Capítulo segundo

Crisis y ciberespacio: hacia un modelo integral de respuesta en el Sistema de Seguridad Nacional

Joaquín Castellón Moreno
Director Operativo
Departamento de Seguridad Nacional del Gabinete de la Presidencia del Gobierno
María Mar López Gil
Jefa de la Oficina de Tecnología y Seguridad. Responsable de Ciberseguridad
Departamento de Seguridad Nacional del Gabinete de la Presidencia del Gobierno

Resumen

La hiperconectividad y los constantes avances tecnológicos nos llevan a enfrentarnos a un mundo completamente desconocido y lleno de incertidumbre. El ciberespacio es un espacio de grandes oportunidades, pero también es imposible ocultar que en él se tensionan los intereses de los Estados con fines distintos, organizaciones terroristas y redes de crimen organizado se sirven de las facilidades que ofrece el medio.

Desde la creación del Departamento de Seguridad Nacional de la Presidencia del Gobierno hemos impulsado un modelo integrado de gobernanza para la ciberseguridad. Un modelo basado en la implicación de todos los actores y recursos del Estado y en la participación del sector privado y de la sociedad en general.

La participación del sector privado en la Seguridad Nacional es hoy en día ineludible y quizás sea la ciberseguridad un ámbito paradigmático en este sentido. Así ha quedado recogido en la Estrategia de Seguridad Nacional, la Estrategia de Ciberseguridad Nacional y, sobre todo, en la Ley de Seguridad Nacional.

El aspecto más innovador de la nueva Ley se encuentra en el articulado dedicado a la gestión de situaciones crisis y muy especialmente en la figura de la «situación de interés para la Seguridad Nacional».

Palabras clave

Seguridad Nacional**,** tecnología, hiperconectividad, ciberespacio, riesgos, amenazas, ciberseguridad, ciberamenazas, ciberataques, gestión de crisis, colaboración público privada, cultura, estrategia.

Abstract

The constant technological development and hyper connectivity are leading us through an uncharted and uncertain world. In this sense, the cyberspace represents great opportunities, but also a space where the diverging interests of states conflict and terrorist organizations and organized crime networks take advantage of its possibilities.

Since the establishment of the National Security Department, within the Presidency of the Government, we have promoted an integrated cybersecurity governance model. This model is based on the involvement of all state actors and their resources together with the participation of the private sector and civil society at large.

Nowadays, the participation of the private sector in National security issues is imperative and the field of cybersecurity is a paradigmatic example to this effect. This main idea has been included in the National Security Strategy, in the National Cybersecurity Strategy and, most importantly, in the recently passed National Security Act.

The most innovative aspect of this Act is found on the sections regulating crisis management and particularly the concept of «situation of interest for the National Security».

Keywords

National security**,** technology, hyperconectivity, cyberspace, risks, threats, cybersecurity, cyberthreats, cyberattacks, crisis management, public and private collaboration, culture, strategy.

Introducción

Desde el Departamento de Seguridad Nacional de la Presidencia del Gobierno (DSN) hemos impulsado a través de las Estrategia de Seguridad Nacional, la Estrategia de Ciberseguridad Nacional y, sobre todo, la Ley de Seguridad Nacional[1], la construcción de un sistema nuevo de gobernanza para la ciberseguridad en España. Un modelo integrado de gobernanza basado en la implicación, coordinación y armonización de todos los actores y recursos del Estado, en la colaboración público-privada y en la participación de la ciudadanía. Además, y dado el marcado carácter global de la ciberseguridad, la cooperación internacional forma parte esencial de este modelo.

En este capítulo recogemos algunos de los avances más importantes que se han dado en este ámbito prioritario de la Seguridad Nacional centrándonos fundamentalmente en la gestión de situaciones de crisis y cómo el sector privado está llamado a jugar un papel cada vez más relevante.

Hace poco más de tres años finalizamos los trabajos de elaboración de la Estrategia de Seguridad Nacional 2013[2]. Lógicamente, un trabajo de esta naturaleza requiere un ineludible esfuerzo previo para tratar de entender el mundo en que vivimos e intentar, al menos a grandes trazos, dibujar nuestro mundo futuro. En el DSN, entendimos el momento actual como una transición a lo que podríamos denominar una nueva era. Una nueva era que se va conformando por infinidad de factores, algunos de singular importancia, como el cambio climático, pero donde, por encima de cualquier otro factor, destacan las nuevas tecnologías y una conectividad sin precedentes.

La hiperconectividad y los constantes avances tecnológicos nos llevan a enfrentarnos a un mundo completamente desconocido y lleno de incertidumbre donde todos, en mayor o menor medida, somos vulnerables, donde se nos plantean nuevos retos, riesgos y amenazas que no pueden ser ignorados. Un mundo que se hace, día a día, cada vez más dependiente del ciberespacio dado que cualquier actividad dentro del ámbito público o privado tiene en este medio el marco idóneo para desarrollarse.

En la mencionada Estrategia de Seguridad Nacional del año 2013 destaca, como un objetivo prioritario de la Seguridad Nacional, garantizar el uso seguro del ciberespacio. Concretamente, la estrategia reconoce que España

[1] Ley 36/2015, de 28 de septiembre, de Seguridad Nacional].

[2] La Estrategia de Seguridad Nacional constituye el marco político estratégico de referencia de la Política de Seguridad Nacional. Contiene el análisis del entorno estratégico, concreta los riesgos y amenazas que afectan a la seguridad de España, define las líneas de acción estratégicas en cada ámbito de actuación y promueve la optimización de los recursos existentes. Se elabora a iniciativa del presidente del Gobierno, quién la somete a la aprobación del Consejo de Ministros. La actual Estrategia de Seguridad Nacional fue aprobada por el Consejo de Ministros en su reunión del 31 de mayo de 2013, disponible en www.dsn.gob.es

está expuesta a los ciberataques, que no solo generan elevados costes económicos, sino también, y lo que es más importante, la pérdida de confianza de los ciudadanos en unos sistemas que, en la actualidad, resultan críticos para el normal funcionamiento de la sociedad.

Plenamente conscientes de la importancia de la cuestión, el Consejo de Seguridad Nacional[3] aprobaba en diciembre de ese mismo año la Estrategia de Ciberseguridad Nacional[4], primer documento del más alto nivel político-estratégico dedicado a la ciberseguridad adoptado en nuestro país y que nos equiparaba a los países más avanzados de nuestro entorno en esta cuestión. La Estrategia implanta un modelo de gobernanza adaptado a la fisionomía de los retos que debemos afrontar.

Como señala el propio presidente del Gobierno en su carta de presentación: «la aprobación del presente documento de carácter estratégico pone de manifiesto las capacidades colectivas y el compromiso de una nación que apuesta firme por garantizar la seguridad en el ciberespacio. Para España, los avances en el ámbito de la ciberseguridad contribuyen además a incrementar nuestro potencial económico, ya que promueven un entorno más seguro para la inversión, la generación de empleo y la competitividad[5]».

Una de las principales novedades de la Estrategia es la puesta en pie de un sistema orgánico para facilitar la toma de decisiones. El centro de esta estructura orgánica es el Consejo Nacional de Ciberseguridad, órgano dependiente del Consejo de Seguridad Nacional.

Cabe destacar, como uno de los principales logros del Consejo Nacional de Ciberseguridad, el desarrollo del Plan Nacional de Ciberseguridad[6] y los Planes Derivados de Ciberseguridad (ver tabla 1).

El Plan Nacional de Ciberseguridad constituye el primer nivel en la planificación de la Estrategia y es donde se definen las amenazas a las que se enfrenta España, se establece la misión y los cometidos concretos para el

[3] El Consejo de Seguridad Nacional, en su condición de Comisión Delegada del Gobierno para la Seguridad Nacional, es el órgano al que corresponde asistir al presidente del Gobierno en la dirección de la política de Seguridad Nacional y del Sistema de Seguridad Nacional, así como ejercer las funciones que se le atribuyan en la Ley de Seguridad Nacional y se le asignen por su reglamento, disponible en www.dsn.gob.es

[4] Asimismo, la Estrategia de Ciberseguridad Nacional desarrolla las previsiones de la Estrategia de Seguridad Nacional de 2013 en el ámbito de la ciberseguridad, fijando como objetivo global lograr que España haga un uso seguro de los sistemas de información y las telecomunicaciones, fortaleciendo las capacidades de prevención, defensa, detección y respuesta a los ciberataques. La Estrategia de Ciberseguridad Nacional fue aprobada por el Consejo de Seguridad Nacional el 14 de diciembre de 2013, disponible en www.dsn.gob.es

[5] Rajoy Brey, Mariano, carta de presentación de la «Estrategia de Ciberseguridad Nacional», Departamento de Seguridad Nacional de la Presidencia del Gobierno, disponible en www.dsn.gob.es

[6] Consejo de Seguridad Nacional, *Plan Nacional de Ciberseguridad*, octubre de 2014.

cumplimiento de los objetivos señalados por la Estrategia y se articula la asignación de responsabilidades de los implicados en la materia[7].

Por otra parte y como parte del Plan, el Consejo de Seguridad Nacional aprobó el Marco General de desarrollo del Plan Nacional de Ciberseguridad, en el cual se apunta el modelo de gobernanza nacional futuro para reforzar la coordinación y la cooperación nacional, internacional y con la Unión Europea a fin de mantener los avances en línea con las estrategias y modelos de los países de nuestro entorno.

Al mismo tiempo, en el Plan Nacional de Ciberseguridad se contemplaba la elaboración de nueve Planes Derivados[8] (ver tabla 2) que desarrollasen, a través de actuaciones concretas, las medidas incluidas en cada una de las Líneas de Acción de la Estrategia (ver tabla 3).

Los Planes Derivados vienen a responder a la necesidad de desarrollar proyectos concretos dirigidos a alcanzar de manera ordenada, coordinada y a través de la creación de sinergias, los objetivos planteados en la Estrategia.

