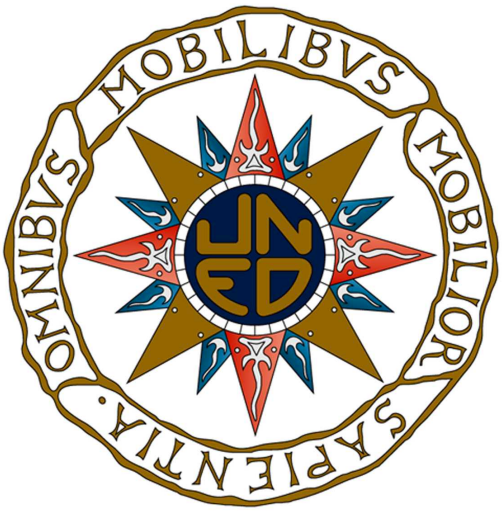
TESIS DOCTORAL

LA CIBERSEGURIDAD EN ESPAÑA 2011 – 2015
UNA PROPUESTA DE MODELO DE ORGANIZACIÓN

UNIVERSIDAD NACIONAL DE EDUCACIÓN A DISTANCIA

FACULTAD DE CIENCIAS POLÍTICAS Y SOCIOLOGÍA

DEPARTAMENTO DE CIENCIA POLÍTICA Y DE LA ADMINISTRACIÓN



Autor: D. Aníbal Villalba Fernández
Enseñanza Superior Militar

Director: Dr. D. Faustino Fernández-Miranda Alonso

Codirectora: Dra. Dña. Margarita Gómez-Reino Cachafeiro

Madrid 2015

Agradecimientos

ÍNDICE

INTRODUCCIÓN

1. Presentación y justificación del objeto de estudio. La pregunta de investigación

El ciberespacio ha introducido una nueva dimensión en las sociedades y su uso se ha incorporado de modo cotidiano y generalizado. Gracias a las nuevas tecnologías y al uso extensivo de internet, se están desarrollando proyectos que abarcan las áreas más diversas de las actividades humanas. Los adelantos en las comunicaciones y el abaratamiento de los costes están generando una red en la que pocos elementos escapan a estar conectados, incluso los objetos de uso cotidiano, en lo que se ha venido a llamar el internet de las cosas.

Los aspectos positivos de la utilización del ciberespacio son numerosos. La generación de nuevas capacidades en campos como las comunicaciones, la investigación científica, los procesos industriales o la gestión del conocimiento son evidentes. Además, el acceso de modo casi generalizado a las redes ha constituido un escenario rico en oportunidades para una gran parte de la población. Esta revolución tecnológica y su impacto social están conformando un escenario que impregna la vida de las sociedades.

No obstante, esta situación presenta nuevos retos a los que no se sustraen los diferentes actores políticos, principalmente los Estados. Entre estos desafíos se encuentran la protección y recuperación de los sistemas de infraestructuras críticas ante agresiones que utilizan el ciberespacio como entorno y vehículo para interferir en las actividades de los ciudadanos y de las instituciones.

De esta forma, hoy en día, los Estados deben hacer frente a ataques contra la seguridad de los sistemas de las Tecnologías de la Información y las Comunicaciones (TIC) de gobiernos, administraciones públicas y empresas con alto valor estratégico. Esta situación ha conformado un nuevo escenario, que precisa atención de los diferentes actores políticos para adaptarse.

España no ha permanecido inmune a las agresiones que utilizan el ciberespacio para atentar contra los más variados aspectos de la seguridad, llegando a verse comprometidos servicios críticos y otros aspectos que afectan a la seguridad nacional.

En este escenario, se han desarrollado diferentes medidas de carácter político, de planeamiento estratégico de la ciberseguridad y de creación de estructuras organizativas y de carácter técnico, con el objetivo de hacer frente a los desafíos que el uso del ciberespacio tiene para la seguridad nacional.

En el ámbito del planeamiento de la seguridad nacional en España, cabe destacar la aprobación por el Consejo de Ministros, el 24 de junio de 2011, de la primera estrategia de seguridad nacional en España: "Estrategia Española de Seguridad. Una responsabilidad de todos", donde por vez primera se incorpora la ciberseguridad a los niveles superiores de planeamiento estratégico nacional.

Esta estrategia se actualizó con la aprobación, por el Consejo de Ministros, el 31 de mayo de 2013, de la "Estrategia de Seguridad Nacional. Un proyecto compartido". Señala la referencia del Consejo de Ministros que "La Estrategia de Seguridad Nacional de 2013, coordinada por el Departamento de Seguridad Nacional de la Presidencia del Gobierno, es una revisión de la Estrategia aprobada en 2011 por el anterior Ejecutivo, y que cuenta con el respaldo político del principal partido de la oposición. El objetivo del Gobierno es reforzar y hacer extensible a todos, este consenso político y social, porque se trata de una verdadera política de Estado."

Continúa la referencia del Consejo de Ministros señalando que "La Estrategia de 2013 concibe la Seguridad Nacional de una forma amplia y global, por lo que incluye muy distintos ámbitos de actuación. Tradicionalmente, el concepto de Seguridad Nacional se ceñía a la defensa y la seguridad pública, pero hoy se extiende a nuevos actores y amenazas y, por ello, la Seguridad Nacional hace frente a nuevos riesgos como las ciberamenazas."

En este sentido, la Estrategia de Seguridad Nacional de 2013 contempla hasta doce riesgos para nuestra seguridad: conflictos armados; terrorismo; ciberamenazas;

crimen organizado; inestabilidad económica y financiera; vulnerabilidad energética; flujos migratorios irregulares; armas de destrucción masiva; espionaje; emergencias y catástrofes naturales; vulnerabilidad del espacio marítimo y vulnerabilidad de las infraestructuras críticas y servicios esenciales.

Es interesante señalar que aunque las ciberamenazas se contemplan como un riesgo en sí mismas, se encuentran presentes en prácticamente todo el resto de riesgos identificados, en mayor o menor medida, a excepción de los flujos migratorios irregulares y las emergencias y catástrofes naturales. Este carácter transversal de las ciberamenazas ha llevado al desarrollo de estrategias específicas, en ámbitos que se consideran prioritarios.

En concreto, derivadas de la Estrategia de Seguridad Nacional de 2013, se han aprobado la Estrategia de Ciberseguridad Nacional y la Estrategia de Seguridad Marítima Nacional, el 5 de diciembre de 2013, y la Estrategia de Seguridad Energética Nacional, el 20 de julio de 2015.

Además de la Estrategia de Ciberseguridad Nacional, que es objeto de análisis en esta tesis, es de destacar el componente de ciberseguridad de que se dotan las Estrategias Nacionales de Seguridad Marítima y de Seguridad Energética.

Estas tres estrategias fueron aprobadas por el Consejo de Seguridad Nacional, órgano creado en el Consejo de Ministros de 31 de mayo de 2013, que según la referencia del Consejo de Ministros: “Equipara a España a países de su entorno donde existen órganos similares, que se reúnen regularmente para discutir colectivamente los objetivos del Gobierno en esta materia y para gestionar crisis que requieren una participación multisectorial.” El Consejo de Ministros definió la composición del Consejo de Seguridad Nacional y le asignó el mandato de elaborar una propuesta de Anteproyecto de Ley Orgánica de Seguridad Nacional. En cumplimiento de este mandato, se promulgó la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional.

El Consejo de Seguridad Nacional ha creado también diferentes Comités especializados, ligados al desarrollo de las estrategias: el Consejo Nacional de

Seguridad Marítima, el Consejo Nacional de Ciberseguridad, y el Comité Especializado de Inmigración, que se han unido al Comité Especializado de Situación, órgano único para la gestión de crisis en el nivel político-estratégico. La Estrategia de Seguridad Energética Nacional prevé la posible creación de un Comité Especializado de Seguridad Energética como órgano de apoyo al Consejo de Seguridad Nacional.

El Consejo Nacional de Ciberseguridad (CNCS) se constituyó formalmente el 24 de febrero de 2014, según decisión del Consejo de Seguridad Nacional de 5 de diciembre de 2013, que creó este Comité Especializado en Ciberseguridad en la estela de la aprobación de la Estrategia Nacional de Ciberseguridad en esa misma fecha.

El Consejo Nacional de Ciberseguridad se encuentra compuesto por representantes de diferentes ministerios que tienen competencia en ciberseguridad en España, y su cometido principal consiste en desarrollar las líneas de acción y los cometidos especificados en la Estrategia Nacional de Ciberseguridad.

Desde la fecha de su constitución, el CNCS ha elaborado un Plan Nacional de Ciberseguridad, que desarrolla la Estrategia Nacional de Ciberseguridad, el cual fue aprobado por el Consejo de Seguridad Nacional el 14 de octubre de 2014.

El Plan Nacional de Ciberseguridad, a su vez, establecía la necesidad de incorporar de modo integral los elementos relacionados con la ciberseguridad que son competencia, en diferentes ámbitos, de distintos organismos. De esta forma, el 14 de julio de 2015, el Consejo Nacional de Ciberseguridad aprobó los nueve Planes Derivados del Plan Nacional de Ciberseguridad, lo que fue comunicado por el presidente del CNCS al Consejo de Seguridad Nacional el 20 de julio de 2015.

Durante este proceso, se han estudiado en profundidad cuáles eran las amenazas y los riesgos derivados de los que se habían identificado en la Estrategia Nacional de Ciberseguridad. Estos elementos fueron la base de partida para organizar el proceso de planeamiento nacional en el campo de la ciberseguridad, que ha dado lugar al Plan Nacional de Ciberseguridad y a sus nueve Planes Derivados.

En esta fase del planeamiento, se han delimitado responsabilidades a los diferentes organismos, se ha creado un marco de referencia de la ciberseguridad nacional, y también se ha llevado a cabo un análisis de las capacidades necesarias en materia de ciberseguridad; todo ello para poder afrontar de modo coherente los restos que plantea la utilización del ciberespacio, su impacto en los intereses nacionales y los riesgos para la seguridad nacional.

Es preciso señalar que el proceso de planeamiento nacional de la ciberseguridad ha generado diversas inquietudes en torno a las competencias de los diferentes ministerios y organismos públicos, y también en la relación con otros actores de los sectores público y privado.

Desde la creación del Consejo Nacional de Ciberseguridad, la participación española en foros internacionales ha incorporado un valor añadido a los tradicionales vectores políticos, diplomáticos y técnicos en el ámbito de la ciberseguridad, principalmente en el marco de Naciones Unidas, Unión Europea, OTAN y OSCE.

La cooperación con estas entidades supranacionales en la esfera de la ciberseguridad ha sido de gran utilidad para identificar las amenazas y riesgos, que en gran medida son compartidos. Además, la colaboración con otros actores estatales ha facilitado en gran medida adecuar la dimensión del problema e intercambiar experiencias que pudieran redundar en un incremento de los niveles de seguridad a nivel internacional.

De la experiencia en estos foros internacionales y del intercambio con otros países se ha extraído además conocimiento de las soluciones que se estaban adoptando por otros actores internacionales en el ámbito de la ciberseguridad, para valorar su posible adaptación e incorporación a la situación en España.

Como se ha mencionado, el desarrollo de este planeamiento de ciberseguridad a nivel nacional en España ha generado un intenso y prolijo debate entre los representantes de los ministerios y organismos representados en el Consejo Nacional de Ciberseguridad, que ha llevado al intento de armonizar los cometidos de estos actores

en materia de ciberseguridad, de acuerdo a las responsabilidades que la legislación asigna a cada uno.

En este estadio, una vez aprobados el Plan Nacional de Ciberseguridad y los Planes Derivados del mismo, se han generado una serie de cuestiones que son objeto de debate relacionadas con la organización de la ciberseguridad en España. Entre estas inquietudes se encuentran algunas como: ¿Cuenta España con las estructuras adecuadas para hacer frente a los desafíos relacionados con la ciberseguridad?, ¿Estos nuevos retos necesitan una nueva organización de seguridad nacional?, ¿Sería más eficiente la adaptación de las estructuras actuales a los nuevos retos generados por el uso del ciberespacio?, ¿Cuáles deberían ser las características de esta hipotética organización?, ¿Cuál podría ser la incardinación más adecuada de este modelo en el sistema de seguridad nacional? En definitiva, **¿Cuál puede ser un modelo apropiado de organización de la ciberseguridad en España?**

Esta última cuestión es la que se ha elegido como ***pregunta de investigación***, que se estima se ajusta a lo analizado por Chuliá y Agulló, en el apartado "la formulación de la pregunta de investigación" [1].

Citan Chuliá y Agulló, en el apartado mencionado, las reglas enunciadas por Bartolini para formular una pregunta de investigación: que el problema de investigación se formule del modo más explícito y comprensible posible, delimitando con precisión el objeto de estudio y los propósitos de la investigación; la necesidad de que el problema y las preguntas tengan una respuesta adecuada al tipo de investigación que se emprenda; y que la pregunta tenga valor o relevancia teórica, contribuyendo al desarrollo y a la ampliación del conocimiento existente.

2. Metodología.

En esta fase del proceso de investigación, se valoró que un modelo de organización de la ciberseguridad en España no podría ser un ente autónomo desligado del sistema

[1] CHULIÁ, Elisa y AGULLÓ, Marco V. *Cómo se hace un trabajo de investigación en Ciencia Política*, Madrid: Los Libros de la Catarata, 2012. ISBN 978-84-8319-688-5, pp. 44-49.

de seguridad nacional. De hecho, este modelo de organización debe ser la consecuencia de un proceso de planeamiento integral de la seguridad nacional, que analiza los diversos ámbitos con impacto en la seguridad, define los riesgos y amenazas, y establece las diferentes políticas y estrategias para generar los niveles que se estiman adecuados de la seguridad nacional.

Después de la enunciación de la pregunta de investigación, se decidió acotar en esta tesis el periodo de estudio de la ciberseguridad en España entre los años 2011 y 2015, por dos motivos. El primero es la mencionada aprobación el 24 de junio de 2011 de la Estrategia Española de Seguridad, donde por vez primera se incorpora la ciberseguridad a los niveles superiores de planeamiento estratégico nacional. En segundo lugar, aunque existen referencias anteriores respecto a las agresiones en que se ha utilizado el ciberespacio contra los intereses nacionales, y en concreto contra organismos de la administración española, cuya protección recae en el Centro Criptológico Nacional (CCN), se estimó que este periodo era suficiente para ofrecer una referencia de la evolución de los incidentes de ciberseguridad en España y su dimensión. No obstante, se han utilizado datos anteriores a 2011 cuando se ha estimado que podían aportar valor a la investigación.

El CCN es el organismo responsable de la prevención y recuperación de los sistemas de información del Estado, y cuenta con capacidad de respuesta a incidentes de seguridad de la información (CERT).

En el diseño de la metodología que podría considerarse de mayor utilidad para proporcionar una respuesta adecuada a la pregunta de investigación, se ha considerado la tesis de Chuliá y Agulló, según la cual: “La investigación en ciencia política comparte con otras disciplinas los fundamentos de la investigación académica”[2].

Chuliá y Agulló explican la pertinencia de la utilización del “método científico” en las ciencias sociales, señalando que esta expresión hace referencia a una serie de

[2] *Ibídem*, p. 14.

criterios, consensuados por la comunidad académica de cada disciplina, relativos a la producción de conocimiento válido. Para ello, estos autores señalan la necesidad de cumplir una serie de condiciones, que sintetizan en los siguientes atributos[3]:

a) Pretende ampliar el saber sobre un objeto de estudio determinado, es decir, aportar conocimiento nuevo u original.
b) Explicita el objetivo concreto que persigue y justifica la elección del objeto del estudio en referencia a la disciplina académica en que se inscribe.
c) Busca y toma en cuanta toda la información accesible sobre el objeto de estudio o una muestra de ella, cuya selección responda a criterios justificables en razón del objetivo de la investigación.
d) Refleja de manera sistemática y consistente las fuentes de las que extrae la información, permitiendo así contrastar esta última y replicar la investigación.
e) Recurre necesaria, aunque no exclusivamente a bibliografía académica (monografías, capítulos de libros compilados y artículos) para adquirir el conocimiento existente y ampliarlo.
f) Desarrolla argumentos lógicos y completos, exponiéndolos ordenadamente de acuerdo con una estructura razonada e internamente consistente.
g) Aspira a alcanzar conclusiones "robustas", pero susceptibles de evaluación crítica y revisión, nunca indiscutibles o irrefutables.

En esta tesis doctoral se ha tenido en cuenta también lo expresado por Chuliá y Agulló sobre las ventajas de afrontar las investigaciones en ciencia política desde una perspectiva abierta a otras ciencias sociales, ya que, como señalan los autores, es tan difícil como desacertado excluir los factores sociales, históricos económicos, jurídicos o culturales de la explicación que pueda aportar la ciencia política. De esta forma, se incentiva la interdisciplinariedad de las ciencias sociales y afloran las ventajas de lo que se ha dado en llamar "fecundación cruzada" (*cross fertilization*)[4].

[3] *Ibídem*, p. 15.

[4] *Ibídem*, p. 20.

En este sentido, se ha valorado lo publicado por Westin, Roy y Kim, en sus referencias teóricas acerca de los dos principales modelos en relación a la fecundación cruzada dominantes en la literatura de la filosofía de la ciencia y la sociología, los modelos "internalista" y "externalista". Por contraste, los seguidores de la corriente internalista, limitada estrictamente a su campo de especialidad, los externalistas sostienen la necesidad de impulsar procesos de evolución científica desde fuera de la disciplina, potenciando la investigación en red, en lugar de por líneas de investigación poco porosas. En este sentido, se ha estimado en esta tesis doctoral que la ciberseguridad constituye un campo tan transversal del conocimiento que la fertilización cruzada externalista debía ser utilizada en la metodología de la investigación, incorporando aspectos políticos, históricos, sociológicos, militares, técnicos, de gobernanza y de teoría de la organización, entre otros[5].

Al reflexionar sobre la "ciencia política", Chuliá y Agulló llaman la atención sobre el hecho de que esta rúbrica no solo reúne el conocimiento de la política que surge de una aproximación empírica a las realidades políticas, sino también a un corpus de conocimientos de naturaleza teórica y filosófica que, desde los días de la Grecia y la Roma clásicas, ha modelado la experiencia práctica y las concepciones políticas de las sociedades. No obstante, señalan estos autores, esto no significa que cultivasen simultáneamente la reflexión teórico-filosófica y la ciencia empírica de la política tal como hoy la conocemos. Esta distinción es un producto contemporáneo de lo que se podría denominar la construcción disciplinar de la ciencia política, que abre dos caminos diferentes y complementarios a la investigación: los que describen y explican los hechos políticos, que se adscriben a la "ciencia política empírica", y los que reflexionan sobre cómo mejorar esa realidad -esto es, sobre cómo deberían ser las

[5] WESTIN, Stu; ROY Matthew; y KIM Chai K.: Cross-Fertilization of Knowledge: Cross-Fertilization of Knowledge: *Cross-Fertilization of Knowledge: The Case of MIS and its Reference Disciplines.* Information Resources Management Journal, University of Rhode Island, primavera de 1994. http://www.irma-international.org/viewtitle/50993/ consulta: 24 de octubre de 2015.

cosas- bajo la denominación de "filosofía política", "teoría normativa" o, simplemente "teoría política"[6].

De los dos modelos que se señalan, este trabajo de investigación se enmarca en el **modelo "teórico"**, y no en el "empírico".

Este modelo teórico se inspira en lo señalado por Chuliá y Agulló al citar a Marsh y Stoker, para señalar que la teoría política incluye entre sus objetivos los de ofrecer una alternativa deseable a lo existente que se encuentre normativamente fundada, evaluar esa realidad conforme a los ideales y valores políticos que se tienen por preferibles y prescribir los medios adecuados –instituciones, procesos y normas– para que las alternativas deseables puedan hacerse realidad[7].

Esto último conforma el espíritu que impregna este trabajo de investigación: ofrecer una alternativa deseable y factible para mejorar el modelo de organización y de gobernanza en España en el ámbito de la ciberseguridad.

Aunque en las investigaciones teóricas predomina el **pensamiento deductivo**, se va a recurrir también al **método inductivo** en esta tesis doctoral, con el fin de alcanzar conclusiones a partir de los casos particulares observados.

López-Barajas explica que la inducción es el proceso de pasar de hechos conocidos a desconocidos, de conocimientos particulares a teorías o leyes generales, siendo el mecanismo por excelencia utilizado en la investigación empírica, sea esta completa o incompleta según se comprueben o no todos y cada uno de los elementos de una clase finita de objetos. Señala también López-Barajas que, dado el problema epistemológico que se plantea en la inducción incompleta para definir en qué condiciones sería válido el tamaño y representatividad de la muestra, el nuevo

[6] CHULIÁ, Elisa y AGULLÓ, Marco V. *Cómo se hace un trabajo de investigación en Ciencia Política*, *opus citada*, pp. 21-22.

[7] MARSH, David y STOKER, Gerry (Eds.): *Teoría y métodos de la ciencia política*. Madrid, Alianza Editorial (citado por CHULIÁ, Elisa y AGULLÓ, Marco V. *Cómo se hace un trabajo de investigación en Ciencia Política*, *opus citada*, p. 29).

concepto de inducción destaca la probabilidad lógica de la hipótesis que se define a partir de lo que ofrece la experiencia personal[8].

Al tratar la deducción, López-Barajas señala que es el acto para llegar a una conclusión, a partir de unas premisas suficientes, en cuyo caso éstas implican o contienen la conclusión. Continúa explicando el autor que tradicionalmente el silogismo ha sido el modo principal de la deducción, pero también cabe la inferencia proposicional, destacando a los representantes de la lógica simbólica[9].

Apunta también que los procesos inductivos amplían las posibilidades de raciocinio, al sugerir nuevos ámbitos de experiencia, por lo que ambas formas o modos de conocer, deductiva e inductiva, se entrecruzan al facilitar explicaciones[10].

López-Barajas cita a Bochenski para señalar que algunos autores consideran que la diferenciación entre procesos inductivos y deductivos consiste en la utilización diferente de las mismas leyes lógicas, y apunta que, no obstante, se plantean problemas teóricos y epistemológicos que han enfrentado secularmente a racionalistas y positivistas[11].

En cuanto al tipo de investigación en teoría política, Chuliá y Agulló definen cinco objetos sobre los cuales giran siempre las investigaciones en este ámbito[12]:

1. Las causas o principios generales que subyacen a los fenómenos políticos.
2. Los conceptos políticos fundamentales.
3. Los ideales y valores que alimentan los proyectos o las realidades políticas.

---

[8] LÓPEZ-BARAJAS ZAYAS, Emilio: *Fundamentos de metodología científica*. Universidad Nacional de Educación a Distancia, Madrid, 1988, quinta reimpresión mayo de 2000, ISBN 84-362-2313-6, p. 27.

[9] *Ibídem*, p. 27.

[10] *Ibídem*, p. 28.

[11] BOCHENSKI, I. M.: Los métodos actuales de pensamiento. Rialp, Madrid, 1981 (citado por LÓPEZ-BARAJAS ZAYAS, Emilio: *Fundamentos de metodología científica*, *opus citada,* p. 26).

[12] CHULIÁ, Elisa y AGULLÓ, Marco V. *Cómo se hace un trabajo de investigación en Ciencia Política*, *opus citada*, p. 84.

4. Las distintas estructuras institucionales, así como las reglas que rigen el funcionamiento de dichas estructuras y los procedimientos en que se articulan.
5. La historia del pensamiento político, las teorías políticas y los sistemas filosóficos formulados en el pasado.

Estos autores pasan a continuación a adjudicar tipos de investigaciones asociados a estos cinco objetos de estudio, explicativo, analítico, prescriptivo, evaluativo e histórico[13]:

a) Las **investigaciones explicativas** se preguntan por los comportamientos de los individuos y los grupos en el seno de las sociedades políticas, por las relaciones que se establecen, por los objetivos, y por los principios generales que los explican. Dada la naturaleza de la explicación que se busca, el investigador carece de la posibilidad de verificar empíricamente sus afirmaciones, por lo que, junto al imprescindible apoyo de los textos clásicos y el eventual recurso a la comprobación histórica, la investigación ha de ser fundamentalmente argumentativa.
b) El **análisis conceptual**, aunque habitualmente utilizado para la clarificación y depuración de los conceptos políticos fundamentales, impregna en muy buena medida la práctica totalidad de las investigaciones que puedan plantearse, ya que es prácticamente imposible que en cualquier tipo de investigación teórica no se necesite esclarecer, precisar, refinar o perfeccionar algunos de los conceptos que se estén utilizando. Este análisis tiene un carácter eminentemente argumentativo que busca la coherencia lógica en el discurso y se basa en tres tareas que se encuentran en íntima conexión: la especificación de sus elementos, a menudo a través de su definición; la síntesis intelectual que establece las conexiones lógicas; y el perfeccionamiento de conceptos.
c) Las **investigaciones prescriptivas** tienen naturaleza instrumental, que relacionan los hechos con los valores, y se interesan por los métodos más apropiados –normas, procedimientos e instituciones– para alcanzar ese mundo

[13] *Ibídem*, pp. 86-93.

político deseable que ya se ha proyectado. Estas investigaciones prescriptivas se fundamentan en las teorías normativas, que formulan y justifican los ideales y valores políticos sobre los que se funda el mundo deseable. De esta forma, se desprende que la prescripción solamente cabe cuando previamente se ha definido el estado ideal de cosas que se pretende alcanzar porque el actual resulta insatisfactorio, y es entonces cuando tiene sentido sugerir remedios que puedan aplicarse en la práctica. Las teorías prescriptivas son tanto aquellas que proponen un mundo político ideal como aquellas que proyectan instituciones o procedimientos concretos para hacer realidad ese mundo deseable.

d) Las **investigaciones evaluativas** tienen como principal objetivo examinar y valorar una concreta realidad política conforme a ciertos ideales y principios normativos ya establecidos. En no pocas ocasiones, y en particular cuando se emprenden investigaciones prescriptivas, esta evaluación se lleva a cabo previamente, bien de manera explícita e implícita, puesto que no se puede prescribir sin antes evaluar. En otras, la investigación evaluativa concluye en una concreta prescripción, o la lleva implícita, dependiendo de cuál haya sido el juicio que merezcan las realidades o las teorías políticas que se están evaluando.
e) Las **investigaciones históricas** se encuentran muy presentes de dos formas en la investigación en teoría política: como historia de acontecimientos o instituciones por un lado, y como historia del pensamiento político por otro. En el primer supuesto, el teórico puede recurrir a las “lecciones de la historia” como criterio de comprobación de alguno de sus postulados explicativos o normativos. En el segundo supuesto, la historia de las ideas políticas puede articular distintas investigaciones: es posible un análisis conceptual separado o combinado con la evaluación comparativa de teorías políticas, y cabe asimismo formular una prescripción concreta a partir de esos análisis y evaluaciones.

Señalan Chuliá y Agulló que la frontera entre los distintos tipos de investigaciones es sutil, y no es infrecuente que alguno de estos tipos, o todos ellos, se presenten combinados en diverso grado en una investigación. Las investigaciones analíticas son

muy a menudo evaluativas y prescriptivas; las investigaciones históricas se basan fundamentalmente en el análisis conceptual y suelen presentar un fuerte componente explicativo o incluso prescriptivo; por su parte, las investigaciones prescriptivas implican una previa comprensión y evaluación de la realidad que pretenden transformar o reforzar[14].

Estos autores citan a Arteta, Guitián y Máiz, para estimar que no pocos autores consideran que, junto al tradicional objetivo de buscar la comprensión y la explicación de la vida política, la teoría política normativa es la "teoría de una actividad práctica", lo que hace que sea, necesariamente, "tanto explicativa como recomendatoria, tanto analítica como descriptiva", y sostienen que es "incompleta si se queda solo en una u otra cosa"[15].

Esta tesis doctoral nace con una vocación que encaja en un tipo de **investigación prescriptiva**, pues es su intención proponer soluciones para mejorar la organización de modelos políticos de gobernanza en el ámbito de la ciberseguridad en España.

No obstante, se van a utilizar recursos que incorporan elementos del resto de tipologías. Parcialmente se van a utilizar aspectos de la **investigación explicativa**, necesarios para comprender los comportamientos de los actores políticos en el ámbito de la ciberseguridad. También se emplearán técnicas que se encuadran en la **investigación histórica[16]**, ya que se considera necesario estudiar la evolución del pensamiento estratégico y del recorrido histórico de las soluciones que se han ido conformando en el campo de la seguridad, las cuales han dado lugar a diferentes modelos organizativos en el dominio de la ciberseguridad. Sobre el **análisis conceptual**, ya se ha apuntado que impregna la práctica totalidad de las investigaciones, debido a que en cualquier tipo de investigación teórica es necesario

[14] *Ibídem*, p. 85.

[15] ARTETA, Aurelio; GARCÍA GUITIÁN, Elena, y MAÍZ, Ramón (Eds.): *Teoría política: poder, moral, democracia*. Alianza Editorial, Madrid, 2003 (citado por CHULIÁ, Elisa y AGULLÓ, Marco V. *Cómo se hace un trabajo de investigación en Ciencia Política*, *opus citada*, p. 85).

[16] ARÓSTEGUI, Julio: *La Investigación Histórica: Teoría y Método*. Editoria Crítica S.L., Barcelona, 2001, ISBN 84-8432-137-1, pp. 360-378.

ocuparse de los conceptos que se están analizando. En este caso concreto, además, los conceptos relacionados con el ciberespacio son novedosos y no se encuentran, en algunos casos, suficientemente consolidados. Por último, esta tesis doctoral también tiene una significativa componente de **investigación evaluativa.** Ya se ha apuntado que cualquier investigación prescriptiva necesita una previa evaluación, ya que debe examinar y valorar una realidad política concreta conforme a principios establecidos y también en evolución. En el ámbito de la ciberseguridad, se considera imprescindible realizar una adecuada evaluación de la situación antes de proponer mejoras en los sistemas organizativos y de gobernanza mediante la propuesta de un modelo nacional de ciberseguridad en España.

Este trabajo de investigación se ha construido como un **estudio de caso**, según lo definen Anduiza, Crespo y Méndez, al explicar que se esta terminología se utiliza para referirse a estudios que se centran en el análisis en profundidad de una sola unidad de análisis, pero desde una perspectiva diacrónica; es decir, teniendo en cuenta variaciones temporales de las propiedades del caso que se estudia, lo que permite examinar la unidad objeto del estudio de modo intensivo[17].

La **construcción del caso** en esta tesis se basa en primer lugar en su elección para servir de plataforma de investigación. Para ello Coller destaca dos aspectos: su relevancia y su naturaleza[18].

En relación a la **relevancia** de este caso, ya se ha explicado en el proceso hasta llegar a la pregunta de investigación la importancia que tiene dotarse de un adecuado modelo de organización de la ciberseguridad en España, con el objetivo de contar con un sistema de ciberseguridad que permita afrontar de modo adecuado los riesgos y amenazas asociados al uso del ciberespacio. En relación a su **naturaleza**, también se ha presentado *de qué es el caso* y *qué uso se le va a dar*: proponer un modelo de

[17] ANDUIZA, Perea; CRESPO, Ismael; y MÉNDEZ LAGO, Mónica: *Metodología de la Ciencia Política*. Centro de Investigaciones Sociológicas, Cuadernos Metodológicos, núm. 28, diciembre de 1999, p. 62.

[18] COLLER, Xavier: *Estudio de casos*. Centro de Investigaciones Sociológicas, Cuadernos Metodológicos, núm. 30, junio de 2000, p. 29.

organización de la ciberseguridad en España que pueda ser realizable y tenga un impacto positivo en el incremento de los niveles de la seguridad nacional.

Coller realiza una clasificación y explicación de los tipos de caso:

Figura 1: Clasificación de los tipos de caso

	Tipo
Según lo que se estudia	- Objeto - Proceso
Según el alcance del caso	- Específico - Genérico (ejemplar, instrumental)
Según la naturaleza del caso	- Ejemplar - Polar (extremo) - Típico - Único (contextual, irrepetible, pionero, excepcional)
Según el tipo de acontecimiento	- Histórico (diacrónico) - Contemporáneo (sincrónico) - Híbrido
Según el uso del caso	- Exploratorio (descriptivo) - Analítico
Según el número de casos	- Único - Múltiple (paralelos o disimilares)

Fuente: COLLER, Xavier: *Estudio de casos*[19].

En relación a la tipología del caso, siguiendo los parámetros establecidos por Coller:

1. Según el **objeto de estudio**, se trata de un caso basado en **procesos**, más que en un objeto.
2. Según el **alcance del caso**, nos encontramos ante un **caso genérico o ejemplar**, ya que no es intrínseco ni constituye una excepcionalidad.

[19] *Ibídem*, pp. 31-51.

3. Según su **naturaleza** o esencia, este caso es también **ejemplar**, ya que constituye un ejemplo ilustrativo de un fenómeno, y además es **típico**, en la medida en que se le considera uno más de un grupo –el de los países afectados por los riesgos y amenazas derivados del uso del ciberespacio– en el que se incorporan en gran medida sus características esenciales, por lo que no se trata de un caso excepcional.
4. Según el **tipo de acontecimiento**, objeto o fenómeno, este caso es de **tipo mixto o híbrido**. Por una parte es contemporáneo, ya que se centra en fenómenos que tienen lugar en el momento en que se desarrolla la investigación, en los sistemas de seguridad nacional afectados por los riesgos y en amenazas derivadas de la utilización del ciberespacio. De otro lado, hace referencia a fenómenos históricos, como la evolución del pensamiento estratégico o la génesis y el desarrollo de las estrategias nacionales de seguridad, que se estiman necesarios para apreciar correctamente la situación en la actualidad.
5. Según el **uso del caso**, este trabajo de investigación tiene vocación de **naturaleza analítica**, ya que persigue estudiar el funcionamiento de un fenómeno y de su relación con otros, no tratándose de detectar y describir los efectos de este fenómeno, sino de buscar sus causas, correlatos y efectos. No obstante, en algunas fases de la investigación podría considerarse un **caso mixto**, ya que se recurre a elementos descriptivos en relación con acontecimientos pasados para explicar el proceso presente que configura el caso.
6. Según el **número de casos**, este trabajo de investigación encaja en el caso **múltiple o colectivo**, ya que es de naturaleza comparativa y se incorporan al estudio casos que se asemejan entre sí o casos denominados paralelos cuya característica principal es que tienen similitud en relación con las variables que son relevantes para la investigación, los riesgos asociados al uso del ciberespacio y las soluciones que ofrecen otros modelos de organización de la ciberseguridad nacional.

