POLÍTICAS Y CAPACIDADES DE CIBERSEGURIDAD DEL MINISTERIO DEL INTERIOR EN RELACIÓN CON LA PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS

FERNANDO J. SÁNCHEZ GÓMEZ
Centro Nacional de Protección de Infraestructuras y Ciberseguridad

Las Tecnologías de la Información y la Comunicación (TIC) se han convertido, por su transversalidad, en el *nexo de unión* que comunica todos los entornos de la vida moderna: desde las redes sociales a los sistemas de control industrial; desde el ámbito doméstico, al empresarial y las instituciones de gobierno. Sin embargo, como todo gran invento de la historia de la humanidad, las TIC e Internet no solo son extraordinarias herramientas para el progreso humano, sino que se emplean habitualmente por los delincuentes para la consecución de sus fines antisociales o criminales.

LA AMENAZA CIBERNÉTICA

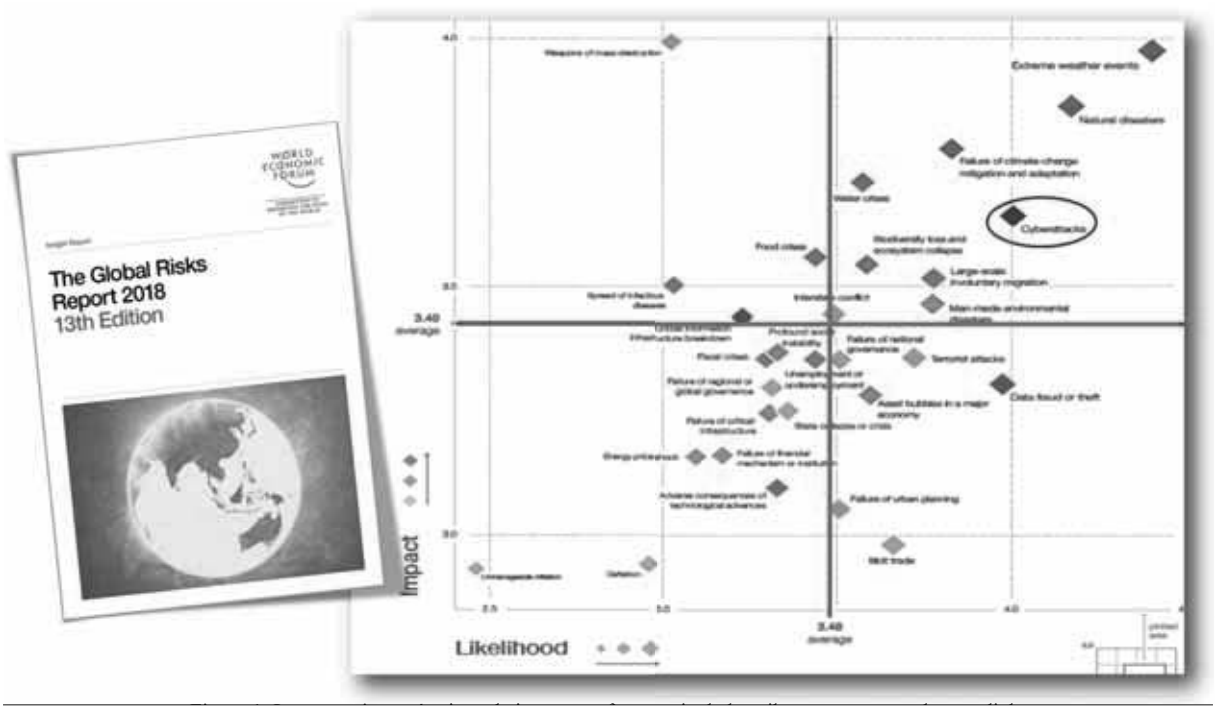
Precisamente ese es el problema con el que ahora nos encontramos. Y es que Internet, o el ciberespacio (1), fue concebido como un espacio cuyo fin fundamental era la comunicación de la forma más ágil y libre posible; hasta ahí bien. Pero es que Internet nunca tuvo en cuenta la seguridad como factor a incorporar. Y el ciberespacio, como ya se ha esbozado previamente, tiene su parte positiva (oportunidades de comunicación social, expansión, inversión, investigación y negocio, etc.) pero también negativa, ya que engendra riesgos, «los ciberriesgos», y posibilita la comisión de delitos.

Los ciberataques son ahora parte de las grandes preocupaciones de los Estados modernos, con claras conexiones con el terrorismo internacional, el espionaje o el crimen organizado. Y esta preocupación no se justifica únicamente por los peligros de los ciberataques como fin último, sino por las posibilidades que ofrecen las redes y las tecnologías para ser empleadas como herramientas para la perpetración de actos que pueden llegar a amenazar la Seguridad Nacional, con la posibilidad cierta de ataques contra nuestras infraestructuras críticas y los servicios esenciales.

En enero de 2018, el Foro Económico Mundial publicó su ya tradicional informe anual sobre Riesgos Globales. En este informe correspondiente a 2018, y tras varios años de aparecer destacados como fenómenos negativos de primer orden, los ciberataques daban un «salto cualitativo» para configurarse como una de las principales amenazas a las que se enfrenta el planeta, tanto por su frecuencia como por su impacto.

Así, por orden de importancia, los ciberataques aparecen en este informe (2) como la tercera amenaza más probable, y como la sexta con efectos potenciales más negativos a escala global, tan sólo tras amenazas tan graves para la propia humanidad como son las armas de destrucción masiva, los eventos climatológicos extremos, las catástrofes naturales, el cambio climático o las

FIGURA 1
IMPORTANCIA EN TÉRMINOS DE IMPACTO Y FRECUENCIA DE LOS CIBERATAQUES A ESCALA MUNDIAL



Fuente: Global Risks Report 2018 WEF

crisis de agua. Esto da idea de la dimensión del problema al que nos enfrentamos.

El Foro Económico Mundial, en el informe en cuestión, cifra el coste estimado del cibercrimen sobre los negocios en 8 billones de dólares a nivel mundial, durante los próximos 5 años. Para ejemplarizar el impacto, también hace referencia también al coste que compañías como Merck, FedEx, o Maersk, tuvieron que afrontar por no estar suficientemente protegidos ante el ciberataque *NotPetya* (junio 2017): alrededor de 300 millones de dólares, tan sólo en el tercer cuatrimestre del año. Y culmina aseverando que «*m*ás allá de su coste financiero, el ataque WannaCry (mayo 2017) interrumpió infraestructuras críticas y estratégicas en todo el mundo, incluidas las de ministerios de gobiernos, ferrocarriles, bancos, proveedores de telecomunicaciones, compañías energéticas, fabricantes de automóviles y hospitales».

Esta última advertencia obliga, cuando de la protección de las infraestructuras críticas y de los servicios esenciales se trata, a poner el foco sobre los sistemas de control industrial, y a abordar singularmente la protección de las tecnologías de la operación (TO) frente a la actual, y mucho más extendida, concepción donde la incipiente cultura de ciberseguridad se centra de manera prioritaria en la protección de las tecnologías de la información (TI) (3). La cuestión es que los sistemas de control industrial fueron creados para lograr un fin determinado (en el caso que nos ocupa, la disponibilidad del servicio esencial), y hasta hace bien poco permanecían completamente aislados… hasta que las necesidades de la nueva sociedad global conectada se han impuesto en sus sistemas adaptativos. La existencia de una interconexión externa e ilimitada (Internet) hace hoy posible que características vulnerables de un sistema (TI) se transfieran al otro (TO), y que su mejor herramienta de desarrollo se convierta a la vez en su punto débil.

A todo lo anterior debe unírsele, necesariamente, la irrupción de otro nuevo concepto, que ha venido a escenificar la existencia de un nuevo *problema*, íntimamente ligado con el que nos ocupa: el de la *amenaza híbrida*, entendida como aquella combinación de acciones militares y no militares, convencionales o no, orientadas a alcanzar objetivos estratégicos, que algunos actores, estatales o no, están llevando a cabo para aprovecharse de las vulnerabilidades de países y sociedades. Dichas acciones combinan aspectos tan diversos como los ataques en la red (ciberataques), la desinformación, las noticias falsas («*fake news*»), la propaganda, la presión económica o diplomática, la subversión, la coerción o la amenaza militar. Su carácter ambiguo (enmascaramiento de los objetivos reales del agresor), siempre por debajo del umbral de la agresión directa, hacen muy difícil su atribución, dificultando con ello una respuesta coordinada y eficaz (4).