Pero, sin duda, el hito más importante a tener en cuenta en la ciberseguridad nacional fue la aprobación de la Ley de Seguridad Nacional. La Ley declara la ciberseguridad como un ámbito de especial interés para la Seguridad Nacional e introduce una serie de novedades encaminadas a dar respuesta a los nuevos riesgos y amenazas a los que nos enfrentamos, todos ellos caracterizados por un marcado carácter transversal y transnacional, como las ciberamenazas.

Quizás el aspecto más innovador de la nueva Ley se encuentre en el articulado dedicado a la gestión de situaciones crisis y muy especialmente en la figura de la «situación de interés para la Seguridad Nacional». Esta nueva situación se concibe como aquella en la que, por la gravedad de sus efectos y la dimensión, urgencia y transversalidad de las medidas para su resolución, requiere de la coordinación reforzada de las autoridades competentes bajo la dirección del Gobierno. Se busca, en definitiva, el funcionamiento óptimo, integrado y flexible de todos los recursos disponibles.

Un ataque cibernético a los principales operadores de un servicio esencial que suponga una suspensión de los servicios durante un tiempo prolongado

[7] Presidencia del Gobierno a través del Departamento de Seguridad Nacional; Ministerio de Asuntos Exteriores y de Cooperación; Ministerio de Justicia; Ministerio de Defensa; Ministerio de Hacienda y Adminstraciones públicasAdminstraciones públicas; Ministerio del Interior; Ministerio de Fomento; Ministerio de Educación, Cultura y Deporte; Ministerio de Empleo y de Seguridad Social; Ministerio de Industria, Energía y Turismo; Ministerio de la Presidencia a través del Centro Nacional de Inteligencia; Ministerio de Economía y Competitividad.

[8] Desarrollados por los grupos de trabajo interministeriales del Consejo Nacional de ciberseguridad, validados por este último y aprobados por el Consejo de Seguridad Nacional.

y con afección directa a la población, sería un caso susceptible de ser declarado «situación de interés para la Seguridad Nacional».

La lucha por el control del ciberespacio

En 1609 publicaba Hugo Grocio su conocido libro *Mare Liberum*, en el cual defendía la libertad de los mares como piedra angular del desarrollo del comercio y argumentaba cómo los océanos eran ilimitados, como lo es el aire, y no pertenecían a ninguna persona o nación en particular. El derecho de su uso y disfrute era común ya que en su origen no eran propiedad de nadie. *Mare Liberum* constituyó un auténtico hito que sentó las bases modernas del Derecho Internacional Marítimo y también inspiró el término moderno de *Global Commons*.

Desde el punto de vista del Derecho Internacional, los *Global Commons* son aquellos espacios y recursos que se encuentran fuera de la soberanía de cualquier país, es decir, todo el mundo puede acceder a ellos y consecuentemente beneficiarse. Son reconocidos como *Global Commons* los océanos, el espacio aéreo, el espacio ultraterrestre, el Ártico y el ciberespacio.

Todos estos espacios, en los que conviven actores estatales y no estatales, ofrecen sin duda grandes oportunidades y riesgos, desde el punto de vista tanto civil como militar. Uno de los principales problemas que presentan es su escasa regulación, normalmente fijada mediante tratados o convenciones internacionales, en forma parcial y no siempre aceptadas por todos los actores.

El gran desarrollo del comercio internacional por vía aérea y marítima originó la adopción de instrumentos normativos internacionales, la Convención sobre Aviación Civil Internacional[9] y la Convención de las Naciones Unidas sobre el Derecho del Mar[10]. En el caso del espacio exterior, su uso queda reducido actualmente a un pequeño número de países que hace que este sea un ámbito poco regulado. Por su parte, el ciberespacio, por su corto recorrido histórico y sus características peculiares se presenta como un ámbito carente de una regulación clara[11].

Los avances tecnológicos y nuestra forma de vida conceden a los *Global Commons* un innegable valor estratégico, como queda reflejado en la Estrategia de Seguridad Nacional del 2015 de los Estados Unidos, promulgada

[9] Convención sobre Aviación Civil Internacional, «Convención de Chicago», diciembre de 1944, disponible en http://www.aviacioncivil.gob.ec/wp-content/uploads/downloads/2015/04/Convenio-de-Aviacion-Civil-Internacional-de-Chicago.pdf

[10] Naciones Unidas, «Convención de las Naciones Unidas sobre el Derecho del Mar», abril de 1982, disponible en «http://www.un.org/depts/los/convention_agreements/texts/unclos/convemar_es.pdf

[11] Kutt Nebrera, Alexander, «La importancia de dominar los global commons en el siglo XXI», Documento Marco 29/12, Instituto Español de Estudios Estratégicos, 2012.

por el presidente Barack Obama[12]: «El mundo está conectado por espacios compartidos –ciberespacio, espacio exterior, aire y océanos– que permiten el libre flujo de gente, bienes, servicios e ideas. Ellos son las arterias de la economía global y la sociedad civil y el acceso a ellos está en riesgo dado el incremento de la competencia y comportamientos ilícitos. Por ello, continuaremos promoviendo reglas para el comportamiento responsable asegurando al mismo tiempo las capacidades que permitan el acceso a esos espacios compartidos».

El control de los *Global Commons* se ha convertido en un objetivo estratégico de primer orden y entre todos ellos a nadie se le escapa que el ciberespacio ocupa el primer lugar. El ciberespacio es un codiciado objeto de deseo, no solo para los propios estados sino también para organizaciones terroristas y grupos de crimen organizado, donde sus fines pueden ser conseguidos a un menor coste y con una asunción de riesgos mucho menor.

El papel nuclear del ciberespacio en la Seguridad Nacional ha quedado recogido en las Estrategias de Seguridad Nacional de los Estados Unidos y Rusia y en la Estrategia Militar China, todas ellas publicadas en el año 2015.

La más reciente de las estrategias presentadas ha sido la Estrategia Global de Política de Seguridad de la Unión Europea, presentada al Consejo Europeo en el pasado mes de junio. En ella se contempla la ciberseguridad como una de las áreas prioritarias junto a la defensa, la lucha contra el terrorismo o la seguridad energética. Ello implica reforzar las capacidades tecnológicas destinadas a mitigar las amenazas y reforzar la resiliencia de las infraestructuras críticas, las redes y servicios, así como la reducción de la delincuencia informática.

La Estrategia apoya la gobernanza digital multilateral y un marco de cooperación mundial en materia de ciberseguridad, respetando la libre circulación de la información, y marca como ejes de actuación la cooperación a nivel político, operativo y técnico entre los Estados miembros, así como con los Estados Unidos y la OTAN.

En el artículo publicado en abril de 2016 por Ignacio Torreblanca en el diario *El País*[13], se compara la pugna entre la Rusia zarista y el Imperio británico por el territorio que se extendía entre Persia y la India, entre 1813-1907, con la lucha actual de los Estados por el control del ciberespacio. Esa competición geopolítica por el corazón de Asia, popularizada por Rudyard Kipling en su genial obra *Kim*, es conocida como «El gran juego»[14]. Para el autor el gran juego actual es la pugna por el control de internet de las grandes potencias,

[12] The White House, Washington, US National Security Strategy, febrero de 2015.

[13] Torreblanca, José Ignacio, «El nuevo gran juego digital», *El País*, 27 de abril de 2016, disponible en http://tecnologia.elpais.com/tecnologia/2016/04/27/actualidad/1461767882_557672.html.

[14] Kipling, Joseph Rudyard, «The Great Game», 1913.

es decir, nos encontramos sumidos en la versión digital de «El gran juego» de Kipling.

El artículo señala que estamos jugando un juego geopolítico y geoeconómico con inmensas consecuencias sobre el poder, la prosperidad y la seguridad de los Estados y las sociedades. Un juego que carece todavía de reglas claras que lo ordenen y hasta que las tengamos habrá margen para malentendidos fatales.

De la gestión de incidentes a la gestión de crisis en el ciberespacio

Uno de los aspectos donde quizás más toca incidir actualmente es el relativo a la gestión de crisis en ámbito del ciberespacio. Una vez sentadas las bases normativas, debemos ahora desarrollar un sistema que nos permita pasar de la gestión de incidentes cibernéticos a la gestión integral de crisis que tengan en el ciberespacio su campo de batalla.

Según recoge el *Informe Anual de Seguridad Nacional* del año 2015[15], el Equipo de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional (CCN-CERT) resolvió durante 2015 un total de 18.232 incidentes de seguridad, de ellos 430 clasificados como muy altos o críticos. En cuanto a la gestión del Centro de Respuesta a Incidentes de Ciberseguridad para empresas, ciudadanos e infraestructuras críticas (CERTSI), durante 2015 se gestionaron alrededor de 50.000 incidentes, lo que supone un 180 % más que el año anterior. Es preciso tener en cuenta que nuestras capacidades de detección son cada vez mayores aunque, indiscutiblemente, también ayuda a que año a año las cifras de incidentes registrados aumenten significativamente.

Uno de los datos más interesantes además del número de incidentes registrados son, sin lugar a dudas, las pérdidas económicas que ocasionan, dato que generalmente no es fácil de estimar. Calcular el perjuicio económico debido a un incidente de cibereseguridad es una tarea sumamente compleja, dado que existe multiplicidad de tipos de ataques, actores y factores. Además, colateralmente, pueden ser muchos los servicios afectados lo que complica enormemente el cálculo de las pérdidas totales. A los costes que podríamos considerar directos hay que sumarle otros muchos como pudieran ser el deterioro de la confianza de los usuarios en un servicio, pérdida de reputación de una empresa, pérdida de la propiedad intelectual, la disminución de la ventaja tecnológica frente a competidores o, incluso, la pérdida de puestos de trabajo.

[15] Departamento de Seguridad Nacional de la Presidencia del Gobierno, *Informe Anual de Seguridad Nacional 2015*, mayo 2016 disponible en www.dsn.gob.es.

