LA PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS

Mónica Miranzo y Carlos del Río[1]
UNISCI

Resumen:
Los ataques contra el World Trade Center en septiembre de 2001 pusieron de relevancia las nuevas amenazas y vulnerabilidades con las que los Estados deben lidiar en la actualidad al plantear la seguridad de las infraestructuras críticas. Un ataque de este tipo conlleva pérdidas tanto de vidas humanas como económicas, así como también afecta a la credibilidad política de los gobiernos. Sumado a la cada vez mayor demanda de unos recursos finitos y menguantes, así como un contexto de cambio climático y reajuste de la balanza de poder internacional, esta situación ha supuesto que las estrategias de seguridad nacionales de muchos países, entre ellos España, den una mayor importancia a la seguridad de las infraestructuras críticas. No obstante, a pesar de que la Estrategia de Seguridad Nacional tanto de 2009 como de 2013 ponen a España en línea con las directivas europeas al respecto, no hemos asistido a un desarrollo de la materia más allá de unas líneas de actuación generales.

Palabras clave: Infraestructuras críticas, Estrategia de Seguridad Nacional, España, nuevas amenazas, ciberseguridad.

***Title in English**:"The Protection of Critical Infrastructures"*

Abstract:
The attacks against the World Trade Center on 9/11 served to underscore the importance of the new threats and vulnerabilities with which States must currently deal when it comes to lay out the security of the critical infrastructures. An attack of this kind entails a loss both economic and of human life, as well as it affects political credibility of governments. Summed up with an ever growing demand of depleting and finite resources, as well as context of climate change and readjustment of the international power balance, this situation has supposed that the national security strategies of many countries, amongst them Spain, have vested a greater deal of importance to the critical infrastructure security dimension. However, although both the 2009 and 2013 National Security Strategy brought Spain in line with European directives on this matter, we have not witnessed a further development beyond general guidelines.

***Keywords:** Critical Infrastructures, Strategy of National Security, Spain, New Threats, Cybersecurity.*

[1] Mónica Miranzo Proy y Carlos del Río son investigadores junior de UNISCI y miembros del Foro Hispano-Argelino.

1. El contexto internacional y los nuevos desafíos a la seguridad

España vive en la actualidad en un contexto estratégico definido por la volatilidad global y regional, la emergencia de nuevos desafíos a la seguridad y el impacto de la crisis económica[2], factores que resultarán determinantes a la hora de definir su política de seguridad nacional.

El aumento de riesgos y amenazas no tradicionales, especialmente el terrorismo internacional y los ciberataques, han tenido como objetivos principales tanto a los individuos como a las infraestructuras, incrementando la vulnerabilidad del Estado y produciendo graves perturbaciones en el normal funcionamiento de la sociedad. Durante los últimos años se ha producido un aumento del número de ataques dirigidos específicamente a aquellos sectores de actividad o infraestructuras que proporcionan "servicios esenciales", de importancia vital para el desarrollo de la vida de los ciudadanos y sus actividades diarias, así como para la continuidad de las funciones del estado.

El alcance de los ataques terroristas del 11 de Septiembre de 2011 sobre el Worl Trade Center, el corazón financiero de los Estados Unidos, tuvo efectos devastadores en el tiempo, así como un gran impacto en términos de vidas humanas, impacto público, económico y político, con una gran pérdida de confianza en la capacidad de las instituciones públicas por parte de la población estadounidense.

También en el año 2007 Estonia, uno de los países más digitalizados del mundo en el que las elecciones parlamentarias se realizan mediante "voto electrónico", así como el 92% de las declaraciones de impuestos, más del 80% de los registros comerciales y el 97% de las transacciones bancarias[3], sufrió un ataque cibernético de tal magnitud contra distintas agencias gubernamentales, la policía, el primer banco del país y varios medios de comunicación, que desembocaron en una crisis nacional con pérdidas económicas irreparables para el país.

Así, aspectos como la ciberseguridad se han hecho más relevantes en los últimos años. De hecho, filtraciones al público general como el caso Snowden, han puesto de manifiesto la vulnerabilidad del ciberespacio y las telecomunicaciones, y la magnitud y escala de las infiltraciones a las que están expuestos por parte de actores estatales y no estatales.

Por otra parte, aumenta la importancia de, por un lado, la propia vulnerabilidad de los sistemas de información, y, por otro, las distintas y cada vez más complejas formas de explotar dichas vulnerabilidades para violar la seguridad de los sistemas. Recientemente, hemos conocido el gran agujero de seguridad, denominado "The Heartbleed Bug", que afecta a dos tercios de internet, debido a un fallo el algunas versiones del código de programación OpenSSL, utilizado por bancos, agencias de información y proveedores de diferentes servicios electrónicos entre otros, comprometiendo información sensible de millones de usuarios.

En este contexto de elevada dependencia de las sociedades modernas de determinadas infraestructuras cuya interrupción o destrucción tendría un impacto mayor en la salud, la

[2]"Preparing the December 2013 European Council on Security and Defence. Final Report by the High Representative/Head of the EDA on the Common Security and Defence Policy", p. 1, en http://eeas.europa.eu/statements/docs/2013/131015_02_en.pdf.

[3]Ganuza, Néstor: "Ciberdefensa. Una prioridad para la OTAN", *Revista Atenea*, nº 39 (septiembre 2012), pp. 54-57.

seguridad o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de los gobiernos de los Estados**,** han convertido a estas en un objetivo prioritario de las estrategias de seguridad estatales, apareciendo un nuevo concepto: el de "infraestructura crítica".