Señala Coller que la solidez de una investigación depende en muchos casos de su naturaleza comparativa, apuntando dos estrategias analíticas apropiadas para los

estudios comparados de caso. La primera es la técnica de la ilustración, donde los casos sirven para elaborar una teoría previa o emergente y el grado de similitud de los casos viene dado por la naturaleza de la investigación. La segunda es la técnica de la comparación analítica, por similitud o por diferencia, donde se desarrollan las conclusiones a partir de la observación y comparación de varios casos[20].

En este trabajo de investigación se ha utilizado el **método de comparación analítica por similitud**.

Señalan Anduiza, Crespo y Méndez que el método comparado basa su aportación a la construcción y verificación de teorías en la comparación sistemática y controlada de un número reducido de casos cuidadosamente seleccionados por sus características. De esta forma, la clasificación y selección de casos son las herramientas de control del método comparado[21].

Dependiendo del estadio de la investigación, en esta tesis doctoral se han realizado varias **selecciones de casos**. Tras presentar la evolución del pensamiento estratégico, del que se alimentan las diferentes teorías políticas que definen las estrategias nacionales de seguridad, se han analizado los casos de **Estados Unidos, China y Rusia**, al ser pioneros en el diseño de estrategias y estructuras nacionales de seguridad, los de mayor complejidad, y en los que se inspiran la mayor parte del resto de las estrategias nacionales de seguridad y sus modelos organizativos. De estos tres casos se han analizado sus estrategias nacionales de seguridad, sus estrategias nacionales de ciberseguridad, y los modelos de organización de la seguridad nacional y de la ciberseguridad que se han establecido.

Posteriormente, se han seleccionado para su análisis diversas organizaciones internacionales, que poseen una componente de seguridad, con el fin de analizar su aproximación al ámbito de la ciberseguridad: **Unión Europea, Naciones Unidas,**

[20] *Ibídem*, p. 50.

[21] ANDUIZA, Perea; CRESPO, Ismael; y MÉNDEZ LAGO, Mónica: *Metodología de la Ciencia Política*, *opus citada*, pp. 118-123.

OTAN y OSCE. Se ha estudiado **fundamentalmente el caso de la Unión Europea**, su Política Exterior y de Seguridad Común (PESC), y su Política Común de Seguridad y Defensa (PCSD), para analizar de modo detallado la ciberseguridad en la Unión Europea. Se ha dado preeminencia a la UE, ya que España se encuentra obligada por el corpus normativo de la Unión Europea y debe realizar trasposiciones de determinada legislación de obligado cumplimiento.

Con posterioridad se han **seleccionado los países de la Unión Europea** en una comparativa que analiza diversos parámetros de la ciberseguridad. Esta selección se ha realizado porque estos países comparten características comunes con el caso español en mayor medida que otros de otras regiones geopolíticas.

Entre los Estados miembros de la Unión Europa **se han seleccionado** tres casos para un estudio de mayor profundidad: **Reino Unido, Alemania y Francia**. Lo que principalmente ha motivado esta selección es que son países que cuentan con estrategias nacionales de ciberseguridad, tienen una dimensión similar a la española, comparten riesgos y amenazas en el ámbito de la ciberseguridad de modo análogo, y cuyas soluciones en relación con el modelo de ciberseguridad nacional podrían ajustarse o inspirar la mejora del modelo nacional de ciberseguridad en España.

El análisis que se realiza en este trabajo de investigación está también inspirado en el movimiento del **neo institucionalismo** (*new institutionalism*). Señala Caballero Míguez que en las dos últimas décadas del siglo XX la ciencia política ha experimentado un renovado y sólido interés en el estudio de las instituciones políticas desde diversos enfoques teóricos. Este “retorno de las instituciones” ha implicado la aparición de un nuevo institucionalismo en ciencia política compuesto por un conjunto de enfoques que sobre bases teóricas diversas han estudiado el papel de las instituciones políticas. De este modo, se ha reconocido la existencia de enfoques como el institucionalismo histórico, el institucionalismo de elección racional, el institucionalismo normativo, el institucionalismo empírico, el institucionalismo

sociológico, el institucionalismo de representación de intereses o el institucionalismo internacional[22].

Apuntan Goodin y Klingemann que este movimiento neo institucionalista se encuentra en algunos casos alineado parcialmente con el movimiento de elección racional –con el individuo como generador de impulsos económicos, sociales y políticos–, una alianza representada entre otros por Ostrom (*Governing the Commons*) y North (*Institutions, Institutional Change and Economic Performance*); aunque señalan también Goodin y Klingemann que en otros autores el neo institucionalismo toma un decidido rumbo sociológico alejado de la línea de elección racional, como demuestran las obras de March y Olsen (*Rediscovering Institutions*), y Skocpol (*States and Social Revolution*). En este escenario, Goodin y Klingemann señalan que el neo institucionalismo tiene, en cualquier caso, una gran potencia para facilitar un modelo integrador para investigaciones complejas sobre las instituciones[23].

Otro aspecto que se tiene presente en este trabajo de investigación, relacionado con el neo institucionalismo que alertaba de la rigidez en las instituciones, las cuales limitan sus posibilidades de cambio, es el fenómeno de las **"trayectorias dependientes"** (*path dependency*), que se dan cuando el resultado de un proceso depende de la entera secuencia de decisiones tomadas por los actores y no solamente de las condiciones del momento[24].

3. Conceptos utilizados y definiciones

[22] CABALLERO MÍGUEZ, Gonzalo: *Nuevo institucionalismo en ciencia política, institucionalismo de elección racional y análisis político de costes de transacción: una primera aproximación*. RIPS. Revista de Investigaciones Políticas y Sociológicas, 6, 2007, ISSN 1577-239X. http://www.redalyc.org/articulo.oa?id=38060201 consulta: 25 de octubre de 2015.

[23] GOODIN, Robert E. y KLINGEMANN, Hans-Dieter (Eds.): *A New Hadbook of Political Science*. Oxford University Press, Oxford, 1996, reimpresión 2000, ISBN 0-19-828015-7, p. 25.

[24] PETERS, B. Guy; PIERRE, Jon; y KING, Desmond S.: *The Politics of Path Dependency: Political Conflict in Historical Institutionalism*. Southern Political Science Association, The Journal of Politics, vol. 67, núm. 04, noviembre de 2005, pp. 1275-1300. http://web.iaincirebon.ac.id/ebook/moon/PoliticsMatters/j.1468-2508.2005.00360.x.pdf consulta: 25 de octubre de 2015.

Los conceptos que se han utilizado en esta tesis doctoral se han ido incorporando adaptándose a las necesidades de la investigación, aportando su definición cuando se ha estimado conveniente para facilitar la comprensión de la argumentación y siempre que aportaran valor al objeto de la investigación.

Al constituir el ciberespacio un ámbito relativamente nuevo de actuación, y encontrarse en una evolución dinámica, aún no se han asentado diferentes conceptos que son utilizados de modo distinto por diferentes Estados, organizaciones y científicos.

En este escenario, en relación a las definiciones específicas de los conceptos vertidos en el entorno de la ciberseguridad, se ha dado prioridad a lo señalado por el Centro Criptológico Nacional de España (CCN), como organismo responsable de la doctrina y formación destinada al personal de la Administración especialista en el campo de la seguridad de las Tecnología de la Información y Comunicaciones (TIC)[25]. En este sentido, se ha utilizado la *Guía de Seguridad CCN-STIC-401. Glosario y Abreviaturas*[26]*.* Dicha guía no se ha incorporado como anexo a esta tesis doctoral debido a su extensión y a su facilidad de consulta en línea.

Para una ampliación de los conceptos y definiciones se recomienda el trabajo de Maurer y Morgus, en el que estos autores realizan una compilación de definiciones relativas a la ciberseguridad y a la seguridad de la información. Esta compilación se basa en las definiciones que se recogen en publicaciones de organizaciones

[25] El Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional, recoge en su artículo 2 que el Centro Criptológico Nacional elabora y difunde normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la Administración, y forma al personal de la Administración especialista en el campo de la seguridad de los sistemas de las tecnologías de la información y las comunicaciones. Se puede acceder a este Real Decreto en el enlace https://www.boe.es/diario_boe/txt.php?id=BOE-A-2004-5051 consulta 10 de septiembre de 2015.

[26] CCN-CERT: *Guía de Seguridad CCN-STIC-401. Glosario y Abreviaturas,* agosto 2015. https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/401-glosario_abreviaturas/index.html consulta: 13 de septiembre de 2015.

internacionales, organismos internacionales de normalización y las estrategias nacionales de ciberseguridad[27].

En el presente trabajo de investigación se ha utilizado la siguiente definición de ciberseguridad[28]:

Conjunto de actuaciones orientadas a asegurar, en la medida de lo posible, las redes y sistemas que constituyen el ciberespacio:

- *detectando y enfrentándose a intrusiones,*
- *detectando, reaccionando y recuperándose de incidentes, y*
- *preservando la confidencialidad, disponibilidad e integridad de la información.*

4. De la pregunta de investigación a la estructura de la investigación.

Se ha considerado necesario establecer, en primer lugar, la dimensión del problema que suponen los riesgos y amenazas, así como su materialización para los intereses nacionales en España. De esta forma, el **primer capítulo de la tesis: "Evolución de los incidentes de ciberseguridad en España 2011-2015"** se dedica a valorar esta dimensión y a identificar las tendencias de las agresiones. De esta forma, aquí se ha analizado la evolución de las agresiones que han sufrido diferentes organismos de la administración pública española, encuadrándolos en un contexto más general, ya que gran parte de las ciberamenazas son compartidas por otros Estados.

Del análisis de los incidentes de ciberseguridad, basado principalmente en la información proporcionada en el documento "Ciberamenazas 2014. Tendencias

[27] MAURER, Tim y MORGUS, Robert: *Compilation of Existing Cybersecurity and Information Security Related Definitions*, New America, octubre de 2014. http://www.giplatform.org/sites/default/files/Compilation%20of%20Existing%20Cybersecurity%20and%20Information%20Security%20Related%20Definition.pdf consulta: 12 de septiembre de 2015.

[28] CCN-CERT: *Guía de Seguridad CCN-STIC-401. Glosario y Abreviaturas, opus citada, p. 213.*

2015"[29] elaborado por el CCN-CERT[30], se desprende el elevado volumen y nivel de criticidad de las agresiones sufridas por los diversos organismos de la Administración española.

En total, en 2014, el CERT Gubernamental Nacional abordó 12.916 incidentes, de los cuales, 132 fueron catalogados como críticos; es decir, aquellos que pueden causar degradación de los servicios para un gran número de usuarios, implicar una grave violación de la seguridad de la información, afectar a la integridad física de las personas, causar importantes pérdidas económicas, u ocasionar daños irreversibles a los recursos de la organización.

En el ámbito global, señala el CCN-CERT que si algo ha caracterizado al año 2014 ha sido la especial virulencia en los ataques contra la seguridad de los sistemas de las Tecnologías de la Información y las Comunicaciones (TIC) de gobiernos, administraciones públicas y empresas con alto valor estratégico. Los incidentes de gran envergadura se han venido sucediendo, mes a mes, en un intento continuo, por parte de los atacantes, de apropiarse de información valiosa o sensible desde los puntos de vista político, estratégico, de seguridad o económico.

En cuanto a las tendencias en el ámbito internacional se señala también el incremento de incidentes de ciberseguridad en 2015, y se espera que en años futuros, aumenten las agresiones relacionadas con el ciberespionaje, así como el incremento de los ataques *como servicio* efectuados por grupos con conocimiento y capacidad técnica para realizarlos con garantías de éxito.

Del análisis de la evolución de los incidentes de ciberseguridad en España 2011-2015 se desprende que España ha sido uno de los países más castigados por las ciberamenazas, especialmente en materia de ciberespionaje y ciberdelincuencia organizada.

[29] https://www.ccn-cert.cni.es/publico/dmpublidocuments/IE-Ciberamenazas2014-Tendencias-2015.pdf

[30] CERT: Capacidad de respuesta a incidentes de ciberseguridad.

Las conclusiones de este primer capítulo sobre la evolución de los incidentes de ciberseguridad en España, en las que se recogen las tendencias al alza en las agresiones que utilizan el ciberespacio, obligan a reflexionar acerca de las capacidades necesarias para hacer frente a estas ciberamenazas en el futuro, y sobre la conveniencia de la revisión del modelo de organización de la ciberseguridad en España para mejorar las capacidades de prevención y respuesta ante los incidentes de ciberseguridad, con el objetivo de favorecer la mejor protección de los intereses nacionales.

Se entiende, por tanto, que, ante unos desafíos de tal calibre sea conveniente valorar la necesidad de disponer de un modelo de organización específico en el ámbito de la ciberseguridad que ofrezca respuestas de modo integral para prevenir las ciberamenazas y que facilite la recuperación de los sistemas que hayan sido atacados. En esta línea, se considera necesario disponer de un modelo adecuado de ciberseguridad nacional en España para hacer frente a los riesgos y amenazas derivados del uso del ciberespacio .A partir de este escenario se atiende a la pregunta de investigación: **¿Cuál puede ser un modelo apropiado de organización de la ciberseguridad en España?**

Para ofrecer una repuesta a la pregunta de investigación ha sido precisa la revisión del estado de la cuestión en el entorno internacional, para lo que se ha realizado un estudio comparado, que ha incluido la descripción y el análisis de la evolución del pensamiento estratégico, las estrategias nacionales de seguridad, las estrategias nacionales de ciberseguridad y los modelos de organización de la ciberseguridad más relevantes que se han ido conformando.

Descrita y valorada la situación de los modelos de organización de la ciberseguridad en el ámbito internacional, se ha realizado un estudio de caso acerca de la situación de la ciberseguridad en España. Se ha analizado el sistema de seguridad nacional, la ley de seguridad nacional, la estrategia de seguridad nacional y la estrategia nacional de ciberseguridad, para posteriormente presentar la estructura actual del sistema de ciberseguridad en España. A continuación se han valorado los condicionantes para un

modelo de organización de la ciberseguridad a nivel nacional en nuestro ordenamiento jurídico.

La premisa de partida se apoya en la consideración de que la ciberseguridad no es un elemento aislado de la seguridad, sino un dominio que se encuentra incardinado en las estructuras de seguridad de nivel superior. En la estela de este razonamiento, se ha comenzado estudiando **la evolución del pensamiento estratégico en el segundo capítulo**, con el objetivo de realizar una reflexión sobre el estado de la cuestión y en qué medida estas corrientes de pensamiento a través de la historia han ido impregnando a las sociedades de criterios sobre los que cimentar su aproximación a la seguridad en la defensa de sus intereses.

Esta evolución del pensamiento estratégico ha conformado diferentes estilos de seguridad, de acuerdo a las circunstancias geopolíticas y sociales de los diferentes actores políticos, aunque las principales corrientes de pensamiento han sobrepasado el ámbito local para incardinarse en mayor o menor medida en los esquemas de seguridad nacionales e internacionales. Pensadores como Sun Tzu, Maquiavelo, Clausewitz, Fukuyama o Huntington, han incorporado sus ideas de modo tan amplio en los esquemas de seguridad de los diferentes Estados y organizaciones internacionales que sin su conocimiento no sería posible comprender la evolución de los esquemas de seguridad. Las diferentes aproximaciones a la ciberseguridad, como derivada de un concepto de seguridad más amplio, se alimenta también de esa corriente de pensamiento estratégico que impregna a los actores políticos que deben conformar sus modelos de organización de ciberseguridad.

El **tercer capítulo de la tesis está dedicado a las estrategias nacionales de seguridad**, como modelo reciente de la organización de la seguridad en los Estados. Se presentan tres casos, el de Estados Unidos de América, la República Popular China y la Federación de Rusia. Se ha limitado el estudio a estos tres modelos porque se estima ofrecen tres visiones diferentes, aunque complementarias, de la organización de la seguridad nacional y por ser las tres principales potencias en el ámbito de la seguridad. Basándose en sus aproximaciones a la seguridad, otros Estados han ido

incorporando diferentes aspectos de estos complejos modelos a sus propias estrategias nacionales de seguridad.

Estados Unidos es el creador del sistema moderno de estrategias nacionales de seguridad, en el que se han inspirado el resto de Estados. La disposición en un formato público de la percepción nacional del ámbito de la seguridad, la descripción de las amenazas y riesgos nacionales, así como los modelos de organización y las aproximaciones estratégicas para garantizar la seguridad nacional y la protección de los intereses nacionales han conformado un estilo que ha sido imitado por numerosos Estados. En el caso estadounidense, además se ha sido pionero en la creación de estructuras para organizar la gestión de la seguridad nacional, entre las que destaca el Consejo de Seguridad Nacional. Organismo que ha sido posteriormente incorporado por la mayoría de los Estados a sus esquemas nacionales de seguridad.

Estados Unidos ha incorporado también diferentes corrientes del pensamiento estratégico al diseño de su seguridad, inspirados en la Roma y Grecia clásicas, Maquiavelo, Clausewitz y, recientemente, una serie de autores estadounidenses entre los que pueden destacarse los Tofler, Fukuyama, Huntington y Brezinski. Precisamente Zbigniew Brzezinski fue Consejero de Seguridad Nacional del gobierno del Presidente de Estados Unidos Jimmy Carter (1977-1981), materializando las líneas de pensamiento estratégico que había publicado a principios de los años 70, cuando advirtió de los riesgos del declive del poder imperial norteamericano y de los efectos de una recomposición de hegemonías planetarias a las que debía corresponder una nueva política de Washington.

La aproximación de China a la seguridad constituye una referencia inevitable por la globalidad de sus intereses, el impacto de sus políticas y el condicionante que supone no solo al área geopolítica asiática sino al resto de espacios geopolíticos mundiales. La compleja organización china es también deudora de la creación estadounidense del sistema de estrategia nacional de seguridad y del Consejo Nacional de Seguridad, en cuyo modelo se inspiran, como reconocen las propias autoridades chinas, según se detalla en este capítulo.

China incorpora al diseño de su seguridad ideas estratégicas que proceden de los grandes clásicos, como Confucio y Sun Tzu, y también de las corrientes de la época más reciente ligada a la revolución china, con Mao Tse Tung como referente ideológico.

El tercer gran actor político del que se analiza su estrategia nacional de seguridad es la Federación de Rusia. El concepto de seguridad en Rusia se encuentra muy ligado a las ideas desarrolladas por Mackinder y la “tierra corazón”; de este modo Rusia percibe su seguridad basada en el espacio geopolítico definido por el territorio continental, entendiendo que es la zona clave para conservar el poder y mantener el control de otros espacios geopolíticos adyacentes, en una región cardial o área pivote definida por Asia Central y Europa Oriental.

La seguridad en Rusia tiene una tradición que ha llevado a que tenga un corpus legislativo integrado relacionado con la seguridad nacional, destacando documentos de estrategia de seguridad, relaciones exteriores, doctrina militar y ciberseguridad.

La Estrategia de Seguridad Nacional de la Federación de Rusia para el año 2020, aprobada en mayo de 2009, y la Doctrina Militar de la Federación de Rusia hasta el 2020, de diciembre de 2014, son los textos estratégicos que diseñan la percepción rusa de la seguridad, de sus intereses nacionales, de las amenazas y riesgos a los que se enfrenta Rusia, y también definen las líneas estratégicas que permiten una capacidad de protección y respuesta en defensa de los intereses nacionales.

Al igual que Estados Unidos y China, Rusia también ha conformado un Consejo de Seguridad Nacional, que está presidido por el Presidente de Rusia, de acuerdo con la Constitución de la Federación de 1993. La Ley Federal "Sobre la Seguridad", de conformidad con el artículo 83 de la Constitución de la Federación de Rusia, define el estatuto del Consejo de Seguridad de Rusia, sus objetivos, funciones, composición y organización de sus actividades.

Del estudio de estos tres grandes actores políticos, con intereses globales en materia de seguridad, se desprenden las siguientes conclusiones: 1. Las estrategias

nacionales de seguridad, iniciadas por Estados Unidos, se han convertido en el modelo de documento maestro del que se desprende la planificación de la seguridad nacional. 2. Estas estrategias nacionales de seguridad obedecen a un esquema similar, en primer lugar se presenta la percepción nacional del escenario global; posteriormente se definen los intereses nacionales; a continuación se analizan las amenazas y riesgos contra los intereses nacionales en distintos ámbitos; después se enuncian las líneas estratégicas que el Estado desarrollará para proteger los intereses nacionales y para recuperar la situación anterior en el caso de que se haya producido una agresión; por último, las estrategias generan unas estructuras que permiten gestionar la seguridad nacional. 3. La integración de los intereses nacionales es total; en especial, destaca la importancia de la capacidad económica como referente transversal de la seguridad. 4. Los tres países se han dotado de un consejo de seguridad nacional que asesora al presidente de la nación. 5. Se ha establecido una jerarquía de los niveles de la seguridad que ha generado diferentes organismos con responsabilidades en esta materia. 6. Los aspectos militares, aunque de gran importancia, se encuentran integrados en las estrategias nacionales de seguridad y responden a lo definido en estos documentos en este ámbito. 7. Las estrategias nacionales de seguridad se desarrollan mediante estrategias sectoriales, como es el caso de las estrategias nacionales de ciberseguridad.

Tras haber analizado las estrategias nacionales de seguridad de Estados Unidos, la República Popular China y la Federación de Rusia, con el fin de enmarcar los principales modelos nacionales de seguridad, en el **capítulo cuarto** se han estudiado **las iniciativas internacionales en el ámbito del planeamiento de la ciberseguridad**, referidas a la Unión Europea, la Organización de las Naciones Unidas, la Organización del Tratado del Atlántico Norte y la Organización para la la Seguridad y la Cooperación en Europa. Se han elegido estas cuatro organizaciones por ser las principales con responsabilidades en el ámbito de la ciberseguridad, tanto a nivel global como regional.

La **Unión Europea** se ha tomado como referencia principal en el ámbito internacional, ya que España, como Estado miembro, se encuentra obligada en el cumplimiento de

la normativa comunitaria, debiendo trasponer la legislación pertinente. Además, España forma parte de las estructuras de seguridad, defensa y ciberseguridad de la UE. Por consiguiente, se ha prestado atención especial a la Política Exterior y de Seguridad Común (PESC) de la UE, y a su derivada, la Política Común se Seguridad y Defensa (PCSD), tras el Tratado de Lisboa.

En el ámbito de la Política Exterior y de Seguridad Común, la entrada en vigor del Tratado de Lisboa ha supuesto el comienzo de un proceso destinado a favorecer que la Unión Europea tenga una estructura más armónica y que le permita afrontar de modo más eficaz los retos en su acción exterior.

La conformación de la personalidad jurídica de la Unión Europea constituye un aspecto de importante calado, que permite a la Unión celebrar acuerdos con Estados u organizaciones internacionales en los ámbitos de la PESC. Esta personalidad jurídica única de la Unión ha robustecido su capacidad de interlocución, convirtiéndola en un actor más eficaz a escala internacional y un socio más visible para otros países y organizaciones internacionales.

La “Estrategia Europea de Seguridad: Una Europa segura en un mundo mejor” se redactó a instancias del Alto Representante de la UE para la Política Exterior y de Seguridad Común (PESC), Javier Solana, y fue presentada al Consejo Europeo, que la adoptó en su reunión del 12 y 13 de diciembre de 2003, en Bruselas. En este documento, el Alto Representante define los retos mundiales y las principales amenazas contra la seguridad de la Unión y clarifica los objetivos estratégicos de la UE para hacer frente a estas amenazas.

La ciberseguridad como tal no aparece recogida en la Estrategia Europea de Seguridad de 2003 y no será contemplada hasta su revisión en 2008, en el “Informe sobre la aplicación de la Estrategia Europea de Seguridad: Ofrecer seguridad en un mundo en evolución”, que analiza el grado de cumplimiento de los objetivos y revisa las amenazas, en el marco de la Política Europea de Seguridad y Defensa, en cuanto parte integrante de la Política Exterior y de Seguridad Común, lo que se menciona

expresamente en el apartado de retos mundiales y principales amenazas, especificando que “las economías modernas dependen en gran medida de las infraestructuras vitales como los transportes, las comunicaciones y el suministro de energía, e igualmente de Internet”.

La Estrategia de la UE para una sociedad de la información segura en Europa de 2006 fue en muchos sentidos pionera de un concepto de la ciberseguridad integral. De esta forma, se señalaba que la confianza es un factor clave para el éxito de la nueva sociedad de la información; añadiendo que la confianza está relacionada con las experiencias de los usuarios y con el deber de respetar su intimidad; por consiguiente, la seguridad de las redes y de la información no debe considerarse simplemente como un aspecto técnico. De esta forma, la seguridad de las redes y de la información debe considerarse como elemento fundamental en la creación del espacio europeo de información, que contribuye al cumplimiento de la Estrategia renovada de Lisboa.

El 7 de febrero de 2013, la Comisión Europea y la Alta Representante de la UE para Asuntos Exteriores y Política de Seguridad presentaron una Comunicación conjunta al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo, y al Comité de las Regiones, titulada: “Estrategia de Ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro”.

Señala la Estrategia de Ciberseguridad de la UE que para que el ciberespacio siga siendo abierto y libre, deben aplicarse en línea los mismos principios, valores y normas que la UE promueve fuera de línea. Los derechos fundamentales, la democracia y el Estado de Derecho deben ser protegidos en el ciberespacio. La libertad y la prosperidad de la Unión dependen cada vez más de una Internet sólida e innovadora. Pero la libertad en línea requiere también protección y seguridad.

El ciberespacio ha de ser protegido de incidentes, actividades malintencionadas y utilizaciones abusivas. A las administraciones públicas les corresponde un papel destacado en la custodia de un ciberespacio libre y seguro. Entre sus tareas figuran

las de salvaguardar el acceso y la apertura, respetar y proteger los derechos fundamentales en línea y mantener la fiabilidad e interoperabilidad de Internet.

En el marco de la Política Común de Seguridad y Defensa (PCSD), las Conclusiones del Consejo de la UE en relación con su Estrategia de Ciberseguridad destacan la necesidad urgente de aplicar y hacer avanzar la PCSD para desarrollar un marco de ciberdefensa; la necesidad de mejorar las capacidades de ciberdefensa de los Estados miembros, en particular mediante el desarrollo de normas comunes; y la concienciación a través de la formación y educación en ciberseguridad, utilizando los recursos de la Escuela Europea de Seguridad y Defensa.

Por último, se reflejan aspectos relacionados con las Cláusulas de Solidaridad y de Defensa Mutua de la Unión Europea en el ámbito del ciberespacio

En **Naciones Unidas** se está desarrollando un proceso de alto nivel en el ámbito de la ciberseguridad, para lo que se ha creado un esquema basado en informes que son elaborados por un Grupo de Expertos en el que se encuentran representados los Estados líderes en el proceso de planeamiento de la ciberseguridad. Los informes de este Grupo de Expertos se presentan al Secretario General de la ONU, quien los eleva a la Asamblea General de las Naciones Unidas, para su discusión en sus reuniones de otoño. El Grupo de Expertos se ha formado en tres ocasiones, en ciclos de un año de duración. Las conclusiones de este Grupo de Expertos recogen elementos que reflejan la posición común de las naciones representadas, y sus conclusiones se encuentran orientadas al impacto de la seguridad en el ciberespacio en el marco de la legalidad y seguridad internacionales.

En la **OTAN** la ciberdefensa lleva ya varios años formando parte de los temas de interés de la Alianza, y desde la Cumbre de Lisboa en 2010 forma parte del Concepto Estratégico de la Alianza. Cabe señalar que después del ciberataque a Estonia, en enero de 2008, se desarrolló la primera Política de Ciberdefensa, que se ha venido revisando hasta la fecha. Así, en 2008 se creó el Centro de Excelencia para la Cooperación de la Ciberdefensa en Tallin. En la Cumbre de Chicago de 2012 se

reafirmó el compromiso de mejora de las ciberdefensas de la Alianza reuniendo todas las redes OTAN bajo una protección centralizada y creándose la NCIA (NATO Communications and Information Agency) en la que se integran las seis agencias existentes relacionadas con las tecnologías de la información y las telecomunicaciones.

En la Política de Defensa Reforzada aprobada por los Ministros de Defensa en junio 2014 y en la Declaración adoptada en la Cumbre de Gales que tuvo lugar los días 4-5 de septiembre de 2014, se recuerda que la principal responsabilidad de la OTAN es defender sus propias redes, y que la asistencia a los aliados debe abordarse de acuerdo a los principios de solidaridad, destacando la responsabilidad de los aliados de desarrollar las capacidades relevantes para la protección de sus redes nacionales.

Finalmente, se ha reconocido, tras un largo debate al respecto, que podría considerarse la posibilidad de invocar el Art. 5 del Tratado de la OTAN de defensa colectiva en caso de un ciberataque a un aliado, si bien se tendrá que decidir caso por caso.

La **OSCE** ha desarrollado un sistema de trabajo en relación con la ciberseguridad dirigido a favorecer las medidas de confianza entre sus miembros. Además, al ser un foro de seguridad regional en el que participan Estados Unidos y Rusia, ha servido para intercambiar posiciones políticas y también técnicas.

La OSCE es una de las organizaciones internacionales de carácter regional más activa en materia de ciberseguridad. En la reunión Ministerial de diciembre de 2013 en Kiev se aprobó una Decisión (No 1106) “Conjunto Inicial de Medidas de la OSCE para el Fomento de la Confianza Destinadas a Reducir los Riesgos de Conflicto dimanantes del uso de las Tecnologías de la Información y la Comunicación”, en la que se establecen 11 medidas de fomento de la confianza que los estados participantes tienen que cumplir, con el objetivo de favorecer la transparencia y evitar situaciones de tensión entre Estados que podrían derivar en conflictos internacionales.

Asimismo se ha creado un Grupo de Trabajo de Expertos en el que se revisa el grado

de cumplimiento de las 11 medidas por los países y la posibilidad de adoptar un segundo paquete de medidas de fomento de la confianza más ambicioso.

Las conclusiones que se han obtenido al analizar los aspectos de ciberseguridad de estas organizaciones internacionales, reflejan que la ciberseguridad es un ámbito de primer orden en las políticas de estas organizaciones que han realizado un planeamiento estratégico acorde a las misiones de la organización, que se desarrolla en un planeamiento en cascada que aspira a favorecer adecuados niveles de seguridad en el ciberespacio para desempeñar las misiones que tienen encomendadas.

El **quinto capítulo** de este trabajo de investigación se dedica al análisis de las diferentes **iniciativas nacionales y la evolución de las estrategias nacionales de ciberseguridad** que han llevado a la construcción de diferentes **modelos nacionales de ciberseguridad**.

Se han estudiado, en el ámbito de la ciberseguridad, los casos de Estados Unidos, China y Rusia, que ya se habían tratado como referencias en el capítulo dedicado al planeamiento estratégico de la seguridad nacional, así como los modelos institucionales a que habían dado lugar. En concreto, todos ellos han establecido un Consejo de Seguridad Nacional, aunque sus estructuras y modelos organizativos difieren de acuerdo a sus propias características nacionales.

A continuación se analiza el estado de la ciberseguridad en los países de la Unión Europea, utilizando cinco bloques de parámetros: fundamentos legales para la ciberseguridad; capacidades operativas; asociaciones público-privadas; planes de ciberseguridad en sectores específicos; y educación en ciberseguridad.

Este análisis ofrece, de modo gráfico, una instantánea de la situación de la ciberseguridad en cada uno de los países de la UE, y los pone en comparación con el resto.

A continuación se estudian con más detalle los casos de Reino Unido, Alemania y Francia, porque, tal como se explicó en el apartado de la metodología, se ha considerado que estos tres actores pueden ofrecer elementos de mayor utilidad que el resto de los países de la UE para el caso español, debido a características de dimensión geográfica, demográfica, económica, de liderazgo en el campo de las relaciones exteriores, y otras.

Cabe destacar de este estudio que estos tres países de referencia en la UE disponen de una Estrategia de Ciberseguridad Nacional, una legislación específica en materia de ciberseguridad, se han dotado de un Consejo Nacional de Ciberseguridad, y disponen de un CERT nacional competente que actúa como coordinador nacional en la comunidad CERT, tanto en el ámbito público como privado.

Se ha incorporado como anexo un gráfico de la organización de la ciberseguridad en Japón, que se ha estimado de utilidad.

Después de haber estudiado los diferentes diseños nacionales de Estados Unidos, China, Rusia, los países de la Unión Europea y, dentro de los casos de la UE, los de Reino Unido, Alemania y Francia, en el **capítulo sexto** se aborda, como estudio de caso, el **planeamiento de la ciberseguridad en España**, incardinado en el sistema de seguridad nacional. De esta forma, se han analizado la reciente Ley de Seguridad Nacional, el Sistema de Seguridad Nacional, las Estrategias de Seguridad Nacional, El esquema Nacional de Seguridad en el ámbito de la Administración electrónica, y la Estrategia de Ciberseguridad Nacional y su desarrollo. Se prestará especial atención al Consejo Nacional de Ciberseguridad, al ser el organismo que ha organizado la gobernanza de la ciberseguridad en España mediante la confección del Plan Nacional de Ciberseguridad y los nueve Planes Derivados del mismo.

En el **capítulo séptimo** se aborda la **propuesta de un modelo de organización de la ciberseguridad en España**.

Para finalizar, se presentan las **conclusiones** de este trabajo de investigación, que aspiran a facilitar la labor de incardinación de esta propuesta de modelo nacional de

organización de la ciberseguridad en España en la Administración General del Estado..

5. Motivaciones personales

Esta tesis doctoral está inspirada en el trabajo que vengo desarrollando desde marzo de 2014 como asesor para ciberseguridad del Presidente del Consejo Nacional de Ciberseguridad (CNCS), el Secretario de Estado Director del Centro Nacional de Inteligencia, General de Ejército D. Félix Sanz Roldán.

Como Vocal Asesor en el Gabinete de la Presidencia del Gobierno, tuve oportunidad de participar en el grupo de trabajo, dirigido por Javier Solana, que elaboró la "Estrategia Española de Seguridad. Una responsabilidad de todos", aprobada en junio de 2011.

En noviembre de 2011 participé en la delegación oficial española en la *Conferencia internacional sobre los problemas del ciberespacio*, celebrada en Londres, y también participé en la última edición de esta iniciativa, celebrada en La Haya en junio de 2015.