En un reciente estudio[16] realizado por la Agencia de Seguridad de las Redes y de la Información (ENISA), delimitado al ámbito de los incidentes producidos en Infraestructuras Críticas, se expone la dificultad para determinar el impacto real del coste de los incidentes de ciberseguridad en términos de recuperación del servicio afectado. Aun así, el estudio muestra una serie de conclusiones interesantes entre las que cabe destacar:

- En algunos países de la Unión Europea se estima que el coste de los incidentes de ciberseguridad podría suponer alrededor del 1,6 % del Producto Interior Bruto del país y que esta cifra, a nivel mundial, podría suponer entre 330 y 506 billones de euros.
- Los sectores financiero, energético y TIC (Sistemas de Información y Comunicaciones) son en los que los ciberincidentes tienen un mayor coste.
- El activo más afectado suelen ser los datos.

Cuando nos enfrentamos a un incidente cibernético, y en relación con el objeto principal de este capítulo, es muy importante poder discernir si nos enfrentamos a un incidente aislado, orientado a un fin concreto y de efecto limitado, o, por el contrario, nos encontramos ante un incidente que puede contribuir a originar una verdadera situación de crisis para una organización concreta o, incluso, para un Estado.

Tradicionalmente se ha tendido a aislar los incidentes de ciberseguridad al plano técnico, al entenderse que se trataba de un problema exclusivamente técnico y consecuentemente la respuesta debía ser también exclusivamente técnica. Este enfoque en ocasiones nos impide calcular las consecuencias reales de un incidente y responder de forma completa y eficiente.

Cuando pensamos en los autores de los ciberataques frecuentemente nos encontramos con potentes redes de crimen organizado, organizaciones terroristas e incluso los propios Estados. Cuando miramos a las consecuencias de los ciberataques nos encontramos en numerosas ocasiones con situaciones inesperadas y de gran impacto sobre los principales sectores económicos, las infraestructuras críticas o las administraciones.

Es fácil deducir que atendiendo a las causas y efectos de un ciberataque una respuesta técnica no será suficiente, en numerosas ocasiones, para afrontar el problema con garantía de éxito, es necesario articular respuestas que abarquen desde el plano técnico-táctico al político-estratégico, igual que en cualquier ámbito de la seguridad.

Se hace necesario intentar definir lo que entendemos por incidente de ciberseguridad y por cibercrisis, cuestión esta no ausente de dificultad. Entre las

[16] European Union Agency for Network and Information Security (*ENISA*), «The cost of incidents affecting CIIs», agosto de 2016.

muchas referencias encontradas creemos que la que más se puede ajustar es la que propone *ENISA*[17].

Bajo su criterio, un incidente de ciberseguridad es una interrupción de los servicios de tecnología de la información (TI) donde la disponibilidad prevista del servicio desaparece por completo o en parte. También puede ser la publicación ilegal, obtención y/o modificación de la información almacenada en los servicios de TI.

ENISA también estima que una cibercrisis es una situación anormal e inestable que amenaza a los objetivos estratégicos de una organización, la reputación o la viabilidad.

Pero este tipo de ataques, además de afectar a las relaciones económicas y políticas entre Estados, tiene un importante impacto en la percepción pública, particularmente con su difusión a través de los medios de comunicación.

Los ciberataques del siglo XXI y sus consecuencias

Prácticamente en todas las crisis que se han producido en el siglo XXI la ciberseguridad ha tenido un papel estelar. Hemos recogido algunos de los casos más conocidos y de mayor impacto, que nos pueden servir para tener una noción aproximada de los riesgos futuros a los que quizás debamos de hacer frente.

La casuística es muy extensa a tenor del propósito, los actores y alcance de los ataques, pero es fácil encontrar elementos comunes como puede ser la enorme dificultad de determinar los autores, la necesidad de contar con una eficaz colaboración internacional o realizar una adecuada gestión de la comunicación para minimizar los efectos.

El soldado de bronce de Tallin

Sin lugar a dudas, una de las crisis paradigmáticas en el ámbito de la ciberseguridad fue la sufrida por Estonia en el año 2007**.** La «maravilla cibernética» creada por Estonia fue gravemente amenazada tras uno de los peores acontecimientos que se recuerdan en el país[18].

Todo surge con el desmantelamiento y traslado del monumento erigido en Tallin a los soldados soviéticos caídos en la II Guerra Mundial. El monumento, conocido como «el soldado de bronce», se encontraba en el centro de Tallin

[17] European Union Agency for Network and Information Security (*ENISA*), «Report on Cyber Crisis Cooperation and Management», noviembre de 2014.

[18] El orden mundial en el siglo XXI: Agosto de 2015, http://elordenmundial.com/2015/08/12/estonia-ciberseguridad-europea/.

desde 1947 y bajo este fueron enterrados los cuerpos de trece miembros del ejército rojo que combatió a los alemanes en este país.

El Gobierno estonio anunció su decisión de desmontar el monumento con el argumento de que su presencia provocaba división entre los ciudadanos. Esta situación incitó una serie de protestas violentas de grupos prorusos contra su retirada y la intervención, a favor y en contra, de varios políticos rusos y estonios en un marco de tensiones diplomáticas.

En este clima de tiranteces y protestas comenzaron a surgir los problemas. La disponibilidad de varios servicios esenciales y los principales sitios web del país fueron interrumpidos, incluyendo el Parlamento, bancos, comercios, ministerios, periódicos y emisoras de radio. Nunca antes se había atacado a todo un país y en casi todos los frentes digitales a la vez.

Los efectos de los ataques sufridos llevaron al país a una verdadera situación de crisis que golpeó a numerosos sectores, principalmente al financiero, causando daños económicos significativos. Dados los servicios afectados, se necesitó de una estrecha coordinación entre el sector público y privado para solucionar la crisis.

La ralentización del Programa nuclear iraní

Otro incidente de alto impacto fue el surgido en el marco de la crisis diplomática sobre el Programa nuclear iraní en 2005, conocido como el virus Stuxnet.

En el año 2002 se reveló la construcción, no declarada, de una planta de enriquecimiento de uranio subterránea en Natanz. En 2005 y en contra de las recomendaciones de la Comunidad Internacional, Irán reactivó su programa nuclear. Ante estos hechos, la Comunidad Internacional se planteó la posible imposición de sanciones económicas e incluso se consideró la opción de un ataque militar. Finalmente, la tensión descendió notablemente cuando en un informe de la Agencia Central de Inteligencia de los Estados Unidos (CIA) se descartaba que el Programa nuclear iraní pudiera permitir el desarrollo de armas nucleares.

En julio de 2010, según un informe publicado por una empresa de *software* de seguridad[19] se descubrió un virus informático que al parecer llevaba activo desde 2005 y cuya concentración de infecciones se encontraba en Irán, lo que probablemente indicaba que este era el objetivo inicial. Concretamente, su descubrimiento dio pie a especulaciones sobre el objetivo del ataque, que habían sido infraestructuras críticas de este país, entre ellas la central nu-

[19] Symantec, «W32.Stuxnet Dossier», febrero de 2011, disponible en http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

clear de Bushehr o el complejo nuclear de Natanz, puesto que aprovechaba varias vulnerabilidades de los sistemas que controlaban estas centrales.

Según las intervenciones recogidas en el Comité del Senado para Asuntos Gubernamentales de Seguridad Nacional de Estados Unidos[20], Stuxnet es un *malware* altamente sofisticado, con una complejidad sin precedentes y una gran amenaza para las infraestructuras críticas.

En las diversas participaciones recogidas en el Comité, se exponen una serie de interrogantes, entre ellas: la dificultad de determinar los motivos y las personas que estaban detrás de los ataques; que se trataba de un ataque complejo producido, posiblemente, a través de una infección interna y, lo último y más importante, que este tipo de ataques podría potencialmente resultar en daño físico, la pérdida de la vida, y crear una serie de incidentes con efectos en cascada que podrían interrumpir los servicios esenciales.

De acuerdo con algunas estimaciones especulativas publicadas en los medios de comunicación, el Programa iraní fue retrasado unos dieciocho meses. El retraso en el programa suponía ganar más tiempo a los esfuerzos por hallar una solución diplomática a la disputa internacional.

En 2015 se firmó el Plan de Acción Conjunto y Completo, donde Irán acordó con Estados Unidos, Rusia, China, Reino Unido, Francia y Alemania una serie de medidas para el desarrollo de un programa atómico civil, garantizando el no hacerse con un arsenal atómico[21].

Ataques a los servicios esenciales en la Europa del Este

Otros ciberataques que han supuesto un efecto colateral importante fueron los sufridos por Georgia en 2008[22] durante la guerra de Osetia del Sur. Según el informe realizado por la *United States Cyber Consequences Unit*, organismo independiente, la colaboración con las autoridades de Estonia fue esencial en la resolución de los ciberataques desde el punto de vista técnico. La razón de la petición de ayuda a Estonia fue, por un lado, por los ataques sufridos por estos en 2007, y, por otro, la falta de una organización internacional con la que ponerse en contacto para pedir ayuda.

[20] United States Senate Committee on Homeland Security and Governmental Affairs, «Securing Critical Infrastructure in the Age of Stuxnet», noviembre de 2010, disponible en http://www.hsgac.senate.gov/hearings/securing-critical-infrastructure-in-the-age-of-stuxnet

[21] The White House Washington, «The Iran nuclear deal: what you need to know about the JCPOA», julio de 2015, disponible en https://www.whitehouse.gov/sites/default/files/docs/jcpoa_what_you_need_to_know.pdf

[22] United States Cyber Consequences Unit, «Overview of the Cyber Campaing against Georgia in August of 2008», agosto de 2009, disponible en http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf

Este mismo informe presenta las consecuencias estratégicas de la campaña cibernética como parte de un esfuerzo a largo plazo de algunos países, con el fin de poner a prueba la capacidad de respuesta internacional a los ciberataques.

Esta lección fue reforzada por los ciberataques contra Lituania a finales de junio de 2008, tras la decisión del Parlamento local sobre la prohibición de la utilización de símbolos soviéticos en reuniones públicas, y los de Kazajstán en enero de 2009, donde se produjo una cobertura internacional casi inexistente.