2. La protección de las infraestructuras críticas en el contexto europeo

En los últimos años se ha desarrollado en España y en la Unión Europea una conciencia respecto a la necesidad de estar preparados en el ámbito de la protección de infraestructuras críticas, especialmente a partir de los atentados del 11 de Marzo de 2004 sobre cuatro trenes de la red de Cercanías de Madrid[4].

La respuesta de la Unión Europea a los atentados de Madrid iba a suponer el inicio de un programa de trabajo que se aproximase a la protección de las infraestructuras críticas desde un punto de vista integral. Especialmente desde el establecimiento de un marco tanto legal como institucional que disponga de suficientes medios y cuente con actores preparados para prevenir riesgos y amenazas y, llegado el caso, intervenir para mitigar el impacto sobre la población, la economía y el territorio en caso de acontecimientos indeseables.

La aprobación de las directivas comunitarias "Prevención, preparación y respuesta a los ataques terroristas" y "Lucha contra el terrorismo: preparación y gestión de las consecuencias", pone de manifiesto la importancia de la protección de infraestructuras críticas en cuanto a objetivos terroristas. Pero será la directiva Comunicación 702 del 20 de Octubre de 2004 sobre "Protección de las infraestructuras críticas en la lucha contra el terrorismo" la que se centre en exclusiva en esta cuestión. Se trata de reconocer, tal y como lo expuso el Comisario de Justicia, Libertad y Seguridad, Franco Frattini, que:

"La seguridad y la economía de la Unión Europea, así como el bienestar de los ciudadanos están ligados a ciertas infraestructuras y servicios. (…) la interrupción de las mismas podría provocar la pérdida de vidas humanas y de bienes materiales, así como la merma de la confianza de los ciudadanos en la UE"[5].

La Comunicación 702 se encargará de dar los primeros pasos en la elaboración de una estrategia global de protección de infraestructuras críticas mediante la adopción de medidas homogeneizadoras y de una definición común:

"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"[6].

[4] "Informe Protección de Infraestructuras Críticas 2011", S2 Grupo, p. 7, en http://www.aeiseguridad.es/descargas/categoria6/4508139.pdf.

[5] "Boletín Quincenal de Información Europea, Europa-Euskadi", nº 210 (diciembre 2006), p. 21, en http://www.euskadi.net/contenidos/informacion/boletin_europa_euskadi/es_boletin/adjuntos/europa-euskadi-210.pdf.

[6] "Comunicación de la Comisión al Consejo y al Parlamento Europeo: "Protección de las infraestructuras críticas en la lucha contra el terrorismo", COM (2004) 702, Bruselas (20 de octubre del 2004), p. 3, en

Así como la descripción de aquellos riesgos y amenazas que enfrentan, destacando el terrorismo y el ciberterrorismo, que pueden tener efectos potencialmente devastadores a todos los niveles de seguridad si se origina un ataque combinado (físico y cibernético) o un efecto de cascada (por un efecto sinérgico entre industrias de infraestructuras interdependientes)[7]. Además, dado que la protección de las infraestructuras críticas depende en su mayor parte de los estados miembros, la directiva ofrece las pautas y criterios de identificación de aquellos factores que determinan el carácter crítico a una infraestructura o al elemento de una infraestructura.

Cabe destacar también, el rol prioritario del sector público como proveedor de seguridad incluso cuando las infraestructuras críticas se encuentran en manos de operadores privados, sin que esto suponga un agravio a la necesaria cooperación público-privada. La estrategia apuesta, además, por un enfoque preventivo con un papel fundamental de la gestión de la seguridad, que permiten el control de las infraestructuras más extensas mediante un sistema de técnicas de gestión de riesgos que sea capaz de identificar de forma efectiva aquellos puntos de máximo riesgo donde se concentrará la protección.

Pero, sin duda, el gran logro de la Comunicación en este ámbito será la puesta en marcha del Programa Europeo de Protección de Infraestructuras Críticas (PEPIC), con el objetivo de promover la creación de listas de infraestructuras críticas por parte de los Estados miembros en su territorio, preparar los análisis de vulnerabilidad y evaluación del riesgo, presentar soluciones y medidas de protección y fomentar la colaboración entre las empresas y las administraciones públicas en la protección de infraestructuras.

El objetivo de la Unión Europea es el de establecer una diferenciación entre las infraestructuras con efectos transfronterizos, que mediante el principio de subsidiariedad[8] quedarán debajo del paraguas de la Unión, y aquellas que son responsabilidad exclusiva de los Estados miembros. A la vez se establece un marco común de actuación y se crea la red de información sobre alertas en infraestructuras críticas (Critical Infrastructure Warning Information Network, CIWIN), con el objetivo de compartir información sobre amenazas comunes y estrategias de gestión de riesgos, y el Comité Europeo de Normalización (CEN)[9], para homogeneizar los marcos regulatorios sectoriales.

Para terminar de completar esta estrategia global de protección de infraestructuras críticas, la Unión Europea aprobará el 8 de Diciembre de 2008 la Directiva 2008/114/CE del Consejo sobre "La identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección"[10], centrado en la protección de las infraestructuras de carácter transfronterizo en los ámbitos de la energía y el transporte, cuya seguridad afecta a toda la Unión teniendo en cuenta el elevado grado de interdependencia de las redes europeas. Se desarrolla así el concepto de "infraestructura crítica europea" o "ICE", definida como:

> *"**L**a infraestructura crítica situada en los Estados miembros cuya perturbación o destrucción afectaría gravemente al menos a dos Estados miembros. La magnitud de la*

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2004:0702:FIN:ES:PDF.