He formado parte del equipo de apoyo de los dos Embajadores en Misión Especial para el Ciberespacio que ha tenido España hasta la fecha, en su función de expertos nacionales en el Grupo de Expertos Gubernamentales para el Ciberespacio de Naciones Unidas, para la redacción del informe sobre seguridad en el ciberespacio que fue presentado al Secretario General de la ONU en julio de 2015.

Como profesor de estrategia y relaciones internacionales del Curso de Estado Mayor de las Fuerzas Armadas, de 2001 a 2005, desarrollé una labor docente y de investigación relacionada con el planeamiento estratégico y la seguridad nacional.

Las diversas publicaciones en las que he participado se enmarcan en la seguridad nacional, Inteligencia, planeamiento estratégico, seguridad en Unión Europea y OTAN, terrorismo, y evolución del pensamiento estratégico.

Los destinos que me fueron encomendados en Naciones Unidas, OTAN y Unión Europea han estado relacionados con el planeamiento estratégico y operacional, y también con labores de asesoría política y militar.

CAPÍTULO 1. EVOLUCIÓN DE LOS INCIDENTES DE CIBERSEGURIDAD EN ESPAÑA 2011-2015

Para valorar el estado de la cuestión relativo a los incidentes de ciberseguridad se ha acotado el estudio en el periodo 2011 al 2015. Se ha considerado que esta horquilla ofrece suficiente recorrido para valorar el impacto y la tendencia de los incidentes que afectan a la seguridad en el ciberespacio. No obstante, en algunas ocasiones se presentarán datos anteriores a este periodo cuando se estime que facilitan la comprensión del fenómeno.

Además, la referencia del año 2011 se encuentra orientada al periodo de aprobación de la primera estrategia de seguridad nacional elaborada en España, que incorporó las amenazas y los riesgos relativos al ciberespacio integrándolos con el resto de desafíos a los que se enfrenta la seguridad nacional.

Se ha considerado necesario realizar este estudio de los incidentes de ciberseguridad en España para comprender la dimensión del impacto de la ciberseguridad en la seguridad nacional, elemento indispensable para poder llegar a proponer un modelo de ciberseguridad nacional que proporcione los adecuados niveles de seguridad para la nación y sus ciudadanos.

El estudio de estos incidentes de ciberseguridad en España se colocará en perspectiva con otros riesgos para la seguridad nacional de diferentes tipos y también, en lo que favorezca la comprensión del fenómeno, se analizarán los incidentes de ciberseguridad en otros entornos internacionales ya que los riesgos derivados de la utilización del ciberespacio son compartidos en gran medida por otros Estados y organizaciones internacionales.

Al ser la ciberseguridad un fenómeno relativamente reciente, en relación con otros elementos clásicos de la seguridad, se irán incorporando al estudio las definiciones de los conceptos que se estimen convenientes para facilitar el análisis.

Se va a analizar en primer lugar la ciberseguridad en el contexto de los riesgos globales, para valorar adecuadamente su dimensión en el panorama global de riesgos y amenazas.

También se pondrán en relación los riesgos asociados al uso del ciberespacio, en el marco de impacto con otro tipo de riesgos, mediante el análisis de conexiones con otros riesgos en áreas económicas, sociales, ambientales y de riesgos geopolíticos.

A continuación, se van a analizar las amenazas derivadas del uso del ciberespacio, para lo cual se van a definir los orígenes o agentes de la amenaza, las víctimas u objetivos que pueden verse atacados y los efectos que se esperan conseguir por los generadores de los ataques.

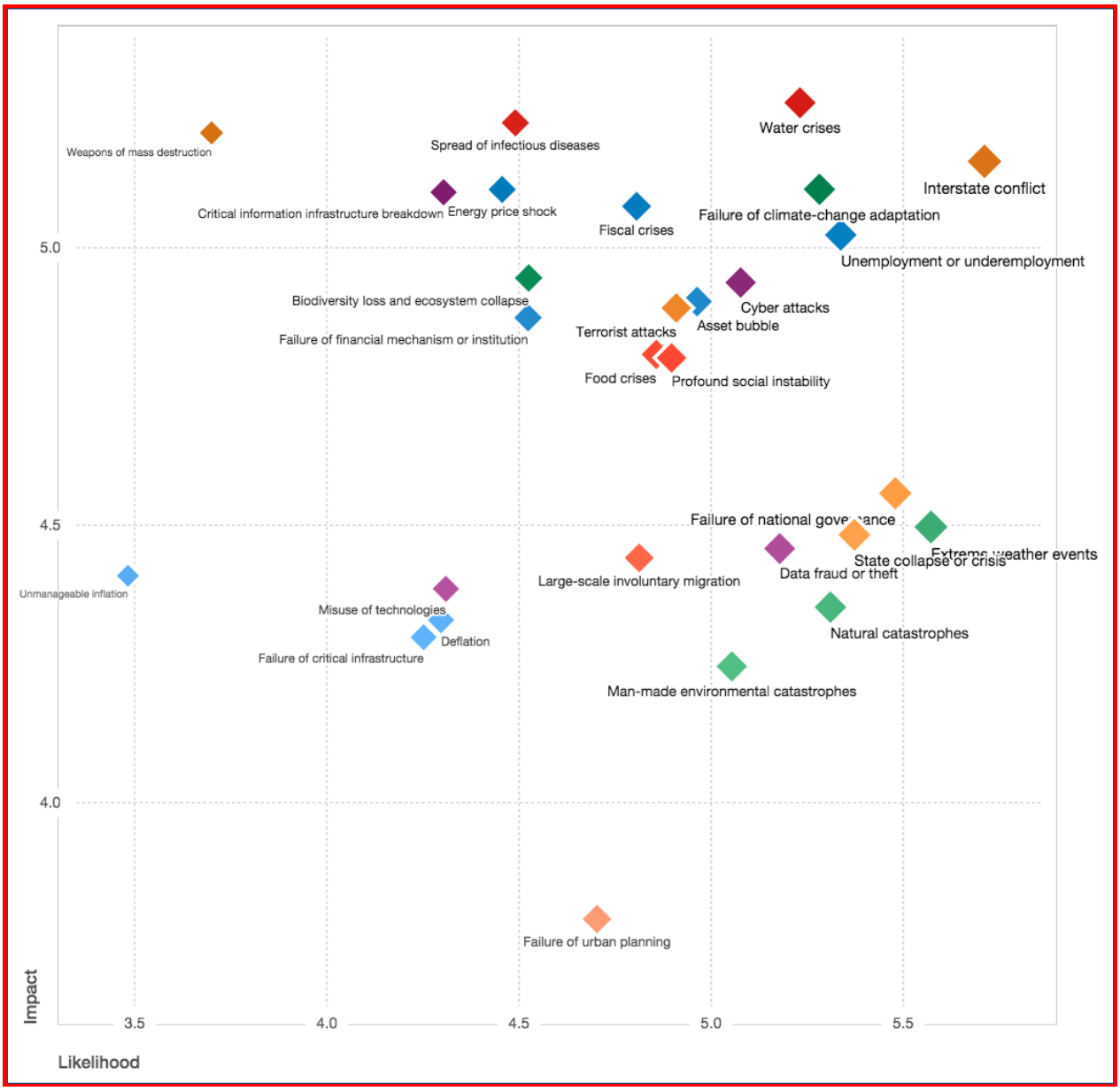
Posteriormente se tratará el caso español, mediante el análisis de los ciberincidentes en España. Se colocará, en primer lugar, en perspectiva con otros países la situación de la utilización del ciberespacio en España, para posteriormente presentar los datos de los ciberincidentes ocurridos en España en el periodo 2011-2015, valorando las tendencias de las tasas de encuentro e infección, las categorías de malware detectadas, su volumen, la evolución en el número de ciberincidentes gestionados por el CCN-CERT, el nivel de peligrosidad de los ciberincidentes en España, y las tendencias de futuro.

1.1. La ciberseguridad en el contexto de los riesgos globales

En primer lugar se van a situar los ciberataques en perspectiva con otros riesgos globales. El Foro Económico Mundial ha publicado el estudio "Riesgos Globales 2015"[31] en el que ofrece un gráfico sobre la percepción del impacto y de la probabilidad de los riesgos globales, que denomina el paisaje de riesgos globales en 2015.

[31] World Economic Forum: *Global Risks 2015*, Ginebra, 2015. http://www3.weforum.org/docs/WEF_Global_Risks_2015_Report15.pdf consulta: 4 de septiembre de 2015.

Figura 2: El Paisaje de Riesgos Globales en 2015



Fuente: World Economic Forum.[32]

[32] World Economic Forum: *Global Risks 2015*. http://reports.weforum.org/global-risks-2015/part-1-global-risks-2015/technological-risks-back-to-the-future/#frame/20ad6 consulta: 4 de septiembre de 2015.

En este estudio del Foro Económico Mundial, se refleja la probabilidad y el impacto de los riesgos individuales, que se establece en una escala de 1 a 7, donde 1 representa el valor inferior en cuanto a la probabilidad e implica un impacto muy limitado y 7 se refiere a un riesgo muy probable y con impactos negativos masivos y devastadores[33].

Los ciberataques tienen asignada una probabilidad de 5,1 y un impacto de 4,9. Los riesgos asociados a los ciberataques son superados solamente, en relación a la combinación de ambos parámetros, por el desempleo, la negativa adaptación al cambio climático, las crisis relacionadas con el agua y los conflictos entre Estados. De este paisaje de riesgos globales se desprende la percepción de la alta probabilidad y el elevado impacto de los ciberataques en comparación con el resto de riesgos globales.

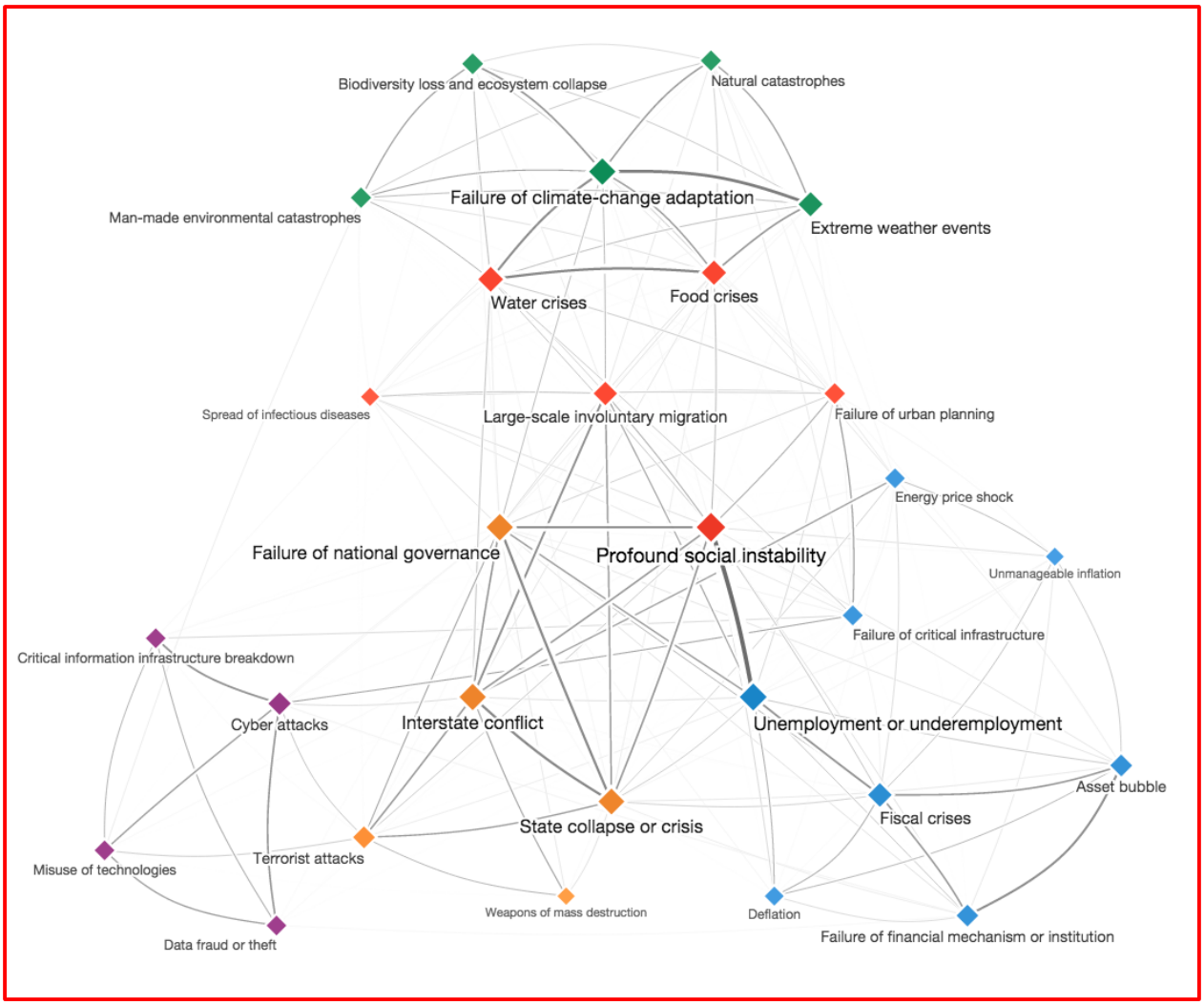
El informe “Riesgos Globales 2015” analiza estos datos en un apartado específico dedicado a los riesgos tecnológicos en un anexo titulado: “Riesgos Tecnológicos: Regreso al Futuro”[34]. En el análisis se recoge que el riesgo de ataques cibernéticos a gran escala se sigue considerado por encima del promedio en las dos dimensiones del impacto y la probabilidad, lo que refleja la creciente sofisticación de los ataques cibernéticos y el surgimiento de la hiperconectividad, con un número cada vez mayor de objetos físicos conectados a Internet, además de la vulnerabilidad que supone el almacenamiento de los datos personales en la nube. Además, el "Internet de las cosas" (IoT en sus siglas en inglés) incrementará esta tendencia al generar nuevos riesgos asociados a la privacidad y adecuado uso de los datos.

El mencionado informe “Riesgos Globales 2015” ofrece también un mapa de interconexión de los riesgos.

[33] Se puede acceder a la metodología utilizada para la investigación del informe “Riesgos Globales 2015” en el enlace: http://reports.weforum.org/global-risks-2015/appendix-b-the-global-risks-perception-survey-2014-and-methodology/ consulta: 5 de septiembre de 2015.

[34] *Ibídem*: *Technological Risks: Back to the Future*. http://reports.weforum.org/global-risks-2015/part-1-global-risks-2015/technological-risks-back-to-the-future/ consulta: 4 de septiembre de 2015.

Figura 3: El mapa de interconexiones de riesgos globales 2015



Fuente: World Economic Forum[35].

En este gráfico se puede observar la conexión directa de los ciberataques con otros riesgos tecnológicos como la ruptura de la infraestructura de información crítica, el mal uso de las tecnologías, el fraude y robo de datos. También existe un enlace directo con un riesgo que en el informe se asocia a la economía, el fallo de infraestructuras críticas. El resto de conexiones directas con otros riesgos caen en el ámbito de los

[35] *Ibídem.*

riesgos denominados geopolíticos, ataques terroristas, fallo de la gobernanza nacional y conflictos entre Estados.

Señala el informe al analizar este gráfico que los riesgos no pueden ser vistos en forma aislada. La retroalimentación entre los riesgos y el hecho de que ellos también son impulsados por las tendencias subyacentes aumentar su complejidad y que sea más difícil el control de los riesgos individuales. Además, según el informe, que es el décimo de estas características, durante los últimos años la velocidad de transmisión de los enlaces entre los riesgos y la fortaleza de las interconexiones se han incrementado.

En el caso de los riesgos asociados al uso del ciberespacio, podemos observar al analizar el gráfico que las conexiones de segundo nivel alcanzan a otros riesgos que tienen unos niveles elevados tanto de probabilidad como de peligrosidad y que se incorporan a áreas económicas, sociales, ambientales y de riesgos geopolíticos.

El anexo “Riesgos Tecnológicos: Regreso al Futuro” mencionado, del informe “Riesgos Globales 2015”, apunta a la necesidad de establecer mecanismos para mantener una red unificada y resistente. De esta forma, del análisis de riesgos globales y su interacción con los relacionados con las nuevas tecnologías se destaca que el ritmo de la innovación y la naturaleza de Internet requieren un nuevo enfoque de la gobernanza de Internet global.

Aparte de los problemas técnicos, cobran más importancia los relacionados con los riesgos derivados de la delincuencia cibernética, la neutralidad de la red, la privacidad y la libertad de expresión. La responsabilidad de la infraestructura técnica de Internet se encuentra repartida entre varias organizaciones, que incluyen el Grupo de Tareas de Ingeniería de Internet (IETF), el Consorcio World Wide Web (W3C), los Registros Regionales de Internet (RIRs), los operadores de los servidores raíz, y la Corporación de Internet para la Asignación de Números y Nombres en Internet (ICANN). Las soluciones que estos organismos proponen, como adopción de políticas, normas, especificaciones o buenas prácticas, se articulan a través de la adopción voluntaria o

la confección específica de convenciones, reglamentos, directivas, contratos u otros acuerdos.

Se continua señalando que esa aproximación no facilita el desarrollo e implementación de soluciones a los problemas globales. En consecuencia, los gobiernos se encuentran con la la presión de adoptar medidas nacionales para hacer frente a la protección de datos de sus ciudadanos y al grado de privacidad. No obstante, si bien las leyes que obligan a la localización de la infraestructura pueden ser soluciones más fáciles a corto plazo que colaborar para definir mecanismos globales para hacer frente a los problemas, el riesgo es que el "nacionalismo de datos" podría poner en peligro los efectos de Internet para impulsar la innovación y crear valor social y económico. Para avanzar en el proceso y contribuir a generar una adecuada gobernanza de Internet, el Foro Económico Mundial se ha embarcado en una iniciativa estratégica para abordar estas cuestiones, como complemento al Foro de Gobernanza de Internet y otras iniciativas.

1.2. Ciberamenazas: orígenes, objetivos y efectos

Una vez puestos en perspectiva los riesgos relacionados con la ciberseguridad con otros riesgos globales, se van a analizar las amenazas, para lo cual se van a definir los orígenes o agentes de la amenaza, las víctimas u objetivos que pueden verse atacados y los efectos que se esperan conseguir por los generadores de los ataques.

Para estudiar estos aspectos del fenómeno se va a partir de lo expresado en el informe “Evaluación de la Ciberseguridad en los Países Bajos”, elaborado por el Centro Nacional de Ciberseguridad de los Países Bajos, que recoge en su una matriz de amenazas globales la correlación entre los orígenes de la amenaza y sus víctimas, explicando los ámbitos de las agresiones y los efectos a conseguir[36].

[36] Centro Nacional de Ciberseguridad de los Países Bajos: Cyber Security Assessment Netherlands 4, La Haya, octubre de 2014, p. 9. Disponible en https://www.ncsc.nl/english/current-topics/news/cyber-securty-assessment-netherlands-4-cybercrime-and-digital-espionage-remain-the-biggest-threat.html consulta: 4 de septiembre de 2015.

Figura 4: Matriz de amenazas globales de ciberseguridad.

	Objetivos		
Origen de la amenaza	**Sector público**	**Sector privado**	**Ciudadanos**
Actores Estatales	Espionaje digital	Espionaje digital	Espionaje digital
	Capacidades ofensivas	Capacidades ofensivas	
Terroristas	Interrupción de Sistemas Toma de control	Interrupción de Sistemas Toma de control	
Profesionales del ciberdelito	Sustracción, publicación o venta de información	Sustracción, publicación o venta de información	Sustracción, publicación o venta de información
	Manipulación de información	Manipulación de información	Manipulación de información
	Interrupción de sistemas	Interrupción de sistemas	Interrupción de sistemas
	Toma de control de sistemas	Toma de control de sistemas	Toma de control de sistemas
Cibervándalos y script kiddies	Sustracción de información	Sustracción de información	Sustracción de información
	Interrupción de sistemas	Interrupción de sistemas	
Hacktivistas	Sustracción y publicación de la información sustraída	Sustracción y publicación de la información sustraída	Sustracción y publicación de la información sustraída
	Desfiguraciones en páginas web	Desfiguraciones en páginas web	
	Interrupción de sistemas	Interrupción de sistemas	
	Interrupción de Sistemas / Toma de control	Interrupción de Sistemas / Toma de control	
Actores internos	Sustracción, publicación o venta de información	Sustracción, publicación o venta de información	
	Interrupción de sistemas	Interrupción de sistemas	
Ciber investigadores	Recibir y publicar información	Recibir y publicar información	
Organizaciones privadas		Sustracción de información (espionaje industrial)	Uso/abuso o reventa información clientes

Niveles de peligrosidad

Bajo: No se han observado nuevas amenazas o tendencias, o se dispone de medidas suficientes para neutralizar la amenaza, o no ha habido incidentes especialmente significativos en el periodo.
Medio: Se han observado nuevas amenazas o tendencias, o se dispone de medidas (parciales) para neutralizar la amenaza, o Los incidentes detectados no han sido especialmente significativos.

Alto: Las amenazas o su tendencia se han incrementado significativamente. Las medidas adoptadas tienen un efecto muy limitado, por lo que la amenaza permanece. Los incidentes detectados han sido especialmente significativos.

Fuente: Centro Nacional de Ciberseguridad de los Países Bajos: *Evaluación de la Ciberseguridad en los Países Bajos*, p. 9.

Como ya se ha mencionado, los riesgos en el ámbito de la ciberseguridad son compartidos por un número significativo de actores. En la estela de este argumento, se ha estimado que este estudio producido por el Centro Nacional de Ciberseguridad de los Países Bajos ofrece de modo gráfico y esquemático las diferentes combinaciones que se dan en la mayor parte de escenarios, por lo que se va a utilizar como referencia para analizar el fenómeno.

Para ello, se van a utilizar como referencia los elementos proporcionados por el Centro Criptológico Nacional (CCN), que en su formato CCN-CERT es la Capacidad de Respuesta a incidentes de Seguridad de la Información de las administraciones públicas (general, autonómica y local), con las que coopera y a las que ayuda a responder de forma rápida y eficiente a los incidentes de seguridad, constituyéndose en centro de alerta nacional[37].

El CCN-CERT en su informe "Ciberamenazas 2014. Tendencias 2015", con el grado de clasificación "sin clasificar", realiza una descripción de los agentes de la amenaza, de la que, a continuación, se extraen los aspectos más significativos para la investigación[38].

[37] Este servicio se creó a finales del año 2006 como CERT gubernamental español, y sus funciones quedan recogidas en el capítulo VII del RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad. Este texto legal, en su artículo 37 señala los servicios que el CCN-CERT ya prestaba desde su constitución (en parte recogidos en el RD 421/2004 de regulación del CCN). Se puede acceder a información sobre el organismo en el enlace https://www.ccn.cni.es/ consulta: 5 de septiembre de 2015.

[38] CCN-CERT: *Ciberamenazas 2014. Tendencias 2015*, IA-09/15, Madrid, marzo de 2015. https://www.ccn-cert.cni.es/informes/informes-de-amenazas-ia/813-ccn-cert-ia-09-15-ciberamenazas-2014-tendencias-2015/file.html consulta: 5 de septiembre de 2015.

Los Estados como agentes de las amenazas

En la matriz de amenazas globales de ciberseguridad presentada se asigna a los Estados, como agentes generadores de la amenaza, posibles acciones de espionaje digital o ciberespionaje y las capacidades ofensivas en el ciberespacio.

Señala el CCN-CERT que la amenaza del ciberespionaje originado en los Estados o por empresas especializadas ha alcanzado, durante 2014, la máxima intensidad conocida hasta la fecha y ha supuesto, sin duda, la mayor amenaza para la ciberseguridad de los intereses nacionales. Se ha producido un incremento del número de casos registrados y de la complejidad e impacto de sus acciones, lo que ha provocado la necesidad de potenciar las capacidades de detección, análisis y respuesta de los servicios públicos competentes en todo el mundo, muy especialmente de los Servicios de Inteligencia[39].

Este ciberespionaje ha fundamentado sus acciones en el uso de técnicas APT (Advanced Persistent Threat), dirigiéndose contra distintos objetivos que, en el caso de España, se han centrado en determinados departamentos de las administraciones públicas españolas, la industria de la Defensa, aeroespacial, energética, farmacéutica, química, TIC, así como los dispositivos móviles del personal directivo de estos sectores. De hecho, este tipo de ataque está detrás de los incidentes con mayor peligrosidad de los gestionados por el CCN-CERT[40]. Además, los Estados también pueden desarrollar sus ataques contratando servicios de otros actores (y operando, en consecuencia, bajo otra bandera) o haciéndose pasar por movimientos hacktivistas[41].

Las autoridades de los Países Bajos también comparten que la mayor amenaza es el espionaje digital, realizado por Estados - amenaza a la que añaden al mismo nivel las

[39] *Ibídem*, p.5.

[40] *Ibídem*, p.5.

[41] *Ibídem*, p.5. No se menciona el origen concreto de este tipo de amenazas, apuntando que el Informe CCN-CERT IA-10/15 de Difusión Limitada recoge un resumen de las principales campañas de ciberspionaje.

acciones realizadas por criminales profesionales, que utilizan diversas formas de delincuencia cibernética - señalando que la amenaza del ciberespionaje por actores estatales se mantienen en los más altos niveles, de tal forma que el número de casos de ciberespionaje ha aumentado, al igual que su complejidad e impacto. Casi todos los servicios de inteligencia exterior ha invertido en capacidades digitales en los últimos años. Por lo tanto, el ciberespionaje ya no está reservado para los grandes y sofisticados servicios de inteligencia[42].

Además, aunque todavía existen escasos precedentes, el impacto potencial de las capacidades ofensivas para realizar operaciones, en ocasiones con carácter militar es elevado, y varios países han desarrollado estas capacidades ofensivas cibernéticas en los últimos años[43].

El terrorismo

El citado informe "Ciberamenazas 2014. Tendencias 2015" señala que, durante 2014, la amenaza de ciberataques provenientes de grupos terroristas no ha sufrido grandes alteraciones respecto de años anteriores. los grupos terroristas todavía no han alcanzado las habilidades precisas o no han tenido acceso a los medios para desarrollar ataques complejos. En todo caso, grupos yihadistas han ejecutado ciberataques a pequeña escala (esencialmente, desfiguraciones de páginas web y ataques DDoS) en diferentes lugares, generalmente en respuesta a pretendidas hostilidades contra intereses islámicos. Más frecuente es la utilización de Internet con fines de financiación, coordinación, propaganda, reclutamiento y radicalización. Sea como fuere, el conocimiento que vienen adquiriendo los grupos terroristas podría tener en el futuro enorme importancia, razón por la cual es necesario adoptar una actitud de permanente vigilancia sobre tales extremos[44].

---

[42] Centro Nacional de Ciberseguridad de los Países Bajos: *Cyber Security Assessment Netherlands 4*, opus citada, p. 7.

[43] *Ibídem*, p. 10.

[44] CCN-CERT: *Ciberamenazas 2014. Tendencias 2015*, *Resumen Ejecutivo*, IA-09/15, Madrid, marzo de 2015, p. 7. https://www.ccn-cert.cni.es/publico/dmpublidocuments/IE-Ciberamenazas2014-Tendencias-2015.pdf consulta: 5 de septiembre de 2015.

La profesionalización de la ciberdelincuencia

El año 2014 ha demostrado que la delincuencia en el ciberespacio se está organizando de manera más profesional, usando Internet para la perpetración de múltiples tipos de delitos y con el objetivo final del beneficio económico. Algunas de sus formas de actuación más destacadas son[45]:

• Ciberataques del tipo denegación de servicio distribuido (DDoS) o introducción de código dañino en los sistemas de información de las víctimas, como forma de chantaje. El ransomware[46] (más innovador y agresivo durante 2014 que nunca) y, en concreto, la aparición del llamado cryptoware, ha ido en aumento y sofisticación en los medios de pago de los rescates (a través de tickets o de moneda digital, como el Bitcoin).

El CCN-CERT ha detectado más de 200 incidentes de este tipo en las Administraciones Públicas.

• Crimen como Servicio (Crime-as-a-Service) en los que terceras partes desarrollan los ciberataques. Este modelo ha crecido en tamaño, complejidad y profesionalidad. Se ha observado también que los precios para el despliegue de botnets[47] y DDoS están disminuyendo gracias a la aparición de otras opciones. En contraposición a lo anterior, el precio de vulnerabilidades nuevas ha crecido significativamente.

• Comercio de servicios o de información robada mediante botnets o código dañino.

• Uso del ciberespacio para desarrollar otras formas de delito al descubrirse la contratación de servicios de determinados hackers por parte de organizaciones del narcotráfico.

---

[45] *Ibídem*, pp-5-6.

[46] El ransomware consiste en el secuestro del ordenador y, en consecuencia la imposibilidad de utilizarlo, y el cryptoware en una derivación de esta modalidad de secuestro que implica el cifrado de los archivos. Ambos ofrecen la promesa de liberar el ordenador tras el pago de una cantidad de dinero por el rescate.

[47] Una botnet es una red de ordenadores infectados que se emplean para actividades ilegales, por ejemplo para lanzar ataques de denegación de servicio distribuido (DDoS) contra un sistema concreto.

Cibervándalos y script kiddies

Se denominan cibervándalos a aquellos individuos que, poseyendo significativos conocimientos técnicos, llevan a cabo sus acciones con el único motivo de demostrar públicamente que son capaces de hacerlo. Por su parte, los denominados script kiddies son aquellos que, con conocimientos limitados y haciendo uso de herramientas construidas por terceros, perpetran sus acciones a modo de desafío, sin ser -en muchas ocasiones- plenamente conscientes de sus consecuencias. En 2014, las acciones imputables a ambos tipos de ciberdelincuentes no han mostrado significativos cambios respecto de años anteriores[48].

Hacktivistas

Se llaman hacktivistas a las personas o grupos, más o menos organizados, cuyas prácticas persiguen el control de redes o sistemas para promover su causa o defender sus posicionamientos políticos o sociales, basados en motivos ideológicos. En los últimos años sus ciberataques (desfiguración de páginas web, ataques DDoS, etc.) pretendían ser respuesta contra determinadas medidas adoptadas por distintos gobiernos. Sus conocimientos y capacidades varían mucho de un grupo a otro. En el plano internacional han destacado los focos hacktivistas paralelos a conflictos sociales o políticos (Israel, Ucrania, Hong Kong, Turquía, Pakistán), así como la actividad individual de varias entidades hacktivistas como el "Syrian Electronic Army", "Anonymous Italia" o "Lizard Squad"[49].

Una de las características más significativas de este tipo de ataques es la dificultad de determinar su autoría concreta que, en muchas ocasiones, se atribuyen simultáneamente grupos distintos. En 2014 ha decaído la presencia hacktivista de entidades locales en España, manteniéndose 'La 9ª Compañía' como único referente operativo. En cambio, se ha observado un incremento leve con respecto al año anterior respecto a la actuación de entidades hacktvistas marroquíes contra objetivos web localizados en España. En Iberoamérica el hacktivismo se ha mantenido estable, con

[48] CCN-CERT: *Ciberamenazas 2014. Tendencias 2015*, *Resumen Ejecutivo*, *opus citada,* pp. 7-8.
[49] *Ibídem,* p. 6.

descensos respecto al año previo en México y Colombia, focos intensos de actividad irregular en Brasil, y emergencia de identidades hacktivistas que buscan impactar sobre objetivos gubernamentales de alto valor en Perú, Chile y, en menor medida, Bolivia[50].

En conjunto se ha observado un aplanamiento de la actividad de 'Anonymous' principalmente con respecto a 2012 y una proliferación de células hacktivistas que operan con distintas narrativas en diversos países con una marcada orientación hacia la producción de ciberataques por deface, con inyección de elaboradas composiciones gráficas en los sitios webs de los objetivos atacados. El ataque por defacement se ha contado por miles contra sitios web de bajo perfil y alta vulnerabilidad en operaciones como las distintas variantes de la #OpIsrael[51].

En general, cuando existen grupos organizados, los conocimientos y habilidades suelen compartirse usando foros específicos, abiertos a las aportaciones de todos; foros que suelen utilizar, asimismo, para exponer públicamente sus conocimientos cuando lo que se persigue es desarrollar una campaña de ataque contra gobiernos o instituciones concretos.

Actores internos

Se denominan actores internos o "insiders" a aquellas personas que tienen o han tenido algún tipo de relación con una organización, incluyendo exempleados, personal temporal o proveedores. Pueden constituir una de las mayores amenazas y su motivación suele ser siempre similar: venganza, motivos financieros o políticos, etc. Además, es preciso tener en cuenta que estos actores internos pueden ser empleados por otros actores agentes de la amenaza, especialmente por Estados y empresas dedicados al ciberespionaje, para la infección preliminar de la red objetivo o para la exfiltración de información de la misma. Este comportamiento no exige necesariamente amplios conocimientos técnicos, la conexión a un ordenador de la

[50] CCN-CERT: *Ciberamenazas 2014. Tendencias 2015*, p. 39.

[51] *Ibídem,* p. 40.

organización de una simple memoria USB conteniendo código dañino puede ser suficiente[52].

Ciberinvestigadores

Se denominan ciberinvestigadores a aquellas personas que persiguen el descubrimiento de las vulnerabilidades que pueden afectar a los sistemas (hardware o software). La publicación de los resultados de sus investigaciones –al objeto de sensibilizar sobre las necesarias medidas de seguridad, por ejemplo- puede suponer que sus revelaciones se usen por terceros malintencionados. Las conferencias internacionales de hackers suelen ofrecer claros ejemplos de revelaciones de vulnerabilidades inéditas hasta entonces. Como es lógico suponer, la exposición pública de las vulnerabilidades de los sistemas, en tanto no son adecuadamente resueltas, ponen en riesgo a los usuarios (personas y organizaciones) de tales sistemas vulnerables[53].

Como quiera que muchos ciberinvestigadores han podido ser acusados de la comisión de ciberataques, diversos actores públicos y privados vienen aplicado desde 2013 la directriz "Divulgación Responsable"[54], que intenta evitar la adopción de acciones legales en contra de los ciberinvestigadores, si estos se adhieren a la citada norma.

Las organizaciones privadas

Las motivaciones para perpetrar ciberataques también se encuentran en las organizaciones privadas cuando, movidas por el interés económico que supone

[52] CCN-CERT: *Ciberamenazas 2014. Tendencias 2015*, *Resumen Ejecutivo*, *opus citada,* p. 8.

