepto de infraestructura crítica y su tratamiento a nivel internacional y nacional.

Palabras clave:

Infraestructuras críticas, protección, estrategia española de seguridad.

Summary:

Critical infrastructures protection is one of the developed states concerns. High level development of western societies lies mostly in a series of basic and essential services, whose provision stems from private sector. The responsibility to guarantee the supplies security to new threats corresponds not only to the administration but it is also necessary the awareness and collaboration of privates suppliers. This document addresses the concept of critical infrastructure and its treatment at international and national level.

Key words:

Critical infrastructures, protection, Spanish Security Strategy.

1. QUÉ SE ENTIENDE POR INFRAESTRUCTURA CRITICA.

Las infraestructuras son necesarias para el funcionamiento normal de los servicios básicos y los sistemas de producción de cualquier sociedad. De tal manera que cualquier interrupción no deseada, ya sea debida a causas naturales, técnicas, ya sea por ataques deliberados, tendrían graves consecuencias en los flujos de suministros vitales o en el funcionamiento de los servicios esenciales, aparte de ser una fuente de perturbaciones graves en materia de seguridad.

Hoy en día una de las fortalezas de las sociedades de Occidente es al mismo tiempo una debilidad, es decir, las sociedades desarrolladas y altamente tecnificadas dependen en extremo de una serie de servicios esenciales, sin los cuales no hay capacidad de subsistencia. Pensemos en servicios tales como el sistema de transportes, el agua, la electricidad, las telecomunicaciones, etc. Por este motivo, hace unos años se acuñó el término infraestructura crítica para referirse a la prestación de estos servicios básicos imprescindibles, junto a la necesidad de su protección.

Los estados modernos se enfrentan actualmente a multitud de desafíos que afectan a su seguridad nacional. Estos nuevos riesgos, que provienen muchos de ellos de la globalización, como el terrorismo internacional, la proliferación de armas de destrucción masiva, el cambio climático o el crimen organizado, se suman a los ya existentes, como el terrorismo tradicional.

Dentro de las prioridades estratégicas de la seguridad nacional se encuentran las infraestructuras, expuestas a una serie de amenazas, para cuya protección se hace imprescindible, por un lado, catalogarlas y, por otro, diseñar un plan con medidas eficaces de prevención y protección contra las posibles amenazas hacia tales infraestructuras, tanto en el plano de la seguridad física como en el de la seguridad de las tecnologías de la información y las comunicaciones.

2. TRATAMIENTO DE LA PROTECCIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS EN EL ÁMBITO INTERNACIONAL

Después del 11 de septiembre de 2001 cambió el escenario de la seguridad mundial. Se configuró un panorama en el que la destrucción o alteración de ciertos objetivos podrían afectar a la vida, salud y bienestar tanto de los ciudadanos como de los Estados. El tratamiento tradicional de la seguridad con relación a estos objetivos ha cambiado completamente, hasta entonces la seguridad era una competencia pública y exclusiva del

Estado, sin embargo, las infraestructuras críticas están en su mayoría en el sector privado, y este sector tiene también una responsabilidad en este ámbito. En el caso de Estados Unidos y tras el 11S se reaccionó con la creación del Departamento de Seguridad Interior[1] y una nueva y amplia regulación de esta materia. A nivel europeo la iniciativa surgió a raíz del 11M. Tras instar el Consejo Europeo a la Comisión Europea a elaborar una estrategia global sobre protección de infraestructuras críticas, se adoptó una "Comunicación sobre protección de las infraestructuras criticas en la lucha contra el terrorismo", con propuestas para mejorar la prevención, preparación y respuesta de Europa frente a atentados terroristas.

Posteriormente se elaboró una Directiva *sobre la* identificación *y designación de infraestructuras Criticas Europeas y* la evaluación *de la necesidad de mejorar su protección* (Directiva 2008/114/CE), que entró en vigor el 12 de enero de 2009. Esta Directiva establece, entre otras cosas, que la responsabilidad principal y última de proteger las infraestructuras críticas corresponde a los Estados miembros y a los operadores de las mismas, e insta a la implantación de una serie de iniciativas y actuaciones por parte de los Estados para su transposición a las legislaciones nacionales.

3. TRATAMIENTO DE LA PROTECCIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS EN EL ÁMBITO NACIONAL

España, debido al terrorismo interior, está más adelantada en esta materia respecto a Europa. En mayo de 2007 la Secretaría de Estado de Seguridad del Ministerio del Interior aprobó un *Plan* Nacional *para* la *Protección de* las *Infraestructuras Criticas,* elaboró el primer Catálogo *Nacional de Infraestructuras* Estratégicas[2], y el Consejo de Ministros aprobó en noviembre de 2007 un *Acuerdo* sobre *Protección de Infraestructuras Críticas.*

Recientemente, en abril de este año, se ha promulgado la Ley 8/2011 de Protección de Infraestructuras Críticas (LPIC)[3] y poco tiempo después, en mayo, el Real Decreto 704/2011 con el Reglamento de protección de las infraestructuras críticas[4]. De este modo, existe ya una normativa con rango de ley sobre la que se sustentan dichas iniciativas, que establece con claridad las responsabilidades y obligaciones de los diferentes agentes involucrados en su protección a nivel nacional.