[7] *Ibid*., pag 3.

[8] *Ibid*., pag 7.

[9] "Informe Protección de Infraestructuras Críticas 2011", S2 Grupo, p. 11, en http://www.aeiseguridad.es/descargas/categoria6/4508139.pdf.

[10] Si bien cabe destacar que el 17 de noviembre de 2005, la Comisión adoptó el Libro Verde sobre un Programa Europeo para la Protección de Infraestructuras Críticas, en el que se exponían las posibilidades de actuación para el establecimiento del Programa y de la Red de información sobre alertas en infraestructuras críticas (CIWIN).

incidencia se valorará en función de criterios horizontales, como los efectos de las dependencias intersectoriales en otros tipos de infraestructuras"[11].

Asimismo la Directiva se encarga de establecer los criterios de responsabilidad en la protección de las infraestructuras críticas, que recae a los Estados miembro y a los operadores, los criterios de identificación y designación de las ICE, los procedimientos de los planes de seguridad de los operadores, la figura del responsable de enlace para la seguridad y, por último, la evaluación de las amenazas que afectan a los distintos subsectores de las ICE.

3. El valor de las infraestructuras críticas en la seguridad nacional de España: el engarce europeo y las Estrategias de Seguridad Nacional de 2011 y 2013

La protección de las infraestructuras críticas aparece en el debate sobre la seguridad nacional española a partir del impulso dado por las iniciativas de la Unión Europea, a través, sobre todo, de la aprobación de la Comunicación 702 del 20 de Octubre de 2004 sobre "Protección de las infraestructuras críticas en la lucha contra el terrorismo" y de la Directiva 2008/114/CE del Consejo sobre "La identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección".

Con la implementación de la Comunicación 702, España pondrá en marcha por primera vez un Plan Nacional para la Protección de las Infraestructuras Críticas (PNPIC), que se materializará en la creación del Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC), encargado de "impulsar y coordinar los mecanismos necesarios para garantizar la seguridad de las infraestructuras que proporcionan los servicios esenciales a nuestra sociedad, fomentando para ello la participación de todos y cada uno de los agentes del sistema en sus correspondientes ámbitos competenciales"[12] .

Además, la aprobación de la Directiva 2008/114/CE del Consejo sobre "La identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección" será la base sobre la que se asiente la actual Ley española 08/2011 por la que se establecen las medidas para la Protección de Infraestructuras Críticas y el Real Decreto 704/2011 por el que se aprueba el Reglamento para la Protección de Infraestructuras Críticas, que desarrolla la ley anterior.

Este sistema de protección se completará con la aprobación, el 24 de junio de 2011, de la Estrategia española de Seguridad Nacional (ESN) que se refiere a las infraestructuras críticas, los suministros y los servicios críticos como elementos están especialmente expuestos y uno de los principales objetivos a proteger de las Nuevas Amenazas. De hecho, se reconoce que son especialmente vulnerables a riesgos y amenazas no tradicionales, tales como los efectos del cambio climático, las consecuencias de la globalización y los ciberataques entre otros. Por tanto, se establece que los mecanismos de prevención en este ámbito deberán ir

[11] "Directiva 2008/114/CE del Consejo de 8 de diciembre de 2008 sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección", *Diario Oficial de la Unión Europea* L 345, p. 77, en http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:ES:PDF.

[12] Centro Nacional para la Protección de las Infraestructuras Críticas, en http://www.cnpic-es.es/.

especialmente orientados en este sentido, así como la necesidad de tener protocolos de reacción debidamente establecidos. La estrategia propone una serie de ámbitos en los que es necesario avanzar para mejorar su seguridad[13]:

-La consolidación de los instrumentos para la protección de las instalaciones.

-La mejora del marco regulador de los sectores críticos, introduciendo criterios de seguridad.

-El establecimiento de medidas que aumenten su fortaleza, incrementen su resistencia y refuercen sus capacidades de adaptación ante condiciones adversas.

-El diálogo y cooperación permanente entre las Administraciones Públicas y los operadores de infraestructuras y servicios.

La Estrategia de Seguridad Nacional del año 2013, va un paso más allá en la definición del papel que juegan las infraestructuras críticas en la seguridad nacional y establece que "El concepto de seguridad en el siglo XXI debe ser amplio y dinámico, para cubrir todos los ámbitos concernientes a la seguridad del Estado, y de sus ciudadanos, que son variables según las rápidas evoluciones del entorno estratégico y abarcan desde la defensa del territorio a la estabilidad económica y financiera o la protección de las infraestructuras críticas"[14]. Así, la protección de las infraestructuras críticas se articula como una de las doce líneas de actuación estratégicas para garantizar la seguridad nacional con un objetivo prioritario: "robustecer las infraestructuras que proporcionan los servicios esenciales para la sociedad"[15].

Se considera que tanto los riesgos como las amenazas sobre las infraestructuras críticas españolas son múltiples y van desde las causas naturales, sanitarias o industriales, al error humano o los imprevistos tecnológicos. Sin embargo, son aquellos ataques de carácter intencional, ya sean físicos (terrorismo) o cibernéticos, los que revisten una mayor peligrosidad. La Estrategia de Seguridad Nacional establece siete líneas de actuación estratégicas con el objetivo de mejorar la seguridad de las infraestructuras críticas[16]:

-Responsabilidad compartida y cooperación público-privada.