[53] CCN-CERT: *Ciberamenazas 2014. Tendencias 2015, opus citada,* p. 31.

[54] La “Divulgación Responsable” (o Responsible Disclosure) es un término que hace referencia a un modelo de revelación de vulnerabilidades en los sistemas de información en el que, generalmente, los actores implicados deciden mantener en secreto tal vulnerabilidad en tanto no esté disponible el correspondiente parche de seguridad. Ciertas compañías independientes ostienen este modelo, contribuyendo económicamente cuando alguien descubre bugs en sus productos, entre ellas: Facebook, Google, Mozilla y Barracuda Networks.

poseer los conocimientos que tiene la competencia, desarrollan acciones de ciberespionaje industrial.

Por otro lado, también se han dado casos de empresas que, como consecuencia de las aplicaciones que venden o los servicios que prestan, recaban datos –en muchos casos, de carácter personal- de sus clientes, que pueden utilizar para propósitos comerciales no legítimos o que, incluso, pueden llegar a vender a terceros, sin solicitar el consentimiento del cliente o le haya sido requerido de manera engañosa o poco informada. Esta problemática adquiere especial relevancia cuando se trata de Servicios Cloud en los que el usuario depende totalmente del comportamiento del proveedor y las medidas de seguridad adoptadas para garantizar el adecuado tratamiento de sus datos[55].

Los analistas que tratan de determinar el origen de un ciberataque encuentran a menudo obstaculizada esta labor por el uso de botnets, o redes de ordenadores infectados que son utilizados como robots. En primer lugar, los ordenadores infectados a través de una botnet pueden estar ubicados en diferentes países de todo el mundo, limitando la capacidad de definir el país de origen del ciberataque. En segundo lugar, la identidad del control de la botnet también puede ser ensombrecida por la utilización de software peer-to-peer o red entre pares (P2P, por sus siglas en inglés). Además, la dirección facilitada por un proveedor de Internet (IP) que podría facilitar la ubicación de un equipo que lanzó un ataque puede ser falsificada (lo que se conoce como "spoofing"), e incluso con una dirección IP válida puede ser prácticamente imposible verificar el actor que se encontraba tras un sistema en el momento en que se produjo el ataque. De otra parte, en las botnets se encuentran equipos que han sido infectados sin el conocimiento del usuario. En este escenario, A nivel de Estado-nación, es plausible un cierto nivel de ausencia de responsabilidad, dada la proliferación de organizaciones de hackers y las herramientas cibernéticas a su disposición, lo que

[55] CCN-CERT: *Ciberamenazas 2014. Tendencias 2015, opus citada,* pp. 31-32.

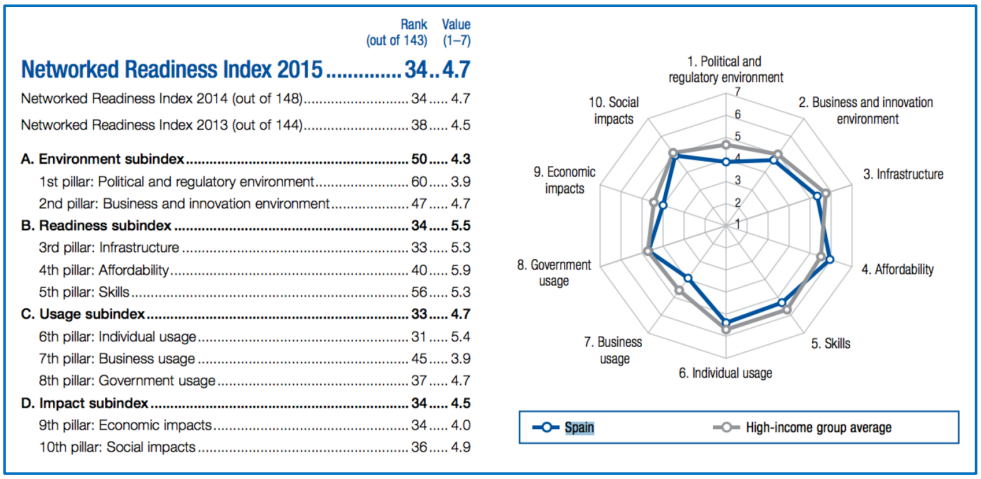
facilita que los Estados pueden reclamar fácilmente la falta de responsabilidad ante ataques que parecen provenir del interior de sus fronteras estatales[56].

1.3. Los ciberincidentes en España

Un documento que se estima relevante, para situar a España en el contexto de la comunidad internacional en el ámbito de las tecnologías de la información y comunicaciones (TIC), es el "Informe Global de Tecnología 2015". Desde 2001, este informe publicado por el Foro Económico Mundial, en colaboración con la Universidad de Cornell y el INSEAD, ha medido diferentes parámetros de 143 países[57].

En este informe se realiza un estudio comparativo de diferentes factores, elaborando una clasificación que en 2015 coloca a España en el puesto número 34 de este estudio, que valora la penetración en la sociedad de las tecnologías de la información y comunicaciones, como se refleja en el siguiente gráfico.

Figura 5: Informe sobre España TIC 2015.



	Rank (out of 143)	Value (1–7)
Networked Readiness Index 2015	**34**	**4.7**
Networked Readiness Index 2014 (out of 148)	34	4.7
Networked Readiness Index 2013 (out of 144)	38	4.5
A. Environment subindex	**50**	**4.3**
1st pillar: Political and regulatory environment	60	3.9
2nd pillar: Business and innovation environment	47	4.7
B. Readiness subindex	**34**	**5.5**
3rd pillar: Infrastructure	33	5.3
4th pillar: Affordability	40	5.9
5th pillar: Skills	56	5.3
C. Usage subindex	**33**	**4.7**
6th pillar: Individual usage	31	5.4
7th pillar: Business usage	45	3.9
8th pillar: Government usage	37	4.7
D. Impact subindex	**34**	**4.5**
9th pillar: Economic impacts	34	4.0
10th pillar: Social impacts	36	4.9

Fuente: DUTTA Soumitra, GEIGER Thierry y LANVIN Bruno[58].

[56] THEOHARY, Catherine A. y HARRINGTON, Anne I: *Cyber Operations in DOD Policy and Plans: Issues for Congress,* Congressional Research Service, Washington D.C., 5 de enero de 2015. http://fas.org/sgp/crs/natsec/R43848.pdf consulta: 27 de septiembre de 2015.

[57] DUTTA Soumitra, GEIGER Thierry y LANVIN Bruno, Eds.: *The Global Information Technology Report 2015,* World Economic Forum & INSEAD, Ginebra, 2015. http://www3.weforum.org/docs/WEF_Global_IT_Report_2015.pdf consulta: 12 de septiembre de 2015.

[58] *Ibídem*, p. 236.

De los datos obtenidos en el estudio, se destaca que Europa es el área donde se encuentran los países mejores conectados y la mayor parte de las economías impulsadas por la innovación. En particular, los países nórdicos, Finlandia (2), Suecia (3), Noruega (5), Dinamarca (15) e Islandia (19) mantienen sus niveles, que les han situado entre los 20 primeros desde 2012. El rendimiento del grupo de países de Europa occidental también es significativo: Países Bajos (4), Suiza (6), Reino Unido (8), y Luxemburgo (9) se encuentran entre los 10 primeros. Irlanda (25) se ha mantenido estable desde 2012, y Francia (26) - que ha perdido tres lugares desde 2012 -, cierra el grupo en la subregión. En Europa meridional, Portugal (28, con mejora de 5), Italia (55, con mejora de 3), y Grecia (66, con mejora de 8) incrementan significativamente sus posiciones desde 2014, mientras que Malta (29), España (34), y Chipre (36) continúan en los márgenes de 2014. Estas tendencias, principalmente positivas, contribuyen a reducir la brecha del sur de Europa con el resto de la región, que se había estado ampliando desde 2012. Gracias a los buenos resultados de Estonia (22) y el aumento constante de Letonia (33, mejorando 6 puestos), prácticamente alcanzando a Lituania (31), los países bálticos han continuado reduciendo la brecha con los países nórdicos y alejándose de lo que antes era un grupo bastante homogéneo de los países europeos que se han unido a la Unión Europea desde 2004: Eslovenia (37, desciende un puesto), la República Checa (43, desciende un puesto), Hungría (53, desciende 6 puestos), Croacia (54, desciende 8 puestos), y la República Eslovaca (59, sin cambios). Mientras tanto Polonia ha avanzado 4 posiciones colocándose entre los 50 primeros, mientras Rumania avanza 12 posiciones para colocarse en el puesto 62, por delante de Bulgaria, que continúa

en el lugar 73[59]. Microsoft, en su informe de inteligencia de seguridad global[60] ofrece datos sobre la situación en España[61].

En relación a las tendencias de las tasas de encuentro[62] y de infección, Microsoft señala que en el cuarto trimestre de 2014 el 16,9% por ciento de los ordenadores en España tuvo un encuentro con malware, en comparación a la tasa de encuentro de todo el mundo en este periodo, que fue del 15,9 por ciento. Además, la herramienta de eliminación de software malicioso de Microsoft, detectó y eliminó el malware de 5,3 de cada 1.000 ordenadores únicos escaneados en España en el cuarto trimestre de 2104 (una puntuación CCM[63] de 5.3, comparada con la medición CCM mundial de 5,9).

La siguiente figura muestra las tendencias de las tasas de encuentro y de infección para España en los últimos cuatro trimestres, en comparación con el mundo en su conjunto.

[59] *Ibídem*, p. 14 del sumario ejecutivo.

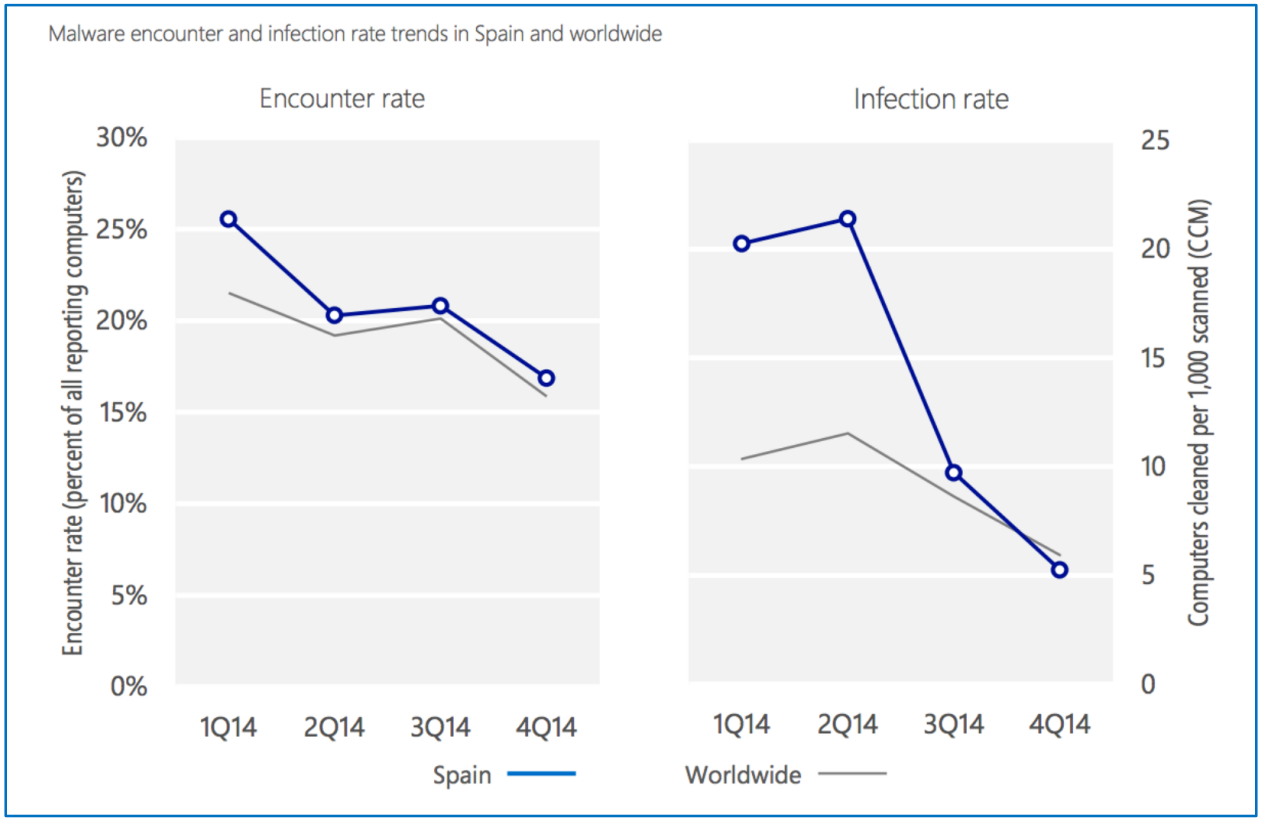
[60] Microsoft Corporation: *Microsoft Security Intelligence Report, Volume 18, julio a diciembre de 2014, España*, Redmond, WA, 2015. http://www.microsoft.com/security/sir/threat/ consulta: 12 de septiembre de 2015.

[61] *Ibídem*, p. 3. Microsoft Corporation señala que las estadísticas son generadas por los programas de seguridad de Microsoft y servicios que se ejecutan en los ordenadores en España. Se utiliza la geolocalización utilizando la dirección IP para determinar el país o la región.

[62] Tasa de encuentro es el porcentaje de equipos que ejecutan productos de seguridad de Microsoft en tiempo real que reportan un encuentro con malware, independientemente de si produce o no la infección en el equipo.

[63] CCM (Computers cleaned per mille) o número de equipos limpiados por cada mil, es una medición de la tasa de infección de ordenadores únicos que ejecutan la herramienta de eliminación de software malintencionado (MSRT), herramienta distribuida a través de los servicios de actualización de Microsoft que elimina más de 200 amenazas de alta prevalencia o graves en ordenadores.

Figura 6: Tendencias de las tasas de encuentro y de infección para España en 2014

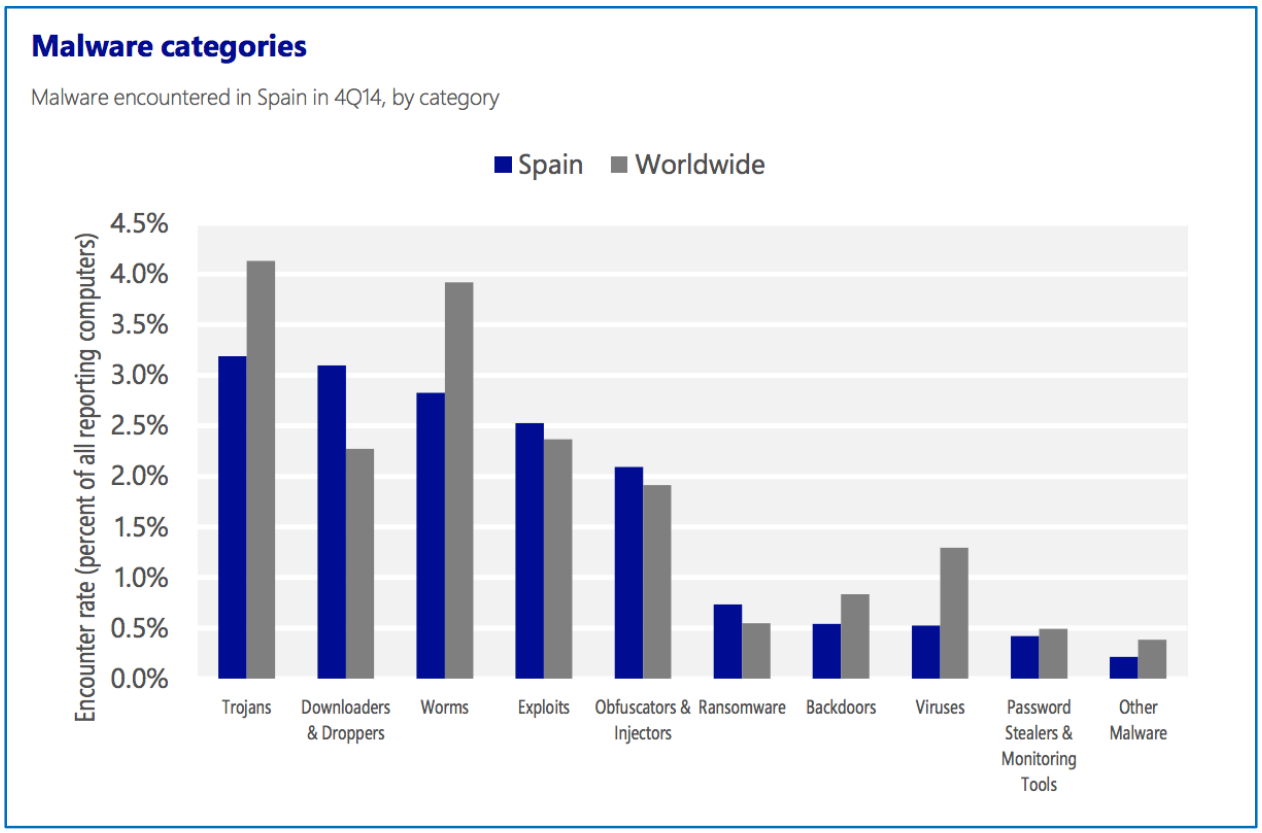


Fuente: Microsoft Corporation: *Microsoft Security Intelligence Report, Volume 18, julio a diciembre de 2014, España,* p. 4.

La categoría de malware más común en España, detectada por Microsoft el cuarto trimestre de 2014, corresponde a los *troyanos*, que fueron encontrados en un 3,2 por ciento de todos los ordenadores, por debajo del 9,4 por ciento contabilizado en el tercer trimestre de 2014. La segunda categoría de malware más común en España en el fue la correspondiente a los *descargadores y cuentagotas* (downloaders & droppers) con un 3,1 por ciento de los ordenadores, frente al 4,4 por ciento en el anterior trimestre. La tercera categoría de malware más común en España el cuarto trimestre de 2014 fue la de los gusanos, que se encontraron en un 2,8 por ciento los ordenadores allí, frente a los 2,3 por ciento del anterior trimestre[64].

[64] Microsoft Corporation: *Microsoft Security Intelligence Report, Volume 18, julio a diciembre de 2014, España, opus citada,* p. 5.

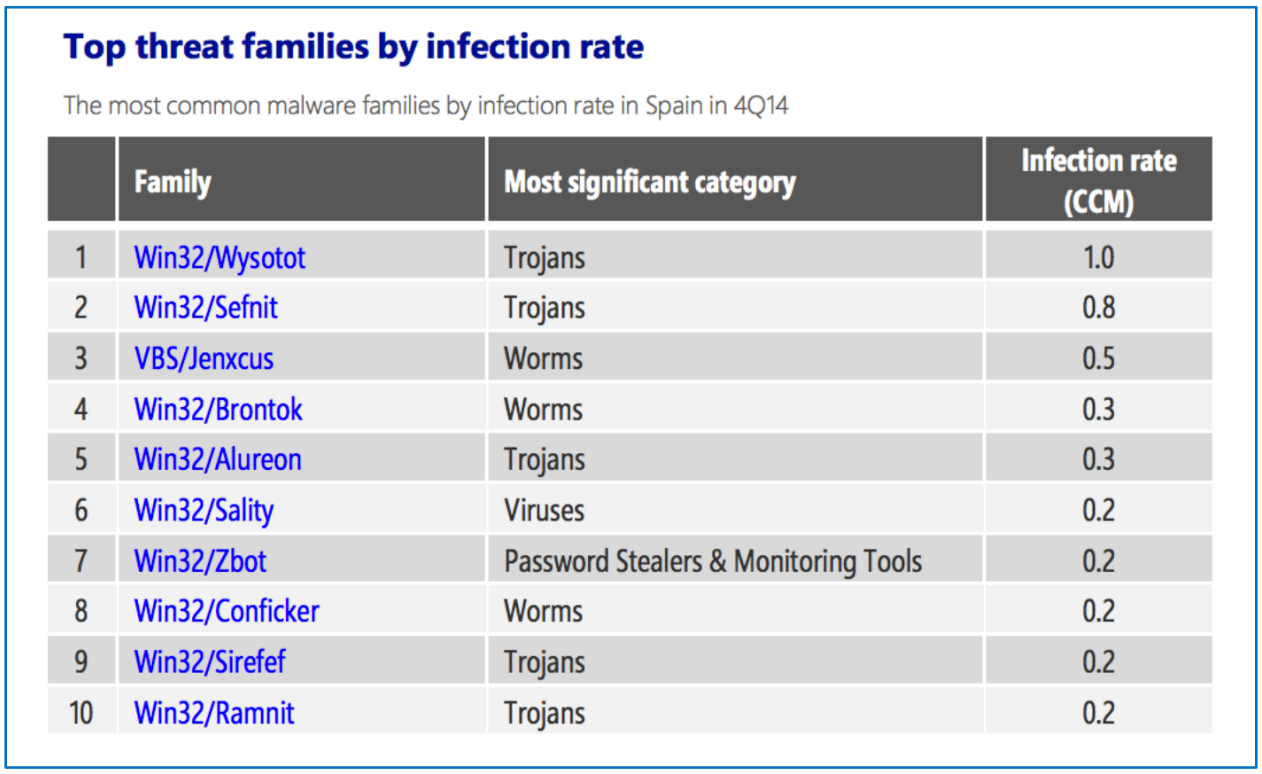
Figura 7: Categorías de malware en España detectadas el cuarto trimestre de 2014



Fuente: Microsoft Corporation: *Microsoft Security Intelligence Report, Volume 18, julio a diciembre de 2014, España,* p. 5.

En cuanto al malware que infectó los equipos en España el cuarto trimestre de 2014, Microsoft ofrece los datos reflejados en la tabla que se muestra a continuación.

Figura 8: Familias de malware por tasa de infección en España el cuarto trimestre de 2014



Top threat families by infection rate

The most common malware families by infection rate in Spain in 4Q14

	Family	Most significant category	Infection rate (CCM)
1	Win32/Wysotot	Trojans	1.0
2	Win32/Sefnit	Trojans	0.8
3	VBS/Jenxcus	Worms	0.5
4	Win32/Brontok	Worms	0.3
5	Win32/Alureon	Trojans	0.3
6	Win32/Sality	Viruses	0.2
7	Win32/Zbot	Password Stealers & Monitoring Tools	0.2
8	Win32/Conficker	Worms	0.2
9	Win32/Sirefef	Trojans	0.2
10	Win32/Ramnit	Trojans	0.2

Fuente: Microsoft Corporation: *Microsoft Security Intelligence Report, Volume 18, julio a diciembre de 2014, España,* p. 9.

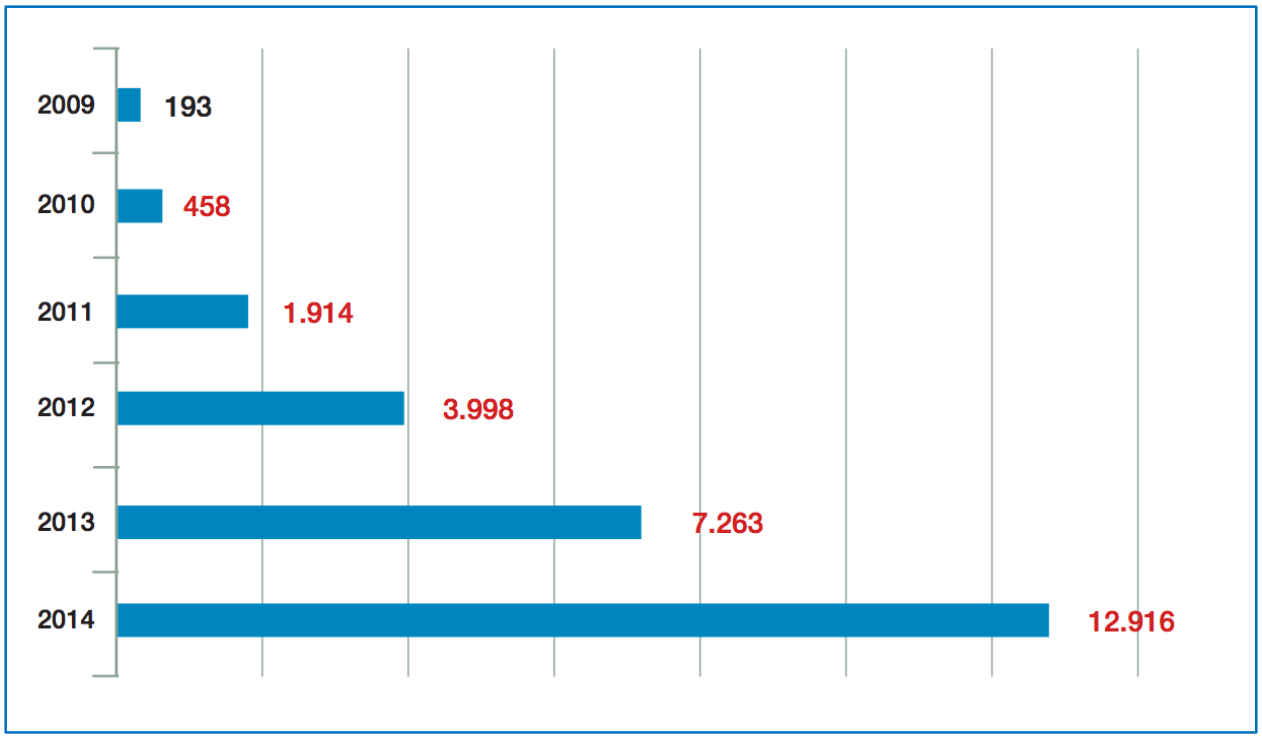
Figura 9: Las cuatro principales familias de malware que infectaron los ordenadores en España en el cuarto trimestre de 2014

Win32 / Wysotot puede modificar la página de inicio del navegador web del usuario, y puede descargar e instalar otros archivos al ordenador. Se instala por publicidad gratuita de software o juegos.
Win32 / Sefnit es una familia de troyanos que puede permitir el acceso de puerta trasera, descargar archivos, y el uso del ordenador y de la conexión de Internet para el fraude de clics para generar ingresos en anunciantes. Algunas variantes pueden rastrear los navegadores web y secuestrar los resultados de la búsqueda.
VBS / Jenxcus es un gusano que da a un atacante el control del equipo. Se transmite por unidades extraíbles infectadas, como unidades flash al puerto USB. También puede ser descargado dentro de un archivo torrente.
Win32 / Brontok es un gusano de correo electrónico que se propaga mediante el envío de copias de sí mismo como archivo adjunto a direcciones recopiladas en el ordenador. Brontok puede desactivar el software de seguridad, y puede conducir ataques de denegación de servicio contra ciertos sitios web.

Fuente: Microsoft Corporation: *Microsoft Security Intelligence Report, Volume 18, julio a diciembre de 2014, España,* p. 9.

Atendiendo a datos suministrados por el CCN-CERT, 2014 ha sido un año especialmente significativo en materia de ciberamenazas. La figura siguiente muestra una comparativa del número de incidentes registrados en los últimos años, y detectados por los Sistemas de Alerta Temprana desplegados por el CCN-CERT en los órganos y organismos de las Administraciones Públicas españolas, así como en aquellas empresas nacionales de interés estratégico adheridas al servicio. Como puede observarse, en 2014 ha crecido significativamente el número de incidentes gestionados[65].

Figura 10: Ciberincidentes en España 2009 – 2014



Fuente: CCN-CERT: *Ciberamenazas 2014. Tendencias 2015*[66].

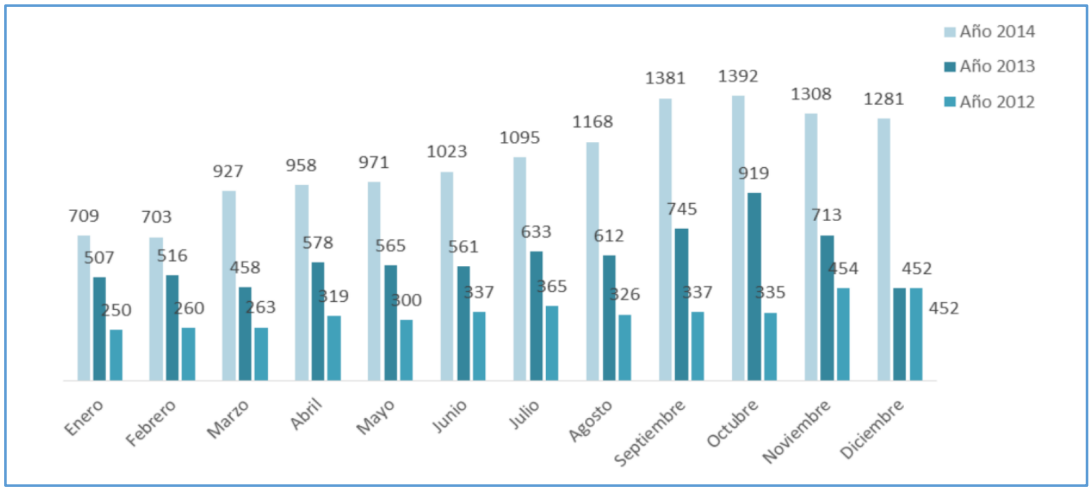
[65] CCN-CERT: *Ciberamenazas 2014. Tendencias 2015, opus citada,* pp. 31-32.

[66] CCN-CERT: *Ciberamenazas 2014. Tendencias 2015*, *Resumen Ejecutivo*, *opus citada,* p. 22.

El CERT Gubernamental Nacional gestionó durante 2014 un total de 12.916 incidentes detectados en las Administraciones Públicas165 y en empresas de interés estratégico. Esta cifra representa un incremento del 78% con respecto al año 2013 en el que se gestionaron 7.259 incidentes. De los incidentes de este 2014, el 10,8% (1.404) fueron catalogados por el equipo de expertos del CERT Gubernamental Nacional con un nivel de riesgo entre muy alto y crítico; es decir, se tiene constancia de que el ataque afectó a los sistemas de la organización y a su información sensible. El CCN-CERT ha constatado, además, un incremento en la intensidad y sofisticación de dichos ataques, tanto a las Administraciones Públicas como a las empresas y organizaciones de interés estratégico para el país, fundamentalmente de los sectores energético, de defensa, aeroespacial, farmacéutico y químico[67].

El siguiente gráfico recoge un aspecto que muestra la tendencia de incremento de ciberincidentes en 2014, en la que se aprecia un aumento mensual, comparado con los años 2012 y 2013, que no era tan significativo.

Figura 11: Evolución mensual de los ciberincidentes gestionados por el CCN-CERT en el periodo 2012-2014.



Fuente: CCN-CERT: *Ciberamenazas 2014. Tendencias 2015*[68].

[67] CCN-CERT: *Ciberamenazas 2014. Tendencias 2015*, *opus citada,* p. 92.

[68] *Ibídem*.

La Guía CCN-STIC 817 Gestión de Ciberincidentes[69], tipifica los incidentes de seguridad, atendiendo a su peligrosidad, en cinco niveles: Bajo, Medio, Alto, Muy Alto y Crítico. La tabla siguiente muestra el nivel de peligrosidad de los ciberincidentes, atendiendo a la repercusión que la materialización de la amenaza de que se trate podría tener en los sistemas de información de las entidades.

Figura 12: Criterios de determinación del nivel de peligrosidad de los ciberincidentes

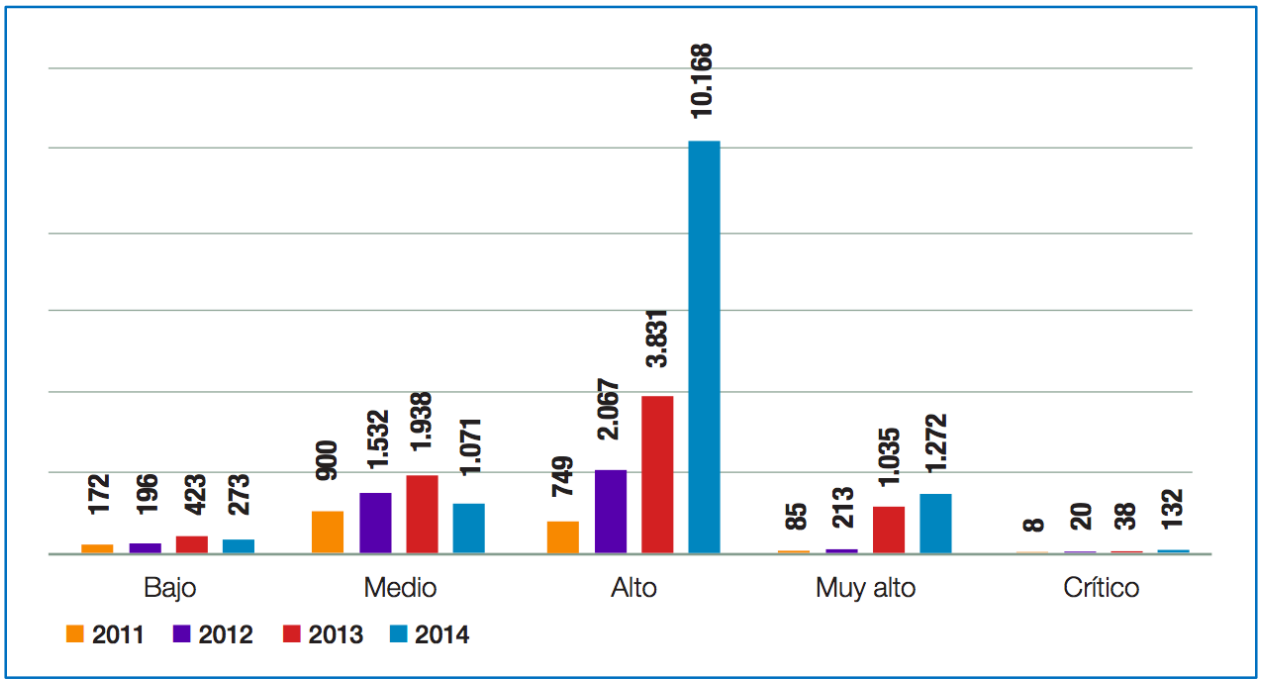
CRITERIOS NIVEL DE PELIGROSIDAD DE LOS CIBERINCIDENTES			
NIVEL	**AMENAZAS SUBYACENTES MÁS HABITUALES**	**VECTOR DE ATAQUE**	**CARACTERÍSTICAS POTENCIALES DEL CIBERINCIDENTE**
CRÍTICO	Ciberespionaje	APTs, campañas de malware, interrupción de servicios, compromiso de sistemas de control ndustrial, incidentes especiales, etc.	Capacidad para exfiltrar información muy valiosa, en cantidad y en poco tiempo / Capacidad para tomar el control de los sistemas sensibles, en cantidad y en poco tiempo
MUY ALTO	Interrupción de los Servicios IT / Exfiltración de datos /Compromiso de los servicios	Códigos dañinos confirmados de Alto Impacto (RAT, troyanos enviando datos, rootkit, etc.) / Ataques externos con éxito	Capacidad para exfiltrar información valiosa, en cantidad apreciable / Capacidad para tomar el control de los sistemas sensibles considerable
ALTO	Toma de control de los sistemas / Robo y publicación o venta de información sustraída / Ciberdelito / Suplantación	Códigos dañinos Medio Impacto (virus, gusanos, troyanos) / Ataques externos compromiso de servicios no esenciales (DoS / DDoS)./ Tráfico DNS con dominios APTs o campañas malware / Accesos no autorizados / Suplantación / Sabotaje / Cross-Site Scripting / Inyección SQL / Spear phising / pharming	Capacidad para exfiltrar información valiosa / Capacidad para tomar el control de ciertos sistemas
MEDIO	Logro o incremento De capacidades ofensivas / Desfiguración de páginas web / Manipulación de información	Descargas de archivos sospechosos / Contactos con dominios o direcciones IP sospechosas / Escáneres de vulnerabilidades / Códigos dañinos de Bajo Impacto (adware, spyware, etc.) / Sniffing / Ingeniería social	Capacidad para exfiltrar un volumen apreciable de información / Capacidad para tomar el control de de algún sistema
BAJO	Ataques a la imagen/ Errores y fallos	Políticas / Spam sin adjuntos / Software desactualizado / Acoso / coacción / comentarios ofensivos / Error humano / Fallo HW-SW	Escasa capacidad para exfiltrar volumen de información /Nula o escasa capacidad para tomar el control de sistemas

[69] CCN-CERT: *Guía de seguridad de las TIC, CCN-STIC-817, Esquema Nacional de Seguridad, Gestión de Ciberincidentes,* mayo 2015. https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/988-ccn-stic-817-gestion-de-ciberincidentes/file.html consulta: 13 de septiembre de 2015.