En cualquier caso, y sin abundar en un aspecto que podría ser objeto de un artículo por sí sólo, es preciso destacar el innegable protagonismo que las TIC y el ciberespacio, tanto como herramienta, como como objeto, desempeñan en esta amenaza de nuevo cuño.

En el ámbito cibernético podría determinarse la existencia, *grosso modo*, de tres grandes bloques de amenazas, para y desde el ciberespacio, que se diferencian por su motivación y por sus capacidades. Encarnadas por:

- Delincuentes: Que actúan con un móvil fundamentalmente económico y que ocupan en cuanto a número de actividades el primer puesto entre todos los agentes de la amenaza. Su impacto sobre la sociedad es muy heterogéneo, abarcando desde delincuentes individuales y pequeños fraudes hasta delitos a gran escala realizados por grandes redes criminales (en relación con el robo de información de tarjetas de crédito o de certificados digitales, con el fraude telemático sobre operaciones bancarias o transacciones desde Internet, con el blanqueo de dinero y con el robo de identidades asociado a inmigración ilegal, por citar tan sólo algunos ejemplos).

- Hacktivistas: De carácter preferentemente ideológico/antisistema, organizados en torno a pensamientos o ideas más o menos radicales, generalmente poco estructurados y con conocimientos técnicos de carácter muy dispar, lo que no impide que lleguen a poseer la capacidad de llevar a cabo acciones potencialmente muy dañinas. Sus acciones incluyen desfiguraciones de webs, redirecciones, ataques de denegación de servicio, robo de información, parodias de sitios web, sustituciones virtuales, sabotajes virtuales y desarrollos de software, entre otras.

  Los últimos años han puesto de manifiesto la importancia de la interacción entre los activistas del mundo físico y los hackers del mundo electrónico. Así, el pasado año 2017, en determinadas campañas centradas en los acontecimientos políticos y sociales, se ha evidenciado la coordinación cada vez mayor entre ambos sectores, lo que ha tenido como consecuencia un mayor impacto en el resultado de las acciones.

- Estados/Gobiernos: Cuya motivación es de carácter político/estratégico. El ciberespionaje es posiblemente la actividad más desarrollada a día de hoy, tanto contra la información sensible de los gobiernos como aquella referente a desarrollos tecnológicos o industriales, con un componente esencialmente económico; pero tampoco son infrecuentes las acciones de sabotaje que podrían conducir incluso, en casos extremos, a la *ciberguerra* (ciberguerra que, en opinión de algunos expertos, ya se está desarrollando encubiertamente en algunos teatros de operaciones, como Ucrania, la región del Cáucaso y Oriente Próximo).

  La participación de los servicios de inteligencia de los Estados, las unidades cibernéticas de sus Fuerzas Armadas y grandes compañías multinacionales confiere a todo ello una especial gradación, al estar dotados de grandes medios y recursos técnicos y de una gran capacidad de acción. Sus actividades son muy prolongadas en el tiempo y el tipo de herramientas que utilizan normalmente muestran unos niveles muy bajos de detección en los sistemas de seguridad de los objetivos.

Pero, de forma transversal a todos estos grupos, y con posibilidades de ser realizadas por cualquiera de estos ellos, de una u otra manera, y con una u otra motivación, están las posibilidades de ataques terroristas valiéndose de la Red: Y la peor de las hipótesis es, precisamente, un ataque contra nuestras infraestructuras críticas y los servicios esenciales que éstas prestan.

Esta posibilidad, reciente y expresamente reconocida por la Organización de Naciones Unidas (5), se basa en la aplicación generalizada de una serie de patrones que las sociedades modernas han adoptado y que nos hacen enormemente dependientes, social, económica y políticamente de este tipo de servicios, caracterizados por su interdependencia, globalidad y repercusión.

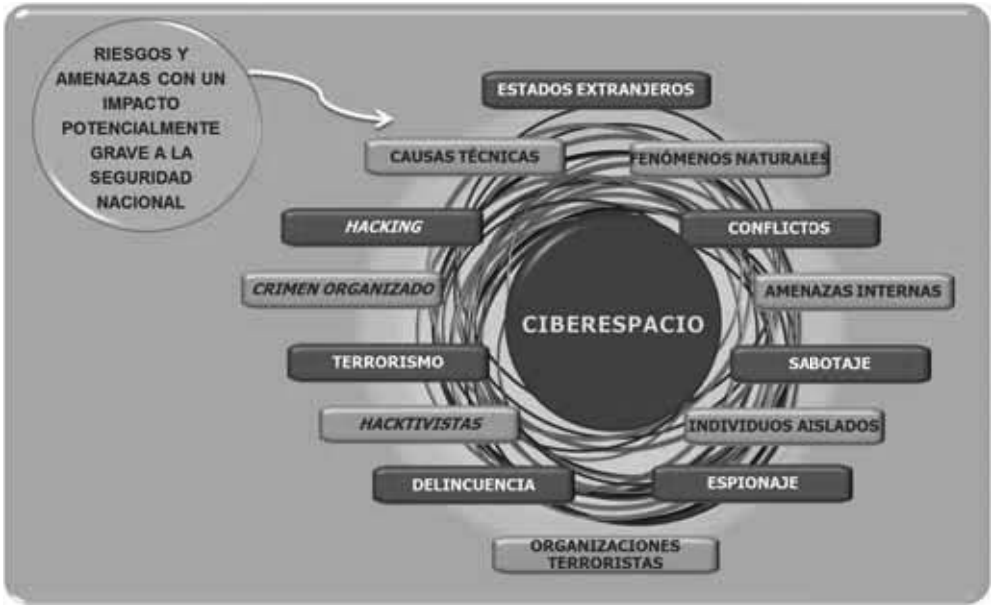
HERRAMIENTAS DEL ESTADO EN LA LUCHA CONTRA LAS CIBERAMENAZAS

Para hacer frente a los diferentes riesgos y amenazas que provienen del ciberespacio, se hace necesario potenciar los instrumentos que tiene el Estado con el fin de mejorar la prevención, detección, reacción, análisis, recuperación, respuesta, investigación y coordinación ante este tipo de incidentes, configurados como una parte de la amenaza asimétrica que debemos contrarrestar. El ciberespacio está siendo utilizado como medio para la realización de actividades ilícitas, acciones de desinformación, propaganda o financiación terrorista y actividades de crimen organizado, entre otras, amplificando la complejidad y la incertidumbre, lo que también pone en riesgo la propia privacidad de los ciudadanos.

España, al igual que los países desarrollados de nuestro entorno, vio hace unos años la necesidad de coordinar los esfuerzos de los organismos competentes en materia de ciberseguridad para conseguir un mayor nivel de protección en nuestro país, a través de la Estrategia Nacional de Seguridad, que fue actualizada en diciembre de 2017.

Entre los objetivos generales que se recogen en la Estrategia Nacional de Seguridad 2017 se destaca la promoción de una cultura de la seguridad, el favorecer el buen uso de los espacios comunes globales, e impulsar la dimensión de seguridad en el desarrollo tecnológico. De forma específica, en materia de ciberseguridad, se plantea como principal objetivo el uso seguro de las redes y los sistemas de información y comunicaciones a través del fortalecimiento de las capacidades de prevención, detección y respuesta a los ciberataques, potenciando y adoptando medidas específicas para contribuir a la promoción de un ciberespacio seguro y fiable. Así, entre sus principales líneas de acción destaca el reforzar, impulsar y promover los mecanismos normativos, organizativos y técnicos, así como la aplicación de medidas, servicios, buenas prácticas y planes de conti-

FIGURA 2
RIESGOS Y AMENAZAS IDENTIFICADOS EN LA ECSN ESPAÑOLA



Fuente: Departamento Nacional de Seguridad. Gobierno de España

nuidad para la protección, seguridad y resiliencia en el sector público, los sectores estratégicos (especialmente en las infraestructuras críticas y servicios esenciales), el sector empresarial y los propios ciudadanos, de manera que se garantice un entorno digital seguro y fiable.

Por su parte, la Estrategia de Ciberseguridad Nacional, aprobada por el Consejo de Seguridad Nacional en diciembre de 2013, se configura como una estrategia de segundo nivel que desarrolla la Estrategia Nacional de Seguridad en el ámbito de la ciberseguridad. Sin perjuicio de ser anterior a ésta última y, por tanto, susceptible de revisión en las próximas fechas, la Estrategia de Ciberseguridad Nacional fue la primera herramienta que nuestro país consigno de manera específica a esta problemática, teniendo como finalidad garantizar un uso seguro de las redes y de los sistemas de información a través del fortalecimiento de las capacidades nacionales de prevención, detección y respuesta a los ciberataques.