-Planificación escalonada.

-Equilibrio y eficiencia.

-Resiliencia.

-Coordinación.

-Cooperación internacional.

[13] "Estrategia Española de Seguridad" (2011), p. 82, en http://www.urjc.es/ceib/investigacion/publicaciones/REIB_05_01_Document03.pdf.
[14]"Estrategia de Seguridad Nacional" (2013), p. 6, en http://www.lamoncloa.gob.es/NR/rdonlyres/0BB61AA9-97E5-46DA-A53E-DB7F24D5887D/0/Seguridad_1406connavegacionfinalaccesiblebpdf.pdf.
[15]*Ibid*., p. 51.
[16]*Ibid*., *Idem*.

-Garantía en la seguridad de las infraestructuras críticas conforme a lo expuesto en el Plan Nacional de Protección de Infraestructuras Críticas (PNPIC).

4. Valoración crítica

El principal aspecto positivo a destacar en cuanto a la Protección de las Infraestructuras Críticas (PIC) se refiere es que la publicación de la Estrategia de Seguridad Nacional de 2011 y la de 2013 demuestra que se asume la necesidad de abarcar este ámbito de manera concreta.

Con anterioridad a estos documentos la PIC se contemplaba dentro de otros ámbitos relativos a la seguridad, debido a la naturaleza misma de estas infraestructuras, que las hace estar ligadas inseparablemente a estos ámbitos. No obstante, resulta imprescindible separar, el concepto de la seguridad del ámbito, de la seguridad de las infraestructuras que utiliza para o en las que se inscribe el desarrollo de su actividad, para garantizar un desarrollo optimizado de ambos aspectos.

En este contexto, España ha realizado un gran avance teniendo en cuenta que, siguiendo las líneas de acción generales establecidas por el Programa Europeo de Protección de Infraestructuras Críticas (PEPIC) y por la Directiva Europea 2008/114/CE[17] del Consejo, sobre la "Identificación y Designación de Infraestructuras Críticas Europeas y Evaluación de la Necesidad de Mejorar su Protección", se ha procedido a la publicación de un marco legal específico mediante un Plan Nacional de Protección de Infraestructuras Críticas y más tarde mediante la Ley 8/2011 sobre "Protección de las Infraestructuras Críticas" (Ley PIC), así como la creación de un Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC)[18].

Estos factores colocan a España en línea con los principales socios europeos, que han seguido en su mayor parte la línea marcada por la UE. No obstante cuando se realiza un análisis comparado con otros socios individualmente se puede observar que en este sentido España ha avanzado de manera inercial puesto que no ha aportado prácticamente ningún factor adicional a lo establecido por el PEPIC y la Directiva 2008/114/CE.

En concreto, otros socios de la UE tales como Francia o Gran Bretaña, han realizado una labor más extensiva en este ámbito, estableciendo un marco según el cual se identifican y priorizan las amenazas en función de su probabilidad e impacto.

En este sentido, la ESN 2011 y la ESN 2013 se limitan a cumplir y exponer los parámetros establecidos desde la Unión Europea, y únicamente en la Ley PIC se menciona una clasificación y priorización pero atañe únicamente a la reacción en caso de graves disrupciones y ataques[19].

El ámbito de la cooperación europea está, no obstante, en este sentido más desarrollado que el ámbito de la cooperación atlántica. Como eje principal de la colaboración en materia de

[17] "Directiva 2008/114/CE del Consejo", *Diario Oficial de la Unión Europea*, L 345/75 (23 de diciembre del 2008), en http://www.cnpices.es/Biblioteca/Legislacion/Generico/Directiva_EPCIP_ES_como_publicada.pdf.
[18] "Ley 8/2011 de 28 de Abril", *Boletín Oficial del Estado*, nº 102 (29 de Abril de 2011), Sección I, p. 43370, en http://www.cnpic-es.es/Biblioteca/Legislacion/Generico/Ley_8-2011_PIC.pdf.
[19] *Ibid.*

seguridad euro-atlántica, la OTAN se perfila como la organización de referencia para la protección de infraestructuras críticas.

De hecho, en años recientes, la OTAN ha prestado un especial interés a este ámbito. Dentro de la redefinición del papel de la Alianza Atlántica en un entorno rápidamente cambiante y mucho más exigente desde el punto de vista de la seguridad, sobre todo debido a la naturaleza de las nuevas amenazas, se ha debatido el papel que esta debe jugar en la protección de las infraestructuras críticas[20].

El principal eje del debate ha girado en torno a cuales son las amenazas más probables y a cuales debe dar una respuesta prioritaria. El punto fundamental del debate radica en que la OTAN es una organización eminentemente militar, y muchas de las amenazas son de carácter no militar o estatal, y por tanto resulta discutible si una intervención de la Alianza resultaría conveniente o incluso si legal desde el punto de vista del derecho internacional. Otro punto fundamental es el hecho de que dada su naturaleza especial, las infraestructuras críticas están expuestas a todo tipo de riesgos y amenazas. En un entorno en el que estos cambian y se refinan constantemente, la evaluación de los mismos resulta una tarea cada vez más complicada.