En este sentido merece también citarse el ciberataque a Ucrania en 2014, sufrido durante las protestas prorusas y en paralelo a la crisis de Crimea, donde los sistemas de comunicaciones quedaron fuera de servicio aislándola de las comunicaciones internas y con el mundo exterior. Otro ciberataque importante fue el sufrido en 2015[23], donde diversas centrales eléctricas del país dejaron de proporcionar sus servicios durante más de seis horas, afectando a un total de veintitrés subestaciones que dejaron de dar servicio durante horas a más de 225.000 usuarios.

Desde los ataques contra Estonia en 2007 se puso de manifiesto que este tipo de ciberataques podían causar graves problemas económicos y psicológicos en un país, sin provocar importantes respuestas internacionales.

Los ataques silenciosos y el robo de información

Otro tipo de ataques silenciosos que se han ido perpetrando a lo largo de estos años son las acciones de ciberespionaje. Desde 1999 se llevan detectando virus cuyo objetivo principalmente ha sido el robo de información: Moonlight Maze[24], Titan Rain[25], Duqu, Flame, Red October[26]o Gauss[27], son algunos de ellos.

---

[23] United States Homeland Security, Industrial Control Systems Cyber Emergency Response Team, «Cyber-Attack Against Ukrainian Critical Infrastructure», febrero de 2016, disponible en https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01

[24] Descubierto a finales de 1999, habían pasado dos años robando información clasificada del Departamento de Defensa, del Departamento de Energía, de la NASA y contratistas militares.

[25] Comenzó en 2003 y se refiere a la ola de ataques a las redes de defensa de Estados Unidos para el robo de información clasificada. No hay datos sobre la cantidad de datos robados, pero el ataque es considerado uno de los más grandes en la historia de espionaje cibernético.

[26] Descubierto en 2012 aunque llevaba cinco años actuando. El *software* malicioso se infiltró en los sistemas informáticos de distintos países con el objetivo de robar información. La mayor parte de los objetivos eran antiguos países soviéticos en Europa del Este, pero fue descubierto en países de todo el mundo.

[27] Descubierto en 2012 era capaz de espiar las transacciones bancarias y robar información de acceso a redes sociales, correo electrónico y mensajería instantánea. Según sus descubridores también podía servir para atacar a infraestructuras críticas.

En concreto, estos fueron lanzados principalmente contra objetivos diplomáticos, gubernamentales, científicos y empresariales robando datos de todo tipo, desde información sensible o clasificada hasta propiedad intelectual.

Pero este tipo de ataques, además de afectar a las relaciones económicas y políticas entre Estados, tiene un importante impacto en la percepción pública, particularmente con su difusión a través de los medios de comunicación.

El ciberespionaje ha impactado profundamente en las relaciones internacionales y probablemente continuará haciéndolo en el futuro. En este sentido cabe destacar el Informe Anual de la Amenaza 2016[28], presentado por el director de Inteligencia Nacional de los Estados Unidos en el Comité de las Fuerzas Armadas del Senado, en el cual plantea las principales amenazas para Estados Unidos y, entre ellas, las actividades maliciosas en el ciberespacio.

Apunta particularmente a la importancia de las acciones de ciberespionaje perpetradas y centradas en el robo de propiedad intelectual y secretos comerciales u otra información confidencial empresarial que permita obtener ventajas comerciales.

Asimismo, muestra especial preocupación por los ataques a los sistemas de las infraestructuras críticas, las acciones propagandísticas ciberterroristas para estimular los ataques de «lobos solitarios» o las acciones cibercriminales dirigidas al robo, la extorsión o el tráfico de drogas.

Las oportunidades del ciberespacio para la amenaza terrorista

La aparición de grupos terroristas en el ciberespacio no pasa desapercibida. La principal amenaza a la seguridad internacional ha supuesto un enorme salto cualitativo y cuantitativo para el ciberterrorismo. Así, la organización terrorista Dáesh[29] ha sabido utilizar las oportunidades que les brinda el ciberespacio para, por un lado, realizar actividades de propaganda, comunicaciones internas, formación y adoctrinamiento, financiación reclutamiento y obtención de información y, por otro, y aún menos desarrolladas, realizar ciberataques que causen terror[30].

Según unas recientes declaraciones del secretario de Estado de Seguridad[31], la mayoría de las operaciones desarrolladas por las Fuerzas y Cuerpos de Seguridad del Estado responden a actuaciones ligadas a la propaganda, ra-

[28] James R. Clapper, «Statement for the Record Worldwide Threat Assessment of the US Intelligence Community», 2016, disponible en http://www.armed-services.senate.gov/imo/media/doc/Clapper_02-09-16.pdf

[29] Al-Dawla al-Islamiya al-Iraq al-Sham.

[30] Consejo de Seguridad Nacional, «Plan Nacional de Ciberseguridad», octubre de 2014.

[31] Sesión inaugural del Encuentro Internacional de Seguridad de la Información, organizadas por el Instituto de Ciberseguridad Nacional, León, 2016.

dicalización y reclutamiento de esta organización terrorista a través de la Red. Asimismo, afirmó que Dáesh ha conseguido atraer a más de 30.000 combatientes extranjeros para luchar en Siria e Irak a través de las redes sociales.

Las comunicaciones de propaganda mediante el uso de internet son ampliamente conocidas. El portavoz de Dáesh, Abu Mohammad Al-Adnani, realizó en 2014 un llamamiento difundido a través de las redes sociales que incitaba a sus seguidores a cometer ataques individuales, indiscriminados y empleando cualquier vía. Este mensaje, que se convirtió en viral, ha servido de inspiración para muchos de los ataques que se han producido en el territorio europeo[32]. Desde entonces, Dáesh ha difundido y distribuido, a través de las redes sociales, vídeos de ejecuciones de prisioneros con el objetivo de crear terror.

Hasta finales de 2015, el Ministerio del Interior del Gobierno de España estimaba que Dáesh había difundido aproximadamente mil vídeos a través de sus cuentas de Twitter (en esa fecha se contabilizaban entre 35.000 y 75.000 cuentas gestionadas directamente por Dáesh). El 16 % de estos vídeos muestran la ejecución de rehenes y en total se habría mostrado al público el asesinato de más de mil quinientas personas.

Por otro lado el uso de la web profunda[33], en la cual la navegación es totalmente anónima, supone una oportunidad para el desarrollo de este tipo de actividades, y más concretamente el denominado internet oscuro, donde imperan actividades englobadas en el marco del mercado negro. Desde hace años se sabe de la existencia de foros extremistas pertenecientes a grupos terroristas, extremistas y radicales utilizados principalmente como medio de captación o para que usuarios se ofrezcan como candidatos para unirse a las causas. Así, también se reconoce su utilización, como parte de sus acciones de financiación, mediante la utilización de la moderna moneda virtual Bitcoin.

Ataques a la reputación e influencia política

Según recoge un comunicado oficial de la Comunidad de Inteligencia de Estados Unidos[34] sobre la exfiltración de *emails* de personas, instituciones y organizaciones políticas de Estados Unidos, indican, además, que los robos y

[32] «si no eres capaz de encontrar una bala o un dispositivo explosivo improvisado, entonces selecciona al impío americano, francés o cualquiera de sus aliados. Golpéale la cabeza con una roca, asesínale con un cuchillo, atropéllale con tu vehículo, tírale desde un lugar elevado, estrangúlale o envenénale.»

[33] Esglobal, Daesh en la 'Deep Web': las profundidades de la Red al servicio de la 'yihad', enero de 2016, disponible en https://www.esglobal.org/daesh-en-la-deep-web-las-profundidades-de-la-red-al-servicio-de-la-yihad/

[34] Department of Homeland Security and Office of the Director of National Intelligence, «Election Security Statement», octubre de 2016, disponible en https://www.dni.gov/index.php/newsroom/press-releases/215-press-releases-2016/1423-joint-dhs-odni-election-security-statement

revelaciones están destinados a interferir en el proceso electoral en Estados Unidos con el fin de influir en la opinión pública. El comunicado expone que algunos Estados también han sufrido incidentes en sus sistemas relacionados con las elecciones sin poder indicar fehacientemente el origen.

No obstante, la Comunidad de Inteligencia y el Departamento de Seguridad Nacional estiman que sería extremadamente difícil alterar el conteo de votos o los resultados de las elecciones a través de un ciberataque, asegurando que las máquinas de votación no están conectados a internet, y que existen numerosos controles y supervisión en el proceso electoral.

Otro incidente no considerado en sí mismo como un ciberataque pero que tuvo un impacto enorme sobre la sociedad americana fue el falso anuncio, en la cuenta de Twitter de la agencia de noticias de Associated Press, de un atentado en la Casa Blanca en el que el presidente Barack Obama había sido herido en el mismo.

La cuenta de la agencia de noticias había sido *hackeada*[35], pero en solo tres minutos, el tiempo que tardó la agencia en anunciar el pirateo de su cuenta, el Dow Jones cayó 150 puntos, lo que causo un efecto cascada en otros índices y la caída del dólar frente al yen.

Las amenazas al sector privado

Un ejemplo del daño que este tipo de acciones pueden suponer para el sector privado son los ciberataques sufridos por Sony Pictures tras el anuncio del estreno de la película *La entrevista*, donde se parodia al líder norcoreano Kim Jong-Un. En este caso, Sony sufrió una serie de ataques que le han supuesto pérdidas de más de 200 millones de dólares[36] por la filtración de información estratégica para la empresa. O el del grupo financiero JP Morgan Chase[37], donde se comprometieron los datos de 76 millones de clientes y siete millones de negocios en Estados Unidos.