Fuente: CCN-CERT: *Guía de seguridad de las TIC, CCN-STIC-817, Esquema Nacional de Seguridad, Gestión de Ciberincidentes,* p. 18.

Siguiendo estos criterios de determinación del nivel de peligrosidad de los ciberincidentes, la siguiente figura refleja la evolución de los ciberincidentes en España entre 2011 y 2014, desglosados por niveles de peligrosidad.

Figura 13: Evolución de los ciberincidentes en España, gestionados por el CCN-CERT en el periodo 2011 – 2014, con expresión del nivel de peligrosidad



Fuente: CCN-CERT: *Ciberamenazas 2014. Tendencias 2015*[70].

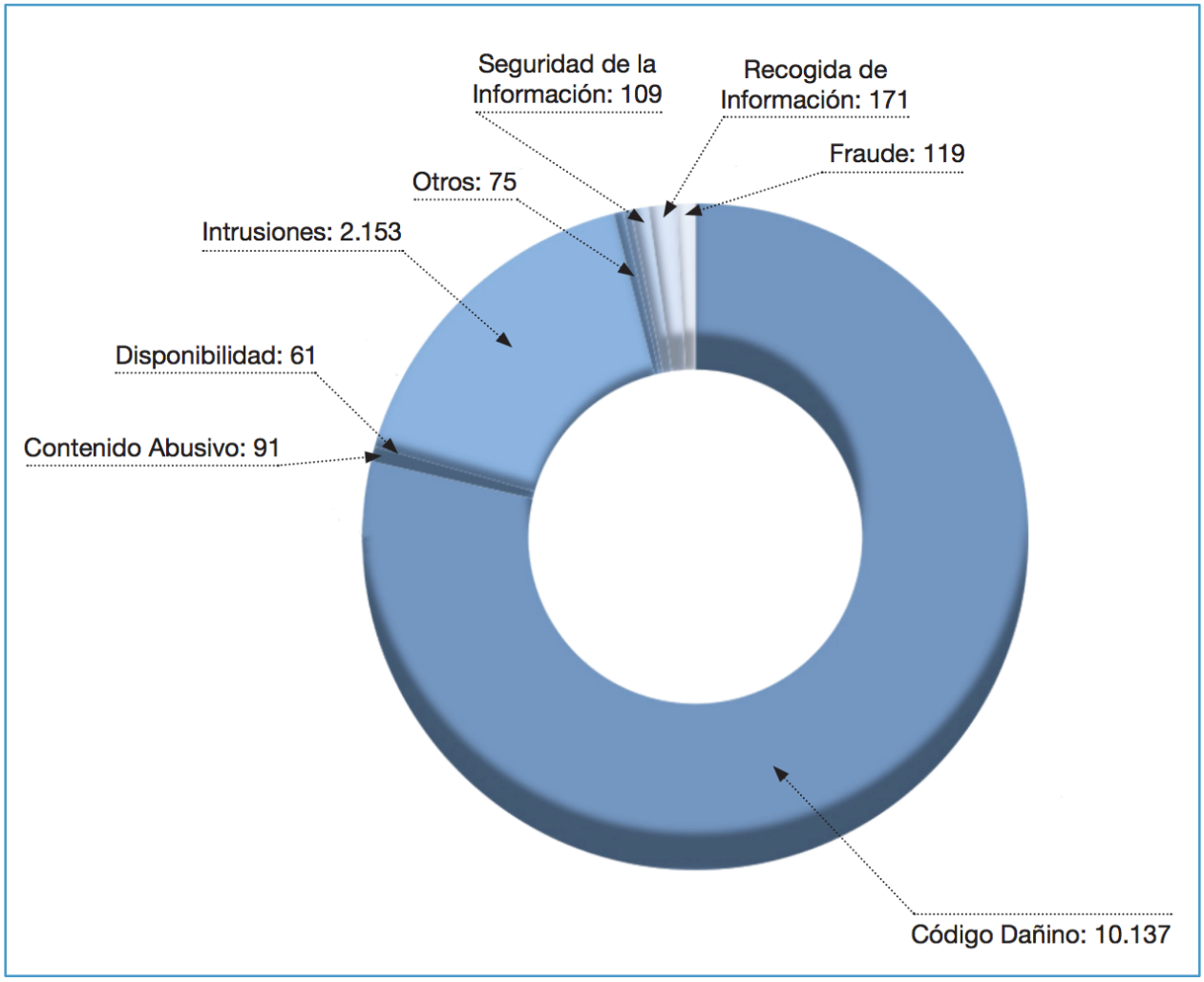
Obsérvese que el número de incidentes tipificados como “Muy alto” y “Crítico” -aquellos que pueden causar degradación de los servicios para un gran número de usuarios, o implicar una grave violación de la seguridad de la información, o pueden afectar a la integridad física de las personas, causar importantes pérdidas económicas, ocasionar daños irreversibles a los recursos de la organización, o se puede incurrir en

[70] CCN-CERT: *Ciberamenazas 2014. Tendencias 2015*, *Resumen Ejecutivo*, *opus citada,* p. 22.

delitos y/o sanciones reglamentarias u ocasionar un daño muy grave en la imagen de la organización- han representado el 10% de todos los ataques gestionados[71].

En relación con la tipología de los ataques, la siguiente figura muestra las principales subcategorías de incidentes gestionados por el CCN-CERT en 2014, donde destacan los ataques utilizando código dañino, seguidos por las intrusiones en los sistemas.

Figura 14: Principales subcategorías de incidentes gestionados por el CCN-CERT en 2014.



Fuente: CCN-CERT: *Ciberamenazas 2014. Tendencias 2015*[72].

[71] CCN-CERT: *Ciberamenazas 2014. Tendencias 2015*, *opus citada,* p. 80.

[72] CCN-CERT: *Ciberamenazas 2014. Tendencias 2015*, *Resumen Ejecutivo*, *opus citada,* p. 23.

1.4. La respuesta a los ciberincidentes

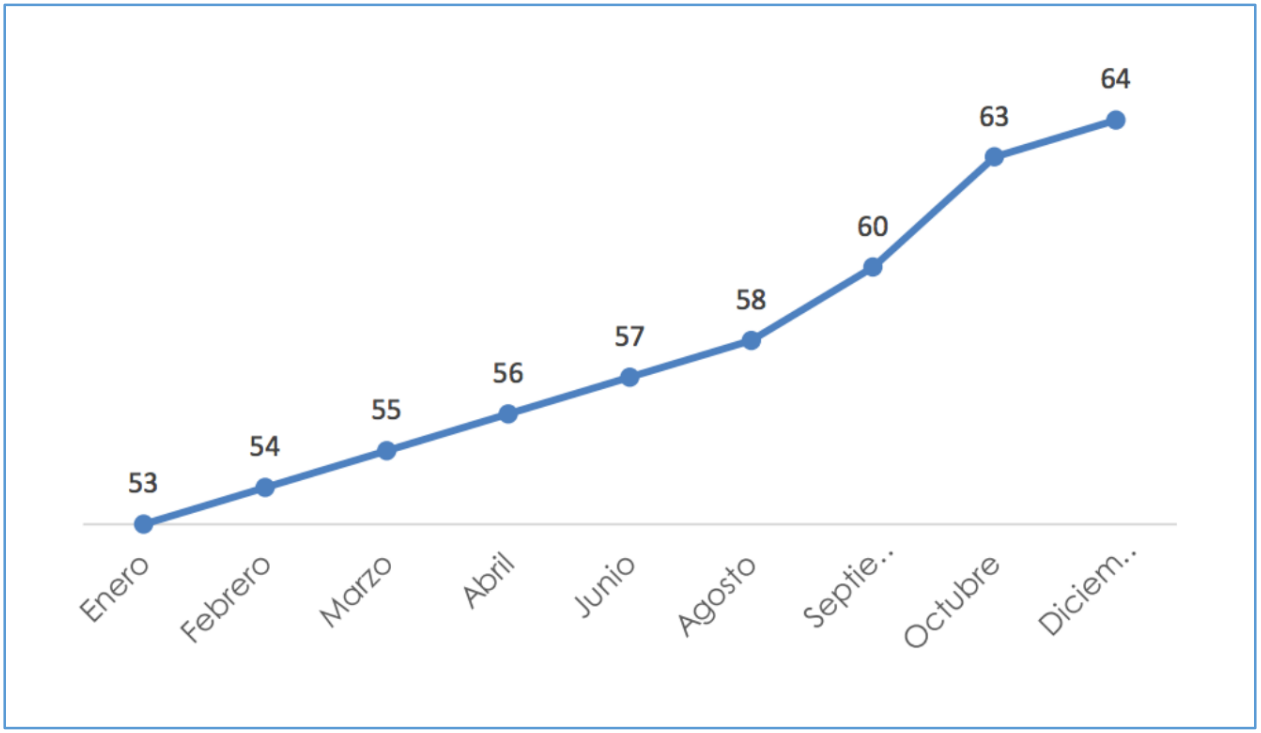
El CCN-CERT señala que para los organismos públicos, el beneficio más significativo de poseer una adecuada capacidad de respuesta a ciberincidentes es abordar su gestión de forma sistemática (es decir, siguiendo una metodología consistente y consolidada), lo que facilita la adopción de las medidas adecuadas. Así, una correcta Capacidad de Respuesta a Ciberincidentes ayuda a los equipos de seguridad responsables a minimizar la pérdida o exfiltración de información o la interrupción de los servicios. Otro de sus beneficios es la posibilidad de utilizar la información obtenida durante la gestión del ciberincidente para preparar mejor la respuesta a incidentes de seguridad futuros y, en su consecuencia, proporcionar una mayor y mejor protección a los sistemas[73].

Además de pretender una mejor prestación de servicios de Administración Electrónica, los órganos y organismos del ámbito de aplicación del ENS deben acomodar su capacidad de respuesta a los ciberincidentes a la normativa legal que resulte de aplicación en cada caso y para cada Administracion territorial o sectorial involucrada. Entre tal regulación cabe destacar la debida observancia a lo dispuesto en la Estrategia de Ciberseguridad Nacional; la Ley 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su normativa de desarrollo; la Ley 11/2007, de 22 de junio, de Acceso de los Ciudadanos a los Servicios Públicos; el Esquema Nacional de Interoperabilidad y su normativa derivada; el Esquema Nacional de Seguridad y su normativa derivada; y la Ley 9/1968, de 5 de abril, sobre Secretos Oficiales, entre otras[74].

[73] CCN-CERT: *Guía de seguridad de las TIC, CCN-STIC-817, Esquema Nacional de Seguridad, Gestión de Ciberincidentes*, *opus citada*, apartado 5.1.2.

[74] *Ibídem*.

Figura 15: Volumen de organizaciones adscritas al Sistema de Alerta Temprana, SAT, de Internet



Fuente: CCN-CERT: Ciberamenazas 2014. Tendencias 2015[75].

1.5. Tendencias

El CCN-CERT destaca las tendencias en relación con los riesgos y amenazas derivados de la utilización del ciberespacio[76]:

Ciberespionaje. Muy probable. El empleo del ciberespacio para la obtención de inteligencia se incrementará por todos los países de nuestro entorno por su eficacia y dificultad de atribución. Debido a la publicación de campañas de ciberespionaje realizada por compañías de seguridad, los países emplearán más recursos en la

[75] CCN-CERT: *Ciberamenazas 2014. Tendencias 2015*, *opus citada,* p. 95.

[76] *Ibídem*, pp. 84-91.

seguridad de sus operaciones aislando infraestructuras y diversificando las Técnicas, Tácticas y Procedimientos (TTP) de ataque.

Los ataques como servicio. Muy probable. A través de grupos con conocimiento y capacidad técnica. Contratar sus servicios y planificar un ataque «a medida», con garantías de éxito. Requerirá ampliar el conocimiento de las redes Deep Web, incrementarse la cooperación incrementarse la cooperación público privada y armonizar la legislación internacional.

Fusión de tácticas, técnicas y procedimientos (TTP) utilizadas por el ciberespionaje y la ciberdelincuencia. Muy probable. Evolución de la actividad cibercriminal a TTP empleados en el ciberespionaje usando herramientas del tipo APT y dirigidas especialmente contra el sector financiero persiguiendo la sustracción de dinero. No es nada nuevo: durante el último año hemos presenciado un aumento de los ataques, sustentados en la acción de código dañino y métodos propios de las APT, cuyo objetivo han sido entidades financieras, persiguiendo la sustracción de dinero, de varias formas: - Control remoto de cajeros automáticos, - Realización de transferencias SWIFT de las cuentas de ciertos clientes, - Manipulación de los sistemas informáticos online para ordenar transferencias ilícitas.

Estabilización de los ataques hacktivistas. Muy probable. A tenor de lo observado en 2014, para 2015 es de esperar un aplanamiento de la actividad de 'Anonymous' y una proliferación de células hacktivistas que operen con distintas narrativas en diversos países con una marcada orientación hacia la producción de ciberataques por desfiguración de paginas web, con inyección de elaboradas composiciones gráficas en los sitios webs de los objetivos atacados.

Herramientas de ataque para dispositivos móviles. Probable. Además de duplicar en 2015 el número de las actuales amenazas de Android, se prevé que el crecimiento de vulnerabilidades en los dispositivos móviles, plataformas y aplicaciones presentará ciertos riesgos de seguridad especialmente graves: los datos almacenados en los dispositivos móviles podrán usarse por los ciberdelincuentes para perpetrar otros

ataques o para su venta en el mercado negro. Como puede observarse en la figura, el volumen acumulado de las amenazas para Android ha ido en aumento desde 2012. Como se ha dicho, es probable que se duplique en 2015. Por otro lado, las vulnerabilidades que hemos visto hasta ahora no sólo residen en los dispositivos , sino también en plataformas y aplicaciones. Alguna amenaza para plataformas -como la vulnerabilidad master key - han permitido a los ciberdelincuentes reemplazar aplicaciones legítimas con versiones falsas o dañinas.

El "secuestro" de organizaciones por ransomware. Probable. Durante 2014 hemos asistido a la "maduración" de los ataques por ransomware, especialmente de su variante más agresiva: el cryptoware. El uso de este tipo de código dañino y el consiguiente lucro obtenido con él han podido dar argumentos a los atacantes para diseñar ataques a mayor escala, todavía más lucrativos: los ataques a grandes empresas o instituciones. Perpetrando un ataque de este tipo, en caso de tener éxito, los agentes de las amenazas lograrían un nivel de compromiso tan grande de los sistemas atacados, que podrían detener la normal actividad de la organización. Esta situación, especialmente más destructiva en las pymes, obligaría presumiblemente a las víctimas a satisfacer el rescate exigido. Obviamente, la publicidad del éxito de un ataque de este tipo alentaría a nuevos atacantes.

Incremento de los ataques contra cajeros automáticos y procedimientos de pago. Probable. Los ataques contra cajeros automáticos perpetrados en 2014 han evidenciado la vulnerabilidad de tales dispositivos, muchos de los cuales siguen ejecutando Windows XP156. Es presumible, por tanto, que 2015 sea testigo de un incremento y evolución tecnológica de los ataques contra estos dispositivos. No es desdeñable, tampoco, la utilización de técnicas APT para, a través de tales equipos, penetrar en la red de la entidad financiera y explotar acciones que persigan mayores objetivos. Este problema puede hacerse extensivo a los ataques dirigidos contra máquinas expendedoras de tickets (muchas de ellas ejecutando también Windows XP) y que, en muchas ocasiones, también aceptan tarjetas de crédito. Presumiblemente, en 2015 asistiremos a nuevas y más sofisticadas acciones tendentes, por ejemplo, a obtener los datos de las tarjetas de crédito utilizadas por los clientes de las máquinas

de ticketing. Además, es de esperar que, en los próximos años, los agentes de las amenazas desarrollen acciones contra sistemas virtuales de pago, atacando los puntos finales (teléfonos móviles, en la mayoría de casos). Este temor puede extenderse al nuevo Apple Pay, que utiliza la tecnología NFC (Near Field Communications) para manejar transacciones de forma inalámbrica. Nos encontramos pues con un mercado maduro para la investigación en seguridad.

Nuevas amenazas a los dispositivos móviles. Probable. Durante el año 2015, y debido a la consolidación (en el caso de Android Wear) y a la comercialización (en el caso de iOS y Apple Watch) de nuevos accesorios para los dispositivos móviles, se incrementarán especialmente los incidentes de seguridad sobre estos complementos o 'wearables' (relojes, pulseras, etc) y sobre los nuevos (y ya existentes) métodos de pago basados en tecnologías inalámbricas, como NFC (Near Field Communications) o monedas virtuales. Pese a que la seguridad de los dispositivos móviles se fortalece con el paso del tiempo, las nuevas funcionalidades que son incorporadas cada año no están exentas de debilidades. En resumen, la tendencia para el año 2015 parece evolucionar hacia escenarios más complejos, avanzados y profesionalizados de ataque, tanto en la investigación y descubrimiento de nuevas vulnerabilidades, como en la explotación de las debilidades existentes en las principales plataformas móviles. Por otro lado, no debe ignorarse la existencia de vulnerabilidades más sencillas de explotar, incluso ya conocidas en otras tecnologías, y que a lo largo del tiempo vuelven a afectar a tecnologías más modernas o de última generación. Asimismo, en 2015 será importante permanecer alerta antes nuevas revelaciones asociadas a la privacidad y seguridad del usuario y a esquemas de espionaje globales por parte de agencias gubernamentales. Desde el punto de vista corporativo, la integración de forma segura de los dispositivos móviles tanto corporativos como personales en las infraestructuras de información de las organizaciones a través de soluciones MDM (Mobile Device Management) sigue siendo un reto complejo que hay que afrontar.

Nuevas vulnerabilidades en software y protocolos habituales. Probable. Las especialmente peligrosas vulnerabilidades reveladas el pasado año en software habitual, (tales como Shellshock, Heartbleed y OpenSSL), han sumido a la comunidad

tecnológica en importantes dudas acerca de la fiabilidad de un software muy común que, a la fecha, permanece sin auditar debidamente. Pese a los esfuerzos de muchas organizaciones, dedicando recursos para analizar tal tipo de software, incluso contratando a grupos de expertos que descubrieran nuevas vulnerabilidades, es muy posible que todavía sean muchas las que permanecen ocultas, algunas de las cuales podrán evidenciarse en 2015.

Ataques contra Infraestructuras Críticas. Posible. La especialmente peligrosa combinación de tecnologías antiguas –sin mantenimiento, en muchos casos- y una superficie de ataque cada vez mayor, hacen a ciertas Infraestructuras Críticas especialmente vulnerables a los ataques. Es sabido que son muchos los estados que están desarrollando capacidades para atacar de forma remota los sistemas SCADA de un enemigo, y otros sistemas críticos. Los analistas coinciden en señalar que las grandes cadenas de fabricación y las redes de energía eléctrica constituyen los objetivos más probables, entre otros sistemas SCADA e IC, para este tipo de ataques.

Ataques contra Linux y OS-X. Posible. Hasta el momento, tanto Linux160 como OS-X161 no han sido objeto de grandes ataques, aunque esto puede cambiar en los próximos años. La adopción masiva de Linux en muchas organizaciones ha provocado un repunte del número de muestras de código dañino para este sistema operativo, tales como Cdorker. Durante 2015, la ampliación de la superficie de ataque supondrá previsiblemente para los agentes de las amenazas un estímulo para perpetrar acciones contra esta plataforma. Por su parte, a pesar de los esfuerzos de Apple para fortificar el sistema operativo de los Mac, se sigue constatando la presencia de código dañino, introducido a través de paquetes de software pirateado. La creciente popularidad de los dispositivos Mac OS-X en todos los ámbitos –junto con la aparición de exploits día cero específicos- está despertando la atención de los ciberdelincuentes por desarrollar malware específicamente dirigido a este tipo de dispositivos. Dada la dificultad que supone penetrar en esta plataforma, y a la vista de que son muchos los usuarios de Mac que están desactivando determinadas medidas de seguridad por defecto –al objeto, generalmente, de permitir la instalación de software pirata-, los agentes de las amenazas están incorporando código dañino camuflado dentro de

programas, al objeto de infectar las máquinas. Quizás, como así se ha considerado por muchos analistas, el mayor motivo de preocupación radica en que, gracias a la imagen de seguridad que hasta ahora han gozado estos equipos, no se han desarrollado significativamente herramientas de seguridad para ellos, lo que puede convertirlos en dispositivos vulnerables.

Los ataques contra el Internet de las Cosas (IoT). Posible. Hasta el momento, los ataques contra el Internet de las Cosas (Internet of Things, IoT) no han ido más allá de unos pocos intentos (a menudo, sobrevalorados) o algunas amenazas sobre la posibilidad de utilizar botnets para desplegar ataques masivos contra televisores o frigoríficos inteligentes. Sin embargo, a medida que un mayor número de estos dispositivos se conecten, asistiremos a un mayor debate sobre los problemas de seguridad y, especialmente, de privacidad derivados de su conexión. En todo caso, es presumible que en 2015 se produzcan ataques contra dispositivos de red, que pueden facilitar a un atacante mantener la persistencia en la organización y desarrollar movimientos laterales dentro de una red corporativa, como parte de una acción APT a mayor escala. En el nivel de los usuarios domésticos, es presumible que las primeras acciones de compromiso de la IoT se traduzcan en la manifestación de ciertas vulnerabilidades de los dispositivos y la posibilidad de incrustar publicidad (adware/spyware) en, por ejemplo, la programación del receptor de televisión inteligente.

Conclusiones del Capítulo 1.

Al analizar el estudio “Riesgos Globales 2015” del Foro Económico Mundial, se observa que el riesgo de ataques cibernéticos a gran escala se estima más elevado que el promedio de otros riesgos, destacando el citado estudio la creciente sofisticación de los ataques cibernéticos y el surgimiento de la hiperconectividad, con un número cada vez mayor de objetos físicos conectados a Internet, además de la vulnerabilidad que supone el almacenamiento de los datos personales en la nube.

Se espera, además, que el "Internet de las cosas" (IoT en sus siglas en inglés) incremente esta tendencia al generar nuevos riesgos asociados a la privacidad y el adecuado uso de los datos

De otra parte, también se desprende que los ciberataques se encuentran relacionados con otros riesgos tecnológicos como las vulnerabilidades de la infraestructura de información crítica, el mal uso de las tecnologías, el fraude, el robo de datos y el funcionamiento de las infraestructuras críticas. El resto de conexiones directas con otros riesgos caen en el ámbito de los riesgos denominados geopolíticos, ataques terroristas, fallo de la gobernanza nacional y conflictos entre Estados.

Una vez puestos en perspectiva los riesgos relacionados con la ciberseguridad con otros riesgos globales, se han analizado las amenazas, para lo cual se han estudiado los orígenes o agentes de la amenaza, las víctimas u objetivos que pueden verse atacados y los efectos que se esperan conseguir por los generadores de los ataques.

Las conclusiones de este análisis de amenazas apuntan como orígenes de la amenaza a Estados, organizaciones terroristas, profesionales del ciberdelito, cibervándalos y script kiddies, hacktivistas, actores internos en las organizaciones, investigadores, y organizaciones privadas.

Estos agentes de la amenaza intervienen contra el sector público, el sector privado y los ciudadanos en general, en diferentes niveles, mediante el espionaje digital; el desarrollo de capacidades ofensivas; la interrupción y toma de control de los sistemas; la sustracción, publicación o venta de información, la manipulación de información; las desfiguraciones en páginas web; y la publicación de información sensible.

En cuanto a los ciberincidentes en España, el CERT Gubernamental Nacional (CCN-CERT) gestionó durante 2014 un total de 12.916 incidentes, detectados en las Administraciones Públicas y en empresas de interés estratégico. Esta cifra representa un incremento del 78% con respecto al año 2013. De los incidentes de 2014, el 10,8% (1.404) fueron catalogados con un nivel de riesgo entre muy alto y crítico; esto es, que el ataque afectó a los sistemas de la organización y a su información sensible. El CCN-

CERT ha constatado, además, un incremento en la intensidad y sofisticación de dichos ataques, tanto a las Administraciones Públicas como a las empresas y organizaciones de interés estratégico para el país, fundamentalmente de los sectores energético, de defensa, aeroespacial, farmacéutico y químico.

Las tendencias apuntan a un significativo incremento del volumen y peligrosidad de los ciberataques; el aumento del ciberespionaje, favorecido por su dificultad de atribución; la continuación de los ataques como servicio, mediante la contratación de grupos con conocimiento y capacidad técnica; la fusión de las tácticas, técnicas y procedimientos (TTP) entre el ciberespionaje y la ciberdelincuencia; la estabilización de los ataques hacktivistas; el "secuestro" de organizaciones por ransomware con ánimo de lucro; el incremento de los ataques contra cajeros automáticos y procedimientos de pago; nuevas amenazas a los dispositivos móviles; nuevas vulnerabilidades en software y protocolos habituales; ataques contra Infraestructuras Críticas; ataques contra Linux y OS-X; y el incremento de los ataques contra el Internet de las Cosas (IoT).

Es en este escenario que dibuja el nivel y la tendencia de incremento de riesgos y amenazas, que se estima apropiado revisar el modelo de la ciberseguridad nacional para incrementar los niveles de alerta, protección, respuesta y recuperación de los sistemas nacionales.

CAPÍTULO 2. EVOLUCIÓN DEL PENSAMIENTO ESTRATÉGICO

Una vez valorada la necesidad de disponer de un modelo de ciberseguridad nacional en España para hacer frente a los riesgos y amenazas derivados del uso del ciberespacio, se va a iniciar el proceso para responder a la pregunta de investigación: "¿Cuál sería un modelo apropiado de organización de la ciberseguridad en España?".

Para responder a esta pregunta de investigación, se quiere hacer notar que el diseño de los modelos y las estructuras en cualquier ámbito de la seguridad deben ser la consecuencia de un proceso de planeamiento descendente. De esta forma, los Estados generan procesos de planeamiento estratégicos, que se fundamentan en la evolución del pensamiento estratégico general, para después desarrollar estrategias nacionales de seguridad, que impulsan otras estrategias subordinadas en ámbitos específicos, como es el caso de la ciberseguridad.

De este modo, las estrategias subordinadas a las estrategias nacionales de seguridad, desarrollan elementos específicos para hacer frente a los riesgos y amenazas en ese ámbito en concreto. Todo ello sin perder de vista la necesaria armonización con el resto de estrategias subordinadas con las que comparten elementos comunes que se derivan de las líneas de acción y objetivos definidos en las estrategias nacionales de seguridad.

Del desarrollo de estas estrategias subordinadas puede desprenderse la conveniencia de crear un modelo del sistema sectorial de seguridad, o bien modificar el existente hasta ese momento, para satisfacer las necesidades puestas de manifiesto en el desarrollo de esas estrategias subordinadas a la nacional.

Este proceso de planeamiento se incardina en el acervo de pensamiento estratégico, tanto global como el que ha ido conformando la seguridad de las diferentes regiones geopolíticas, así como el de las alianzas y organizaciones de que los diferentes actores nacionales forman parte.

En este escenario, se expondrán a continuación las principales corrientes del pensamiento estratégico global y regional, que han ido conformando el modo de pensar y la manera establecer patrones de seguridad nacional, para llegar al diseño de las estrategias nacionales de seguridad y su posterior desarrollo en estrategias sectoriales subordinadas, como las estrategias nacionales de ciberseguridad.

El concepto de seguridad y la conformación de los elementos que lo fundamentan forman parte de un proceso en el que se entremezclan elementos sociales, políticos, económicos y religiosos, entre otros factores ligados a las circunstancias geoestratégicas y otras de tipo coyuntural.

La evolución de los pueblos ha incorporado la necesidad de establecer las estrategias de seguridad que les permitan protegerse en cada escenario y así poder avanzar en su desarrollo como sociedad.

Esta evolución es un proceso dinámico, que se encuentra interconectado y que ha ido desarrollándose de forma natural, utilizando para ello en numerosas ocasiones el binomio ensayo y error, pero que también ha tenido una base ligada al pensamiento científico, todo ello adaptado a la percepción de éste en las diferentes épocas, de acuerdo a las corrientes de pensamiento dominantes.

El objeto de este apartado es efectuar un recorrido por la evolución del pensamiento estratégico, presentando en su contexto histórico, político y social a los principales autores y sus teorías[77].

[77] Este apartado del capítulo es un extracto de la publicación VILLALBA FERNÁNDEZ, Aníbal: "La evolución del pensamiento estratégico", en *Fundamentos de la estrategia desde el siglo XXI*, pp. 67-140. Monografías del CESEDEN número 67. Ministerio de Defensa. Madrid, marzo 2004. Esta publicación se puede consultar también en formato digital en http://www.portalcultura.mde.es/Galerias/publicaciones/fichero/00876.pdf Aunque se ha extractado la publicación para adaptarla al objeto de la investigación, se ha respetado la mayor parte del aparato crítico para facilitar una posible consulta.

Las estrategias de seguridad nacional y sus estrategias sectoriales derivadas, entre las que se incluyen las estrategias nacionales de ciberseguridad se van a inspirar en estos modelos de pensamiento.

2.1. Discontinuidad y escasez de literatura estratégica

Señala Coutau-Bégarie que la Estrategia no es una disciplina independiente, sino que constituye una rama de un dominio más amplio, aquel de la conducción de la guerra y más generalmente del conflicto en la terminología actual. Esta estrategia ha adoptado diferentes denominaciones dependiendo del momento histórico, “ciencia militar” en tiempos de los romanos, "arte de la caballería" en la Edad Media, "arte militar" a principios de la Era Moderna, o "arte de la guerra" en el siglo XVIII[78].

Al igual que la guerra ha sido una preocupación universal y su reflejo ha sido plasmado en diferentes documentos a lo largo de la Historia, no ha ocurrido lo mismo con el pensamiento estratégico, que ha estado imbricado en el fenómeno de la guerra, de tal forma que hasta el final de la Segunda Guerra Mundial el concepto de estrategia no se pensaba ni ponía en práctica más que tras el desencadenamiento de las hostilidades, y su teoría no era más que un elemento de la teoría de la guerra. No obstante, hay que señalar que aunque no haya habido una diferenciación clara con respecto a la guerra, o que la literatura escrita sobre estrategia sea escasa o discontinua, no quiere decir que no haya existido el pensamiento estratégico.

Coutau-Bégarie profundiza en las causas de esta discontinuidad, sugiriendo cinco razones epistemológicas e históricas[79]

1. El pensamiento estratégico debe responder a una necesidad. El historiador norteamericano Wheeler[80], basándose en el estudio comparado del desarrollo

[78] COUTAU-BÉGARIE, Hervé: *Traité de Stratégie*, Economica, p. 132. París, 1999.

[79] *Ibídem,* pp. 134-137.

[80] WHEELER EVERETT, L.: "The Origins of Military Theory in Ancient Greece and China". Actes des colloques de la Commission Internationale d’Histoire Militaire, número 5, Bucarest, 1980. Citado por COUTAU-BÉGARIE, Hervé: *opus citada*, p. 134.

simultáneo de la teoría militar en Grecia y China, en el siglo IV a. de C., propone esa idea. En esa época, tanto en China como en Grecia, existía una gran inestabilidad política y una actividad guerrera muy intensa. Estas condiciones se dieron en la Europa de finales del siglo XVIII y principios del XIX.

2. Supone cierta apertura, poner en disposición de otros, recetas, preceptos, máximas, etc. Muchas veces, los estrategas militares consideraban su arte como una propiedad personal, que no transmitían más que a sus discípulos escogidos.

3. El pensamiento estratégico supone, a la vez, experiencia práctica y una predisposición a la reflexión, que raramente se encuentran en la misma persona. Además, los jefes militares solamente disponían de tiempo para escribir en los periodos de inactividad, a lo que había que añadir la necesidad de un cierto nivel de instrucción literaria.

4. Supone un sesgo en el carácter hacia la abstracción. Griegos y bizantinos han producido literatura estratégica porque eran dados a reflexiones filosóficas o teológicas. Los romanos, en cambio, no produjeron casi ninguna, al ser un pueblo de carácter más práctico.

5. También implica una orientación hacia la eficacia. Como la ciencia económica, la ciencia estratégica postula el comportamiento racional del sujeto hacia un fin único. No se busca sino la victoria sobre el enemigo. Todo lo que pueda contribuir a alcanzarla será utilizado, sin demasiadas consideraciones éticas.