Para solventar el debate en cierta medida, la OTAN ha puesto su prioridad en aquellos riesgos y amenazas que puedan tener un origen estatal, centrándose especialmente en los ámbitos de seguridad tecnológicos y logísticos y dando la menor prioridad al ámbito económico, centrándose así en temas como la seguridad de la infraestructura energética y de transporte y la ciberseguridad[21].

En este sentido, España queda igualmente descolgada dado que al no existir la priorización y clasificación de riesgos y amenazas resulta muy difícil establecer planes de acción y, sobre todo, de prevención concretos y eficaces.

En este mismo hilo, la principal crítica a realizar a la ESN 2011 y 2013 es su nula aportación en este ámbito. Es cierto que como considera la OTAN los riesgos y amenazas en el nuevo contexto son cambiantes y crecientemente complejos, y que las infraestructuras críticas de una forma u otra están expuestas a todos ellos, pero resulta imprescindible analizarlos y evaluarlos individualmente y en conjunto para establecer un sistema coherente de clasificación en función de su probabilidad y su impacto en cada ámbito concreto, para así poder comenzar a garantizar la seguridad de dichos ámbitos.

Sin un sistema de clasificación organizado y coherente, resulta mucho más difícil establecer e implementar planes de evaluación, prevención y mitigación de los riesgos y amenazas sea cual sea su naturaleza.

La ausencia de un marco temporal también va ligada a la ausencia de definición de riesgos y amenazas. Teniendo en cuenta que en España no existía un ámbito exclusivo de seguridad dedicado a la protección de las Infraestructuras Críticas antes de 2011, uno de los primeros pasos a tomar debería haber sido sin duda la elaboración de un calendario de acción,

[20] "Improving NATO's capabilities", OTAN, en http://www.nato.int/cps/en/natolive/topics_49137.htm?selectedLocale=en.
[21] "NATO and cyber defence", OTAN, en http://www.nato.int/cps/en/natolive/topics_78170.htm?selectedLocale=en.

que estableciese una serie de fechas y objetivos basados en la clasificación antes mencionada y en los recursos disponibles.

En este sentido, únicamente se ha seguido la estela marcada por la UE, sin concretar planes de acción específicos. El punto ausente más notable es el no establecimiento de mecanismos de prevención eficaces. El modelo de protección de las infraestructuras críticas es esencialmente reactivo, especialmente en lo referente a las nuevas amenazas.

Otro aspecto parcialmente erróneo de la estrategia es el hincapié que hace sobre la importancia de fomentar la colaboración público-privada para la protección de las infraestructuras críticas. Se parte de la consideración de que muchas de estas infraestructuras se encuentran bajo gestión completamente privada y que por lo tanto resulta inevitable que parte de la responsabilidad de su seguridad recaiga en manos de sus gestores.

Sin embargo, consideraciones de tipo tanto teórico como empírico pueden llevar a la conclusión de que este modelo es contrario al interés nacional a medio y largo plazo y probablemente también a corto. Desde el punto de vista teórico se puede afirmar que el objetivo de una empresa privada en un contexto de mercado libre es el beneficio por encima de cualquier otra consideración, incluido el interés nacional; en la práctica se ha podido comprobar recientemente como la infraestructura de determinados sectores críticos para el bienestar general y la prosperidad económica nacional, cuya gestión se encuentra en manos privadas, tales como el sector de la banca o la energía, se ha visto mermada o ha presentado graves disfunciones que han afectado tanto a ciudadanos individuales como a la Nación en su conjunto.

En este sentido estamos asistiendo recientemente a un discurso político que aboga por continuar en este sentido, es decir el de depositar la gestión de infraestructuras críticas en manos privadas. El ejemplo más notable es probablemente el del proyecto de privatización de una parte de la red de sanidad. En este sentido, la seguridad de la infraestructura sanitaria no quedaría garantizada, dado que quedaría sujeta a la rentabilidad que pudiera generar. Tampoco queda garantizado un incremento en la inversión a largo plazo dado que siempre quedaría sujeta a las exigencias del mercado, que por otro lado esta globalizado y es cada vez más competitivo. Esto a largo plazo podría significar que la gestión de parte de la infraestructura crítica nacional estaría en manos no sólo privadas sino además extranjeras, con la consiguiente pérdida de soberanía en general y vulnerabilidad de sectores esenciales.

Un último punto que cabe destacar, y que engarza directamente con el tema de la globalización de los mercados, es el relativo a la protección de las infraestructuras críticas en el extranjero. Cabe destacar que sectores fundamentales como la banca, la energía, las telecomunicaciones o el transporte disponen de parte de su infraestructura en el extranjero. Si bien un ataque, accidente o alguna otra disrupción grave en su funcionamiento no supondrían un impacto muy grave contra ciudadanos españoles, si podrían suponer un grave impacto económico cuyas repercusiones se harían sentir también en España, así como un posible impacto político tanto de cara a la política interior como exterior.

Los documentos ESN 2011 y 2013 no suponen un avance en este sentido dado que la protección de estos activos en el extranjero queda obviada. Si tenemos en cuenta que la gestión de estas infraestructuras se encuentra en manos privadas, el único apoyo estatal proveniente de España para contribuir a su seguridad son las gestiones diplomáticas que se puedan llevar a cabo en cada momento y circunstancia, y que dependerán enormemente de las buenas relaciones o no que se mantengan con el país que acoja dichas infraestructuras.