El último gran ciberataque relacionado con el robo de información ha sido el relacionado con la empresa americana de medios de comunicación y servicios de internet Yahoo, que ha sufrido el robo de más de quinientas cuentas

[35] *USA Today*, «AP Twitter feed hacked; no attack at White House», abril de 2013, disponible en http://www.usatoday.com/story/money/markets/2013/04/23/stocks-gyrate-wildly-after-fake-terror-tweet/2107089/

[36] *EFE*, «Pérdidas de Sony Pictures por el ciberataque superarán los 200 millones de dólares», diciembre de 2014, disponible en http://www.emol.com/noticias/magazine/2014/12/22/695769/perdidas-de-sony-pictures-por-el-ciberataque-superaran-los-200-millones-de-dolares.html

[37] *The New York Time*, «JPMorgan Chase Hacking Affects 76 Million Households», ocubre de 2014, disponible en http://dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber-security-issues.

con información de clientes[38] desde 2014. Esta información además, se ha hecho pública durante el anuncio de compra de Yahoo por parte de Verizon, el mayor operador de telecomunicaciones de Estados Unidos. Aunque la compra aún está pendiente de la autorización de los reguladores, el incidente podría afectar a un ajuste del precio de la compra.

Por último, resaltar los ataques sufridos el pasado mes de octubre por uno de los proveedores más importantes de soluciones de *DNS* (*Domain Name System*)[39], la compañía americana DynDNS (Dynamic Network Services, Inc.). La empresa sufrió un tipo de ataque denominado de denegación de servicios distribuida (*DDos*)[40].

Los ataques, cuyo origen aún se desconoce, podrían estar relacionados con la *botnet*[41] Mirai, conexa con el Internet de las Cosas. El ataque afectó a la disponibilidad de los servicios de importantes empresas americanas, bien ralentizando el acceso a sus páginas web o incluso llegando a afectar a la disponibilidad total de algunas de ellas.

Sus efectos están por llegar. La falta de disponibilidad de los servicios de las empresas afectadas ha acarreado, con total certeza, la pérdida de ingresos, ya sea por servicios o publicidad, además de la disminución de la confianza de los usuarios y daños a su reputación. Además, Dyn DNS tendrá que hacer frente también a la pérdida de confianza de sus clientes, a demandas legales y, por supuesto, al efecto reputacional que esto conlleva. Aún no se puede traducir en cifras el coste del ataque, pero seguro que alcanzará varios millones de dólares.

Pero, además, este tipo de ataques ya se preveía. En 2002 la seguridad del sistema de nombres de dominios (*DNS*) ya se encontraba en entredicho. En este sentido, la Internet Corporation for Assigned Names and Numbers (ICANN)[42], creó el Comité de Seguridad y Estabilidad ante la inquietud de empresas y Gobiernos por la fiabilidad del Sistema de Nombres de Dominio. Además, varios expertos ya habían avisado sobre la posibilidad de que un ataque contra los principales servidores de nombres de dominio a nivel internacional, podrían echar abajo internet por el efecto cascada que podría suponer. Una de las principales empresas de nombres de dominio negó por entonces esta posibilidad.

---

[38] *Business Wire*, «An Important Message to Yahoo Users on Security», septiembre de 2016 disponible en http://www.businesswire.com/news/home/20160922006198/en/

[39] Sistema que traduce de números (direcciones IP) a nombres a las páginas web.

[40] Ataque que busca saturar las conexiones de una web o de un servidor con peticiones aparentemente lícitas pero que en realidad provienen de equipos infectados con *software* malicioso (conocidos como *bots*), a fin de hacerlos inaccesibles.

[41] Las *botnets* se forman por un conjunto de dispositivos conectados a internet (Internet de las Cosas) e infectados por algún tipo de *software* malicioso. Su control remoto permite que dichos dispositivos infectados puedan ser usados como medio para lanzar ataques.

[42] Organismo privado que gestiona los dominios de internet.

Ataques con efectos cinéticos

A pesar de que todos estos ciberataques se encuentran dirigidos a la consecución de diferentes fines, una de las amenazas más significativas que podrían darse en un futuro no muy lejano son aquellos incidentes que podrían causar directa o indirectamente daño físico, lesión o muerte, los denominados ciberataques con efectos cinéticos[43]. Esto es, aquellos ciberataques en los que el mundo físico y el virtual se aproximan.

Casos como el del virus Stuxnet o el reportado[44] por la Oficina Federal para la Seguridad de la Información en Alemania (BSI) sobre el daño causado en una fábrica de acero alemana, en la cual fue imposible apagar el alto horno originando un daño masivo al sistema y provocando cortes que interrumpieron la producción.

La dependencia tecnológica y la hiperconectividad, incluida la de los servicios esenciales e infraestructuras críticas, implican una ciberamenaza cinética significativa y el reto por excelencia de todo el desarrollo en ciberseguridad. Si bien los ejemplos anteriores no afectaron a vidas humanas, sí afectaron a infraestructuras que podrían ocasionar un daño físico mayor.

La gestión de crisis en el Sistema de Seguridad Nacional

Entre las principales responsabilidades del Gobierno se encuentran las de proporcionar seguridad y protección a los ciudadanos y a sus propiedades, garantizar la integridad territorial, contribuir al buen funcionamiento de los mercados y al sostenimiento de la infraestructura estratégica del país. Tanto los ciudadanos como el sector privado esperan que el Gobierno esté preparado para hacer frente a una amplia gama de posibles situaciones de crisis que pudiesen afectar a estos elementos esenciales.

La Ley de Seguridad Nacional se aprobó precisamente con el propósito de mejorar la coordinación de las diferentes Administraciones públicas en la prevención y la respuesta integral frente a situaciones de crisis de elevada complejidad, bajo la dirección del presidente del Gobierno y en el marco del Sistema de Seguridad Nacional. A estos efectos, tal y como se apunta en la introducción de este capítulo sobre la gestión de situaciones crisis, la Ley diseña un modelo de gestión que contempla la prevención, detección, respuesta, retorno a la normalidad y evaluación, basado en la gradualidad y amplia

[43] Applegate, Scott, «The Dawn of Kinetic Cyber». 5th International Conference on Cyber Conflict. NATO CCD COE Publications, junio de 2013.

[44] Bundesamt für Sicherheit in der Informationstechnik, «Die Lage der IT-Sicherheit in Deutschland 2014», noviembre de 2014, disponible en https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf?__blob=publicationFile

participación de todos los actores afectados, espacio donde cobra especial sentido la colaboración público-privada.

Antes de detallar el sentido y la instrumentalización de la participación del sector privado en la gestión de las actuaciones relativas a crisis de ciberseguridad, es preciso referirse a la situación de interés de Seguridad Nacional y a la estructura orgánica que se ha establecido bajo la dirección del Gobierno para hacer frente a estas crisis.

Esta nueva situación constituye la frontera con el estado más leve de las denominadas situaciones de anomalía constitucional agrupadas en la Ley Orgánica[45] de los estados de alarma, excepción y sitio, concretamente, el estado de alarma.

Se trata de situaciones en las que, sin concurrir las circunstancias extraordinarias que dan lugar a los estados de alarma y excepción, ni requerir de la adopción de las medidas en ella contempladas, sin embargo, por la gravedad de sus efectos y la dimensión, urgencia y transversalidad de las medidas para su resolución, precisan de la coordinación reforzada de las autoridades competentes en el desempeño de sus atribuciones ordinarias, bajo la dirección del Gobierno, en el marco del Sistema de Seguridad Nacional, garantizando el funcionamiento óptimo, integrado y flexible de todos los recursos disponibles.

La situación de interés para la Seguridad Nacional se afrontará con los poderes y medios ordinarios de las distintas Administraciones públicas. En ningún caso supondrá la suspensión de los derechos fundamentales y libertades públicas en los términos previstos constitucionalmente para la declaración de los estados de excepción y sitio.

Esta categoría responde a la morfología de las crisis actuales o potenciales que se deben encarar en la sociedad del riesgo del siglo XXI, que vienen marcadas por su transversalidad, su naturaleza abierta o su incierta evolución, y a ella subyace la necesaria activación en tiempo útil de los medios necesarios del Estado, siempre primando la prevención y mitigación, en aras de proveer una actuación más ágil, modular, eficaz y eficiente.

Las actuaciones a desarrollar deben ir encaminadas a poner en marcha la estructura del Sistema de Seguridad Nacional prevista en la Ley[46] de Seguridad Nacional, en el marco de la regulación de la gestión de crisis del Título III, entendida como el conjunto ordinario de actuaciones dirigidas a detectar y valorar los riesgos y amenazas concretos para la Seguridad Nacional, facilitar el proceso de toma de decisiones y asegurar una respuesta óptima y coordinada de los recursos del Estado que sean necesarios[47].

[45] Ley Orgánica 4/1981, de 1 de junio, de los estados de alarma, excepción y sitio.
[46] Ley 36/2015, de 28 de septiembre, de Seguridad Nacional.
[47] Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, art. 22.1.

La participación de las distintas Administraciones públicas es un principio ineludible del Sistema de Seguridad Nacional[48], y para ello el sistema contará, cuando se constituya, con la actuación cooperadora de la Conferencia Sectorial para asuntos de la Seguridad Nacional[49], así como con los mecanismos de enlace y coordinación necesarios que se determinen oportunamente, que aseguran la participación de los órganos de las autoridades competentes, para garantizar la coordinación de las actuaciones[50].

En cuanto a la estructura orgánica que la Ley de Seguridad Nacional establece en el marco del Sistema de Seguridad Nacional y su desempeño en la gestión de las actuaciones de crisis, es preciso referirse al Consejo de Seguridad Nacional, el Comité Especializado de Situación y el Departamento de Seguridad Nacional.

En su condición de Comisión Delegada del Gobierno para la Seguridad Nacional, al Consejo de Seguridad Nacional le corresponde asistir al presidente del Gobierno en la dirección de la política de Seguridad Nacional y del Sistema de Seguridad Nacional. En este sentido, el Consejo de Seguridad Nacional se reúne a iniciativa del presidente del Gobierno como mínimo con carácter bimestral.

El Consejo es un órgano permanente de dirección de las actuaciones de gestión de crisis. Además de ser el responsable de determinar los mecanismos de enlace y coordinación necesarios para que el Sistema de Seguridad Nacional se active preventivamente y realice el seguimiento de los supuestos susceptibles de derivar en una situación de interés para la Seguridad Nacional; asesorará al presidente del Gobierno cuando la situación requiera la aplicación de medidas excepcionales previstas en los instrumentos de gestión de crisis de las organizaciones internacionales de las que España sea miembro.