Es un hecho que para la mejora de las capacidades es necesario que confluyan una serie de actividades dirigidas hacia un objetivo común y definido. Además, estas actividades deben ir acompañadas de una asignación de recursos y estructuras orgánicas que guíen y garanticen su adecuado cumplimiento.

Es precisamente esto lo que plantea la Estrategia de Ciberseguridad Nacional Española, que define como objetivo global «*lograr que España haga un uso seguro de los Sistemas de Información y Telecomunicaciones, fortaleciendo las capacidades de prevención, defensa, detección y respuesta a los ciberataques*».

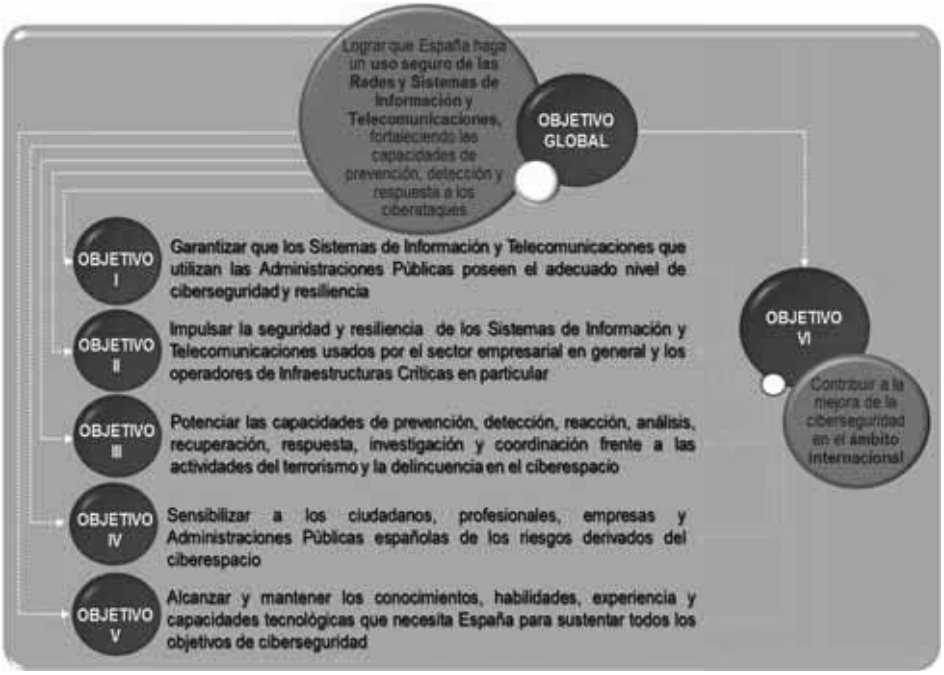
La Estrategia de Ciberseguridad define 8 líneas de acción, enmarcados en 6 objetivos, para hacer frente a estas amenazas, que se concretan en las siguientes:

1. Capacidad de prevención, detección, respuesta y recuperación ante las ciberamenazas
2. Seguridad de los Sistemas de Información y Telecomunicaciones que soportan las Administraciones Públicas.
3. Seguridad de los Sistemas de Información y Telecomunicaciones que soportan las infraestructuras críticas.
4. Capacidades de detección y persecución del ciberterrorismo y de la ciberdelincuencia.
5. Seguridad y resiliencia de las Tecnologías de la Información y la Comunicación (TIC) en el sector privado.
6. Conocimientos, competencias e I+D+i.
7. Cultura de ciberseguridad.
8. Compromiso internacional con otros países y organismos.

Precisamente sobre esta base es sobre la que desde el Ministerio del Interior se han adaptado las actividades, recursos y estructuras necesarios para lograr un adecuado cumplimiento de las competencias y responsabilidades asignadas, según se detalla a continuación.

Para la coordinación y desarrollo de las líneas de acción plasmadas en la Estrategia de Ciberseguridad española, se creó el Consejo Nacional de Ciberseguridad, órgano que responde ante el Consejo Nacional

FIGURA 3
OBJETIVOS DE LA ECSN ESPAÑOLA



Fuente: Departamento Nacional de Seguridad. Gobierno de España

FIGURA 4
LA CIBERSEGURIDAD EN EL SISTEMA DE SEGURIDAD NACIONAL

Fuente: Departamento Nacional de Seguridad. Gobierno de España

de Seguridad y en el que están representados aquellos Departamentos Ministeriales y organismos que tienen responsabilidad en materia de Ciberseguridad (entre ellos, el Departamento de Seguridad Nacional de Presidencia del Gobierno, el Ministerio de Defensa, el Ministerio de Industria, Energía y Turismo, el Ministerio de Asuntos Exteriores, el Centro Nacional de Inteligencia, y el Ministerio del Interior, como agentes principales).

Con fecha 31 de octubre de 2014, el Consejo de Seguridad Nacional aprobó el Plan Nacional de Ciberseguridad, en el que los diferentes Ministerios establecen sus prioridades y las actividades y programas a seguir en este ámbito.

Sin embargo, desde mucho tiempo antes, ya se está trabajando operativamente en proporcionar ciberseguridad a la población española. Los conocidos como CERTs, CSIRTs (6), o Centros de Respuesta a Incidentes Cibernéticos, son los responsables de estas actividades, tan oscuras como importantes.

EL PAPEL DEL MINISTERIO DEL INTERIOR ESPAÑOL EN LA PROTECCIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS Y EN LA CIBERSEGURIDAD NACIONAL

Escenario general

En España, el Ministerio del Interior es el Departamento responsable del mantenimiento de la seguridad ciudadana y del orden público, debiendo garantizar la protección de personas y bienes y el mantenimiento de la tranquilidad de los ciudadanos. Esto incluye, por lógica (no en vano el término ciberseguridad es parte de un concepto más amplio que es la de la seguridad como un todo), la vertiente referida al ciberespacio, abarcando las acciones relativas a la lucha contra la delincuencia, el terrorismo, o la protección de infraestructuras críticas, así como la regulación de la seguridad privada.

En todo caso, debe tenerse en cuenta que la amenaza cibernética es de carácter poliédrico y ha de considerarse de forma global. Nos encontramos, así, con un panorama en el que, desde el punto de vista del Ministerio del Interior, deben destacarse los siguientes tipos de riesgo:

- Por el número de casos, con diferencia sobre el resto de tipologías, es el cibercrimen la modalidad de amenaza cibernética más extendida, que alcanza a las múltiples y diversas actividades ilícitas a las que se aplican las organizaciones criminales (destacando los delitos que afectan a la libertad e indemnidad sexual de los menores y los fraudes y estafas informáticos), que se ven facilitadas e incluso potenciadas por las enormes ventajas que ofrecen estas tecnologías. En 2017, a nivel mundial, el ciberdelito ocupó más del 60% de casos conocidos, con un coste de alrededor de $ 600.000 millones (0,8% del PIB mundial) para la economía global (7), tan solo superado por la corrupción y por el tráfico de drogas.

- Por la gravedad de sus consecuencias, la principal amenaza, contrastada y compartida por todos los Estados occidentales es el ciberterrorismo. El ciberespacio se ha configurado como una herramienta esencial utilizada por los grupos yihadistas para la consecución de sus fines. Son sobradamente conocidos los perversos efectos que ofrecen las Tecnologías de la Información y las Comunicaciones (TIC) e Internet en la radicalización de individuos y colectivos, en la financiación de grupos y organizaciones terroristas, en la divulgación de técnicas y herramientas para la comisión de atentados y en el adiestramiento de terroristas. Paralelamente, se remarca la importancia del *hacktivismo*, caracterizado por su motivación ideológica y por el ataque a instituciones y entidades, estando en la base de numerosas actividades antisistema.

- Íntimamente relacionado con ello, la amenaza contra las infraestructuras críticas, con una posibilidad cierta de causar un colapso a través de las redes mediante una caída en cadena de nuestros servicios esenciales. Precisamente por ello, la Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información, destaca en su Preámbulo que dicho tipo de acciones constituyen una amenaza creciente en la Unión y en el resto del mundo, y que cada vez es más preocupante la posibilidad de ataques terroristas o de naturaleza política contra los sistemas de información que forman parte de las infraestructuras críticas de los Estados miembros y de la Unión. La Ley 8/2011, que regula la protección de las infraestructuras críticas en España, y su reglamento de desarrollo, el Real Decreto 704/2011 inciden también en la necesidad de considerar la ciberseguridad como parte indispensable de la protección de los activos que proporcionan los servicios esenciales.