Las infraestructuras en el extranjero suponen además un reto adicional para la seguridad, dado que siguiendo los mecanismos de externalización para la optimización de costes y especialización de las funciones del trabajo, muchas veces la seguridad física y virtual *in situ* de estas infraestructuras se encuentra en manos de Estados o empresas extranjeras, que pueden tener sus propias agendas e intereses contrapuestos a los de España.

5. La aplicación de los principios de la estrategia

Las ESN 2011 y 2013 establecen una serie de principios de aplicación en todos los ámbitos de seguridad[22]:

- Unidad de acción y armonización de recursos del estado e implicación de la sociedad.

- Anticipación y prevención.

- Priorización de recursos y optimización del empleo.

- Capacidad de resistencia y recuperación de los recursos humanos y materiales.

Analizando el planteamiento en el documento respecto a la protección de las infraestructuras críticas, desgraciadamente se puede afirmar que estos principios no se aplican en su mayoría en este ámbito concreto, y que además, tal y como está planteado, su aplicabilidad queda en duda.

El problema de base es la falta de definición ya mencionada de los riesgos y amenazas a los que se ven expuestas las infraestructuras críticas, y un sistema de priorización de los mismos. Esto conlleva una dificultad añadida para elaborar planes de acción y prevención concretos. Sin planes elaborados y optimizados resulta a su vez muy difícil conseguir una unidad de acción y una armonización de los recursos, así como una optimización del empleo por parte del Estado.

A esto hay que añadir que a los actores que participan en la protección y en la mitigación del daño causado por cualquier disrupción en las infraestructuras críticas ven muchas veces sus competencias solapadas. Un ejemplo claro de esto puede ser la Unidad Militar de Emergencias, que está preparada para responder a emergencias de carácter militar, como ataques RNBQ, pero que a su vez ha venido desarrollando labores de protección civil, tales como rescates o intervención en extinción de incendios. Este último tipo de intervenciones quedan muy distantes del ámbito de actuación que debería tener una unidad militar y constituyen un ejemplo claro de falta de armonización de recursos y optimización del empleo.

Por el mismo problema de base, resulta muy difícil desarrollar mecanismos óptimos de prevención de riesgos y anticiparse a los mismos. Teniendo en cuenta que el marco legal

[22]"Estrategia de Seguridad Nacional" (2013), en http://www.lamoncloa.gob.es/NR/rdonlyres/0BB61AA9-97E5-46DA-A53E-DB7F24D5887D/0/Seguridad_1406connavegacionfinalaccesiblebpdf.pdf.

actual únicamente clasifica los riesgos y amenazas en función de su impacto, el sistema de protección de las infraestructuras críticas es fundamentalmente reactivo.

Esto a su vez conlleva un problema de mitigación del daño. La legislación introduce el concepto de Resiliencia como fundamental[23]. Es decir, da una gran importancia a que en caso de cualquier disrupción, ya sea accidental o intencionada, las infraestructuras críticas puedan seguir prestando el servicio que proporcionasen a la sociedad, aunque sea a niveles reducidos o sub-óptimos. Sin embargo, hay que señalar que sin un mecanismo de prevención y anticipación adecuado, es mucho más difícil aplicar el concepto de la Resiliencia. La implementación de mecanismos de anticipación eficaces no supone una garantía de seguridad ni de evitar al 100% accidentes o ataques, pero si que añaden una posibilidad elevada y real de impedirlos parcialmente o mitigar su impacto, lo que supone a su vez un añadido a la hora de garantizar que las infraestructuras sigan cumpliendo con su función.

De lo anteriormente expuesto se puede deducir que si no cambia el planteamiento base de la protección de infraestructuras críticas, los principios de la estrategia no sólo van a no estar aplicados en este ámbito, sino que su aplicabilidad será muy complicada. Sin establecer definiciones claras desde el punto de partida de los problemas que este ámbito enfrenta en la actualidad, y a los que previsiblemente deba hacer frente en el futuro, resulta muy difícil abordar el tema de manera eficaz.

6. La protección de las infraestructuras críticas en otros países: nuevas perspectivas

Durante los últimos años han sido varios los países entre los que ha crecido la preocupación por garantizar la seguridad y reducir la vulnerabilidad de las infraestructuras esenciales del estado frente a amenazas y riesgos de distinta naturaleza. Así lo han puesto de manifiesto las últimas estrategias de seguridad nacional aprobadas por Finlandia, Japón, Reino Unido, Estados Unidos, Australia y Francia.

La estrategia de seguridad finlandesa[24] analiza la protección de las infraestructuras críticas de forma exhaustiva, haciendo hincapié en la importancia de mantener un enfoque holístico en materia de seguridad. Pone especial énfasis en la seguridad de la cadena de suministros y el fomento de los mecanismos de resiliencia, con el objetivo de mantener las funciones básicas vitales del Estado. Además, el nuevo papel de los actores privados en las funciones vitales sociedad obliga a intensificar la cooperación entre el Gobierno y la comunidad económica, atendiendo a los nuevos desafíos planteados por la crisis económica y la mayor interdependencia de una sociedad globalizada, entre ellos la posibilidad de deslocalizar en otros países infraestructuras esenciales.