En cuanto al Comité Especializado de Situación, como órgano colegiado y experto de muy alto nivel y de carácter único para el conjunto del Sistema de Seguridad Nacional, la fuerza de actuación que puede desarrollar en la gestión de cibercrisis es de singular importancia. En el desarrollo de sus funciones se le asignan cometidos que engloban: desde la valoración de las primeras acciones de alerta temprana, tan indispensable en las cibercrisis; hasta la valoración del impacto y los efectos ocurridos. Además, propondrá las directrices de una política informativa coordinada cuyo fin sea informar a la sociedad sobre la situación acontecida.

Así, y en el caso de que la situación fuese declarada situación de interés para la Seguridad Nacional, sus cometidos se amplían sobre todo en lo que se refiere a la coordinación de mecanismos y medios nacionales e internacionales.

[48] Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, art. 22.2.
[49] Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, art. 6.
[50] Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, arts. 11.1 y 18.2.

Por último, bajo la dependencia orgánica y funcional de su Director, y como órgano de asesoramiento al presidente del Gobierno en materia de Seguridad Nacional, el DSN, entre otras funciones, es el organismo permanentemente responsable de realizar el análisis de la evolución de los riesgos y amenazas a la Seguridad Nacional y de sus potenciadores.

Este análisis se realiza de una manera inclusiva y en coordinación con los órganos y autoridades competentes, así como con el sector privado, lo que le permite realizar un seguimiento continuo y constante 24 × 7 permitiéndole, con ello, realizar la alerta temprana y asesorar sobre acciones preventivas, de anticipación o de preparación en la respuesta. También es el responsable de mantener y asegurar el adecuado funcionamiento del Centro de Situación de la Presidencia del Gobierno, y las comunicaciones especiales de la Presidencia del Gobierno, así como proteger su documentación.

El DSN cumple además un importante papel de fomento de una amplia cultura de Seguridad Nacional inclusiva de la sociedad en todas sus manifestaciones y de potenciación y desarrollo de la colaboración público-privada en materia de Seguridad Nacional.

Por tanto, el DSN es un organismo llamado a establecer una acción coordinada a nivel internacional, europeo y nacional en aquellas cuestiones de nivel estratégico relacionadas con la alerta temprana y seguimiento de los riesgos, amenazas a la ciberseguridad, así como en el apoyo en la dirección y coordinación de las actuaciones de gestión de las situaciones de cibercrisis. Ejemplo de ello es su actuación como punto de contacto nacional en el ámbito del Dispositivo Integrado de Respuesta Política de la Unión Europea a las Crisis (*IPCR*)[51].

De manera especialmente relevante, es importante partir de la premisa de que sin esta colaboración no es posible una respuesta ajustada a las crisis de ciberseguridad. Para hacer frente de forma efectiva a las eventuales situaciones de crisis que puedan provocarse, la inclusión del sector privado en actuaciones de prevención, defensa, detección, respuesta y recuperación es esencial.

Colaboración público-privada y gestión de crisis de ciberseguridad en el Sistema de Seguridad Nacional

El sector privado es uno de los principales agentes de la Seguridad Nacional. Así se encuentra recogido en la Ley de Seguridad Nacional, y así se refleja en su posible participación en el Sistema de Seguridad Nacional, tanto en la

[51] Consejo de la Unión Europea, «Dispositivo Integrado de Respuesta Política de la Unión Europea a las Crisis» disponible en http://www.consilium.europa.eu/en/documents-publications/publications/2014/eu-ipcr/

formulación y ejecución de la política de la Seguridad Nacional, como en la gestión de crisis y la contribución de recursos.

Se debe seguir avanzando de manera coordinada en distintos aspectos de la gestión de crisis que deben materializarse a través de proyectos y actuaciones concretas, tal y como establece la Ley.

En este sentido, varias son las actividades que el Departamento de Seguridad Nacional viene desarrollando con el sector privado. En las líneas que siguen, se destacarán algunas de estas, tales como: la organización del primer seminario[52] público-privado nacional sobre gestión de crisis en el ámbito de la ciberseguridad; la coordinación del proyecto para aumentar la ciberseguridad en el ámbito marítimo; la instrumentalización de la participación del sector privado a través de planes de actuación que contempla su colaboración e inclusión tanto en el plano estratégico, como en el operativo y táctico; la llamada de la Directiva de Seguridad de las Redes y de la Información (Directiva NIS)[53] a contemplar su papel en la implementación de una orgánica que abunde en el fomento de sinergias cooperativas entre los Estados miembros de la Unión Europea; el establecimiento de protocolos o la implantación de un modelo nacional de ejercicios de ciberseguridad de amplio espectro.

Respecto del seminario público-privado de ciberseguridad, al margen de la novedad de su celebración que amplifica y da voz al mensaje de que «no hay ciberseguridad real sin un sector privado bien plantado y comprometido», son varias las ideas fuerza que de un foro de este nivel se pueden extraer: la necesaria determinación de modelos de gobernanza de la ciberseguridad a nivel internacional, europeo y nacional; la ampliación del compromiso basado en la cooperación para la prevención, defensa, detección, respuesta y recuperación a los ciberataques; el aumento de la confianza entre los actores implicados para fomentar el intercambio de información; trabajar conjuntamente en las implicaciones estratégicas de la gestión de crisis; la singular importancia de los ejercicios de ciberseguridad y el necesario compromiso

[52] Una de las actuaciones desarrolladas por el Departamento de Seguridad Nacional, en colaboración con la Agencia Europea de Seguridad de las Redes y de la Información (ENISA), fue la organización del primer seminario público-privado nacional sobre gestión de crisis en el ámbito de la ciberseguridad.
El seminario, impartido por la Agencia Europea de Seguridad de las Redes y de la Información (ENISA) así como por el Departamento de Seguridad Nacional, tuvo como objetivo plantear las distintas implicaciones de la Ley de Seguridad Nacional para el ámbito de la ciberseguridad, además de exponer los diversos proyectos nacionales realizados tras la aprobación de la Estrategia de Ciberseguridad Nacional y la puesta en marcha del Consejo Nacional de Ciberseguridad.

[53] La Directiva de Seguridad de las Redes y de la Información adoptada por el Parlamento Europeo el 6 de julio de 2016 con entrada en vigor en agosto, comunicado de prensa de la Comisión Europea del 5 de julio de 2016.

para progresar en la sensibilización y concienciación mediante el desarrollo de una fuerte cultura de ciberseguridad nacional.

Asimismo, las actuaciones del Consejo Nacional de Ciberseguridad, abierto a la participación del sector privado y los órganos y organismos responsables de la ciberseguridad en España, han venido respondiendo a estas necesidades a través del ya mencionado Plan Nacional de Ciberseguridad, su marco general de desarrollo y los planes derivados de ciberseguridad.

En cuanto se refiere a la coordinación del proyecto para aumentar la ciberseguridad en el ámbito marítimo, la iniciativa parte del Consejo Nacional de Seguridad Marítima en coordinación con el Consejo Nacional de Ciberseguridad. El DSN, en colaboración con el Clúster Marítimo Español y el Instituto Nacional de Ciberseguridad, ha desarrollado un plan integral para aumentar la ciberseguridad en el sector marítimo que engloba actuaciones concretas dirigidas al sector privado que van desde la elaboración de guías de buenas prácticas sobre medidas de ciberseguridad a la organización de ejercicios de ciberseguridad en este ámbito.

Uno de los aspectos que contemplan los Planes Derivados, y punto nuclear de este artículo es el englobe de actuaciones concretas relativas a la gestión de crisis, llevadas a cabo en el marco de la colaboración público-privada, y que implican a las tres esferas que debe cubrirse en la gestión de crisis.

Para el nivel estratégico, es necesario desarrollar un Sistema Nacional Integral de Comunicación e Intercambio de Información[54] con la finalidad de crear mecanismos e instrumentos de enlace y coordinación para la prevención, detección, respuesta, retorno a la normalidad y evaluación ante situaciones de crisis en el ámbito de la ciberseguridad, esto es, un punto único de coordinación público-privado, ya contemplado en la Estrategia y en la Ley de Seguridad Nacional.

Las aportaciones de ambos sectores en el sistema, además de beneficiar el conocimiento sobre la las ciberamenazas y contribuir a plantear aquellas situaciones que le alertan o le son de interés, servirá para identificar fuerzas y debilidades, analizar áreas potenciales de cibercrisis y mantener el enlace del sector privado con los organismos del Sistema de Seguridad Nacional, centrados en el Consejo de Seguridad Nacional, el Comité Especializado de Situación y el Departamento de Seguridad Nacional.

Así, también es de vital importancia el intercambio de información sobre ciberamenazas[55] en el plano operativo, dados los posibles efectos de la ejecución de ciberataques que pudieran plantearse de manera simultánea sobre los sectores públicos y privados nacionales y, especialmente, sobre las infraestructuras críticas tal y como se planteó al principio de este artículo.

[54] Actividad recogida en el «Plan de fortalecimiento y potenciación de capacidades y aseguramiento de la cooperación para la ciberseguridad y la ciberdefensa».

[55] «Plan de intercambio de información sobre ciberamenazas».

En este sentido es necesario contar con herramientas tecnológicas y mecanismos que permitan llevar a cabo este intercambio de información de manera proactiva con el sector privado y a través de puntos de contacto concretos para ello. Además, la información podrá ser sectorial, dado que las ciberamenazas no afectan de igual manera a todos los sectores y las respuestas tampoco tienen por qué serlo.

Por tanto, este mecanismo supone integrar, definir, desarrollar e implantar los procedimientos de actuación en un marco singular de colaboración directa con el sector privado. Un ejemplo de implantación de estas iniciativas ha sido la creación de la Oficina de Coordinación Cibernética del Ministerio del Interior que sirve como mecanismo de enlace entre las Fuerzas y Cuerpos de Seguridad del Estado, el Centro Nacional de Protección de Infraestructuras Críticas y el sector privado.