A estas amenazas, claramente delimitadas por la legislación española en el marco competencial del Ministerio del Interior, se le deben añadir otras líneas de acción, vitales para la ciberseguridad de nuestro país, pero que deben ser ejercidas por otros Departamentos Ministeriales, entre ellas:

- La protección de los sistemas militares y de defensa, a cargo del Ministerio de Defensa.

- La búsqueda de la mejor protección de las TIC en el sector privado, el impulso al desarrollo industrial y el refuerzo del I+D+i en materia de ciberseguridad, competencia del Ministerio de Energía, Turismo y Agenda Digital.

- La cultura de ciberseguridad, la formación de profesionales. o el compromiso internacional, con altas responsabilidades para los Ministerios de Educación y Ciencia, o el de Asuntos Exteriores y Cooperación.

- La protección contra las actividades de ciberespionaje, sobre la que es competente el Centro Nacional de Inteligencia.

- La coordinación de todas estas actividades, ejercida desde la Presidencia del Gobierno, a través del Departamento de Seguridad Nacional.

Aproximación del Ministerio del Interior a la ciberseguridad

Como anteriormente me refería, la aproximación a la ciberseguridad, si bien de nuevo cuño, no debe, ni puede, ser tratada de forma distinta, conceptualmente hablando, del de la SEGURIDAD, con mayúsculas, que es el concepto superior que le da cobertura. Y es que, en el momento en el que el prefijo «ciber» es retirado, volvemos al mundo físico, a un contexto mucho mejor conocido, con amenazas sobradamente estudiadas.

Y por supuesto, con los mismos agentes de la amenaza, que no varían en absoluto, como ya pudimos observar líneas atrás

FIGURA 5
PILARES DE LA CIBERSEGURIDAD Y AGENTES RESPONSABLES

Fuente: Departamento Nacional de Seguridad. Gobierno de España

Ello nos lleva a que la ciberseguridad no es un elemento ni ajeno, ni distinto, al concepto global de seguridad, como bien reconoce nuestra propia Estrategia de Seguridad Nacional. La aproximación a la ciberseguridad requiere, así, de la aplicación de una estrategia integral, y cualquier estrategia relacionada con la seguridad debe abarcar de manera transversal cuatros pilares básicos de actuación: *prevención*, *protección*, *respuesta* y *persecución* (8).

De esta manera, la ciberseguridad debe ser abordada, por supuesto, con las herramientas, medios y metodologías propias de las nuevas tecnologías, pero sin perder de vista la perspectiva integral, innovadora y aglutinadora de acciones en los cuatros pilares antes referidos, que permitan conectar las políticas y acciones que se implanten con otros campos existentes en nuestra Estrategia de Seguridad Nacional.

Como se ha podido ver en páginas anteriores, en el aspecto técnico de las acciones destinadas a dotar a nuestro país de la ciberseguridad adecuada, son los Centros de Respuesta a Incidentes Cibernéticos (o CSIRTS) nacionales, así como los organismos con capacidades de ciberseguridad, los competentes para llevar a cabo las actuaciones en los pilares de *prevención*, *protección* y *respuesta*. Destacan así el CCN-CERT, competente en lo referido a la ciberseguridad de las Administraciones Públicas, el INCIBE-CERT, en lo relativo al sector privado y ciudadanos, el MCCD, en materia de ciberseguridad de redes y sistemas militares, así como las unidades del Ministerio del Interior en el ejercicio de sus propias atribuciones. A todos ellos deben añadirse otros protagonistas cada vez más importantes para la seguridad nacional: las organizaciones privadas, que tienen sus propias capacidades para salvaguardar sus activos, y de paso, los servicios que proporcionan.

Sin embargo, el último ámbito, el de la *persecución*, es exclusivo del ministerio del Interior. Y es que, desde el momento en que se produce un ciberataque, estamos hablando de una cuestión que, en principio, puede ser judicializada y por tanto, el resto de actuaciones estarían totalmente condicionadas al concepto de *policía judicial* que es, como es bien sabido, cuestión exclusiva de las Fuerzas y Cuerpos de Seguridad.

De esta manera, es importante resaltar que, en España, el único Ministerio presente en todo el ciclo de vida de la ciberseguridad, conforme a los cuatro pilares ya reseñados es el del Interior y, como se verá más adelante, el pivote sobre el que gira la coordinación en estos cuatro pilares es el Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC) (9).

Protección de las infraestructuras críticas y ciberseguridad: el CNPIC

Dentro de las competencias del Ministerio del Interior, una labor crucial en el mantenimiento de la seguridad de las redes y el ciberespacio en España lo llevan ejerciendo las unidades tecnológicas de las Fuerzas y Cuerpos de Seguridad del Estado (tanto las que investigan los ciberdelitos, como las que ejercen su actividad luchando contra el terrorismo). Sin embargo, es el CNPIC el órgano responsable en materia de protección de infraestructuras, lo que incluye el ámbito de la ciberseguridad a través de su Oficina de Coordinación Cibernética.

FIGURA 6
LOGO DEL CENTRO NACIONAL DE PROTECCIÓN DE INFRAESTRUCTURAS Y CIBERSEGURIDAD

Fuente: Departamento Nacional de Seguridad. Gobierno de España

Siendo el CNPIC, dependiente de la Secretaría de Estado de Seguridad del Ministerio del Interior, el órgano responsable de impulsar, coordinar y supervisar todas las actividades relativas a la protección de las infraestructuras críticas en el territorio nacional, desde su creación en 2007, una de las primeras medidas adoptadas fue la integración de la ciberseguridad en los procesos de identificación, evaluación y seguimiento de las mismas.

De este modo, todas las iniciativas desde aquel momento han tenido como fondo común la integración de la ciberseguridad y de la seguridad física más tradicional en un proceso unitario. De hecho, cabe destacar que en la legislación española no se hace referencia particular a ninguna de ellas; por este mismo motivo, el concepto elegido por el CNPIC para hacer referencia a esta aproximación fue el de *seguridad integral*, concepto que se ha impuesto y ha quedado firmemente implantado en el mundo de la seguridad española.

No obstante, de cara a equilibrar la percepción de ambos tipos de seguridad, a nivel interno se detectó la necesidad de acrecentar el nivel de concienciación en ciberseguridad, no sólo de cara a los propios operadores críticos (en su mayoría del sector privado), sino también incluyendo a otros organismos públicos competentes, tanto dentro como fuera del Ministerio del Interior.

Para ello, se determinó que lo más apropiado era crear un ente con capacidades de coordinar las capacidades del Ministerio del Interior, a la vez de enlazar con las capacidades de terceros organismos implicados, tanto del sector público como privado. Todo ello resultó en la creación, en noviembre de 2014, de la Oficina de Coordinación Cibernética (OCC), integrada en la Secretaría de Estado de Seguridad y dependiente orgánicamente del CNPIC.

De este modo, el CNPIC se vio obligado a cambiar su estructura orgánica en materia de ciberseguridad, para adaptar las nuevas capacidades que se le asignaban, y sobre todo para garantizar un adecuado engarce con las actividades que ya se venían desarrollando en materia de protección de infraestructuras críticas. Esto se confirmó en julio de 2018, a través del Real Decreto 952/2018, por el que se desarrolla la estructura orgánica básica del Ministerio del Interior; este reglamento no sólo asigna misiones concretas a la mencionada Oficina de Coordinación Cibernética, sino que cambia la propia denominación del CNPIC, que sin mudar sus siglas pasa a denominarse desde ese momento *Centro Nacional de Protección de Infraestructuras y Ciberseguridad*.

El CNPIC, por lo que se acaba de ver tiene, por tanto, una doble orientación claramente definida: una, la más tradicional, está dirigida a la protección de las infraestructuras críticas y los servicios esenciales; tiene un carácter integral, y por tanto engloba también la necesidad de dotar de ciberseguridad a nuestras infraestructuras, redes y sistemas.

Y la segunda, más reciente, está dedicada a las funciones de coordinación de los cometidos de ciberseguridad encomendados al Ministerio del Interior.