[1] Department of Homeland Security. Véase: http://www.dhs.gov/files/programs/editorial_0827.shtm
[2] La custodia del catálogo pertenece al CNPIC, véase en: http://www.cnpic.es/index.html.
[3] Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, (más conocida ya como LPIC).
[4] Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.

El fin primordial de la ley y del reglamento es el establecimiento de una serie de medidas en materia de protección de infraestructuras críticas que proporcionen un soporte adecuado sobre el que se asiente una eficaz coordinación de las administraciones públicas y de las entidades y organismos gestores o propietarios de infraestructuras que presten servicios esenciales para la sociedad, con el fin de lograr una mejor seguridad global. Estos servicios se asientan en 12 sectores estratégicos, subdivididos a su vez en subsectores, ámbitos y segmentos: Administración, Alimentación, Energía, Espacio, Sistema Financiero y Tributario (por ejemplo, banca, valores e inversiones), Agua (embalses, almacenamiento, tratamiento y redes), Industria Nuclear, Industria Química, Instalaciones de Investigación, Salud, Tecnologías de la Información y las Comunicaciones y Transporte (aeropuertos, puertos, instalaciones intermodales, ferrocarriles y redes de transporte público, sistemas de control del tráfico).

Objetivos de la LPIC

La LPIC transpone a la legislación nacional las medidas incluidas en la *Directiva de la UE 2008/114/CE,* en concreto, la identificación y clasificación de las Infraestructuras Críticas Europeas y la implantación por parte de los operadores afectados de los pertinentes Planes de Seguridad del Operador y de la figura del Responsable de Seguridad y Enlace. Para ello, se cuenta con la participación de los Estados miembros que, deben garantizar el cumplimiento de estas obligaciones y avalar, tanto frente a terceros Estados como frente a la Comisión Europea, la idoneidad de los procedimientos y de los niveles de seguridad existentes en dichas infraestructuras.

Las Infraestructuras Críticas (IC), según se definen en la Ley 8/2011, es el conjunto de recursos, servicios, tecnologías de la información y redes, que en el caso de sufrir un ataque, causarían gran impacto en la seguridad, tanto física como económica, de los ciudadanos o en el buen funcionamiento del Gobierno de la Nación. Este impacto se mide según unos criterios horizontales que determinan la criticidad de una infraestructura. Se han establecido tres: el número potencial de victimas, el impacto económico y el impacto público.

La citada Ley tiene como objetivos primordiales, establecer las estrategias y las estructuras adecuadas que permitan dirigir y coordinar las actuaciones de los distintos órganos de las Administraciones Públicas en materia de protección de Infraestructuras Críticas, previa identificación y designación de las mismas, impulsando, además, la colaboración e implicación de los organismos gestores y propietarios de dichas infraestructuras, a fin de optimizar el grado de protección de éstas contra ataques deliberados de todo tipo. Asimismo, la presente Ley regula las especiales obligaciones que deben asumir tanto las

administraciones públicas como los operadores privados de aquellas infraestructuras que se determinen como Infraestructuras Críticas.

Los objetivos centrales de la ley son abordados en detalle, por el reglamento de desarrollo de aquella. Estos son:

- Establecer una terminología y un marco de referencia común en lo relativo a la protección de los activos contra ataques deliberados, que puedan ser utilizados tanto por los poderes públicos como por el sector privado.

- Crear una estructura organizativa a nivel nacional (el Sistema de Protección de Infraestructuras Críticas), en la que se distribuyan las funciones y responsabilidades que los diversos agentes, tanto públicos como privados, deben tener en el marco de la seguridad de las infraestructuras que proveen a la sociedad de los servicios esenciales, contando como pieza central del mismo con el CNPIC, como órgano director y coordinador. Se trata de afianzar el concepto de asociación público-privada y una base de confianza mutua entre el sector privado y los órganos públicos.

- Diseñar un sistema de planificación que se integre en una estrategia de seguridad que permita la interacción y el reparto de responsabilidades entre las Administraciones públicas y los operadores de infraestructuras críticas. Los instrumentos de este sistema de planificación serán el conjunto de planes que, comenzando por el Plan Nacional de Protección de las Infraestructuras Criticas y los Planes Estratégicos Sectoriales (los dos de carácter estratégico y responsabilidad del Estado), continuará por los Planes de Seguridad del Operador y los Planes de Protección Específicos (ambos con un alcance más limitado y responsabilidad de los titulares de infraestructuras críticas) y culminará con los Planes de Apoyo Operativo (de carácter operativo y responsabilidad de las Fuerzas y Cuerpos de Seguridad y, por tanto, de la Administración, de manera que quede así cerrado el sistema).

- Marcar hitos para la implantación de planes integrales de seguridad que contemplen las amenazas, de carácter físico y cibernético, contra los activos a proteger.