Se podría decir que la ciencia estratégica se ha visto favorecida en sociedades evolucionadas, amenazadas con riesgos de guerra, abiertas a la discusión, proclives a la abstracción y gobernadas por un cierto utilitarismo.

El resultado es que la Estrategia como ciencia es mucho menos conocida que la ciencia política, filosófica, económica o táctica[81]. Sólo muy recientemente se ha plasmado la evolución del pensamiento estratégico. Hay que destacar, en este sentido, las obras dirigidas por Edward Mead Earle[82] y Peter Paret[83].

A pesar de que en la Antigüedad la destrucción de escritos era muy frecuente y probablemente un gran número de obras habrán quedado desconocidas al no haber sobrevivido el fuego, se puede considerar que el pensamiento estratégico se ha desarrollado principalmente en tres focos: en China, dónde sólo han sobrevivido los escritos de algunos escritores, el mundo griego, con sus prolongaciones romana y bizantina y el espacio europeo moderno, de donde parte el pensamiento estratégico contemporáneo, que encuentra en Estados Unidos su prolongación.

Los documentos más antiguos conocidos sobre la guerra no se ajustan al modelo de los tratados teóricos, adoptando la forma narrativa para glosar mediante poemas épicos o textos en prosa que conmemoran hazañas bélicas, como aparecen en antiguos monumentos egipcios, babilonios y asirios. Del espíritu de la época en que se conformaron estos testimonios emana la voluntad de transmitir la ejemplaridad a través de la excelencia, con lo que los hechos históricos dejan paso a versiones adaptadas de la realidad.

2.2. Pensamiento estratégico en la antigua China

En China se produce un nuevo tipo de testimonio diferente del poema épico o la prosa novelada referente al fenómeno de la guerra. Después de la caída del Imperio Chou, hacia el año 400 a. de C., China se divide en diferentes facciones que luchan entre sí

[81] Apunta COUTAU-BÉGARIE, Hervé: *opus citada*, p. 138, que excluida de la universidad, la Estrategia se ha encontrado circunscrita a la enseñanza militar superior, lo que ha limitado su audiencia.

[82] MEAD EARLE, Edward: *Makers of Modern Strategy: Military Thought from Machiavelli to Hitler*. Princeton University Press, Princeton, 1944, traducción en español Creadores de la Estrategia moderna: El pensamiento militar desde Maquiavelo a Hitler. Círculo Militar. Buenos Aires, 1968.

[83] PARET, Peter: *Makers of Modern Strategy: from Machiavelli to the nuclear age*, Princeton University Press, Princeton, 1986, traducción en español Creadores de la Estrategia moderna: desde Maquiavelo a la era nuclear. Ministerio de Defensa. Madrid, 1992.

confrontando ejércitos profesionales. Entre los años 400 y 200 a. de C. algunos de los generales parecen haber plasmado por escrito sus experiencias de combate, aunque otras versiones apuntan a la mitificación de la figura de los más famosos de estos generales, atribuyéndoles textos de otros autores que de esta forma aumentaban su prestigio.

A diferencia de los poemas épicos o la prosa novelada sobre las campañas militares, que eran considerados de dominio público y que eran recitados, leídos o incluso grabados en piedra, los textos chinos fueron tratados como secretos de Estado. De esta naturaleza se desprenden sus nombres: *Las enseñanzas de los seis secretos de Ta'i Kung; Los métodos de Ssu-Ma; Tres estrategias de Huang Shih-Kung* y *Los métodos militares*, obra atribuida a Sun Pin[84].

Algunos de los textos que han llegado hasta nuestros días tienen el formato de consejos proporcionados por los jefes militares a los dirigentes políticos como carta de presentación para ofrecer los servicios de su ejército[85]. Otros documentos adoptan forma de aforismos, pequeñas frases que son atribuidas a un prestigioso general y que son ampliadas y explicadas por otros o ilustradas con ejemplos históricos.

Señala Van Creveld que es importante para aproximarse a estos textos reflexionar sobre la filosofía china respecto a la guerra, que no es contemplada como un instrumento en manos de la política, ni mucho menos un fin en sí misma. De hecho, la guerra es vista como un elemento del mal, aunque alguna vez fuera necesaria debido a las imperfecciones del mundo. La guerra se observaba como un abandono de la "armonía cósmica" o *Tao*. Por definición el *Tao* solamente puede ser restituido por el *Tao*. De esta forma el bando que acreditara las mayores virtudes sería el vencedor[86].

[84] CREVELD, Martin van: *The Art of War, War and Military Tought*, pp. 24-25. Londres, Cassell, 2002.

[85] Uno de los más significativos ejemplos de este estilo lo constituye la exposición por parte de Wunt Zu al marqués de Wei.

[86] CREVELD, Martin van: *opus citada*, p. 29.

Aunque el *Tao Te Ching* condena las armas y la guerra, Wang Chen[87] señala en sus comentarios militares a esta obra que el Ejército es un elemento indispensable como mecanismo disuasorio y que la lucha a veces es la única alternativa, apuntando no obstante que los sabios no emplean los medios militares por indignación o enfado, ni para conquistar terreno o vengar enemistades; deben por el contrario establecer y preparar un ejército para estar preparados contra el mal y desbaratar los planes de los que se alejan de la sabiduría.

Destaca en el pensamiento estratégico chino Sun Tzu Wu, general que se estima vivió en China alrededor de 500 años a. de C. y al que se le atribuye la obra: *Bing Fa*, traducida como *El arte de la guerra*. El estilo de la obra sigue el patrón ya enunciado anteriormente de presentar una serie de aforismos del maestro que posteriormente son explicados por diferentes autores. Los trece artículos que vertebran el documento fueron escritos en una época convulsa de la historia de China e ilustran de modo ejemplar el comportamiento que debe tener un general.

Sun Tzu comparte los principios morales del *Tao* y señala que: "Por regla general, hacer la guerra no es lo mejor. Sólo la necesidad debe obligar a emprenderla. Independientemente de su resultado y su naturaleza, los combates resultan funestos incluso para los propios vencedores. Únicamente hay que librarlos si la guerra no se puede conducir de otra forma. Si al soberano le mueve la cólera o la venganza, no debe declarar la guerra ni movilizar tropas"[88].

No obstante, señala en su *Artículo I, sobre la evaluación*: "La guerra es de vital importancia para el Estado. Es el dominio de la vida y de la muerte; de ella depende la conservación o la pérdida del Imperio; es forzoso manejarla bien. No reflexionar seriamente sobre todo lo que le concierne es dar prueba de una culpable indiferencia

[87] SAWYER, Ralph D.: *The Tao of War. The Martial Tao Te Ching*, p. 31. Westview Press. Cambridge, 2003.

[88] SUN TZU: *Los trece artículos sobre el arte de la guerra*. Ministerio de Defensa. Madrid, 1998.

en lo que respecta a la conservación o la pérdida de lo que nos es más querido, y ello no debe ocurrir entre nosotros"[89].

Señala Frédéric Encel que: "Sun Tzu inscribe completamente la guerra en la lógica (la "continuación", que dirá Clausewitz) de la política en general"[90].

Apunta Miguel Ángel Ballesteros que: "Las reflexiones de Sun Tzu gozan de un alto grado de abstracción y de conceptualización que hacen de *El arte de la guerra* un texto clásico, útil para la resolución de las crisis en el ámbito de las relaciones internacionales, mercantiles e incluso personales. Allá donde haya un choque de intereses entre seres humanos, los aforismos de Sun Tzu son útiles"[91].

Sun Tzu es, junto con Clausewitz, el pensador estratégico más ampliamente conocido, lo que no quiere decir que haya sido interpretado de modo correcto a través de la Historia, especialmente desde la óptica occidental, donde se buscaban recetas allí donde solo existía sabiduría.

2.3. Pensamiento estratégico en la Grecia y Roma clásicas

Al contrario que en China, los documentos que han llegado a nuestros días del mundo greco-romano, desde Enéas *el Táctico* a Vegecio en un periodo que abarca desde el siglo IV a. de C. hasta el final del siglo IV d. de C., proceden de personas que no tuvieron el mando de tropas en combate ocupando las jerarquías más elevadas. Indudablemente no es por la ausencia de grandes generales como Alejandro Magno, Aníbal, Escipión o Julio César, pero, a excepción de este último, ninguno plasmó sus experiencias de las campañas por escrito, ni mucho menos elaboró una teoría o tratado sobre el arte de la guerra.

---

[89] *Ibídem*, p. 31.

[90] ENCEL, Frédéric: *El arte de la guerra. Estrategas y batallas*, p. 24. Alianza Editorial. Madrid, 2002.

[91] BALLESTEROS, Miguel Ángel: "Para lograr la paz". Revista de Política Exterior, p. 175, volumen XVI, número 88. Madrid, 2002.

Se tiene constancia de que Enéas *el Táctico* escribió varios tratados relacionados con la guerra [92], de los que sólo ha llegado a nuestros días *Poliorcética*[93], que se estima se escribió entre los años 365 y 360 a. de C.[94]. A pesar de que este escrito trata de una cuestión singular y bastante técnica como es la defensa de una ciudad sitiada, su exposición está salpicada de razonamientos que se elevan del plano puramente táctico, proponiendo reflexiones de carácter estratégico[95].

Tucídides, nacido en Atenas y que se estima vivió entre los años 460 a 399 a. de C., es uno de los más importantes historiadores de la Antigüedad. Está considerado uno de los creadores de la ciencia histórica, renunciando a las narraciones legendarias o a las intervenciones de los dioses para explicar la Historia, exponiendo las causas profundas y superficiales de los conflictos, subrayando como valores esenciales en los actos humanos la fuerza y el espíritu de justicia, analizando los anhelos, desilusiones y recelos de los hombres y sus sociedades, como paso previo para profundizar en la comprensión de un determinado hecho[96]. Relata Tucídides en la *Historia de la guerra del Peloponeso*[97] entre Atenas, en su apogeo como potencia marítima, y Esparta y sus aliados. Tucídides describe, desde la forma de un discurso de Pericles, una Atenas segura de su victoria basada en su preponderancia marítima que tras una década

[92] "Preparaciones militares", "Financiación de la guerra", "Campamentos", "Complots", "Tácticas navales", "Ilustraciones históricas" y "Guerra de sitios". CREVELD van: *opus citada*, p. 47.

[93] Esta palabra ha llegado a nuestros días con el significado de "arte de atacar y defender las plazas fuertes", según se recoge en el Diccionario de la Lengua Española de la Real Academia Española en su vigésima primera edición.

[94] CHALIAND, Gérard: *Anthologie mondiale de la stratégie: des origines au nucléaire*, p. 21. Robert Laffon, París, 1990, nueva edición actualizada, 2001.

[95] En este sentido se diferencia de otros autores que no se recogen en el ensayo por dedicar sus reflexiones al campo de la Táctica, como ASCLEPIODOTUS con su Esbozo de Táctica, que elaboró sus estudios ajustándose al significado literal de la palabra griega "táctica" como "orden". De esta forma estudió las distancias, movimientos, etc., de la falange griega.

[96] Véase MARTÍNEZ TEIXIDÓ, Antonio, director: *Enciclopedia del arte de la guerra*, p. 56. Planeta. Barcelona, 2001.

[97] De la que es contemporáneo (431-404 a. de C.).

victoriosa se ve abocada a la derrota tras una desastrosa expedición en Sicilia[98]. La obra de Tucídides está salpicada de reflexiones de carácter estratégico y político.

Jenofonte, cuya vida se sitúa alrededor del periodo entre los años 428 y 356 a. de C., fue discípulo de Sócrates[99] y sirvió en la caballería ateniense abandonando Atenas tras la victoria de Esparta en la guerra del Peloponeso. Junto con 10.000 mercenarios griegos se desplaza a Persia para apoyar a Ciro *el Joven* en su intención de ocupar el trono de su hermano Artajerjes II. Pero tras la muerte de Ciro los griegos debieron batirse en retirada después de que sus generales fueran asesinados. Jenofonte es entonces elegido jefe de la expedición y dirigirá durante ocho meses y 2.500 kilómetros una retirada de su ejército en un terreno desfavorable sin dejar de combatir. Jenofonte relata en su obra: *Anábasis*, conocida como: *La retirada de los diez mil*, las vicisitudes de una de las más complicadas maniobras militares[100].

El reclutamiento de 10.000 mercenarios griegos por parte de Ciro abre un nuevo periodo en la historia militar de la Antigüedad: el de los ejércitos profesionales. Hasta el siglo IV a. de C. las *polis* o "ciudades estado" griegas tenían ejércitos de ciudadanos-soldados, que se procuraban su propio armamento, los *hoplitas*. La guerra del Peloponeso, larga y compleja [101] , originó la primera demanda de soldados especializados, los *epíkouroi*, que entrenaban a grupos de soldados aficionados. Eran los inicios de un cambio histórico, con consecuencias políticas y sociales, que se aceleró tras el final de la guerra y las crisis de las *polis* en el siglo IV a. de C., sin las

[98] Véase ALONSO TRONCOSO, Víctor: *Neutralidad y neutralismo en la guerra del Peloponeso*, 431-404 a.C. Universidad Autónoma. Madrid, 1987.

[99] En la obra Memorables o Recuerdos de Sócrates da a entender que Jenofonte se consideraba no sólo discípulo sino también amigo íntimo del filósofo, aunque algunos historiadores cuestionan que perteneciera a su círculo más íntimo.

[100] ENCEL, Frédéric*: opus citada*, p. 35, señala que es el arte del mando lo que destaca en esta obra de Jenofonte, además de la buena formación geopolítica que tenía del mundo helénico, mostrándose también como un gran táctico.

[101] La guerra entre Atenas y Esparta, el tema de Historia de la guerra del Peloponeso, no fue simplemente el choque entre dos ciudades-estado. Atenas y Esparta mantenían alianzas con muchas ciudades-estado más pequeñas, tan complejas y difíciles de administrar como los dos bloques de la guerra fría. KAPLAN, Robert D.: El retorno de la Antigüedad: La política de los guerreros, p. 85. Ediciones B. Barcelona, 2002.

cuales el soldado mercenario no hubiera tenido el importante papel que desempeñó en ese siglo y en los reinos helenísticos tras la muerte de Alejandro[102].

La producción literaria de Jenofonte es amplia y variada, abordando diversos géneros: historia, ensayo, biografía, etc., destacando la ya citada *Anábasis, Helénicas*, que pretende continuar la *Historia de la guerra del Peloponeso* de Tucídides, *Ciropedia*, que evoca la educación de Ciro el Grande, rey de Persia en el siglo VI a. de C., y donde reflexiona sobre el modelo de virtudes que deben acompañar a un caudillo. Escribió también Jenofonte dos obras técnicas sobre la caballería, Hipárquico, que en griego significa "jefe de la caballería" y *Sobre la equitación*, donde se aportan consejos para mejorar la caballería ateniense.

Polibio (Megalópolis, 202-120 a. de C. aproximadamente), fue un griego al servicio de Roma. De formación militar, probablemente es, junto con Tucídides, el más importante historiador de la Antigüedad. Llamado por Escipión Emiliano presencia en 146 la destrucción de Cartago. Polibio relata y analiza la historia del triunfo de Roma sobre Cartago, así como la expansión romana hacia el oriente griego y helenizado. Su obra *Historias* constituye una relación detallada de este proceso a la que acompaña un profundo análisis, lo que ha convertido sus escritos en referentes indispensables de la estrategia de Roma. Su relato de la batalla de Cannas (216 a. de C.), donde los cartagineses derrotan en inferioridad numérica a los romanos, constituye un documento preciso del arte de Aníbal en una de sus victorias más extraordinarias. Polibio señala en *Historias* que: "Es tan imposible escribir bien sobre las operaciones de la guerra si un hombre no ha tenido experiencia en servicio activo, como hacerlo sobre política sin haber estado envuelto en vicisitudes políticas"[103].

[102] Para una explicación más completa consultar: Jenofonte: *Anábasis*, pp. 18-20. Edición y traducción de Carlos Varias. Cátedra. Madrid, 1999.

[103] Citado por DEBS HENIL, Robert Jr.: *Dictionary of Military and Naval Quotations*, p. 147. United States Naval Institute. Annapolis, 1966.

A pesar de que la obra de Julio César (101-44 a. de C.), tiene un valor político de mucho mayor calado que su faceta estratégica[104], sus *Comentarios*[105] ofrecen también reflexiones de carácter estratégico que impregnan su obra. Asimismo Julio César en el resto de obras dedicadas a la conquista de las Galias[106] y en su *Guerra Civil* ofrece, al convertirse en historiador de sus propias hazañas, un amplio campo al análisis de las intenciones que realmente presidieron su comportamiento como general y político.

Señala Martínez Teixidó que: "En sus obras, Julio César nos ha legado la comprensión de la guerra imperial, que revestía la forma de expedición realizada con bastante superioridad de medios materiales, de prestigio, de técnicas y de instituciones. El objetivo era la anexión de territorios y poblaciones, como corolario de una guerra victoriosa. Representa el triunfo de la disciplina sobre la valentía turbulenta, y de la economía estricta sobre la improvisación y el instinto. En su obra: *De bello civili* definió una aproximación al poder político que se ampara en el acierto militar y en el talento administrador de las victorias"[107].

Salustio (86-35 a. de C.) es uno de los grandes historiadores romanos que acompañó a César a la campaña de África, llegando a ser en 46 a. de C. el primer gobernador de la nueva provincia de África. Después del asesinato de su mentor abandona la política dedicándose a escribir. Desgraciadamente la mayor parte de sus escritos se ha perdido y aunque su *Conjuración de Catalina*[108] es su obra más conocida, realizó una minuciosa descripción y profunda reflexión en: *La guerra de Jugurtha*, de las tácticas del débil y el fuerte, considerado modelo de las guerras de guerrilla[109].

---

[104] COUTAU-BÉGARIE, Hervé: *opus citada*, p. 152.

[105] JULIO CÉSAR: *Comentarios de la Guerra de las Galias*. Espasa Calpe. Madrid, 1980.

[106] JULIO CÉSAR: *Guerra de las* Galias, Libros I, II y III. Gredos, Madrid, 1945.

[107] MARTÍNEZ TEIXIDÓ, Antonio: *opus citada*, pp. 76-77.

[108] SALUSTIO: *Conjuración de Catilina, versión literaria por Manuel C. Díaz y Díaz*. Gredos. Madrid, 1979.

[109] CHALIAND, Gérard: *opus citada*, p. 104.

Onosander (siglo I a. de C.), de origen griego, escribió: *El Estratega*, El General, libro dedicado a los romanos, especialmente a aquellos que habían alcanzado la dignidad senatorial y a quienes habían llegado a cónsul o general. En la obra discute aquellos aspectos que deben acompañar al comandante en jefe, templanza, autocontrol, vigilancia, frugalidad, dedicación al trabajo, alerta, libre de avaricia, ni muy joven ni muy mayor, padre a ser posible, lector atento y buena reputación[110].

Sextus Justius Frontinus (40-106 d. de C.), oficial romano, llegó a ser gobernador de Bretaña (75-78). Autor de un comentario militar de Homero y de un tratado militar que se han perdido, pero que Vegecio utilizó en el siglo IV, no ha sobrevivido de sus obras más que *Strategemata*, que constituye un apéndice del tratado perdido y que recoge 583 estratagemas organizadas en siete libros[111]. Cada capítulo contiene una lista de acciones desarrolladas por comandantes en el planeamiento y la conducción de las operaciones. Como ejemplo: "Cuando Alejandro de Macedonia tenía un fuerte ejército elegía el tipo de guerra que le permitía luchar en campo abierto"[112].

Otros autores que colaboran a la evolución del pensamiento del arte de la guerra son Plutarco (46-120 d. de C.), que relata la expedición de Craso contra los Partos, Tácito (55-120 d. de C.) que describe con rigor las características militares de los germanos y Flavio Arrien (92-75 d. de C.) que relata la epopeya de Alejandro en su conquista de Asia y escribe un tratado de táctica[113]

No es hasta finales del IV siglo d. de C., que aparece una obra sobresaliente cuando Flavio Renato Vegecio escribe *Epitoma Rei Militaris*, *Tratado del arte militar o*

[110] Para una explicación más completa consultar: CREVELD, Martin van: *opus citada*, pp. 49-52.

[111] COUTAU-BÉGARIE, Hervé: *opus citada*, p. 152.

[112] CREVELD, Martin van: *opus citada*, p. 53.

[113] Para profundizar en estos autores se recomienda acudir a: CHALIAND, Gérard: *opus citada*, pp. 133-182.

Instituciones Militares[114], una compilación rigurosa del saber romano del arte de la guerra. Entre las fuentes que maneja Vegecio se encuentran Catón, Salustio y Frontinus, así como las ordenanzas militares de Augusto, Trajano y Adriano[115].

2.4. Transición hacia la Edad Moderna en Occidente

El tratado del arte militar más conocido del Imperio Bizantino es *Strategicon*, patrocinado por el emperador Mauricio entre 582 y 602. Escrito a continuación de las grandes campañas de los generales Belisario y Narses, aporta elementos de la práctica del arte militar bizantino en su cenit. Mauricio apuntó las reformas necesarias para la reestructuración del ejército, estableciendo una nueva estructura, intentando encuadrar en su ejército elementos nativos[116] y se mostró partidario de que todos los jóvenes recibieran instrucción militar, eliminando la distinción anterior entre el contribuyente y el soldado potencial.

Aunque *Strategicon* sobresale entre las obras en Bizancio, el primer texto conocido es una obra anónima de principios del siglo VI, *De Re Strategica*, que ofrece un plan completo aunque esquemático de la ciencia militar[117].

No es hasta el siglo X[118] que se retoma la producción de carácter estratégico cuando el emperador León VI (886-912), llamado *el Sabio* o *el Filósofo*, publicó: *Consejos Estratégicos y Tacticon*, un ensayo en organización militar y desarrollo de la batalla

---

[114] VEGECIO RENATO, Flavio: *Instituciones Militares*. Ministerio de Defensa. Madrid, 1988, que recoge el mismo título de la edición facsímil de 1764, prologada por Jaime de Viana, editada por la Escuela Superior del Ejército. Madrid, 1978.

[115] CREVELD, Martin van: *opus citada*, p. 54.

[116] Justiniano había intentado dominar la influencia de los elementos extranjeros dentro del Ejército, pero sin éxito, debido a su política de conquista y expansión que exigía un esfuerzo no disponible con medios propios. La lealtad incierta de los mercenarios se volvió un desafío a la cohesión del ejército. La lealtad del soldado era hacia el superior inmediato. Mauricio invirtió la tendencia, reservando para sí la autoridad de promover a todos los militares por encima del grado de centurión.

[117] CHALIAND, Gérard: *opus citada*, p. 205.

[118] La importancia del diseño militar de Mauricio en el Strategicon, e institucionalizado durante su reino, impregna el ejército entre 300 y 500 años después de su reinado, lo que se apunta como una causa de la limitación de la producción estratégica.

que recopila el saber militar desde Onosander hasta el emperador Mauricio. En *Tacticon*, al igual que en *Strategicon*, se analiza la cultura estratégica de los pueblos de la periferia del Imperio, sugiriendo la manera de combatirles[119].

Cabe reseñar que tras las principales obras del arte militar de los emperadores Mauricio y León VI, durante los reinos de Heraclio (610-641) y Basilo II (976-1025), la superioridad del arte de la guerra bizantino inspiró una nueva expansión del Imperio comparable a las conquistas de Justiniano, consolidando la solidez de la institución militar bizantina.

La historia de las instituciones militares de un periodo no puede separarse de la historia de la sociedad en que están inmersas. Señala Gilbert[120] que la organización militar de la Edad Media era una parte integrante del mundo medieval y declinó cuando la estructura social se desintegró. En una sociedad impregnada por el sentimiento religioso, en la que Dios constituía la jerarquía suprema, el caballero y el ejército servían a Dios. Al mismo tiempo, estos servicios militares estaban a disposición de su señor[121] que tenía confiada por la Iglesia la supervisión de sus actividades[122].

Además de estos aspectos de carácter espiritual y religioso, el compromiso militar entre el vasallo y el señor tenía un doble componente legal y económico. En un sistema de intercambio de servicios, que se ajustaba a la estructura agrícola y al sistema señorial de la Edad Media, el señor ponía a disposición del caballero unas tierras, el

---

[119] Apunta CHALIAND, Gérard: *opus citada*, p. 233 que el emperador León analiza las causas del éxito del islam y estudia el modo de limitar su expansión.

[120] GILBERT, Félix: "Maquiavelo: el renacimiento del arte de la guerra", en PARET, Peter: *Makers of Modern Strategy: from Machiavelli to the nuclear age*. Princeton University Press, Princeton, 1986, traducción en español *Creadores de la Estrategia moderna: desde Maquiavelo a la era nuclear*, pp. 26-29. Ministerio de Defensa. Madrid, 1992.

[121] El rey reinaba "por la gracia de Dios" y su monarquía gozaba de aureola divina. Sin embargo, sus súbditos tenían derecho a la resistencia y a la rebelión si dejaba de gobernarlos justamente y no les daba la debida protección. BROOKE, Christopher: Europa en el centro de la Edad Media 962-1154, p. 131. Traducción de Matilde Vilarroig. Aguilar. Madrid, 1973.

[122] RAMOS-OLIVEIRA, Antonio: *Historia crítica de España y de la civilización española, la Edad Media*, p. 271. Oasis, México, D.F., segunda edición, 1974, pone como ejemplo a España señalando que "la Reconquista convirtió a la Iglesia en una institución semimilitar".

feudo, que al ser aceptadas por el caballero comprometían a éste a prestar sus servicios militares al señor en caso de necesidad.

Estas connotaciones religiosas de la guerra como acto de hacer justicia[123], la restricción del empleo de las armas a la clase social de los caballeros que poseían tierras, así como la existencia de un código tanto legal como moral, constituían los factores determinantes del arte militar en la Edad Media. Los ejércitos medievales se organizaban solamente para el combate, con los consiguientes problemas relativos al entrenamiento de las tropas y su reflejo en la dificultad de mantener la disciplina. Además, como la guerra representaba el cumplimiento de una obligación moral sujeta a un estricto código, existía una tendencia a conducir las guerras y batallas de acuerdo a normas rígidas que dejaban poco margen a la experimentación de nuevas estrategias e incluso de métodos para conducir la guerra.

De otra parte, la batalla era una solución radical, que se concebía como una alternativa a la guerra, pero que se evitaba en lo posible por ser considerada una solución final plagada de inconvenientes y de incertidumbres. Más allá del choque frontal con el ejército enemigo, los beneficios de la guerra solían venir del asedio y la toma de sus lugares fortificados, todo ello como fase previa a la conquista de sus castillos y ciudades, verdaderas llaves del dominio territorial. Operaciones de sitio, castigo y desgaste constituían la forma cotidiana de la guerra medieval, y no batallas campales[124].

Vegecio fue un autor muy leído y copiado en la Edad Media e influyó en que Occidente tuviese una historia militar distinta a la del Imperio Bizantino. Especialmente desde la segunda mitad del siglo XIII, los ejércitos de la cristiandad occidental tratan de amoldarse a sus principios. Como consecuencia, los ejércitos de la Europa de la Baja

[123] SÁNCHEZ PRIETO y BELÉN, Ana: *Guerra y guerreros en España según las fuentes canónicas de la Edad Media*, p. 53. Servicio de Publicaciones del Estado Mayor del Ejército. Colección Adalid. Madrid, 1990.

[124] MITRE FERNÁNDEZ, Emilio y ALVIRA CABRER, Martín: "Ideología y guerra en los reinos de la España medieval", en Revista de Historia Militar, pp. 308-309. Ministerio de Defensa. Mayo, 2001.

Edad Media se parecen al romano del siglo IV mucho más que a los de ninguna otra época[125].

Ya se ha mencionado que la organización militar era un reflejo del sistema social general de la Edad Media, de modo que cuando se produjo una rápida expansión de la economía de mercado y las bases de la agricultura se derrumbaron[126], sus efectos sobre la Institución Militar fueron inmediatos. Los nuevos protagonistas, las ciudades y los grandes comerciantes, pudieron pagar por su seguridad. De este modo los nuevos protagonistas iniciaron un protocolo de doble acción, por una parte pagaban regularmente por los servicios militares a ejércitos que fueron teniendo mayor permanencia, además de recibir dinero de aquellos a los que se les proporcionaba seguridad y no querían tener obligaciones militares. No obstante, como señala Gilbert[127], la transformación de un ejército feudal en un ejército profesional, de un Estado feudal a otro burocrático y absolutista, fue lenta y alcanzó su máximo desarrollo en el siglo XVIII.

En este sentido, en los ejércitos de las potencias más importantes (Aragón, Francia e Inglaterra) convivían elementos heredados del sistema feudal de recluta eventual con otros de tipo profesional. No obstante, debido al creciente poderío económico de las ciudades italianas el fenómeno del ejército profesional se fue imponiendo[128]. Desde el siglo XIV, las ciudades italianas fueron base de reclutamiento para aquellos caballeros que querían hacer fortuna con la guerra. Las *Compagnie di ventura*, dirigidas por los *condottieri*[129], ofrecían sus servicios a cualquier soberano que les pagara. El nuevo

[125] BLANCO FREIJEIRO, Antonio, en el prólogo de VEGECIO RENATO, Flavio: *Instituciones Militares*, p. 23. Ministerio de Defensa. Madrid, 1988.

[126] ROMANO, Ruggiero y TENENTI, Alberto: *Historia Universal del siglo XXI:* "Los fundamentos del mundo moderno"; "Edad Media tardía"; "Renacimiento" y "Reforma", pp. 9-23, octava edición. Madrid, 1978.

[127] GILBERT, Félix: opus citada, p. 27.

[128] ROMANO, Ruggiero y TENENTI, Alberto: *opus citada*, p. 49.

[129] BOUDET, Jaques, director: *Historia Universal de los Ejércitos, 1300-1700, de Soliman a Vauban,* p. 136. Robert Laffont. París, 1965. Edición española Hispano Europea. Barcelona, 1966.

sistema económico dio mayores oportunidades para que hombres, despojados de las tradiciones militares precedentes, entraran al servicio de las armas únicamente por el dinero, y con ellos se empezaron a introducir nuevas armas y formas de lucha[130].

A pesar de que el pensamiento militar medieval es escaso y que hasta el año 1400 los tratados son compilaciones de obras anteriores, Coutau-Bégarie apunta algunas obras de la época: Alfonso X *el Sabio*, rey de Castilla, que hacia el año 1280 recoge las recomendaciones de Vegecio; Edigio Colonna que redacta también hacia el año 1280: *De Regimine Principium*, de gran éxito en la época; Honoré Bonet, monje benedictino, escribe: *El árbol de las batallas* (1386), también obra popular, aunque con una componente moral muy acusada; Christine de Pisan con su *Libro de hechos de armas y de la Caballería* (1406); Jean de Bueil, almirante de Francia escribe *El Doncel*, pequeño tratado narrativo sobre la guerra, que recomienda una táctica más prudente de la que llevó a la caballería a los desastres de Poitiers y Azincourt. Se debe señalar que estas obras se enmarcan en los dominios de la Táctica, no apareciendo pensamientos estratégicos salvo en anotaciones fugaces. La Estrategia comienza a aparecer más nítidamente a partir de la segunda mitad del siglo XIII, en los proyectos de las cruzadas, que desarrollan planes mejor estructurados[131].

No obstante, la reflexión militar propiamente dicha no se desarrolla hasta la segunda mitad del siglo XV, cuando el impacto de la artillería se hace notar más intensamente. El pensamiento militar se vuelve más activo, apareciendo en España el *Libro de la guerra* (1420), del marqués de Villena y el *Tratado de la perfección del triunfo militar* (1459) de Alfonso Hernández de Palencia. En Francia se publica *La Nef des Princes et des batailles de noblesse* (1502) de Robert de Balsac. En Inglaterra aparece el *Tratado del arte de la guerra* de Beraud Stuart y en Alemania *Kriegsbuch* de Philipp von Seldeneck, al final del siglo XV[132].

---

[130] GILBERT, Félix, *opus citada*, p. 28.

[131] COUTAU-BÉGARIE, Hervé: *opus citada*, p. 159.

[132] *Ibídem*, p. 160.

2.5. De Maquiavelo a Clausewitz

En el siglo XVI sobresale la figura de Maquiavelo, que ocupa una posición singular en el campo del pensamiento militar debido a que sus ideas estaban basadas en el reconocimiento del enlace existente entre los cambios que ocurrieron en la organización militar y los movimientos revolucionarios que se produjeron en la esfera política y social. El descubrimiento de la pólvora y la invención de las armas de fuego y la artillería hicieron inevitable un colapso en la organización militar de la Edad Media, en la que los caballeros jugaban un papel decisivo[133].

En las ciudades italianas del Renacimiento, los oficiales de las Cancillerías solían ser funcionarios grises que se limitaban a ejecutar las medidas tomadas por el círculo de poder. Maquiavelo fue una excepción; se convirtió en un personaje político importante en la República de Florencia entre 1498 y 1512[134].

La contribución más importante de Maquiavelo, en cuanto a temas militares, fue la redacción de la ley por la que se creaba la milicia florentina en el año 1505[135], con el objetivo de crear un ejército regular[136].

La clave del pensamiento de Maquiavelo está en la inseparable unión que existe entre la idea política y su necesaria fuerza militar. Su propósito es alentar la aparición de un príncipe, un hombre nuevo que mediante la fuerza establezca la unidad de la península Itálica, para lo cual debe establecer una milicia nacional[137].

---

[133] GILBERT, Félix: *opus citada*, p. 25.

[134] *Ibídem*, p. 29.

[135] La Ley, llamada la Ordinanza, preveía la formación de una milicia de 10.000 hombres comprendidos entre los 18 y los 50 años, elegidos por un comité especial y que deberían vivir en los distritos rurales de Toscana, perteneciente a Florencia. *Ibídem*, p. 31.

[136] Señala Marcu, que la idea de llamar bajo bandera a los habitantes de Toscana no era original de Maquiavelo, ya que era una vieja reclamación de los populares extremistas partidarios de Savonarola. MARCU, Valeriu: *Maquiavelo, la escuela del poder*, p. 154. Espasa Calpe. Madrid, 1967.

[137] MARTÍNEZ TEIXIDÓ, Antonio: *opus citada*, p. 153.

Maquiavelo fue un escritor prolífico que practicó diversos géneros como la comedia, la poesía o el ensayo político e histórico. Destacan entre su producción literaria: *Discurso sobre la primera década de Tito Livio* (1513), *El Príncipe* (1513), la inconclusa *Historia de Florencia* (comenzada en 1520) y *El arte de la guerra* (1521)[138].