En lo relativo al primero de los cometidos del Centro, el de protección de infraestructuras críticas en su más amplio sentido, el fin fundamental es el *disponer de un sistema coordinado (el Sistema PIC) entre las instituciones de gobierno y la empresa para una mejor protección de las infraestructuras críticas y los servicios esenciales del país.* Esto se lleva a cabo a través de tres objetivos estratégicos:

1. Que los operadores, sean éstos públicos o privados, tomen medidas para optimizar la seguridad de sus infraestructuras críticas y sus redes. Es, por tanto, obvio que la ciberseguridad debe ser parte de esos esfuerzos de planificación e implantación de una seguridad integral.

2. Garantizar la seguridad y derechos de los ciudadanos y su acceso a los servicios esenciales, como bien básico sobre el que se apoya nuestra vida y nuestro sistema de convivencia. Y, finalmente,

3. La evolución del sistema al cambio tecnológico y al cambio del modelo de seguridad nacional. Por eso, este sistema, que nació siendo eminentemente físico y sobre objetivos definidos ha evolucionado hacia un concepto de seguridad integral, que prioriza los servicios y los sistemas sobre las infraestructuras concretas.

El Sistema PIC está compuesto por 8 departamentos ministeriales, y por otros tantos organismos de la Administración General del Estado, y la administración auto-

FIGURA 7
OBJETIVOS ESTRATÉGICOS DEL SISTEMA PIC

Fuente: Departamento Nacional de Seguridad. Gobierno de España

nómica y local. A esto se le deben añadir los operadores críticos (aquellos que gestionan las infraestructuras críticas y los servicios esenciales), una figura creada por primera vez por la Ley 8/2011. Esto fue en su momento un hecho sin precedentes, ya que se dio la oportunidad, por primera vez en España, a actores del sector privado, a participar en la propia seguridad nacional.

El Sistema PIC está presidido por el Secretario de Estado de Seguridad, con el apoyo del CNPIC. Como ya se ha subrayado, los operadores de los sectores estratégicos juegan un papel clave, donde las relaciones se basan principalmente en la confianza, en el intercambio de información y en la confidencialidad de los datos intercambiados por ambas partes.

Actualmente, el Sistema PIC está compuesto por alrededor de 220 actores, de los cuales más de 170 son operadores críticos, y constituye todo ello la mayor comunidad de cooperación público-privada de España en seguridad. En un momento en que en materia de ciberseguridad se aboga por la necesaria cooperación público-privada, debe tenerse en cuenta este caso de éxito para extenderlo, como ya se está haciendo por el CNPIC, también al ámbito de la ciberseguridad.

En la segunda de las misiones del CNPIC, la dirigida exclusivamente a la ciberseguridad, el rol que el Ministerio del Interior ha querido dar a este Centro es el de constituirse en correa de transmisión entre los diferentes agentes, participando en todo el ciclo de vida de la ciberseguridad. Todo ello, a través de:

1. La integración, coordinación y contacto de tipo técnico con los CSIRT nacionales en las fases de prevención, protección y respuesta. Cabe recordar que el CNPIC participa de forma activa en el INCIBE-CERT, y mantiene contacto y coordinación permanente con los otros dos.

2. La transmisión de información e inteligencia a las FCSE para la persecución del ciberdelito. Al tener acceso a gran cantidad de información técnica, el CNPIC tiene posibilidad de trasladar a las unidades de ciberdelincuencia y ciberterrorismo de los cuerpos policiales datos para su explotación y para su judicialización e investigación, algo que sólo pueden hacer las Fuerzas y Cuerpos de Seguridad.

3. Finalmente, y de cara a los operadores críticos, la pieza clave del Sistema PIC, es obligado decir que esta misma información puede y debe ser trasladada (obviamente bajo el presupuesto básico de *necesidad de conocer*) para prevenir nuevos ataques, responder a los existentes y recuperarse mejor de aquellos padecidos.

Como ya se ha indicado en líneas anteriores, esta segunda función se realiza a través de la Oficina de Coordinación Cibernética.

LA OFICINA DE COORDINACIÓN CIBERNÉTICA (OCC)

La Oficina de Coordinación Cibernética tiene por misión principal el asegurar la coordinación técnica entre el Ministerio del Interior y sus organismos dependientes y el CERT de Seguridad e Industria, asesorando asimismo al Secretario de Estado de Seguridad en materia de ciberseguridad (10).

FIGURA 8
OBJETIVOS ESTRATÉGICOS DE LA CIBERSEGURIDAD EN EL CNPIC

Fuente: Departamento Nacional de Seguridad. Gobierno de España

FIGURA 9
LOGO DE LA OFICINA DE COORDINACIÓN CIBERNÉTICA

Fuente: Departamento Nacional de Seguridad. Gobierno de España

De este modo para el cumplimiento de su misión, la Oficina de Coordinación Cibernética debe asegurar que dispone de la información estratégica y técnica necesaria. Todo ello se consigue mediante la consecución de los siguientes objetivos específicos:

1. Implementación de mecanismos de coordinación de respuesta ante ciberincidentes que recaigan en los ámbitos competenciales del Ministerio del Interior, teniendo capacidades para llevar a cabo los siguientes cometidos:

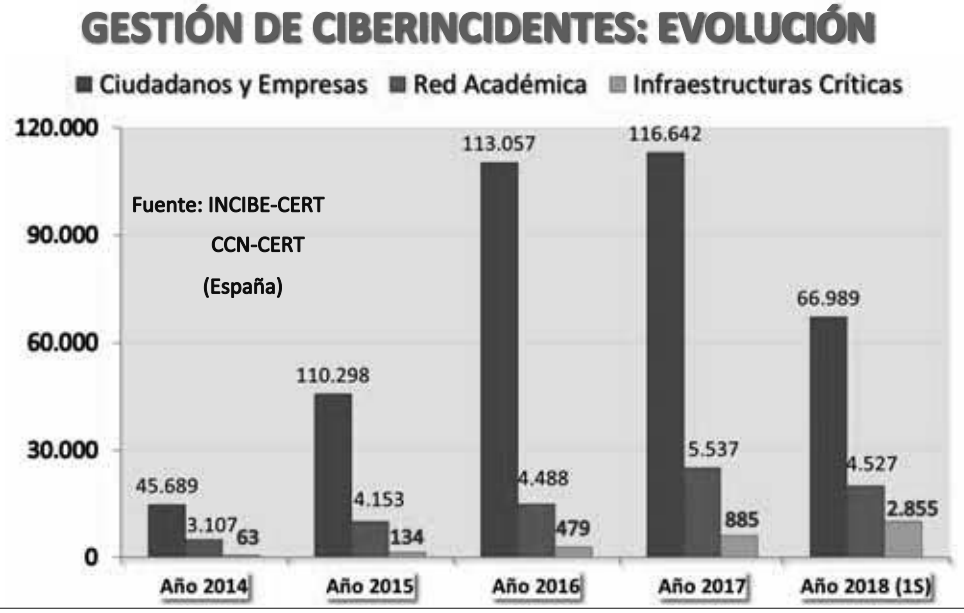
   - Llevar a cabo una definición de protocolos específicos con el INCIBE-CERT y con el CCN-CERT, en los ámbitos competenciales de cada uno de estos organismos técnicos así como, en su caso, con el CSIRT del Mando de Ciberdefensa. Todo ello, en colaboración con los responsables técnicos de los sistemas afectados y con el objeto de facilitar la adecuada gestión del incidente y la posterior resolución y recuperación de los sistemas implicados.

   - Proporcionar a las unidades tecnológicas de las Fuerzas y Cuerpos de Seguridad del Estado (Guardia Civil y Cuerpo Nacional de Policía) aquella información técnica extraída de las actividades de los CSIRT nacionales, o de aquellos otros agentes que en este campo puedan ser de utilidad. Todo con objeto de complementar en la medida de lo posible las capacidades de investigación y persecución del delito que llevan a cabo estas unidades.

   - Recibir y procesar oportunamente datos de interés que, procedentes de las actividades de las unidades tecnológicas de las Fuerzas y Cuerpos de Seguridad del Estado, puedan suponer una mejora en la gestión de incidentes.

2. Conocimiento del estado general de situación sobre ciberamenazas y avances tecnológicos. Para ello, la Oficina de Coordinación Cibernética de-

FIGURA 10
EVOLUCIÓN DE CIBERINCIDENTES GESTIONADOS POR EL CCN-CERT, EL INCIBE-CERT Y LA OCC SOBRE OPERADORES CRÍTICOS



Fuente: Departamento Nacional de Seguridad. Gobierno de España

sarrolla los siguientes cometidos en materia de ciberseguridad:

- Estudios y análisis de situación en materia de ciberseguridad.
- Desarrollo de guías, procedimientos y buenas prácticas de ámbito técnico.
- Difusión de procedimientos específicos de resolución de incidentes relacionados con vulnerabilidades concretas, notas informativas, estudios de amenaza, alertas o incidentes, obtenidos en el desempeño de sus funciones.