La estrategia de seguridad japonesa[25] se centra, principalmente, en la prevención de ataques cibernéticos a sus infraestructuras de interés nacional como principal amenaza. Hace una mención especial a la posibilidad de que los Estados sean responsables de estas actuaciones y busca como objetivo último la mejora de la base intelectual del país para

[23] *Ibid.*
[24] "Finnish Security and Defence Policy", Prime Minister Office, Helsinki (2012), pp. 91-93, en http://vnk.fi/julkaisukansio/2012/j05-suomen-turvallisuus-j06-finlands-sakerhet/PDF/VNKJ0113_LR_En.pdf.
[25] "Japan National Security Strategy", Japan Prime Minister, Tokyo (17 de diciembre del 2013), pp. 17-19, en http://www.cas.go.jp/jp/siryou/131217anzenhoshou/nss-e.pdf.

mejorar las capacidades tecnológicas, especialmente las capacidades de comunicación, que suponen el motor de la fuerza económica y de seguridad japonesa.

Una aproximación similar articula el Libro Blanco de la Defensa de Francia[26], que concentra sus esfuerzos en la protección del potencial científico y técnico de la nación como vía prioritaria para prevenir los ataques a sus infraestructuras. La estrategia cataloga 12 sectores de actividad considerados vitales para la continuidad de las funciones esenciales del Estado y se centra en la lucha contra los ataques cibernéticos, especialmente aquellos que apunten a los sistemas de información estatales. Para garantizar su seguridad Francia considera indispensable mantener la capacidad de producir dispositivos de seguridad autónomos de detección de ataques y mejorar su competencia en las comunicaciones electrónicas, sobre todo en la fabricación de equipos y componentes.

En cuanto a las estrategias de seguridad del mundo anglosajón (Australia, Reino Unido y Estados Unidos), presentan diferencias notables. La estrategia australiana[27] es la más somera respecto a este tema, centrándose en la importancia de reforzar la resiliencia de la población, activos, infraestructuras e instituciones, para lo que han creado un foro de debate con expertos en la materia. La aproximación estadounidense[28] se centra en la reducción de la vulnerabilidad frente a ataques y ciberataques en ámbitos concretos considerados prioritarios: la red de transportes, la red eléctrica y la economía, esta última considerada especialmente vulnerable a los ataques cibernéticos, lo que convierte al ciberespacio es un área clave de la actuación estatal. La estrategia de Reino Unido[29], por el contrario, nos ofrece un análisis y priorización exhaustiva de los riesgos y amenazas que enfrenta cada sector de actividad de las infraestructuras críticas, mediante el desarrollo de una metodología propia de prevención de riesgos. El papel de la ciberseguridad también es prioritario en la estrategia concluyendo que una mejora de la inversión en el binomio tecnología-capital humana será determinante para garantizar la seguridad del país.

7. Un nuevo enfoque para la protección de las infraestructuras críticas en España

El punto básico y necesario para un nuevo enfoque en la protección de infraestructuras críticas en España debe ser el de subsanar las lagunas más importantes respecto al actual, como realizar una definición clara del sujeto, que incluya no sólo el objeto que debe ser protegido, sino también los riesgos y amenazas a los que se ve expuesto y a los que previsiblemente se verá expuesto en un futuro próximo, así como un marco en que quede claramente establecido cuales son los objetivos prioritarios. En este sentido resulta aconsejable seguir un modelo de elaboración del documento similar al de Gran Bretaña, que

[26]Livre blanc sur la Défense et la Sécurité Nationale", Ministerio de defensa, París (2013), pp. 104-107, en http://www.gouvernement.fr/sites/default/files/fichiers_joints/livre-blanc-sur-la-defense-et-la-securite-nationale_2013.pdf.

[27]"Strong and Secure. A Strategy for Australia's National Security", Australian Government-Office of the Prime Minister, Canberra (2013), p. 21, en http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?lng=en&id=167267.

[28]"National Security Strategy of the United States of America", White House, Washington (May 2010), pp. 27-33, en http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.

[29]"A Strong Britain in an Age of Uncertainty: The National Security Strategy", Ministry of Defence, Londres (Octubre 2010), pp. 28-35, en https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf.

establece un sistema claro de evaluación de riesgos y amenazas en función de su impacto y probabilidad, basado en una metodología también incluida en el documento.

Otro punto fundamental es establecer una serie de objetivos realistas en función de dicha definición, tales como la elaboración de planes específicos para cada sector, que definan los riesgos y amenazas generales a los que cada uno está expuesto y que actores deben intervenir en cada una de las fases (evaluación, prevención y mitigación del daño) y bajo que jerarquía administrativa y territorial, aprovechando el marco jurídico ya proporcionado por las directivas europeas y la Ley PIC. Así mismo resulta imprescindible la elaboración de un calendario realista para alcanzar estos objetivos.

Se debe distinguir también entre aquellas amenazas y riesgos que correspondan a la seguridad y aquellos que correspondan a la defensa para así poder llevar a cabo una división eficaz del trabajo y una optimización de los recursos humanos y materiales de la Nación.

En el caso concreto de España, los principales riesgos y amenazas a los que las infraestructuras críticas están probablemente expuestas es a ataques terroristas, ciberataques y las consecuencias perniciosas derivadas de la cada vez mayor pérdida de soberanía económica. A largo plazo, hay que añadir los efectos disruptores ligados a las consecuencias de la crisis económica, a la inestabilidad en nuestra área geográfica más próxima y a los efectos del cambio climático sobre nuestro territorio nacional y las necesidades y exigencias que previsiblemente genere.