En *El Príncipe*, Maquiavelo considera el poder como uno de los ámbitos de realización del espíritu humano, subrayando el fenómeno político como la expresión suprema de la existencia histórica que involucra todos los aspectos de la vida. *El Príncipe* es la síntesis de la disolución de un mundo, el Medioevo, y la redefinición de los valores que representa el hombre. Para Maquiavelo la razón suprema no es sino la razón de Estado, que constituye un fin en sí mismo, situado por encima del orden moral y los valores éticos tradicionales. El bien supremo no es ya la virtud, la felicidad, la perfección de la propia naturaleza, el placer u otros aspectos propuestos por los moralistas, sino la fuerza y el poder del Estado. El bien del Estado no se subordina al bien del individuo, situándose en un plano superior. Si la política debía ser el arte de lo posible, para Maquiavelo ello significaba que ésta debía de basarse en realidades. En la esencia de *El Príncipe* se encuentra la reivindicación del Estado moderno como articulador de las relaciones sociales[139].

El Príncipe y *El arte de la guerra* presentan características complementarias, la búsqueda de un líder que conjugue los aspectos político y militar de un hombre de Estado, y por ello los príncipes deben dedicarse enteramente al arte de la guerra. Maquiavelo es el iniciador de la escuela realista de pensamiento político, que rompe con la ética medieval e impone la "razón de Estado" como motivo para guiar la

[138] Otras obras de Maquiavelo son *Anales de Italia, Vida de Castruccio, La Mandrágora* (comedia), *Clizia* (comedia), *Comedia en prosa sin título, Belfegor* (novela), *Ordenanza de la Infantería, Ordenanza de la Caballería, Discurso sobre la Lengua, y Discurso Moral*.

[139] Señala Conde que el concepto de Estado en Maquiavelo, se contrapone a la moltitudine inordinata. De este modo, el Estado, como figura perfecta, debe sujetar el movimiento humano colectivo a un orden, hacer de la materia humana colectiva una figura perfecta y terminada, mantenerla en equilibrio estable, así como enderezarla por cauce racional de modo que su curso sea previsible y calculable. El único modo de ordenar este movimiento es dirigirlo. CONDE, Francisco Javier: *El saber político en Maquiavelo*, pp. 195-196. Instituto Nacional de Estudios Jurídicos. Madrid, 1948.

conducta de los gobernantes[140]. Al señalar en *El Príncipe* que la guerra justa es la guerra necesaria, corta el nudo gordiano conformado por las interminables discusiones medievales acerca de la guerra justa desde San Agustín a Santo Tomás de Aquino[141].

En el siglo XVI, la epopeya del descubrimiento de América por España[142], abre nuevas vías al pensamiento estratégico, destacando Hernán Cortés, que en sus *Cartas de Relación de la Conquista de Méjico* exponía su aventura a los soberanos españoles, apuntando reflexiones de orden militar que interactúan con la política.

España es la potencia militar dominante en este periodo, con un nuevo modelo de ejército que se conforma a partir de 1534, el Tercio, que marca el ocaso de la preponderancia de la caballería. Estos cambios organizativos van acompañados de una intensa reflexión[143].

La península Itálica, teatro de la rivalidad de las potencias europeas, produce asimismo una nutrida literatura militar. Venecia, expuesta al mar Adriático produce más libros militares entre 1492 y 1570 que todo el resto de Europa.

El pensamiento en Inglaterra es reflejo de la regresión que siguió a la guerra de los Cien Años y su aislamiento respecto al continente. El estudio del arte de la guerra no es fecundo y se produce un enroque en su pasado glorioso. Esta falta de vitalidad en el pensamiento militar explica la mediocridad de los dos bandos que protagonizan la guerra civil del siguiente siglo[144].

---

[140] MARTÍNEZ TEIXIDÓ, Antonio: *opus citada*, p. 153.

[141] CREVELD, Martin van: *opus citada*, p. 73.

[142] CORTÉS, Hernán: "Cartas de Relación", Historia 16. Madrid, 1985, edición de Mario Hernández, Madrid, 1985.

[143] Señala Gil Picache que: "Todo el periodo histórico del arte militar durante la Edad Media, queda analizado al estudiar los adelantos que en la materia tuvieron lugar en nuestra España". GIL PICACHE, Baltasar: *Elementos de Historia Militar*, p. 71. Imprenta del Colegio de Santiago para Huérfanos del Arma de Caballería. Valladolid, 1908.

[144] COUTAU-BÉGARIE, Hervé: *opus citada*, p. 163. Además, para un estudio más detallado refiere a BRUCE, Anthony: *A Bibliography of British Military History from the Roman Invasions to the restoration 1660*. Saur. Londres, 1981.

En Francia, en cambio, las circunstancias fueron distintas ya que las guerras italianas proporcionaron un escenario que permitió experimentar en el campo de batalla y que tuvo una traslación al pensamiento francés relativo al arte militar[145].

Es en definitiva el siglo XVI un periodo que se muestra fecundo en cuanto a la producción de obras de pensamiento militar, algunas de carácter táctico pero otras de una mayor profundidad abarcando no solamente los aspectos militares sino su interacción con los factores sociales, políticos y económicos, destacando este último aspecto que adquiere creciente relevancia afirmando algunos autores que la economía, la capacidad de sostener a las tropas en el combate, es la que decidirá el resultado de las campañas, valorando de otro lado la importancia de que la guerra suponga además una fuente de ingresos.

En el siglo XVII destacan las innovaciones llevadas a cabo por Mauricio de Nassau en la organización del Ejército profesional holandés, que suscitaron una abundante literatura en los Países Bajos. En Inglaterra, en los años que preceden a la guerra civil, aparecen tratados sobre la disciplina militar que preparan el camino al: *New Model Army de Cromwell.* Dinamarca es también un país activo, con la recopilación de estratagemas en *Manipulus Stratagematum* (1632) de Elias Winstrup y *Un nuevo tratado de la guerra* (1644) de Fromhold von Elerdt. Por el contrario, en Alemania, devastada por la guerra de los Treinta Años, apenas se publica, con excepciones como *Kriegsbuch* (1607) de Wilhelm Dilich. En Hungría, el conde Miklós Zrínyi funda el pensamiento estratégico magiar con *El bravo capitán* (1650) inspirado en Maquiavelo[146]

Estas innovaciones en Europa del Norte no implican una decadencia de la reflexión en los países europeos meridionales. En España, Francisco Barado recoge una bibliografía con varias decenas de títulos que cubren todo el espectro del arte de la guerra[147]. La producción italiana es menos abundante que en el siglo precedente, dado

[145] *Ibídem*, pp. 163-164.

[146] *Ibídem*, pp. 165-166.

[147] BARADO, Francisco: *Literatura militar española*. Ministerio de Defensa. Madrid, 1996.

que la Península deja de ser el teatro de las operaciones militares en Europa. En Francia, mención especial merece Vauban, que nace en 1633 y desarrolla su actividad hasta final del siglo, gran ingeniero militar de actividad febril durante el reinado de Luis XIV, que gozó de inmenso prestigio y cuyos escritos y trabajos de ingeniería respecto a fortificación sobrepasaron el marco técnico para influir en el arte de la guerra, recogiendo en sus memorias, tituladas: *Ociosidades*, el espíritu del racionalismo científico[148].

La Paz de Westfalia (1648) que puso fin a la guerra de los Treinta Años acabó con los estímulos religiosos y políticos que habían mantenido a Europa en continua agitación. El concepto de "equilibrio de poder" pasó a ser la idea política dominante, según la cual, ningún estado debería llegar a ser tan potente como para suponer una amenaza a la independencia y a la existencia de los demás[149].

Los esfuerzos de los Estados europeos por el poder pasaron, de feroces luchas a vida o muerte, a movimientos políticos en búsqueda de alianzas, dentro de ese marco, generalmente aceptado, de equilibrio de poder. La mayoría de las guerras de esa época pasaron a ser, por tanto, guerras de coalición; coaliciones que se mantenían sólo por intereses particulares y cálculos políticos. En la segunda mitad del siglo XVII comienzan a surgir ejércitos y armadas permanentes, fruto del desarrollo de los elementos de la administración.

Es en esta segunda mitad del siglo XVII que resalta el modenés Raimondo Montecuccoli, teniente general y mariscal de campo del Ejército austriaco de los Habsburgo, brillante jefe militar y pensador estratégico. Couteau-Bégarie considera que Montecuccoli merece ser calificado como el fundador de la ciencia estratégica moderna[150].

---

[148] Es altamente recomendable acudir al ensayo: GUERLAC, Henry: "Vauban: El impacto de la ciencia en la guerra", en PARET, Peter: *Creadores de la Estrategia moderna: desde Maquiavelo a la era nuclear*, pp. 77-100. Ministerio de Defensa. Madrid, 1992.

[149] Idea, cuya expresión política quedó reflejada también en el Tratado de Paz de Utrecht en 1713.

[150] COUTAU-BÉGARIE, Hervé: *opus citada*, p. 169.

En el siglo XVIII comienzan a aparecer obras con una dimensión estratégica más pronunciada, entre las que pronto sobresale Mauricio de Sajonia, comandante en jefe del Ejército francés durante la guerra de Sucesión Austriaca (1740-48). Su obra más importante es *Rêveries*, publicada en 1756 tras su fallecimiento, que comienza con una frase muy citada posteriormente: "La guerra es una ciencia cubierta de tinieblas, en medio de las cuales no se puede avanzar con paso seguro; la rutina y los prejuicios son la base, consecuencia natural de la ignorancia. Todas las ciencias tienen unos principios, sólo la guerra no tiene ninguno; los grandes capitanes que han escrito sobre ella no nos han legado ninguno; es necesario ser perfecto para entenderlos"[151].

Frente a las tesis de Mauricio de Sajonia –operaciones sin batallas– aparecen las de Federico II de Prusia, que al invadir Silesia inesperadamente en el año 1740, dio un ejemplo de lo que posteriormente se llamaría la guerra relámpago (*blitzkrieg*). El rey desarrolló posteriormente sus ideas en un *Testamento político*, compuesto en 1752 para uso privado de sus sucesores en el trono. Entre las obras que hizo públicas destaca: *El arte de la guerra*, serie de ensayos políticos y memorias donde explicaba sus éxitos militares[152].

El pensamiento militar del siglo XVIII, que participa de las luces de la Ilustración, está dominado por el racionalismo y la búsqueda de leyes. Hay una abundante producción estratégica en todos los países, prueba evidente del fin de la estrategia intuitiva que caracterizó el siglo XVII y evidenciado por el crecimiento de los efectivos y el perfeccionamiento del arte de la guerra. Se comienza a vislumbrar el paradigma de la batalla, impuesto por la Revolución Francesa.

Será contra este racionalismo de inspiración francesa que surgirá un idealismo alemán cuya primera transposición será atribuir al azar un carácter decisivo a la guerra.

---

[151] *Ibídem*, p. 171.

[152] PALMER, R. R.: "Federico el Grande, Guibert, Bülow: De las guerras dinásticas a las nacionales", en PARET, Peter: Creadores de la Estrategia moderna: desde Maquiavelo a la era nuclear, pp. 107-108. Ministerio de Defensa. Madrid, 1992.

De 1789 a 1815, Europa está casi continuamente en guerra y el arte de la guerra sufre una transformación profunda. El pensamiento estratégico en Prusia, espoleado por la catástrofe de 1806, bebe de la Ilustración y del idealismo alemán y genera un sinnúmero de precursores de Clausewitz.

En esa época de transición entre la antigua forma militar y la Estrategia moderna destacan Von Bülow (paradigma de la aproximación geométrica) y el archiduque Carlos de Austria, el más grande de los rivales de Napoleón.

Pero todos ellos quedan eclipsados por dos figuras monumentales Jomini y Clausewitz. Ambos analizan con detalle las campañas de Napoleón y Federico el Grande, plasmando un estudio estratégico de tal naturaleza, que su validez, en la mayor parte de los aspectos, ha llegado hasta nuestros días y son obligados puntos de referencia.

El coronel suizo Henri Antoine de Jomini (1779-1869), sirvió en el Ejército francés en su campaña de Rusia (1812)[153], aunque sintiendo que sus actuaciones como jefe de Estado Mayor de Ney en la batalla de Bautzen (1813) no fueron debidamente reconocidas, ofreció sus servicios al zar, llegando a crear la Academia Militar rusa, haciéndose cargo en 1837 de la instrucción del gran duque heredero, para lo cual redactó su Compendio del arte de la guerra (1838)[154].

La principal inquietud de Jomini fue la de ofrecer definiciones y clasificaciones precisas con el objetivo de dotar a la Estrategia de personalidad científica[155]. Señala Shy que más que Clausewitz, Jomini se merece el título de fundador de la Estrategia moderna[156].

---

[153] SHY, John: "Jomini", en PARET, Peter: *Creadores de la Estrategia moderna: desde Maquiavelo a la era nuclear*, p. 157. Ministerio de Defensa. Madrid, 1992.

[154] MARTÍNEZ TEIXIDÓ, Antonio: *opus citada*, pp. 198-199.

[155] HITTLE, J. D.: *Jomini and his Summary of the Art of War*, p. 15. Military Service Publishing Company. Harrisburg, 1974.

[156] SHY, John: *opus citada*, pp. 158-159.

Jomini escribe que: "El arte de la guerra, en su acepción general, se divide en cinco ramas puramente militares: la estrategia, la táctica sublime, la logística, el arte del ingeniero y del artillero, de creciente importancia debido a los progresos de las ciencias implicadas y por último la táctica de detalle"[157].

Su trascendencia radica en que proporcionó una nueva nomenclatura estratégica, ligada a los teatros geográficos, creando un canevás estratégico de bases de operaciones, líneas de operaciones, puntos y frentes estratégicos, líneas de comunicaciones y objetivos que, unido a su principio fundamental del arte de la guerra: escoger y coordinar la maniobra que conduzca al punto decisivo, han constituido el fundamento en las concepciones estratégicas del siglo XIX[158].

Carl von Clausewitz (1780-1831) es el más conocido de todos los pensadores militares. Su obra maestra es: *De la guerra*, que se ha convertido en una referencia constante y obligada en la elaboración y comprensión de la Estrategia.

Clausewitz fue un hombre que tuvo una larga experiencia en la vida militar pero que no tuvo nunca el mando de grandes unidades. Escribió un gran número de trabajos históricos sobre las campañas de Turenne, de Federico II de Prusia y de la Revolución y el Imperio. Es a partir de esa base histórica que se lanza a la redacción de su obra magna. Ésta debía comprender tres libros: un tratado de gran guerra, o sea de Estrategia; un tratado sobre la guerra menor; y un tratado de Táctica. La muerte prematura de Clausewitz impidió la realización de este programa colosal.

A pesar de su amplitud, enfoque sistemático y estilo preciso: *De la guerra* no es una obra acabada[159]. *De la guerra* es un amplio compendio, en el que el autor pretende introducirse en lo más profundo de la guerra: en su naturaleza, en sus orígenes, para lo cual le da a su estudio un carácter más filosófico que práctico, buscando en todo

[157] JOMINI, Henri Antoine de: *Compendio del arte de la guerra*, p. 41. Ministerio de Defensa. Madrid, 1991.

[158] MARTÍNEZ TEIXIDÓ, Antonio: *opus citada*, p. 199.

[159] PARET, Peter: "La génesis de la guerra", en CLAUSEWITZ, Carl von: *De la guerra*, p. 25. Ministerio de Defensa. Madrid, 1999.

momento las raíces del "fenómeno guerra". Tal vez sea ésta la causa de la permanencia de sus agudas percepciones pues, contrariamente al camino seguido por otros tratadistas militares, que han estudiado la guerra más por sus efectos que por sus causas profundas, y a los que los avances tecnológicos y las nuevas normas políticas de convivencia han limitado en el tiempo sus teorías aparcando gradualmente la validez de sus conclusiones, Clausewitz se eleva al nivel filosófico del conocimiento buscando un concepto de la guerra que resulte omnicomprensivo y para ello recurre al método de crear una tesis, para inmediatamente enfrentarla a su antítesis.

Respecto a la excesiva carga filosófica achacada al método de Clausewitz, Brodie señala que la ligerísima infusión de metafísica de Clausewitz en su obra no plantea especiales dificultades. La mayor desgracia que se ha derivado de ello ha sido la reputación que se ha atribuido a Clausewitz, como alguien profundamente filosófico, en el sentido metafísico del término. Su coetáneo y rival Antoine Henri Jomini ya hizo comentarios parecidos sobre él, calificando también su obra de "excesiva y arrogante"[160].

Las campañas de 1793 y 1794 situaron a Clausewitz en el camino de reconocer la guerra como un fenómeno político. Las guerras, como todo el mundo sabía, se libraban por razones políticas o, por lo menos, siempre tenían consecuencias políticas. La consecuencia siguiente no era tan evidente. Si la guerra se dirigía al logro de un fin político, todo lo que formaba parte de ella (preparación social y económica, planeamiento estratégico, conducción de operaciones, uso de la violencia a todos los niveles) debería ser definido por este fin o, a menos, de acuerdo con él. La relación apropiada entre política y guerra ocupó a Clausewitz durante toda su vida[161].

Las aportaciones principales de Clausewitz se encuadran en la concepción profunda del fenómeno de la guerra como fenómeno extensivo de la política y en sus rasgos

[160] BRODIE, Bernard: "La permanente importancia de De la guerra", en CLAUSEWITZ, Carl von: *De la guerra*, p. 73. Ministerio de Defensa. Madrid, 1999.

[161] PARET, Peter: *opus citada*, p. 28. 1999.

filosóficos y psicológicos [162] . La descripción de conceptos como el azar, la incertidumbre, la fricción, la superioridad de medios en el combate, el centro de gravedad, la destrucción del enemigo, la fortaleza de la defensiva estratégica, su dialéctica con la ofensiva, el punto límite de la victoria, la moral como elemento más importante de la guerra, su trilogía de la guerra –pueblo, ejército y gobierno– y su justa armonía ante el acto bélico han sido recuperados por Occidente en la actualidad, constituyendo el legado de Clausewitz[163].

Clausewitz reconoció que la radical transformación de la escala y la naturaleza de la guerra en su tiempo fue debida a un fenómeno con cierta profundidad, la reciente participación de la ciudadanía como un nuevo actor en la política, una intervención que caracterizó la transición al concepto de estado nación[164].

No obstante, la influencia de Clausewitz ha tenido altibajos y aún no siempre fue bien entendido, en este sentido, la preponderancia de la política y la superioridad de la defensiva son ideas que frecuentemente fueron rechazadas. Desde el año 1971, tras el fracaso norteamericano en Vietnam, Clausewitz volvió a ser estudiado y forma parte de los planes de lección de las escuelas de estado mayor de todo el mundo[165].

Señala Rothenberg que dos grandes soldados, Helmuth von Moltke y Alfred von Schlieffen, predominaron en el pensamiento militar pruso-germánico desde la mitad del siglo XIX hasta la Primera Guerra Mundial e incluso más allá de ésta. Ellos enseñaron y practicaron un modo de guerra ofensiva que adaptaba los preceptos de

---

[162] HOWARD, Michael: "La influencia de Clausewitz", en CLAUSEWITZ, Carl von: *De la guerra*, pp. 51-52. Ministerio de Defensa. Madrid, 1999.

[163] MARTÍNEZ TEIXIDÓ, Antonio: *opus citada*, pp. 199-200.

[164] BEYERCHEN, Alan D.: "Clausewitz Nonlinearity, and the Importance of Imagery", en Complexity, Global Politics and National Security, pp. 155-156. Editado por David S. Alberts y Thomas J. Czerwinski. National Defense University, Washington D. C., 1997, En este muy original ensayo, Beyerchen apunta que Clausewitz fue el pionero que concibió la guerra de modo no lineal.

[165] Tras la traumática guerra de Vietnam se produce una nueva lectura de Clausewitz. DESPORTES, Vincent: "Vies et morts de Clausewitz aux Etats-Unis", en Défense Nationale, pp. 39 y 47. París, febrero 2002.

Napoleón a la era industrial, con el fin de buscar una decisión rápida a través de la batalla decisiva y destruir al enemigo en ella[166]

2.6. Del siglo XX a nuestros días

A principios del siglo XX aparecen tres hechos dignos de reseñar por su influencia en los conceptos estratégicos imperantes en la época: el nacimiento de la Geopolítica, la aparición de la Jeune Ecole y la Primera Guerra Mundial.

Nace la Geopolítica de la mano del alemán Ratzel con su tesis del "espacio vital", que influyó de manera notable en la mentalidad alemana de la Primera Guerra Mundial.

Tras Ratzel, el político y geógrafo inglés Halford John Mackinder, en 1904, lanza su teoría de la "tierra corazón", en la que se inclina por el poder terrestre en oposición a las ideas de Mahan, señalando que el poder se basa en el espacio geopolítico definido por el territorio continental, en el entendimiento que es la zona clave para conservar este poder y mantener el control de otros espacios geopolíticos adyacentes.

Esta región cardial o área pivote se define por Asia Central y Europa Oriental, y se encuentra rodeada de una franja intermedia donde se encuentran los ámbitos terrestre y marítimo. La teoría establece que en esa zona el poder terrestre tendría una mayor ventaja frente al dominio marítimo por su inaccesibilidad por mar, el aprovechamiento de los rápidos medios de comunicación terrestres y por la explotación de los recursos del área. Se afirma que el actor que lograra conquistarla sería una potencia mundial.

La escuela de Haushofer fue fiel seguidora de las ideas de Mackinder y, asimilando las ideas de Ratzel, dio impulso a la concepción estratégica alemana durante la Segunda Guerra Mundial.

Surge en esta época la teoría de la Jeune Ecole, defendida por un grupo de jóvenes oficiales franceses que se enfrenta a las ideas sostenidas por Mahan. La aparición del

[166] ROTHENBERG, Gunther E.: "Moltke, Schlieffen y la Doctrina del Envolvimiento Estratégico", en PARET, Peter: *Creadores de la Estrategia moderna: desde Maquiavelo a la era nuclear*, p. 313. Ministerio de Defensa. Madrid, 1992.

submarino y la utilidad del torpedo fueron la base de las teorías de este grupo, que pretendió echar por tierra las doctrinas tradicionales que defendían que el objetivo principal y racional de la guerra en la mar era la fuerza organizada enemiga.

La Primera Guerra Mundial, hizo que los acontecimientos tomaran un curso no previsto por los pensadores de finales del siglo XIX. Por un lado, se dedujo precipitadamente que la industrialización haría que la guerra se acabase como tal, debido a los valores prácticos y morales. Por otro lado, aquellos que aún admitían la vigencia de la guerra, estaban convencidos de que un conflicto "moderno" tendría que ser corto y decisivo, pues la compleja estructura de la sociedad industrial no podría soportar las interrupciones e impactos sociales de una guerra prolongada. Es decir; se pensaba en la línea de acción estratégica más rápida antes que en la más segura. Pero la guerra no desapareció en el siglo XX, ni se desarrolló en el sentido de acciones decisivas rápidas, ni la sociedad industrial se descompuso bajo la prolongada interrupción de sus procesos normales de producción.

Durante el periodo de la Primera Gran Guerra, el pensamiento militar estuvo en gran parte dominado por figuras como Foch y Ludendorff. Las obras de Foch, especialmente sus: *Principios de la guerra*, fueron determinantes en la formación del pensamiento militar francés previo a la guerra. Aunque el desarrollo del conflicto pareció restarles valor, el prestigio alcanzado por Foch en la fase final del mismo y su victoria final rehabilitaron la obra. No obstante, tras la guerra, el modelo que proponía Foch, basado en la acción ofensiva y la superioridad de los valores morales, se vio muy atemperado por la terrible experiencia en los campos de batalla, volviéndose a la defensiva como una fase importante del combate. Con el tiempo, esta actitud más tibia se acentuaría dentro del Ejército francés, llevando finalmente a la construcción de la línea Maginot.

En cuanto a Ludendorff, su habilidad como estratega y sus escritos posteriores al conflicto, especialmente sus Memorias, influirían de forma importante en el posterior pensamiento militar y político de Alemania. Sus ideas acerca del carácter total y trascendente de la guerra, como mejor muestra de la vitalidad de una sociedad, serían

recogidas por el nazismo, que, sin embargo, no compartiría su teoría acerca de la supremacía de lo militar sobre lo político.

Esta auténtica guerra industrial fue distinta de las que podríamos llamar guerras preindustriales de Napoleón, Clausewitz o Mahan. En el año 1914 las grandes potencias adoptan la ofensiva en un esfuerzo que acaba siendo de toda la nación, sufriendo grandes pérdidas. La guerra no es ya simplemente un conflicto entre elementos profesionales en lucha, sino el esfuerzo supremo de todos.

Del periodo entre guerras hay que destacar las tres escuelas de pensamiento que se generan: la primera, trata de reemplazar la parálisis estratégica a la que condujo el desarrollo de la Primera Guerra Mundial, sus doctrinas defienden la movilidad de la ofensiva y el ataque por sorpresa, siendo su máximo representante Liddell Hart; la segunda, pretende demostrar la eficacia de los medios propagandísticos y la subversión como medida previa a los combates decisivos, siendo los nazis los verdaderos maestros en su aplicación; la tercera y última, responde a las teorías que destacan el gran potencial del "poder aéreo" hasta el punto de reducir las operaciones bélicas a ataques contra la población civil del enemigo, su pensador más representativo es el general italiano Giulio Douhet[167].

La teoría de Liddell Hart, al contrario que Douhet, se opone a la guerra total y pretende limitar la guerra por medios políticos, y devolverle su carácter decisivo mediante la movilidad y la sorpresa. La idea clave de los escritos de Liddell Hart es el concepto de "estrategia indirecta". El autor entiende por tal la persecución del objetivo político sin encaminarse incondicionalmente hacia enfrentamientos sangrientos, abarcando los medios de esta estrategia no solamente los militares y diplomáticos sino las fuerzas económicas, tecnológicas y psicológicas del Estado. Tampoco creía que el "poder

[167] MACISAAC, David: "Voces desde el azul del cielo: los teóricos del poder aéreo", en PETER, Paret: *Creadores de la Estrategia moderna: desde Maquiavelo a la era nuclear*, p. 643. Ministerio de Defensa. Madrid, 1992.

aéreo" pudiera inclinar la balanza a favor del atacante[168]. El objetivo de la guerra no puede ser la victoria decisiva y absoluta sino asegurar la continuación de la política en tiempo de paz en el plazo más breve posible[169].

Tras la Segunda Guerra Mundial, la evolución del pensamiento estratégico gira alrededor de la preponderancia de las dos superpotencias y de la constitución de los dos grandes bloques, siendo la aparición del arma nuclear factor determinante en dicha evolución.

Del lado francés, el general André Beaufre (1902-1975) cobra especial protagonismo en el diseño del pensamiento estratégico. Su obra recoge una trilogía muy aplaudida que incluye: *Introducción a la Estrategia; Disuasión y Estrategia*; y *Estrategia de la acción*, todas ellas de la década de los sesenta. A él se debe la división de la Estrategia en diferentes niveles de decisión, desde el político al operativo, en lo que se conoce como "pirámide estratégica". Beaufre se mueve entre la Estrategia convencional, la revolucionaria y la nuclear, recomendando para esta última la disuasión multilateral, esto es, la disuasión concertada entre Estados Unidos y Europa[170].

En Estados Unidos destaca John M. Collins (1921), coronel estadounidense que ha alternado su experiencia en operaciones con las de tratadista, educador y asesor presidencial. Merece un puesto relevante entre los tratadistas gracias a una obra de amplia difusión y marcado interés divulgativo: *La gran estrategia. Principios y prácticas* (1973). Como él mismo señala, una de sus intenciones es proporcionar a los ciudadanos elementos de reflexión y criterios para la comprensión de los temas de defensa. En consecuencia, la obra abarca aspectos muy diversos de la Estrategia, desde la evolución del pensamiento hasta su encuadramiento y la naturaleza de la guerra para, posteriormente, centrarse en las características de la estrategia contemporánea estadounidense, diferenciando la Estrategia Nacional, la "gran

[168] BOND, Brian y ALEXANDER, Martin: "Liddell Hart y De Gaulle: las doctrinas de los recursos limitados y de la defensa móvil", en PARET, Peter: *Creadores de la Estrategia moderna: desde Maquiavelo a la era nuclear*, p. 627. Ministerio de Defensa. Madrid, 1992.

[169] BAHNEMANN, Jorg: *opus citada*, p. 18.

[170] MARTÍNEZ TEIXIDÓ, Antonio: *opus citada*, p. 529.

estrategia" y la Estrategia Militar. Las ideas principales de Collins han versado sobre el enfoque de la Seguridad Nacional como elemento central de la Estrategia, así como el uso de una matriz estratégica, en la que intervienen como ingredientes los fines, medios, amenazas y alianzas, para elaborar la "gran estrategia", esto es, el uso del poder nacional para conseguir los objetivos de la Seguridad Nacional[171].

Alvin y Heidi Toffler, escritores ampliamente reconocidos en el ámbito de la prospectiva, han desarrollado teorías que han influido en la evolución de la Estrategia y la Doctrina Militar estadounidense. Entre sus obras pueden destacarse: *El shock del futuro* (1970), obra en la que advierten sobre el shock de su advenimiento y los menores tiempos de reacción; *La tercera ola* (1980), dedicada a la ola de la información; *El cambio del poder* (1990), en el que argumentan el trasvase del poder desde el dinero al conocimiento; *Las guerras del futuro* (1993), donde reflexionan sobre la tipología de guerras que traerá la nueva ola y *Creando una nueva civilización* (1995). Su éxito radica en lo sugestivo de su planteamiento y la sencillez de su exposición. Ante la proximidad del Tercer Milenio, el matrimonio Toffler reflexiona sobre la "antiguerra", entendida como el establecimiento de estrategias que faciliten la paz. Los Toffler opinan que la humanidad ha vivido unas transiciones críticas que han llevado a la creación de nuevas civilizaciones. La primera ola ligada a la agricultura, la segunda a la revolución industrial y la tercera a la información. Cada una de estas olas lleva asociada un tipo determinado de guerra[172].

Edward N. Luttwak, nació en Transilvania en 1942. Ha sido asesor del Consejo de Seguridad Nacional y del Departamento de Defensa. Luttwak ha creado un modelo sugestivo de estrategia, contrastándolo con esquemas y acontecimientos históricos. Entre sus obras se encuentran *Diccionario de la Guerra Moderna* (1971); *La gran estrategia del Imperio Romano* (1976); *La gran estrategia de la Unión Soviética* (1983), *Estrategia, la lógica de la guerra y de la paz* (1987) y *Érase una vez el sueño americano* (1994). Concibe la estrategia en cinco niveles: el técnico, el táctico (el elemento

[171] *Ibídem*, p. 530.

[172] Véase FRANCO SUANCES, F. Javier en *Las ideas estratégicas para el inicio del Tercer Milenio*, pp. 207-218.

humano del combate), el operacional (relacionado con la conducción de operaciones militares), el de teatro (que define la relación fuerza militar-territorio) y finalmente el nivel de la "gran estrategia", la de los resultados finales. Estos niveles interactúan entre sí y también de forma horizontal en la lucha con los contrarios[173].

Zbigniew Brzezinski nació en Varsovia en 1928 y fue consejero de Seguridad Nacional del presidente Carter (1977-1981). Su pensamiento ha influido de forma notoria en la cúpula política y diplomática de Estados Unidos. Durante la guerra fría destacó como uno de los sovietólogos más notables con obras como: *Political Power: USA-USSR* (1964); *Africa and the Communist World* (1963); *Soviet Bloc Unity and Conflict* (1967) y *Ideology & Power in Soviet Politics* (1976). En otras obras fue ensanchando el horizonte de sus estudios estratégicos: *The Fragil Blossom*; *Grises and Change in Japan* (1972) y *Between Two Ages* (1976).

Tras su experiencia como asesor presidencial, en *Power and Principie* (1983) recogió las memorias de los acontecimientos de los que él había sido testigo y expuso interesantes reflexiones sobre el papel de Estados Unidos en el mundo. En su obra: *Game Plan* (1986) trató con gran acierto los interrogantes que se planteaban tras la elección de Gorbachov como nuevo líder soviético. Su libro: *The Birth and Death of Communism* in the 20th Century (1990) fue ampliamente difundido. En *The Grand Failure* (1989) y *Out of Control* (1993) analiza momentos clave en la crisis rusa. Su obra *The Grand Chessboard*, (El gran tablero de ajedrez) define las líneas maestras de la política exterior norteamericana que pueden permitir a Estados Unidos seguir actuando como único gran árbitro global de las relaciones internacionales, además de mostrar lo esencial del liderazgo estadounidense para la paz mundial[174].

Francis Fukuyama nació en el seno de una familia de origen japonés en 1952, en Chicago, licenciándose en Harvard. Durante su carrera escribió sobre democratización y política económica internacional, especializándose en la política exterior de la

[173] Véase ROMERO SERRANO, José M.ª: en *Las ideas estratégicas para el inicio del Tercer Milenio*, pp. 147-154. Véase MARTÍNEZ TEIXIDÓ, Antonio: *opus citada*, pp. 558-559.

[174] Véase PARDO DE SANTAYANA GÓMEZ DE OLEA, José M.ª en *Las ideas estratégicas para el inicio del Tercer Milenio*, pp. 249-256.

antigua Unión Soviética. También trabajó para el Departamento de Estado de Estados Unidos. En 1989, Fukuyama escribió un artículo llamado "El fin de la Historia", que luego dio origen al libro: *El fin de la Historia y el último hombre*, donde se afirmaba que la caída del comunismo y el triunfo de las democracias liberales marcaban el comienzo de la etapa final en la que no había más lugar para largas batallas ideológicas. En este sentido, la Historia habría terminado. Para el politólogo norteamericano la democracia liberal es la forma ideal de gobierno, la etapa final de la historia. Fukuyama hace notar que los países que pudieron obtener un alto nivel de desarrollo industrial como Estados Unidos, Japón o Europa Occidental, son los que lograron generar democracias estables, lo que sugeriría que existe una correlación entre el desarrollo económico de un país y la capacidad de sostener esos sistemas representativos[175].