De este modo, como se puede observar, una de las funciones de la Oficina de Coordinación Cibernética es la de operar conjuntamente con el INCIBE-CERT, apoyándole en su gestión, cuando se trate de la protección y seguridad de operadores críticos de carácter privado.

En el ámbito de la gestión de incidentes, alerta temprana e intercambio de información, la Oficina de Coordinación Cibernética ha llevado a cabo ya, en colaboración bien con el INCIBE, bien con el CCN-CERT, más de 4.300 actuaciones desde su creación. Tan sólo en el primer semestre de 2018 se gestionaron 2.855 que de alguna forma afectaban a operadores de servicios esenciales españoles. Todo ello es indicativo de que, a la par de que el nivel de actividades maliciosas en el ciberespacio está aumentando, el nivel de preparación, colaboración y cooperación entre los distintos organismos responsables es cada vez mayor.

Actividades

Como proceso derivado de la integración de nuevas capacidades, la Oficina de Coordinación Cibernética del CNPIC ha reforzado las actividades propias en materia de ciberseguridad, que en relación con la protección de las infraestructuras críticas se pueden agrupar en las siguientes:

Concienciación

La concienciación en materia de ciberseguridad es un aspecto fundamental que debe sustentar el desarrollo de actividades más concretas. En este sentido, desde el CNPIC se ha fomentado la participación activa en foros en los que poder discutir asuntos relativos a la protección de las infraestructuras críticas y el impacto de su dependencia tecnológica. Durante 2018 se ha participado en un total de 44 foros internacionales, fundamentalmente en Europa e Iberoamérica. Del mismo modo, existen relaciones fluidas con la Comisión Europea (el CNPIC es el punto de contacto español en materia de protección de infraestructuras críticas), ENISA y la Organización de Estados Americanos (OEA) que hacen que el Centro juegue un papel relevante en la exposición de políticas nacionales en materia de ciberseguridad y protección de infraestructuras críticas en el exterior.

Mención especial merece el denominado proceso MERIDIAN. Este proceso conjuga una serie de iniciativas que tienen por objeto promover la ciberseguridad en el ámbito de la protección de las infraestructuras críticas de la información (CIIP (11)) a nivel internacional. Ejemplo de estas iniciativas fueron el desarrollo de un Directorio que integra los puntos de contacto CIIP a nivel mundial, la

publicación de la revista digital «CIIP Matters», la creación de un grupo de trabajo específico sobre sistemas de control industrial (MPCSIE (12)), así como guías para la planificación de estrategias CIIP. El CNPIC ha venido participando activamente en este foro desde el año 2008, ostentando su presidencia en 2015.

Ejercicios

Los ciberejercicios son una forma de poner en práctica las capacidades existentes, posibilitando la adquisición de nuevos conocimientos que sirvan para reforzar los mecanismos de prevención, detección y respuesta frente a incidentes, fundamentalmente. El CNPIC, a través de la Oficina de Coordinación Cibernética, ha tenido una presencia muy activa, tanto a nivel nacional como internacional, en los siguientes:

- **Cyber-EX**. Dentro de las actividades llevadas a cabo junto con INCIBE, en el marco del convenio de colaboración existente en materia de ciberseguridad, se han venido llevando a cabo distintos ejercicios nacionales orientados a promover la protección de las infraestructuras críticas, más concretamente en lo que respecta a la mejora de las capacidades de respuesta y coordinación.
    - En 2014 el ejercicio giró en torno a la aparición de una amenaza persistente avanzada (APT), para la que se requería simular una respuesta al incidente por cada uno de los participantes.
    - La versión del año 2015 del Cyber-EX estuvo centrada en el sector financiero. Aprovechando la disponibilidad de su respectivo Plan Estratégico Sectorial, se pretendía fomentar el nivel de concienciación y cultura de la seguridad en el sector.
    - La edición de 2018 tuvo un carácter multisectorial, con cuatro objetivos fundamentales: la evaluación y mejora de la capacidad de respuesta ante incidentes; el refuerzo de la coordinación interna entre entidades; la profundización en la concienciación y sensibilización de los riesgos a todos los niveles; y la mejora de la imagen y reputación de la organización. El carácter multisectorial permite la inclusión de variables interdisciplinares y la participación de roles en las áreas de marketing y comunicación, continuidad de negocio y financiero o legal, por encima del responsable de seguridad o ciberseguridad, más habitual en anteriores ediciones.
- **Cyber-EX Internacionales**. La Organización de Estados Americanos (OEA), el Instituto Nacional de Ciberseguridad y el CNPIC pusieron en marcha en junio de 2015 la primera edición de los ciberejercicios ***International CyberEx***, que se han convocado anualmente. El desarrollo de los International CyberEx contemplan la ejecución de un ciberejercicio en el marco de los Estados Miembros de la Organización de los Estados Americanos (OEA) que permite el fortalecimiento de las capacidades de respuesta ante incidentes cibernéticos, así como una mejora de la colaboración y cooperación ante este tipo de incidentes. Los destinatarios de esta experiencia son equipos formados por expertos en ciberseguridad que trabajan en diferentes Centros de Respuesta a Incidentes de Ciberseguridad de los 34 Estados Miembros de la OEA, así como otros países observadores invitados. La participación por países permite la configuración interna de cada país de un equipo que incluye profesionales de distintos ámbitos y refuerza la colaboración entre instituciones. En la edición de 2018 se incorporaron como novedad dos centros de seguimiento: la sede de INCIBE, donde participan los miembros del CNPIC, y la de la OEA, en Washington.
- **CyberEurope**. Desde la primera edición de estos ciberejercicios, llevada a cabo en 2010, el CNPIC ha venido participando activamente tanto en la planificación como en la ejecución de la mayoría de sus ediciones. Los ejercicios CyberEurope se convocan cada dos años; en todas las ediciones, el CNPIC ha estado presente como jugador a la vez que asesorando al Departamento de Seguridad Nacional (DSN) en el desarrollo del escenario con el auspicio de ENISA, en aquellos aspectos relativos a la protección de las infraestructuras críticas. La edición de 2018 se incardinó en el sector aéreo, con la implicación de instalaciones aeroportuarias y compañías aéreas. La colaboración con el Departamento de Seguridad Nacional (DSN) en la coordinación y difusión de elementos claves para el desarrollo del ejercicio y la activación del Plan Estratégico Sectorial del transporte en el Subsector aéreo serán implicaciones relevantes de CNPIC en este ejercicio.
- **CIISC-T2**. El proyecto «*Critical Infrastructure: Improvement of Security Control Against the Terrorist Threat*» es un proyecto cofinanciado por la Comisión Europea a través del programa CIPS en el que el CNPIC, y el Centro de Inteligencia contra el Terrorismo y el Crimen Organizado (CITCO) del Ministerio del Interior actúan como co-beneficiarios. Enmarcado en este proyecto, el Servicio de Ciberseguridad y OFICINA DE COORDINACIÓN CIBERNÉTICA del CNPIC participó en 2014 como coordinador del ciberejercicio presentado en las II Jornadas PSCIC (13). Este ciberejercicio está centrado en un escenario en el que los sistemas SCADA juegan un papel fundamental, en un ejercicio que a nivel europeo plantea la necesidad de incrementar el nivel de concienciación y protección de los sistemas de control industrial.
- **CMX (Crisis Management Exercise)**. El CNPIC participó como planificador y jugador en el ejercicio CMX 2014, organizado por OTAN con la participación de los países aliados. A nivel nacional, estos ejercicios son liderados por el CESEDEN. Como resultado de estos trabajos, se planificó un escena-

rio referido a la respuesta frente a un ciberataque sufrido por una infraestructura crítica nacional. En la misma línea la edición del año 2016 realizó una simulación de afectación en los servicios esenciales de gestión de pasajeros y de mercancías en el aeropuerto de Las Palmas con la activación del Plan de Apoyo Operativo del Operador, y en 2017 se realizó un desarrollo de APT con intención político-delincuencial dirigido a varias infraestructuras de carácter crítico dentro de un entorno históricosocial y político norteafricano.