En el plano técnico, el fomento del intercambio de información sobre incidentes de ciberseguridad entre los sectores público y privado[56] supone la creación de sinergias significativas y el aumento de eficacia de las actividades de los Equipos de Respuesta ante incidentes de ciberseguridad públicos y privados.

La puesta en marcha de iniciativas que faciliten la cooperación en el intercambio de información de nivel técnico entre el sector público y privado, permite aumentar los niveles de prevención, defensa, detección, respuesta y recuperación a incidentes de ciberseguridad. Ejemplo de ello es el desarrollo de la herramienta ICARO[57] por el Equipo de Respuesta ante Incidentes de Ciberseguridad de Seguridad e Industria (CERTSI_)[58]. Un servicio de compartición de información sobre incidentes de ciberseguridad, particularmente diseñado para el intercambio de información con el sector privado y basado en el proyecto *MISP* (*Malware Information Sharing Platform*)[59].

Por lo que se refiere a la cooperación en la gestión de incidentes entre los sectores público y privado[60] en el marco de la Directiva NIS, cabe recordar que la Comisión Europea presentó en febrero de 2013 la propuesta de Direc-

[56] Actividad recogida en el «Plan derivado de ciberseguridad del sector privado y la industria».

[57] Equipos de respuesta ante incidentes de Ciberseguridad de Seguridad e Industria, «Icaro» disponible en: https://www.certsi.es/servicios-operadores/icaro

[58] El CERT de Seguridad e Industria, es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Ministerio de Industria, Energía y Turismo y del Ministerio del Interior. Operado técnicamente por INCIBE, y bajo la coordinación del CNPIC e INCIBE, el CERTSI se constituyó en el año 2012 a través de un Acuerdo Marco de Colaboración en materia de ciberseguridad entre la Secretaría de Estado de Seguridad y la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información. Actualmente es regulado mediante Acuerdo de 21 de octubre de 2015, suscrito por ambas Secretarías de Estado.

[59] *Malware Information Sharing Platform*, disponible en http://www.misp-project.org/

[60] Actividad recogida en el «Plan derivado de ciberseguridad del sector privado y la industria».

tiva[61] para su consideración por el Consejo de la Unión Europea y el Parlamento Europeo. La entonces propuesta de Directiva era una de las medidas recogidas en la *Estrategia de ciberseguridad de la Unión Europea: un ciberespacio abierto, protegido y seguro*. Finalmente, y tras varios años de negociaciones, la Directiva fue adoptada por el Parlamento Europeo el 6 de julio de 2016 y entró en vigor en agosto del mismo año.

La Directiva NIS establece los requisitos mínimos comunes que deben cumplir los Estados miembros en materia de seguridad en las redes y de la información, y obliga, entre otras cuestiones, a: identificar y comunicar a la Comisión los operadores de servicios esenciales y los proveedores de servicios digitales de los Estados miembros[62]; comunicar y notificar a la Comisión incidentes con efecto perturbador significativo; desarrollar y comunicar a la Comisión la Estrategia nacional de seguridad de las redes y sistemas de información o definir un marco de gobernanza[63] que se coordine con las estructuras europeas de manera que pueda aplicarse la Directiva.

Algunos de los aspectos relevantes que incluye la Directiva es la cooperación y el intercambio de información, por lo que también obliga a: cooperar a escala nacional y a escala internacional. Esta última se realizará a nivel técnico a través de la creación de una red de Equipos de Respuesta ante Incidentes de Ciberseguridad a fin de intercambiar información; a nivel estratégico con la creación del Grupo de Cooperación formado por representantes de los Estados miembros, la Comisión y ENISA. Además de definir y establecer las disposiciones legales, reglamentarias y administrativas, en coordinación con aquellos que posean competencias en la materia.

Impulsar un esquema de cooperación público-privada como el previsto por la Directiva NIS es de singular importancia a fin de identificar, prevenir y mitigar los ciberataques que puedan afectar a Europa y a España, además,

[61] La Directiva de Seguridad de las Redes y de la Información adoptada por el Parlamento Europeo el 6 de julio de 2016 con entrada en vigor en agosto, «Comunicado de prensa de la Comisión Europea del 5 de julio de 2016».

[62] Energía, transporte, banca, infraestructuras de los mercados financieros, sector sanitario, suministro y distribución de agua potable, infraestructura digital y proveedores de servicios digitales (mercado en línea, motores de búsqueda y servicios de computación en nube) y Administraciones públicas que hayan sido identificadas como como operadores de servicios esenciales. Quedan excluidas: las microempresas y pequeñas empresas que sean proveedores de servicios digitales y las empresas que están sujetas a los requisitos de las Redes Públicas de Comunicaciones, así como los proveedores de servicios de confianza (firma digital, sellos de tiempo, etcétera).

[63] Designar una o más Autoridades Competentes que supervisarán la aplicación de la Directiva a escala nacional y estén facultadas para adoptar directrices nacionales sobre la notificación de incidentes. Designar un único punto de contacto nacional que se encargue de coordinar las cuestiones relacionadas con la seguridad de las redes y sistemas de información y de la cooperación transfronteriza a escala de la Unión. Designar uno o varios Equipos de Respuesta ante Incidentes de Ciberseguridad (CSIRT), responsables de la gestión de incidentes.

y puesto que esta obliga a la cooperación a escala nacional, la trasposición de la Directiva ayudará a implementar el modelo de gobernanza nacional.

Por otra parte, la colaboración del sector privado en las decisiones relativas a la trasposición de la Directiva son de especial relevancia y el proceso incluye la consulta pública al sector, a fin de realizarla con total eficacia y transparencia.

En cuanto a la creación del Modelo Nacional de Ejercicios de Ciberseguridad[64] y participación y ejecución de ejercicios de ciberseguridad[65], sin duda y en todo el contexto presentado, es de vital importancia que las organizaciones españolas se encuentren preparadas para hacer frente a los ciberataques, disponiendo de los recursos más adecuados en cada momento y adaptados a cada situación.

Para verificar la idoneidad de los medios empleados en los distintos procesos de la gestión de crisis de ciberseguridad, es necesario realizar periódicamente ejercicios de ciberseguridad. En estos ejercicios deben simularse desde las distintas fases de gestión de crisis, como los distintos niveles de actuación y de toma de decisiones (niveles técnico, operacional y político-estratégico) con el fin de verificar el grado de coordinación entre instituciones responsables ante cada una de las fases y de estas con el sector privado. Asimismo, sirven para entrenar los protocolos existentes y valorar su funcionamiento, poner a prueba el conocimiento de capacidades, la comunicación y el intercambio de información entre ambos sectores, lo que favorece la creación de un marco de confianza y colaboración directa.

Para mejorar la gestión de los recursos disponibles a nivel nacional, se debe elaborar un Catálogo Nacional de Ciberejercicios que persiga el identificar áreas deficitarias a potenciar tanto por el sector público como por el sector privado, promuevan la participación de ambos sectores, al presentar una planificación coordinada y ordenada a nivel nacional y de estos con aquellos ejercicios que se desarrollen a nivel internacional y europeo.

Por último, además de las actividades señaladas anteriormente, se deben añadir aquellas recogidas en los planes que indirectamente influyen en la prevención de cibercrisis. En este sentido caben resaltar las acciones e iniciativas en marcha que persiguen aumentar la conciencia en ciberseguridad mediante el desarrollo de la Cultura Nacional de Ciberseguridad y otras complementarias que incluyen el aumento de las capacidades de inteligencia; el aumento de confianza entre sector público privado o la apuesta por el desarrollo del mercado nacional de la ciberseguridad; la I+D+i o la capacitación y formación en materia de ciberseguridad.

[64] Actividad recogida en el «Plan de fortalecimiento y potenciación de capacidades y aseguramiento de la cooperación para la ciberseguridad y la ciberdefensa».

[65] Actividad recogida en el «Plan de intercambio de información sobre ciberamenazas».

De la acción a la puesta en práctica. El ejercicio *Cyber Europe*

Finalmente, el modelo planteado y las actuaciones propuestas no funcionan si no se practican y ejercitan mediante decisiones y procedimientos simulados. Los ejercicios no solo ofrecen oportunidades para analizar los incidentes de ciberseguridad a nivel técnico, sino que, además, se puede elevar su complejidad operativa y estratégica a fin de examinar situaciones de continuidad de negocio y de gestión de crisis complejas.[66] España ha avanzado significativamente en este sentido con su participación en el ejercicio *Cyber Europe*[67].

El Ejercicio *Cyber Europe*, organizado cada dos años por la Agencia de Seguridad de las Redes y de la Información (ENISA), es el mayor ciberejercicio que se realiza a nivel mundial. En estos ejercicios se simulan incidentes de ciberseguridad a gran escala, que se intensifican hasta convertirse en una crisis de ciberseguridad a nivel europeo.

El principal objetivo de las diferentes ediciones ha sido trabajar en la cooperación y el intercambio de información a nivel europeo entre los Estados miembros y de estos con la Agencia, involucrando, asimismo, al sector privado en su ejecución.

En este sentido, el DSN, como coordinador de la participación nacional y punto único de contacto con ENISA, ha participado en las ediciones de 2010, 2012, 2014 y 2016.

Sin duda, a lo largo de estos años la coordinación y planificación nacional ha ido avanzando con una mayor implicación del sector privado. Si bien en 2010 España tan solo participó como observador, en las ediciones de 2012, 2014 y 2016 se ha evolucionado significativamente en la planificación y en una mayor colaboración y participación del sector público y del sector privado.

Dado que la edición del ejercicio *Cyber Europe* 2016 se encuentra en proceso de ejecución, sus conclusiones aún no se encuentran disponibles, pero sin duda es importante resaltar que este año España ha participado con la aportación de once empresas y los órganos y organismos con competencias en materia de ciberseguridad del sector público.

En la edición de 2014, el ejercicio fue el mayor y más completo ciberejercicio de la Unión Europea realizado hasta el momento. Su ejecución se dividió en tres fases, probando por primera vez tres niveles de respuesta a una situación de cibercrisis: el técnico; el operativo y el estratégico-político.