La PIC debería enfocarse en estos aspectos. Se debería también fomentar mucho la colaboración europea y atlántica, pero también se debería definir mucho mejor la participación de España en la misma así como las aportaciones específicas que puede realizar, por ejemplo como nexo con Hispanoamérica y con el Mediterráneo, donde se encuentran situadas muchas infraestructuras críticas tanto españolas como del resto de socios de la UE, y trabajar activamente por demostrar los resultados de estas aportaciones aunque suponga un esfuerzo presupuestario.

Además es esencial que el enfoque siga un planteamiento realista respecto al contexto en el que se encuentra específicamente España. La escasez presupuestaria traída por la crisis económica actual supone graves limitaciones en todos los ámbitos de las políticas públicas, incluidas las políticas de seguridad y defensa. Resulta por lo tanto fundamental que el documento asuma cuales deben ser las prioridades fundamentales para garantizar la seguridad de las infraestructuras críticas.

Se debe poner un énfasis mucho mayor en el desarrollo del potencial científico y técnico de la nación, haciendo especial mención a la importancia de mantener una red de centros de investigación nacionales que abarquen todos los ámbitos y que puedan realizar aportaciones aplicables a todos los ámbitos de seguridad, incluyendo las infraestructuras críticas, con especial enfoque hacia las nuevas amenazas.

Adicionalmente, el nuevo enfoque debe superar algunas concepciones obsoletas en las que actualmente está basado. Se debe considerar especialmente que el entorno actual está sujeto a cambios cada vez más rápidos y de mayor calado. La balanza de la seguridad internacional se inclina cada vez más hacia los actores y las regiones emergentes, lo que está alterando las prioridades de todos los actores. En este contexto se inscriben las nuevas amenazas, y la adaptación a las mismas será crucial en el futuro.

Resulta fundamental reconocer la relevancia del papel que los estados juegan a la hora de prevenir, pero también al desarrollar sus capacidades ofensivas utilizando estas nuevas estrategias. En concreto, resulta imprescindible tener en cuenta que las capacidades ofensivas electrónicas y digitales están siendo desarrolladas rápidamente por las principales potencias militares del mundo, y uno de los principales fines para el desarrollo de estas capacidades es el ataque a las infraestructuras críticas de los países objetivo, lo cual puede provocar daños difícilmente reversibles a cualquier afectado.

Es necesario asumir que, en el contexto actual, las infraestructuras críticas se ven expuestas de manera cada vez mayor a amenazas digitales de origen no estatal, pero también estatal. Estas amenazas se han vuelto crecientemente complejas, sobrepasando en muchos casos las capacidades de reacción de muchos estados, llegando a afectar a infraestructuras críticas a todos los niveles[30]. El papel de los servicios de inteligencia, en estrecha colaboración con sectores muy especializados de las esferas civil y militar, es fundamental para la prevención y mitigación del daño en estos casos, pero también lo es en el caso contrario.

Hasta el momento, los ataques se han centrado principalmente en el espionaje. Los casos de ataques directos contra infraestructuras más importantes hasta la fecha han sido contra Estonia en el año 2007 y contra Irán en el año 2010. Además, recientemente se ha hecho público que durante este mismo año se ha detectado un virus informático, denominado Turla, con un grado de sofisticación no visto hasta la fecha, cuya función es el espionaje y cuyo objetivo principal han sido los países miembros de la OTAN. Si bien la mayoría de analistas coinciden en que el probable origen de este ataque sea Rusia[31], resultaría imposible confirmarlo a menos que el propio Estado reclama la autoría de los hechos. Estos ataques tomaron como objetivo las infraestructuras industriales y la administración de dichos países, causando graves daños al funcionamiento de las mismas y a las economías nacionales.

En este contexto, hay que tener en cuenta que España ocupa el sexto lugar en cuanto al ranking mundial de países con mayor número de ciberataques[32]. Esto pone de manifiesto por un lado la gran vulnerabilidad de las infraestructuras críticas nacionales, y por otro la necesidad inmediata de desarrollar las capacidades de prevención y mitigación del daño en este ámbito. En el caso español, resultan especialmente importante asegurar las infraestructuras relativas al suministro de agua y energía.

Hacer frente a estas amenazas debe ser una de las principales prioridades de seguridad en cualquier contexto, ya que representan un riesgo real y probable. Resulta por tanto fundamental que en el nuevo enfoque de seguridad se priorice de manera consistente la seguridad en este ámbito y se prevea el destino de recursos suficientes para garantizar por un lado un grado razonablemente alto de prevención de ataques en este sentido, y por otro, y fundamentalmente la resiliencia de las infraestructuras críticas ante la eventualidad de un ataque.

---

[30] Richmond, Riva: "Malware Hits Computerized Industrial Equipment", *The New York Times*, 24 de Septiembre de 2010, en http://bits.blogs.nytimes.com/2010/09/24/malware-hits-computerized-industrial-equipment/?_php=true&_type=blogs&_php=true&_type=blogs&_r=1.

[31] Apps, Peter y Finkle, Jim: "Suspected Russian Spyware Turla Targets Europe, United States", *Reuters U.S. Edition*, 7 de Marzo de 2014, en http://www.reuters.com/article/2014/03/07/us-russia-cyberespionage-insight-idUSBREA260YI20140307.

[32] Top 20 países por ciberataques, en "Cybercrime: Top 20 Countries", Europol, The Center to Fight Cybercrime (2010), en http://www.intellectualtakeout.org/library/chart-graph/countries-cyber-attack.