- **Locked Shields**. Este ciberejercicio, organizado por el Centro de Excelencia de Ciberdefensa (CCD-COE) de la OTAN, contó con la presencia, en la edición del 2017 y del 2018, de personal del CNPIC. Este personal estuvo conformado por expertos destacados en análisis de vulnerabilidades y protección de sistemas y redes de comunicación IT/OT, que se integró en el equipo nacional liderado por el Mando Conjunto de Ciberdefensa (MCCD). En la edición del 2018 la misión del equipo CNPIC se trataba de proteger varias máquinas de la Red de suministro eléctrico y de la planta purificadora de agua, quedando patente la alta dependencia de los sistemas OT con IT.

- **Cyber Coalition Exercise**. Patrocinado por el Mando Conjunto de Ciberdefensa (MCCD), enfocado al entorno de sistemas de radar, especialmente relativo al ADS (Air Defence System) de la OTAN, la participación de los componentes del CNPIC consiste en el análisis forense de PLC encargado del control de un sistema guiado y de localización (Radar) de espacio aéreo.

Implementación normativa

El creciente número de operadores estratégicos definidos (más de 170 a día de hoy) tras la implantación de la normativa PIC (Ley 8/2011 y RD 704/2011) hace que aumente igualmente la cantidad de planes de seguridad que deben ser revisados y aprobados por el CNPIC. Actualmente la mayoría de operadores críticos han aportado ya sus respectivos planes de seguridad del operador, y poco a poco van presentando también los consecuentes planes de protección específicos de cada una de las infraestructuras catalogadas como críticas. La inmensa mayoría de éstos serán también objeto del ámbito de aplicación del Real Decreto-Ley 12/2018, de seguridad de redes y sistemas de información, recientemente aprobado.

En todo este proceso de revisión y aprobación, siguiendo el criterio de uniformidad en la evaluación de la seguridad física y la ciberseguridad, la Oficina de Coordinación Cibernética hace las oportunas aportaciones y comentarios que en el marco de la ciberseguridad garanticen una apropiada protección de las infraestructuras críticas nacionales.

De forma paralela, dada la multiplicidad de las iniciativas emprendidas tanto a nivel europeo como internacional, la Oficina de Coordinación Cibernética hace un seguimiento continuo y participa activamente, en su caso, en aquellas actividades que puedan tener relación con la protección de las infraestructuras críticas nacionales, o que puedan afectar a las políticas que actualmente se siguen en la materia a nivel nacional.

Gestión de incidentes

Tal y como ya se ha mencionado, el INCIBE-CERT es operado conjuntamente por personal de INCIBE y del CNPIC. En este último caso, esto se materializa gracias a la asignación de personal de la Oficina de Coordinación Cibernética para cumplir con esta tarea. Cabe destacar que, si bien se utilizan sistemas conjuntos entre INCIBE y CNPIC, éste último tiene personal asignado en las oficinas de INCIBE, en León, para asegurar la correcta sincronización de los protocolos empleados, agilizando la coordinación interna.

El incremento producido en el número de incidentes gestionados (más de 123.000 en 2017, como se ha podido ver en la tabla anterior) se debe, entre otros factores, a la mejora de las capacidades del INCIBE-CERT. Pero, además, se debe tener en cuenta que, en el caso concreto de la comunidad que aglutina a los operadores de servicios esenciales, el número de beneficiarios ha crecido en los últimos años como consecuencia de nuevas designaciones y de los trabajos relativos a la definición de nuevos planes estratégicos. A esto debe unirse la labor que el CCN-CERT realiza sobre el público objetivo del sector público y administración, algunos de los cuales son también operadores críticos y proveedores de servicios esenciales.

En el caso particular de los operadores críticos, cabe destacar que los servicios que se ofertan a través del INCIBE-CERT deben ir sustentados en la firma de un acuerdo de confidencialidad que permite garantizar el adecuado tratamiento de la información intercambiada y gestionada, aspecto que desde su creación el CNPIC ha venido promoviendo en todos sus ámbitos de actuación.

Finalmente, cabe destacar que la Oficina de Coordinación Cibernética fue también designada como punto de contacto español, para la comunicación entre los Estados miembros y con la Comisión Europea, de aquellos ataques contra los sistemas de información previstos por la Directiva 2013/40/UE, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información. Como consecuencia de esta directiva, se transpusieron una serie de nuevos tipos a nuestro Código penal (14).

Esta Directiva, concretamente de su artículo 13, determina que los Estados miembros deberán «*garantizar la existencia permanente de un punto de contacto nacional operativo a efectos del intercambio de información sobre ciberataques*». Así mismo, establece la necesidad de que se cuenten con aquellos medios y procedimientos para que, en caso de solicitud de ayuda urgente, la autoridad competente pueda indicar, en un plazo máximo de ocho horas a partir de la recepción

FIGURA 11
FUNCIONES DE LA OCC DERIVADAS DE LA DIRECTIVA 2013/40/UE

Fuente: Departamento Nacional de Seguridad. Gobierno de España

de la solicitud de ayuda, si la misma podrá ser atendida, y la forma y el plazo aproximado de ello.

En este sentido, y a los efectos de lo estipulado por el artículo 13 de dicha Directiva, la Oficina de Coordinación Cibernética del CNPIC, actúa hoy día como punto de contacto operativo nacional en esta materia. Esta designación quedó reflejada tanto en la Instrucción 2/2016 de la Secretaría de Estado de Seguridad como en el propio Real Decreto 952/2018 varias veces mencionado.

CONCLUSIONES

Como se ha presentado en estas líneas, El Gobierno de España está apostando decididamente por la ciberseguridad de nuestro país. Esto implica, no sólo el desarrollo de cuerpos normativos y regulatorios, así como de estrategias específicas, sino también la dotación de capacidades y medios, económicos, humanos, materiales y tecnológicos.

Desde el Ministerio del Interior español y desde el CNPIC, en una perspectiva más limitada, se concibe la ciberseguridad como uno de los aspectos que posibilitan el fomento de la seguridad pública y ciudadana. En el caso particular de las infraestructuras críticas, cuya alteración o interrupción tendría consecuencias imprevisibles que alterarían en cualquier caso el normal desempeño de nuestro desarrollo como sociedad moderna, es aún más destacada la necesidad de incrementar las capacidades de ciberseguridad. En este sentido, a lo largo de estos últimos años se ha trabajado en la definición de un nuevo modelo de trabajo que posibilitase esta potenciación de capacidades, lo que ha resultado en una adecuación de la estructura del CNPIC para cubrir todas las funciones encomendadas por la Ley.

El crecimiento de capacidades propias ha resultado en la ejecución, con resultados altamente satisfactorios, de distintas actividades orientadas fundamentalmente a ofrecer servicios extraordinarios a los operadores críticos nacionales, que complementen los que éstos ya implementan de forma óptima.

Todo el éxito obtenido hasta el momento en materia de ciberseguridad en el ámbito de la protección de las infraestructuras críticas ha sido posible gracias a la inestimable colaboración de los propios operadores críticos, en un ejercicio de colaboración público-privada ejemplar, sin cuya confianza y soporte no hubiese sido posible avanzar de la manera en que se ha hecho.

Finalmente, pero no por ello menos importante, la colaboración con los países amigos y aliados es una premisa del mayor interés para fortalecer la seguridad de nuestros activos críticos y de nuestros ciudadanos.

NOTAS

[1] En su novela *Neuromancer* (1.984), el escritor de ciencia ficción William Gibson acuñó el término ciberespacio para describir un mundo virtual que apenas se estaba gestando pero que parecía podía absorber la realidad en un ecosistema en el que la información sería aún más esencial que la materia. Con el tiempo, el

término «ciberespacio» ha acabado siendo aceptado ampliamente como un sinónimo de Internet.

[2] Según datos de este mismo informe, el impacto de Internet y las redes sociales es imparable. Globalmente, la empresa consultora y de investigación de las tecnologías de la información Gartner, calcula que en 2017 existían cerca de 8.400 millones de dispositivos con conexión a Internet (superando ya en más de mil millones el número de habitantes del planeta, cifrado en 7.600 millones de personas). Pero es que en 2020 los dispositivos con conexión a Internet (el Internet de las cosas) serán alrededor de 20.400 millones.

[3] Las tecnologías de la información (TI) se refieren a la aplicación de sistemas computacionales, como ordenadores, redes, televisiones o teléfonos, dedicados al almacenamiento, recuperación, transmisión o manipulación de información. Se trata, por tanto, de un término amplio que abarca distintos elementos tanto hardware como software. Estas tecnologías se caracterizan, de forma general, por su empleo en entornos domésticos o profesionales que requieren una interacción humana directa. En ella imperan grandes proveedores de datos y aplicaciones corporativas, HP, IBM, Microsoft, Oracle y otros productos Open Source basados en Linux.