---

[66] Agencia Europea de Seguridad de las Redes y de la Información, «Cyber Exercises» disponible en https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme

[67] Agencia Europea de Seguridad de las Redes y de la Información, «Cyber Exercises» disponible en https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme

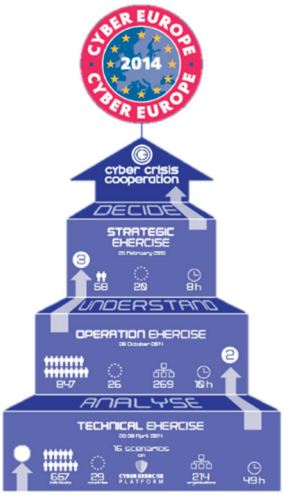

Fig. 2.1. Ejercicio Cyber Europe 2016. Fuente: ENISA.

Como lecciones aprendidas se concluyó que había que seguir avanzando en la mejora de los procedimientos de escalada a nivel estratégico, sobre todo en la cooperación internacional; la diferenciación entre las causas, el medio y las consecuencias, en cuanto a que las consecuencias deben ser gestionadas por otros organismos no relacionados con la ciberseguridad; en que el intercambio de información en el nivel técnico y operacional está fundamentalmente basado en la confianza, pero que a nivel estratégico debe plantearse bajo otro enfoque y basarse en acuerdos formales; en la utilización del *IPCR* (*Integrated Political Crisis Response*)[68], sistema para responder a crisis de nivel estratégico/político y donde existe una conexión entre todos los Estados miembros y el Consejo, y, por último, en la inexistencia de un Organismo europeo con competencias coordinadoras para la ciberseguridad.

Los retos y oportunidades que plantea la participación en este tipo de ejercicios permiten probar el nivel de cooperación, colaboración y comunicación público-privada y público-pública a distintos niveles y en tiempo real (táctico-técnico, operacional y estratégico).

Asimismo, incrementa el conocimiento sobre los recursos y capacidades para la prevención, detección y respuesta a los ciberataques y la gestión de crisis, ejercitando la gestión en la toma de decisiones para cada uno de los niveles involucrados, además de permitir practicar y coordinar la comunicación pública de forma coordinada y bajo un liderazgo único.

[68] Consejo de la Unión Europea, «Dispositivo Integrado de Respuesta Política de la Unión Europea a las Crisis» disponible en http://www.consilium.europa.eu/en/documents-publications/publications/2014/eu-ipcr/

Conclusiones y retos

Crisis y ciberespacio son palabras que no será raro verlas juntas en un mundo donde la tecnología y la hiperconectividad condicionan cada vez más el desarrollo de nuestra sociedad. El ciberespacio es un espacio de grandes oportunidades, si bien es imposible ocultar que en él se tensionan los intereses de los Estados con fines distintos y organizaciones terroristas y redes de crimen organizado se sirven de las facilidades que ofrece el medio.

Desde la creación del Departamento de Seguridad Nacional de la Presidencia del Gobierno, en el verano de 2012, hemos impulsado un modelo integrado de gobernanza para la ciberseguridad. Un modelo basado en la implicación de todos los actores y recursos del Estado y en la participación del sector privado y de la sociedad en general. La participación del sector privado en la Seguridad Nacional es hoy en día ineludible y, quizás, sea la ciberseguridad un ámbito paradigmático en este sentido. Así ha quedado recogido en la Estrategia de Seguridad Nacional, la Estrategia de Ciberseguridad Nacional y, sobre todo, en la Ley de Seguridad Nacional.

Quizás el aspecto más innovador de la nueva Ley se encuentre en el articulado dedicado a la gestión de situaciones de crisis y muy especialmente en la figura de la «situación de interés para la Seguridad Nacional». La nueva Ley contempla la participación de las distintas Administraciones públicas y del sector privado, para lo cual se activarán los mecanismos de enlace y coordinación del Sistema de Seguridad Nacional necesarios, centrados en el Consejo de Seguridad Nacional, el Comité Especializado de Situación y el Departamento de Seguridad Nacional.

Es verdad que hemos trabajado mucho y bien en estos últimos años pero el horizonte se vislumbra repleto de nuevos retos que seguirán requiriendo la participación decidida de todos. Entre los principales a corto plazo merecen destacarse, a nuestro juicio:

- Trasladar al plano nacional la Directiva de Seguridad de las Redes y de la Información de la Unión Europea.
- Mejorar nuestros sistemas y protocolos de intercambio de información, tanto a nivel nacional como internacional y entre el sector público y privado y a distintos niveles.
- Planear y ejecutar ciberejercicios con la participación de la Administración y del sector privado en todos los niveles de gestión de crisis.
- Desarrollar una fuerte cultura de ciberseguridad que incremente los niveles de prevención y, por tanto, una minimización del riesgo.

Las iniciativas presentadas en este capítulo nos han llevado a mejorar sustancialmente nuestras capacidades para «garantizar un uso seguro de las redes y los sistemas de información a través del fortalecimiento de nuestras capacidades de prevención, detección y respuesta a los ciberataques»[69].

[69] Estrategia de Seguridad Nacional, objetivo para la ciberseguridad nacional, p. 42.

Desde el Departamento de Seguridad Nacional de la Presidencia del Gobierno seguiremos trabajando con ilusión por mejorar nuestra ciberseguridad nacional, en la idea y el propósito de que se trata de un proyecto compartido, de todos y para todos.

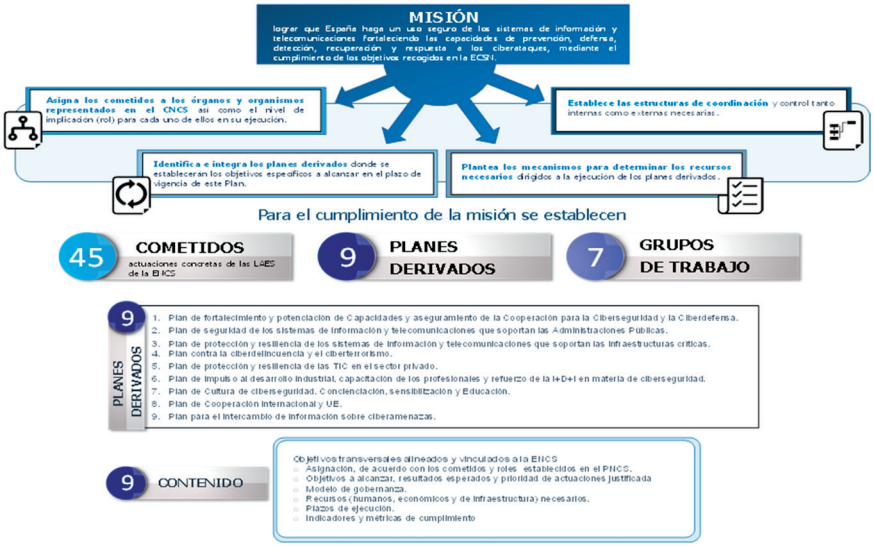

Fig. 2.2. Estructura del plan nacional de ciberseguridad

TABLA 2.1. Planes derivados de ciberseguridad

N.º	NOMBRE DEL PLAN DERIVADO
1	Plan de fortalecimiento y potenciación de capacidades y aseguramiento de la cooperación para la ciberseguridad y la ciberdefensa.
2	Plan de seguridad de los sistemas de información y telecomunicaciones que soportan las Administraciones públicas.
3	Plan de protección y resiliencia de los sistemas de información y telecomunicaciones que soportan las infraestructuras críticas.
4	Plan contra la ciberdelincuencia y el ciberterrorismo.
5	Plan de protección y resiliencia de las TIC en el sector privado.
6	Plan de impulso al desarrollo industrial, capacitación de los profesionales y refuerzo de la I+D+i en materia de ciberseguridad.
7	Plan de cultura de ciberseguridad. Concienciación, sensibilización y educación.
8	Plan de cooperación internacional y Unión Europea.
9	Plan para el intercambio de información sobre ciberamenazas.

TABLA 2.2. Líneas de acción de la estrategia nacional de ciberseguridad

LÍNEA DE ACCIÓN		OBJETIVOS
1	**Capacidad de prevención, detección y respuesta ante las ciberamenazas**	Incrementar las capacidades de prevención, defensa, detección, explotación, análisis, recuperación, respuesta y coordinación ante las ciberamenazas, haciendo énfasis en las Administraciones públicas, las Infraestructuras Críticas, las capacidades militares y de Defensa y otros sistemas de interés nacional.
2	**Seguridad de los Sistemas de Información de las Administraciones públicas**	Garantizar la implantación del Esquema Nacional de Seguridad, reforzar las capacidades de detección y mejorar la defensa de los sistemas clasificados.
3	**Seguridad de las Redes y los Sistemas de Información y Telecomunicaciones que soportan las Infraestructuras Críticas**	Impulsar la implantación de la normativa sobre Protección de Infraestructuras Críticas y de las capacidades necesarias para la protección de los servicios esenciales.
4	**Capacidad de investigación y persecución del ciberterrorismo y la ciberdelincuencia**	Potenciar las capacidades para detectar, investigar y perseguir las actividades terroristas y delictivas en el ciberespacio, sobre la base de un marco jurídico y operativo eficaz.
5	**Seguridad y resiliencia de las TIC del sector privado**	Impulsar la seguridad y la resiliencia de las infraestructuras, redes, productos y servicios empleando instrumentos de cooperación público-privada.
6	**Conocimientos, competencias e I+D+i**	Promover la capacitación de profesionales, impulsar el desarrollo industrial y reforzar el sistema de I+D+i para la ciberseguridad.
7	**Cultura de ciberseguridad**	Concienciar a los ciudadanos, profesionales y empresas de la importancia de la ciberseguridad y del uso responsable de las nuevas tecnologías y de los servicios de la Sociedad de la Información.
8	**Compromiso internacional**	Promover un ciberespacio internacional seguro y confiable, en apoyo a los intereses nacionales.