- Establecer una red de comunicaciones segura en la que se garantice la confidencialidad y protección de los datos existentes sobre las diferentes instalaciones sensibles y estén representados todos los agentes del Sistema de Protección de Infraestructuras Críticas. Todo ello, bajo la coordinación del CNPIC y teniendo como eje el Catálogo Nacional de Infraestructuras Estratégicas.

4. PRESENCIA EN LA ESTRATEGIA ESPAÑOLA DE SEGURIDAD

En el Consejo de Ministros de 24 de junio se aprobó la Estrategia Española de Seguridad. Esta estrategia, con un horizonte de una década y revisable cada cinco años, identifica las amenazas y riesgos más importantes para la seguridad y señala cómo responder a ellos. En su capítulo 4 aparecen contemplados las infraestructuras, suministros y servicios críticos. En concreto, considera que "fenómenos naturales extremos, atentados terroristas o *ciberataques*, entre otros de las amenazas y riesgos analizados, pueden dañar las infraestructuras críticas, suministros y servicios críticos que sustentan nuestra vida y el desenvolvimiento de nuestra sociedad. Debemos proteger y garantizar su normal funcionamiento para no perjudicar el bienestar y la economía de un país avanzado como el nuestro" [5].

A estas infraestructuras les puede afectar entre otros, el terrorismo, la inseguridad económica y financiera, la vulnerabilidad energética, las ciberamenazas. "Es preciso garantizar su funcionamiento y capacidad de resistencia y recuperación ante posibles amenazas".

En sus conclusiones, la Estrategia plantea crear un Consejo Español de Seguridad que incorpore a los ministros y altos cargos relevantes, que cuente con comisiones interministeriales que desarrollen áreas concretas y una unidad de apoyo en Presidencia del Gobierno.

Apuesta por promover la cooperación con las comunidades autónomas e impulsar un foro social de expertos como órgano consultivo. Asimismo, pide actualizar los instrumentos normativos necesarios, especialmente en lo referente a la gestión de las situaciones de crisis, la protección civil, los secretos oficiales y el planeamiento frente a emergencias y catástrofes. Además, se establecerá una Comisión Coordinadora para luchar contra el crimen organizado y se elaborarán estrategias sectoriales, entre las que cita una sobre ciberseguridad.

5. EL ASPECTO CIBERNETICO

Dado el alto nivel de dependencia de las infraestructuras del aspecto tecnológico, además de los ataques de tipo físico, la legislación contempla los ataques de tipo lógico. Es una realidad que un ataque a una infraestructura mediante medios lógicos puede igualar al realizado con

[5] La estrategia española de seguridad se puede consultar en la página web del IEEE: http://www.ieee.es/Galerias/fichero/RecursosInteres/Nacional/EstrategiaEspanolaSeguridad_junio2011.pdf .

medios físicos, en cuanto al cese o alteración de la provisión de un servicio. En este caso se engloban los denominados sistemas de supervisión, control y adquisición de datos (SCADA)[6], empleados en entornos industriales para la manipulación y control de componentes mecánicos[7].

El aspecto cibernético es una nueva capacidad de causar daño que no ha pasado desapercibida para los grupos terroristas y del crimen organizado, que lo han incluido como una clara alternativa para la comisión de sus atentados y delitos, respectivamente. Para mejorar la prevención y respuesta frente a ataques lógicos, los gobiernos están llevando a cabo distintas medidas, orientadas hacia la creación de centros de coordinación que aglutinen todo tipo de información relevante para una mejora de la protección de las infraestructuras críticas. España con la Ley 8/2011 ha apostado claramente por otro enfoque novedoso: abordar la protección de nuestras infraestructuras desde una perspectiva global donde se consideren todos los tipos de amenaza, y no solo las de carácter físico, sino también las cibernéticas. De esta forma, los planes que se diseñen en el marco de la ley y del reglamento deberán contemplar necesariamente en sus análisis de riesgos la integridad de la amenaza y las medidas adoptadas y propuestas para minimizar dicho riesgo[8].

Mª José Caro
Analista Principal del IEEE

[6] Recuérdese el ataque mediante el gusano Stuxnet a una de las centrales nucleares de Irán. Véase : https://www.ccn-cert.cni.es/index.php?option=com_content&view=article&id=2541%3Aics-cert-alerta-sobre-stuxnet&catid=5&Itemid=197&lang=es&filter=

[7] El Centro Criptológico Nacional apoya al CNPIC en el tratamiento de los ciberataques sobre infraestructuras críticas y en la actualización de información sobre vulnerabilidades SCADA e incidentes de seguridad informáticos relacionados con las mismas. Ha publicado una serie de guías SCADA que pueden consultarse en: https://www.ccn-cert.cni.es/index.php?option=com_content&view=article&id=2687&Itemid=211&lang=es

[8] Este aspecto también se contempla en la Estrategia Española de Seguridad donde las ciberamenazas son uno de los riesgos y el aspecto tecnológico es considerado como un potenciador del riesgo.