Por su parte, las tecnologías de la operación (TO), aunque se pueden considerar parte de las primeras, en lo que respecta a la gestión de datos e información, pero la interacción humana se minimiza. Esto es así porque los sistemas TO están diseñados para controlar entornos industriales o físicos, de modo que tienen por objeto monitorizar o manipular físicamente otros sistemas o piezas industriales o físicas, como puede ser el caso de subestaciones eléctricas, vías ferreas, plantas químicas, factorías de producción, centrales logísticas de distribución o centrales nucleares, entre otros. De hecho, el término TO surgió en cierto modo para demostrar las diferencias tanto técnicas como funcionales que existían entre estos entornos industriales y corporativos con sistemas TI más tradicionales.

[4] La Unión Europea, para aproximarse a este problema, adoptó en abril de 2016 la Comunicación Conjunta de la Comisión y la Alta Representante relativa a un Marco de Lucha contra las Amenazas Híbridas (http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52016JC0018&from=es), efectuando la siguiente definición de la amenaza híbrida: «combinación de acciones convencionales y no convencionales, militares y no militares, abiertas y encubiertas, que pueden ser utilizadas de manera coordinada por agentes estatales o no estatales para lograr objetivos específicos, al tiempo que se mantienen por debajo del umbral de la guerra declarada oficialmente. Se centran en las vulnerabilidades críticas y tratan de crear ambigüedad para obstaculizar una toma de decisiones rápida y eficaz. La gama de medidas aplicadas como parte de una campaña híbrida puede ser muy amplia: desde ciberataques a sistemas de información críticos, pasando por la interrupción de servicios críticos, como el suministro de energía o los servicios financieros, hasta socavar la confianza pública en las instituciones gubernamentales o explotar las vulnerabilidades sociales».

[5] La Resolución 2341, aprobada por el Consejo de Seguridad en su 7882ª sesión, de 13 de febrero de 2017, establece, entre otros, los siguientes considerandos:

«Reconociendo la creciente importancia de garantizar la fiabilidad y la resiliencia de la infraestructura crítica y su protección frente a atentados terroristas para la seguridad nacional, la seguridad pública y la economía de los Estados afectados, así como para el bienestar de su población»(..)

«Reconociendo que, como consecuencia de la creciente interdependencia entre los sectores de infraestructura crítica, algunas infraestructuras críticas pueden ser objeto de un número cada vez mayor y una variedad cada vez más amplia de amenazas y vulnerabilidades que plantean nuevos problemas de seguridad» (..)

«Expresando preocupación por el hecho de que los atentados terroristas contra la infraestructura crítica podrían perturbar considerablemente el funcionamiento del gobierno y del sector privado por igual y tener repercusiones más allá del sector de la infraestructura» (..)

«Reconociendo a este respecto que la protección de las infraestructuras críticas es mucho más eficaz cuando se basa en un enfoque en que se tienen en cuenta todos los peligros y las amenazas, especialmente los atentados terroristas, y cuando se conjuga con consultas y cooperación periódicas y sustantivas con los operadores de infraestructuras críticas y los agentes de las fuerzas del orden y de seguridad encargados de la protección de infraestructuras críticas, así como, cuando procede, con otros interesados, incluidos propietarios del sector privado» (..)

[6] El término CSIRT proviene de las siglas en inglés Computer Security Information Response Team , y viene a definir a un equipo de personas altamente especializado, dedicado a la implantación y gestión de medidas tecnológicas con el objetivo de mitigar el riesgo de ataques contra los sistemas informáticos de la comunidad a la que se proporciona el servicio.

[7] Datos extraídos del informe «*Economic Impact of Cybercrime – No Slowing Down*», del CSIS (Center for Strategic and International Studies), en asociación con McAfee. Febrero 2018. El mismo informe, de 2014, establecía el coste del ciberdelito en $ 445.000 millones, por lo que el incremento en tan sólo 4 años ha sido de más de un tercio.

[8] Los 4 pilares fueron consagrados por vez primera en la Estrategia Europea de lucha contra el Terrorismo (30.11.2005), revisada en junio de 2014. Previamente a esa estrategia, dichos términos ya aparecieron en sendos documentos «Declaration on combating terrorism» (29.03.2004) y «EU Plan of Action on Combating Terrorism» (15.06.2004).

En términos generales, estos conceptos (prevenir, proteger, responder, perseguir) se usan a nivel internacional en cualquier estrategia sobre seguridad. La Organización para la Seguridad y la Cooperación en Europa (OSCE) ya lo incorpora a sus documentos habitualmente, mientras que en Estados Unidos se emplean de una manera más amplia, vinculados al concepto de resiliencia (Estrategia Defensa nacional de 2011).

[9] El CNPIC es el órgano responsable del impulso, coordinación y supervisión de todas las políticas y actividades relacionadas con la protección de las infraestructuras críticas españolas y con la ciberseguridad en el seno del Ministerio del Interior. Depende del Secretario de Estado de Seguridad, máximo responsable del Sistema Nacional de Protección de las Infraestructuras Críticas y de las políticas de ciberseguridad del Ministerio.
El CNPIC fue creado en el año 2007, mediante Acuerdo de Consejo de Ministros de 2 de noviembre, siendo sus competencias reguladas por la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas y por el Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.

[10] El funcionamiento, dependencias y misiones de la Oficina de Coordinación Cibernética está delimitado por sendas Instrucciones del Secretario de Estado de Seguridad (la 19/2014, de 19 de noviembre y la 2/2016, de 20 de mayo), así como por el Real Decreto 952/2018, de 27 de julio, por el que se desarrolla la estructura orgánica básica del Ministerio del Interior.

[11] Critical Information Infrastructure Protection.

[12] Meridian Process Control System Information Exchange.

[13] Protección de Sistemas de Control en Infraestructuras Críticas.

[14] El preámbulo de la Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, en su ordinal XIII, reza literalmente:
«Se modifican los delitos relativos a la intromisión en la intimidad de los ciudadanos, con el fin de solucionar los problemas de falta de tipicidad de algunas conductas.
El vigente artículo 197 contempla como delito, por un lado, el apoderamiento de cartas, papeles, mensajes de correo electrónico o cualesquiera otros documentos de naturaleza personal de la víctima y, por otro lado, la interceptación de cualquier tipo de comunicación de la víctima, sea cual fuere la naturaleza y la vía de dicha comunicación interceptada. Ambas conductas exigen la falta de consentimiento de la víctima.
Los supuestos a los que ahora se ofrece respuesta son aquellos otros en los que las imágenes o grabaciones de otra persona se obtienen con su consentimiento, pero son luego divulgados contra su voluntad, cuando la imagen o grabación se haya producido en un ámbito personal y su difusión, sin el consentimiento de la persona afectada, lesione gravemente su intimidad.
La reforma lleva a cabo la transposición de la Directiva 2013/40/UE, de 12 de agosto, relativa a los ataques contra los sistemas de información y la interceptación de datos electrónicos cuando no se trata de una comunicación personal.
Las modificaciones propuestas pretenden superar las limitaciones de la regulación vigente para ofrecer respuesta a la delincuencia informática en el sentido de la normativa europea.
De acuerdo con el planteamiento recogido en la Directiva, se introduce una separación nítida entre los supuestos de revelación de datos que afectan directamente a la intimidad personal, y el acceso a otros datos o informaciones que pueden afectar a la privacidad pero que no están referidos directamente a la intimidad personal: no es lo mismo el acceso al listado personal de contactos, que recabar datos relativos a la versión de software empleado o a la situación de los puertos de entrada a un sistema. Por ello, se opta por una tipificación separada y diferenciada del mero acceso a los sistemas informáticos.
Con el mismo planteamiento, y de acuerdo con las exigencias de la Directiva, se incluye la tipificación de la interceptación de transmisiones entre sistemas, cuando no se trata de transmisiones personales: la interceptación de comunicaciones personales ya estaba tipificada en el Código Penal; ahora se trata de tipificar las transmisiones automáticas –no personales– entre equipos.
Se tipifica la facilitación o la producción de programas informáticos o equipos específicamente diseñados o adaptados para la comisión de estos delitos.
Se regulan separadamente, de un modo que permite ofrecer diferentes niveles de respuesta a la diferente gravedad de los hechos, los supuestos de daños informáticos y las interferencias en los sistemas de información.
Finalmente, en estos delitos se prevé la responsabilidad de las personas jurídicas.»