Samuel P. Huntington es un prestigioso politólogo nacido en Estados Unidos en 1927. Formó parte del Consejo de Seguridad Nacional de la Casa Blanca entre 1977 y 1978. En la actualidad es profesor de Ciencias Políticas en la Universidad de Harvard. Huntington ha trazado una brillante línea de pensamiento expuesta en sus principales obras: *El orden político en las sociedades en cambio* (1968), considera que las causas de la violencia e inestabilidad en los países en vías de desarrollo radican en el retraso del surgimiento de las instituciones políticas apropiadas para permitir el cambio social y económico; *La tercera ola* (1991), donde analiza las causas y la naturaleza de las transiciones democráticas ocurridas entre 1974 y 1990, evalúa las posibilidades de estabilidad de estos regímenes y explora las perspectivas de otros países con respecto al mismo tema. Su conclusión es que estas transiciones constituyen la tercera ola de la democratización del mundo moderno, después de otras dos a las que siguieron movimientos de reflujo que devolvieron a los países en cuestión a un gobierno autoritario; y, finalmente: *El choque de civilizaciones* (1997), libro que lo ha llevado a la primera línea del debate intelectual a nivel mundial, con el que dio un vuelco a la teoría política al afirmar que los conflictos mundiales volverían probablemente a las viejas guerras arraigadas en la cultura. El choque de civilizaciones dominará la política

[175] Véase HUESO GARCÍA, Vicente en *Las ideas estratégicas para el inicio del Tercer Milenio*, pp. 197-205.

a escala mundial; las líneas divisorias entre las civilizaciones serán los frentes de batalla del futuro. Huntington afirmó que los conflictos entre civilizaciones definirían el futuro. Por otra parte, Huntington sostiene que la civilización occidental, incluyendo Estados Unidos, está declinando, en detrimento del alza de otras civilizaciones. Esta teoría quedó demostrada, según Huntington, con los ataques terroristas del 11 de septiembre de 2001[176].

Respecto al pensamiento estratégico en Iberoamérica, es de destacar el elevado interés de la obra: *Pensamiento y pensadores militares iberoamericanos del siglo XX y su influencia en la Comunidad Iberoamericana*[177], que recoge las ricas reflexiones que en algunos casos arrancan de pensadores del siglo XIX.

Conclusiones del Capítulo 2.

Tras examinar en el primer capítulo la evolución de los incidentes de ciberseguridad en España en el periodo comprendido entre 2011 y 2015 e identificar las tendencias de las agresiones, se ha considerado oportuno mostrar en el presente capítulo un resumen de la historia del pensamiento estratégico.

Mediante este breve recorrido por la evolución del pensamiento estratégico se ha tratado de presentar a los principales autores y sus teorías en su contexto histórico, político y social. El objetivo no ha consistido en realizar una exposición exhaustiva de todos y cada uno de los pensadores, sus ideas o sus escuelas. Más bien, se ha ofrecido un recorrido por los principales hitos, corrientes y tendencias con el fin de permitir la obtención de una visión general y coherente de los avances más notables en el campo del pensamiento estratégico a lo largo de la historia, procurando proporcionar las referencias documentales que permitirán al eventual lector profundizar en los temas que aquí se han expuesto.

[176] HUESO GARCÍA, Vicente: *opus citada*, pp. 239-247.

[177] Obra dirigida por QUESADA GÓMEZ, Agustín: "Pensamiento y pensadores militares Iberoamericanos del siglo XX y su influencia en la Comunidad Iberoamericana", Monografía del CESEDEN número 63. Ministerio de Defensa. Madrid, 2003.

Puede observarse que el pensamiento estratégico evoluciona al compás de los conflictos que asolan los diferentes pueblos de la tierra, y que en el proceso de evolución se han fusionado elementos culturales muy variados: sociales, políticos, económicos y religiosos, entre otros, combinados con determinadas circunstancias geoestratégicas. Asimismo, puede constatarse que los distintos sistemas de pensamiento estratégico que se han generado adquieren cada vez mayor complejidad en correspondencia con los diferentes adelantos tecnológicos, y es preciso reconocer que la nueva situación planteada en el siglo XXI en el campo de la ciberseguridad, que es el tema que motiva la realización de la presente tesis doctoral, no puede ser abordada apropiadamente sino es en un contexto amplio y universal.

Como se podrá comprobar a través de la lectura de los distintos capítulos que siguen a esta introducción histórica, no parece que sea recomendable abandonar el estudio de la historia del pensamiento estratégico si se pretende entender la realidad del pensamiento estratégico actual en las diferentes naciones y explorar las vías más apropiadas para elaborar planes estratégicos de seguridad nacional.

A continuación se expondrá un análisis de las más recientes estrategias nacionales de seguridad de tres de los actores fundamentales en el panorama geopolítico internacional: los Estados Unidos, la República Popular de China y la Federación de Rusia. La finalidad principal de este análisis consistirá en discutir los tres modelos propuestos para poder comprobar de este modo la viabilidad de una eventual adaptación de algunos de sus elementos básicos.

CAPÍTULO 3. LAS ESTRATEGIAS NACIONALES DE SEGURIDAD

Las diferentes corrientes que han ido conformado el pensamiento estratégico han influido en la definición de las distintas políticas de seguridad. De este modo, las sociedades han incorporado este acervo, adaptándolo tanto a su situación geopolítica como a elementos coyunturales.

El acceso al pensamiento estratégico se ha vuelto más fluido en la actualidad. Esta situación se ha producido por un cambio de paradigma en la mentalidad de las sociedades, especialmente en las más abiertas de cara a la opinión pública. Este impulso para facilitar el conocimiento de asuntos estratégicos se ha visto muy favorecido por las capacidades de acceso a la información que permite la tecnología. Lo que en ocasiones, a lo largo de la historia, ha estado oculto al público y se ha limitado su acceso al círculo más íntimo del poder o a élites de las diferentes sociedades ha cobrado un protagonismo público.

Tradicionalmente los pueblos, las naciones y los Estados debían establecer las políticas, estrategias, estructuras y mecanismos para asegurar unos niveles de protección que les permitieran sobrevivir y tener un grado de autonomía suficiente para poder progresar. Podría considerarse que la historia de la humanidad es una lucha de voluntades que tratan de favorecer sus criterios, lo que habitualmente genera fricciones, cuando no colisiones directas.

En este espíritu de favorecer los intereses propios en un entorno a veces muy hostil, el pensamiento estratégico propio ha sido protegido, salvo en lo que pudiera generar una capacidad de influencia y favorecer la dominación. De otra parte, en diferentes épocas ha existido una permeabilidad mayor en el intercambio de las ideas estratégicas, lo que ha generado un conocimiento més profundo de las diferentes posibilidades de incorporar aquellas ideas que favorecieron los intereses propios.

La conformación del Estado-nación ligada a la Paz de Westfalia (1648) conformada en los tratados de paz de Osnabrück y Münster, al final de la guerra de los Treinta Años en Alemania y la de los Ochenta Años entre España y los Países Bajos, pone fin al sistema feudal y genera un nuevo orden basado en la soberanía nacional y que reconoce la integridad territorial como fundamento de la existencia de los Estados.

Ya se ha expuesto el impacto que tuvo para el pensamiento estratégico este nuevo orden y la conformación de actores que a partir de este momento incorporaran estas ideas estratégicas en un nuevo marco de relación geopolítico.

Tras los diferentes conflictos bélicos, en especial tras las dos Guerras Mundiales y el periodo de la tensión entre bloques, los Estados han ido conformando un corpus de seguridad inspirado en las diferentes corrientes del pensamiento estratégico expresadas anteriormente.

Solo muy recientemente estos flujos de pensamiento geoestratégicos han devenido en la creación de estrategias de seguridad nacional propiamente dichas, en un proceso de confección de estos documentos liderado por Estados Unidos.

Tras la articulación del sistema de estrategias de seguridad nacional de Estados Unidos, otros Estados, y también algunas organizaciones internacionales, han desarrollado sus propias estrategias de seguridad, inspirándose en las diferentes corrientes del pensamiento estratégico, en su entorno geopolítico, en sus capacidades y también en las circunstancias del momento, para conformar sus modelos de estrategia de seguridad nacional.

A continuación, se van a presentar algunas de las estrategias de seguridad, nacionales e internacionales, y sus estructuras nacionales de seguridad. significando que no se pretende analizar de modo exhaustivo todo el abanico de estrategias existentes, que no es el objeto del estudio. Se van a presentar los modelos más significativos, en los que se inspiran muchas otras estrategias nacionales de seguridad, para identificar aquellos elementos que han servido para articular los sistemas de seguridad nacional

por medio de las estrategias nacionales y así poder incorporar en la cadena de planeamiento estratégico las estrategias nacionales de ciberseguridad.

Se van a presentar las estrategias y los modelos nacionales de seguridad de Estados Unidos, China y Rusia, por ofrecer elementos significativos en sí mismos para estas potencias, pero también porque han inspirado otras numerosas estrategias nacionales de seguridad y modelos de organización.

3.1. ESTADOS UNIDOS DE AMÉRICA

3.1.1. La generación del sistema de estrategias nacionales de seguridad

La génesis de la generación del sistema de estrategias nacionales de seguridad arranca en Estados Unidos de América, en un escenario de debate político interno sobre el modelo de las Fuerzas Armadas estadounidenses y su estructura de mando.

De 1982 a 1986, los Comités de las Fuerzas Armadas del Congreso y del Senado estadounidenses estuvieron debatiendo una estructura militar más adecuada y un más eficiente modelo de organización de la cadena de mando. El resultado de este proceso dio lugar al Acta Goldwater-Nichols[178], que tomó el nombre del Senador Barry Goldwater y del Congresista William Flynt Nichols y fue firmada por el Presidente de Estados Unidos Ronald Reagan el uno de octubre de 1986[179].

Esta pieza legislativa abordó la necesidad de incorporar una más eficiente estructura que permitiera solucionar los problemas causados por la rivalidad entre los distintos servicios que había surgido durante la guerra de Vietnam, y que se evidenció

[178] Acta Goldwater-Nichols de reorganización del Departamento de Defensa. Public Law. pp. 99-433. 1 de octubre de 1986. http://history.defense.gov/Portals/70/Documents/dod_reforms/Goldwater-NicholsDoDReordAct1986.pdf consulta 3 de agosto de 2015.

[179] REAGAN, Ronald: Intervención en la firma del Acta Goldwater-Nichols de reorganización del Departamento de Defensa. 1 de octubre de 1986. http://www.reagan.utexas.edu/archives/speeches/1986/100186e.htm consulta 3 de agosto de 2015.

posteriormente en la fallida misión de rescate de los rehenes en Irán en 1980, así como en la invasión de Granada en 1983[180].

El Acta Goldwater-Nichols se considera el mayor cambio legislativo que afecta a la seguridad nacional de Estados Unidos desde la aprobación del Acta de Seguridad Nacional de 1947, por la que se creó el Departamento de Defensa, el Consejo Nacional de Seguridad, la Agencia Central de Inteligencia y la Junta de Jefes de Estado Mayor. Tras modificaciones menores del Acta de Seguridad Nacional en 1949 y la Ley de Reorganización de 1958, que reforzaron la autoridad del Secretario de Defensa y el papel del Jefe de la Junta de Jefes de Estado Mayor respectivamente[181].

El Acta Goldwater-Nichols introdujo además un elemento que no estaba previsto en el diseño de las responsabilidades a los Comités de las Fuerzas Armadas del Congreso y del Senado. El Acta modificó el Código de Estados Unidos para solicitar al Presidente de Estados Unidos de América una estrategia de seguridad nacional[182]:

> 50 USC § 404A - Informe Anual de la Estrategia de Seguridad Nacional
>
> (a) Remisión al Congreso
>
> (1) El presidente remitirá al Congreso cada año, un informe completo sobre la estrategia de seguridad nacional de los Estados Unidos (en adelante, en esta sección se refiere como un "informe sobre la estrategia de seguridad nacional").
>
> (2) El informe nacional de la estrategia de seguridad para cualquier año se presentará en la fecha en que el Presidente presenta al Congreso el presupuesto para el próximo año fiscal bajo la sección 1105 del título 31[183].
>
> (3) No más tarde de 150 días después de la fecha en que un nuevo presidente asuma el cargo, el presidente remitirá al Congreso un informe nacional sobre la estrategia de seguridad según lo establecido en esta sección. Ese informe

[180]COLE, Ronald H.: *Grenada, Panama and Haiti: join operational reform*. Joint Force Quaterly. Otoño-invierno 1988-1989. http://www.dtic.mil/dtic/tr/fulltext/u2/a422959.pdf consulta 3 de agosto de 2015.

[181] WILSON, Charles A.: *Goldwater-Nichols. The next evolution reorganizing the Joint Chiefs of Staff.*U.S. Army War College, Carlisle Barracks, PA 17013-5050. 2002.

handle.dtic.mil/100.2/ADA404408 consulta 3 de agosto de 2015.

[182] Código de Estados Unidos. 50 USC § 404A – *Annual National Security Strategy Report.* National Security Strategy Archive. http://nssarchive.us/50-usc-%C2%A7-404a-annual-national-security-strategy-report/ consulta 3 de agosto de 2015.

[183] Código de Estados Unidos. 31 § 1105 - *Budget contents and submission to Congress.* Cornell University Law School. https://www.law.cornell.edu/uscode/text/31/1105 consulta 3 de agosto de 2015.

será adicional al informe para ese año presentado en el momento especificado en el párrafo (2).

(b) Contenido

Cada informe de estrategia de seguridad nacional deberá establecer la estrategia de seguridad nacional de los Estados Unidos y deberá incluir una descripción completa y la discusión de lo siguiente:

(1) Los intereses globales en el mundo, metas y objetivos de los Estados Unidos que son vitales para la seguridad nacional de los Estados Unidos.

(2) La política exterior, los compromisos internacionales y las capacidades de defensa nacional de los Estados Unidos necesarios para disuadir la agresión y para poner en práctica la estrategia de seguridad nacional de los Estados Unidos.

(3) Las propuestas a corto y largo plazo que se proponen para la utilización de los elementos políticos, económicos, militares y otros del poder nacional de los Estados Unidos para proteger o promover los intereses y lograr las metas y los objetivos mencionados en el párrafo (1).

(4) La adecuación de las capacidades de los Estados Unidos para llevar a cabo la estrategia de seguridad nacional de los Estados Unidos, incluyendo una evaluación del equilibrio entre las capacidades de todos los elementos del poder nacional de los Estados Unidos para apoyar la aplicación de la estrategia de seguridad nacional.

(5) Cualquier otra información que puede ser necesaria para facilitar la información al Congreso sobre las cuestiones relativas a la estrategia de seguridad nacional de los Estados Unidos.

(c) Modo de Clasificación

Cada informe de estrategia de seguridad nacional se presentará en modo clasificado y también no clasificado.

3.1.2. Las estrategias de seguridad nacional en Estados Unidos

Ronald Reagan fue el primer Presidente de Estados Unidos en presentar una estrategia de seguridad nacional en 1987[184].

Señala Snider, que dado que la legislación Goldwater-Nichols se aprobó a finales de 1986, la Estrategia de Seguridad Nacional de 1987 se preparó en un período muy limitado de tiempo y refleja fundamentalmente la intención de documentar la corriente estratégica de pensamiento dominante. En sus dos secciones principales, relativas a

[184] REAGAN, *Ronald: Estrategia de Seguridad Nacional de los Estados Unidos 1987*. Uudley Knox Library Naval postgraduate School Monterey, California 93943.5002. Ejemplar firmado por el Presidente Reagan.

http://history.defense.gov/Portals/70/Documents/nss/nss1987.pdf consulta 3 de agosto de 2015.

la política exterior y a la política de defensa, el documento refleja la fuerte orientación de la administración hacia el tipo de gobierno de gabinete del Presidente Reagan, así como una orientación casi exclusiva hacia los instrumentos militares. El documento retrata, eso sí, un enfoque estratégico integral hacia la Unión Soviética. Además, la sección sobre la integración de los elementos del poder se incardina en el "Sistema del Consejo Nacional de Seguridad"[185].

La Estrategia de Seguridad Nacional de 1988[186] se considera, por el citado Sinder, el primer documento con el carácter propio de una estrategia nacional. Este documento hizo hincapié en la importancia de la integración de todos los elementos del poder nacional, en particular el aspecto económico, a lo que contribuyó que este informe de 1988 fue escrito en el contexto de déficits importantes en el presupuesto federal y balanza comercial. A su vez, el documento dio lugar a la presentación de estrategias diferentes para las distintas regiones geográficas con una integración planificada de forma independiente de las herramientas de poder[187].

La definición de los elementos de poder nacional de esta Estrategia de Seguridad Nacional de 1988 son: ejemplo moral y político, fortaleza militar, vitalidad económica, alianzas, diplomacia pública, asistencia de seguridad a los aliados, ayuda al desarrollo, cooperación científica y tecnológica, diplomacia multilateral y participación en organizaciones internacionales, y mediación diplomática[188]. De un modo u otro, estos elementos han sido incorporados a otras ediciones de las sucesivas estrategias nacionales de seguridad estadounidenses y han inspirado la redacción de las estrategias nacionales de seguridad del mundo occidental.

---

[185] SNIDER, Don M.: *The National Security Strategy: Documenting Strategic Vision*. pp. 6-7. Segunda edición. Strategic Studies Institute, U.S. Army War College, Carlisle Barracks, PA 17013-5050, 1995 http://nssarchive.us/wp-content/uploads/2012/05/Snider.pdf consulta 3 de agosto de 2015.

[186] REAGAN, *Ronald: Estrategia de Seguridad Nacional de los Estados Unidos 1988*. http://nssarchive.us/NSSR/1988.pdf consulta 4 de agosto de 2015.

[187] SINDER, Don M.: *opus citada*, p. 7.

[188] REAGAN, *Ronald: Estrategia de Seguridad Nacional de los Estados Unidos 1988*. *opus citada*, pp. 7-8.

La relevancia del aspecto económico de esta **ESN** de 1998, ya mencionada, queda reflejada al señalar que “El poder nacional de Estados Unidos se fundamenta en la fuerza de nuestra

economía domestica. Una economía creciente, resistente y tecnológicamente vigorosa es vital para nuestra seguridad nacional. En tiempos de paz es la base fundamental de nuestras capacidades de defensa nacional. En una crisis o en tiempos de guerra proporciona la capacidad de responder rápidamente con personal cualificado, capacidad ampliada de producción y suministro de materiales críticos. La Primera y Segunda Guerras Mundiales demostraron la importancia vital de una fuerte economía nacional capaz de producir de forma rápida y eficiente los bienes necesarios para nuestra defensa y la de nuestros aliados”[189].

Pero probablemente lo más significativo de esta estrategia de 1988 sea el espíritu que impregnó la redacción del documento, cuando en el prefacio explica el Presidente Reagan: “Remito este informe con la confianza de que ayudará al Congreso y al pueblo estadounidense a comprender mejor nuestra estrategia de seguridad nacional y contribuir con el consenso necesario para que podamos cumplir con nuestras responsabilidades como líder del las democracias del mundo” [190]. Para lo que recomienda su lectura a todos los estadounidenses.

Este enfoque, al incentivar la lectura del documento donde se expone la visión estratégica de Estados Unidos, el papel que se quiere desarrollar en el mundo, la integración de todos los elementos nacionales en aras de la seguridad nacional, las amenazas que se sienten y las estrategias para contrarrestarlas, van a inspirar un modelo que será seguido años más tarde por gran parte de los países que desarrollaron sus estrategias nacionales de seguridad.

[189] *Ibídem*, p. 11.

[190] *Ibídem*, prefacio.

Posteriormente en Estados Unidos se han presentado otras estrategias de seguridad nacional, continuando, en gran medida, el esquema de la estrategia mencionada de 1988.

Figura 16: Estrategias de Seguridad Nacional de los Estados Unidos de América

Año	Presidente	Denominación de la Estrategia
2015	Barack Obama	National Security Strategy[191]
2010	Barack Obama	National Security Strategy[192]
2006	George W. Bush	The National Security Strategy of the United States of America[193]
2002	George W. Bush	The National Security Strategy of the United States of America[194]
2001	Bill Clinton	A National Security Strategy For A Global Age[195]
2000	Bill Clinton	A National Security Strategy For A New Century[196]
1998	Bill Clinton	A National Security Strategy For A New Century[197]
1997	Bill Clinton	A National Security Strategy For A New Century[198]
1996	Bill Clinton	A National Security Strategy of Engagement and Enlargement[199]
1995	Bill Clinton	A National Security Strategy of Engagement and Enlargement[200]

[191] Puede consultarse en: http://nssarchive.us/wp-content/uploads/2015/02/2015.pdf consulta 4 de agosto de 2015.

[192] Puede consultarse en: http://nssarchive.us/NSSR/2010.pdf consulta 4 de agosto de 2015.

[193] Puede consultarse en: http://nssarchive.us/NSSR/2006.pdf consulta 4 de agosto de 2015.

[194] Puede consultarse en: http://nssarchive.us/NSSR/2002.pdf consulta 4 de agosto de 2015.

[195] Puede consultarse en: http://nssarchive.us/NSSR/2001.pdf consulta 4 de agosto de 2015.

[196] Puede consultarse en: http://nssarchive.us/NSSR/2000.pdf consulta 4 de agosto de 2015.

[197] Puede consultarse en: http://nssarchive.us/NSSR/1998.pdf consulta 4 de agosto de 2015.

[198] Puede consultarse en: http://nssarchive.us/NSSR/1997.pdf consulta 4 de agosto de 2015.

[199] Puede consultarse en: http://nssarchive.us/NSSR/1996.pdf consulta 4 de agosto de 2015.

[200] Puede consultarse en: http://nssarchive.us/NSSR/1995.pdf consulta 4 de agosto de 2015.

1994	Bill Clinton	A National Security Strategy of Engagement and Enlargement[201]
1993	George H. W. Bush	National Security Strategy of the United States[202]
1991	George H. W. Bush	National Security Strategy of the United States[203]
1990	George H. W. Bush	National Security Strategy of the United States[204]
1988	Ronald Reagan	National Security Strategy of the United States[205]
1987	Ronald Reagan	National Security Strategy of the United States[206]

Fuente: National Security Strategy Archive[207].

Estas estrategias se han nutrido de diferentes corrientes de pensamiento estratégico, en especial de los autores clásicos. En este sentido, señala Karger que la estrategia no se puede formular en un vacío político o intelectual. Esta afirmación engarza con otro elemento que también apunta Karger en relación con lo expresado por Clausewitz respecto a la fricción, incorporando este concepto como la diferencia entre la estrategia ideal y la aplicada; de este modo la fricción es una consecuencia natural de la caótica y compleja naturaleza del entorno estratégico que no puede ser eliminada, pero puede ser entendida y utilizada en mayor o menor medida en la formulación de la estrategia[208].

Yarger también señala la integración de la estrategia de seguridad nacional en un entorno estratégico global, en el que conviven los intereses nacionales con las estrategias de los diversos niveles, donde están incorporados los elementos de

[201] Puede consultarse en: http://nssarchive.us/NSSR/1994.pdf consulta 4 de agosto de 2015.

[202] Puede consultarse en: http://nssarchive.us/NSSR/1993.pdf consulta 4 de agosto de 2015.

[203] Puede consultarse en: http://nssarchive.us/NSSR/1991.pdf consulta 4 de agosto de 2015.

[204] Puede consultarse en: http://nssarchive.us/national-security-strategy-1990/ consulta 3 de agosto de 2015.

[205] Puede consultarse en: http://nssarchive.us/NSSR/1988.pdf consulta 3 de agosto de 2015.

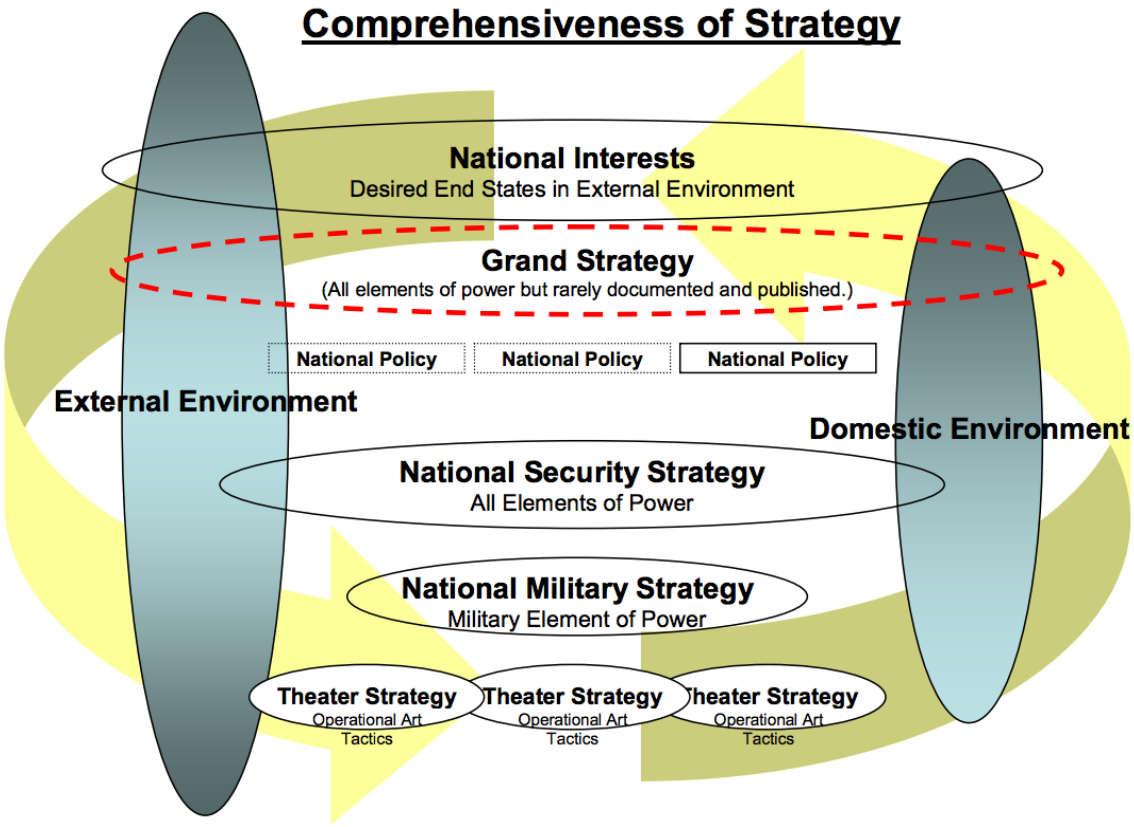
[206] Puede consultarse en: http://nssarchive.us/NSSR/1987.pdf consulta 3 de agosto de 2015.

[207] National Security Strategy Archive. http://nssarchive.us/ consulta 4 de agosto de 2015.

[208] YARGER, Harry R.: *Strategic theory for the 21st Century: The little book on big strategy.* pp. 9-10. Strategic Studies Institute, U.S. Army War College,Carlisle, PA 17013-5244, febrero 2006. http://www.comw.org/qdr/fulltext/0602yarger.pdf consulta: 4 de agosto de 2015.

poder, tanto en un entorno externo como local, según se muestra en la siguiente figura:

Figura 17: La Estrategia de Seguridad Nacional en el entorno estratégico global



Fuente: YARGER, Harry R.[209].

En este sentido se pronuncia también la Estrategia de Seguridad Nacional de 2015 de Barack Obama, al señalar la importancia de integrar todos los instrumentos de poder de Estados Unidos, señalando la mayor capacidad de influencia a través de la combinación de las ventajas estratégicas. Además del valor de las fuerzas armadas y la diplomacia, Obama señala la trascendencia de contar con una economía fuerte y bien regulada para promover el comercio y la inversión, a la vez que se protege el

[209] *Ibídem*. p. 9.

sistema financiero internacional. La calidad de la obtención, análisis y producción de inteligencia, junto con el respeto a la ley, la ciencia, la tecnología, y las relaciones interpersonales, maximizarán los efectos estratégicos del poder nacional[210].

Apunta Al-Rodhan que el diseño de la estrategia se encuentra ligada a la cultura estratégica de un país determinado, tiene numerosas fuentes y está obligada a comportarse de modo elástico, incorporando los diversos factores que influyen en la formación de la cultura nacional, el pensamiento estratégico y la política de seguridad. Algunos principios esenciales se pueden extraer de los encuadres teóricos de la cultura estratégica. Factores como la geopolítica, normas y costumbres, percepciones de los roles regionales e internacionales, los sistemas políticos y el reparto del poder se solidifican en la memoria colectiva y la identidad a través de las narraciones políticas, los programas de educación, representaciones artísticas y populares de episodios históricos o interpretaciones de los recuerdos comunes[211].

En este sentido, el diseño de las estrategias de seguridad nacionales en Estados Unidos se encuentra impregnado de los pensadores mencionados cuando se trató la evolución del pensamiento estratégico, en especial por Clausewitz y más recientemente por los Toffler, Luttwak, Brzezinski, Fukuyama y Huntington.

3.1.3. La estructura de seguridad nacional en Estados Unidos

El Consejo Nacional de Seguridad es el principal foro del Presidente para examinar las cuestiones de seguridad y política exterior nacional con sus principales asesores de seguridad nacional y funcionarios del gabinete. Desde su creación bajo la presidencia de Truman, la función del Consejo ha sido la de asesorar y asistir al Presidente en la seguridad nacional y la política exterior. El Consejo también sirve como brazo principal del Presidente de la coordinación de estas políticas entre los

[210] OBAMA, Barack: *Estrategia de Seguridad Nacional 2015*. p. 4. http://nssarchive.us/NSSR/1997.pdf consulta 4 de agosto de 2015.

[211] AL-RODHAN, Nayef: Strategic Culture and Pragmatic National Interest. Global Policy, 22 de julio de 2015. http://www.globalpolicyjournal.com/blog/22/07/2015/strategic-culture-and-pragmatic-national-interest consulta: 4 de agosto de 2015.

diversos organismos gubernamentales. El Consejo de Seguridad Nacional está presidido por el Presidente. Sus componentes son el Vicepresidente, el Secretario de Estado, el Secretario de Hacienda, el Secretario de Defensa y el Asistente del Presidente para Asuntos de Seguridad Nacional. El Jefe de la Junta de Jefes de Estado Mayor es el consejero militar y el Director de Inteligencia Nacional es el asesor de inteligencia. El Jefe de Gabinete del Presidente, los Asesores del Presidente y el Asistente del Presidente para la Política Económica están invitados a asistir a cualquier reunión del Consejo. Los directores de otros departamentos y agencias, así como otros altos funcionarios, están invitados a asistir a las reuniones del Consejo de Seguridad Nacional cuando sea apropiado[212].

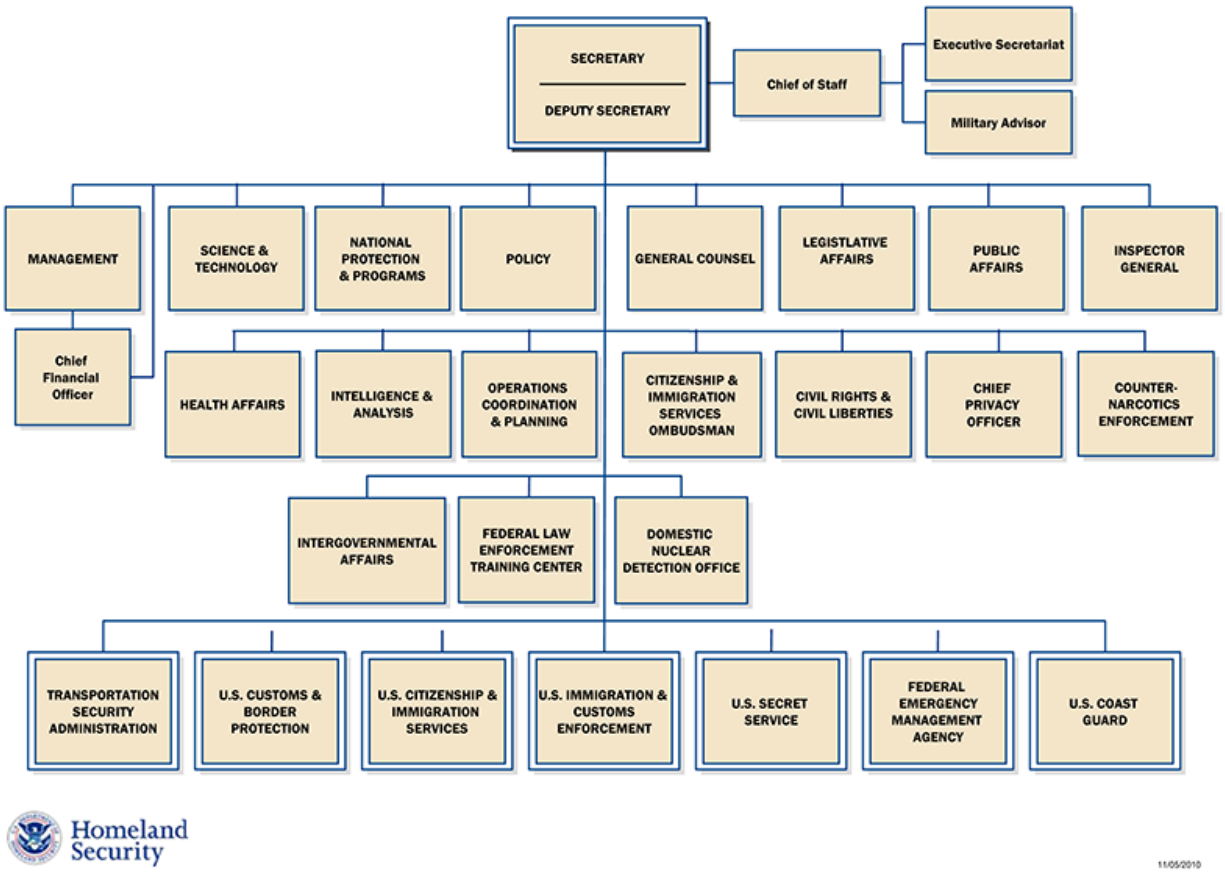
La creación del Departamento de Seguridad Nacional (Department of Homeland Security), tras los atentados terroristas del 11 de septiembre de 2011 en Estados Unidos[213], introdujo un nuevo elemento en el proceso de integración de las estrategias de seguridad en diferentes niveles de la Administración de Estados Unidos. Las misiones del Departamento de Seguridad Nacional incluyen la prevención del terrorismo y la mejora de los niveles de seguridad; la gestión de las fronteras; la administración de las leyes de inmigración; la protección del ciberespacio; y la garantía de la capacidad de recuperación ante desastres[214].

[212] El Consejo de Seguridad Nacional fue establecido por el Acta de Seguridad Nacional de 1947 (PL 235-61 Stat 496;. USC 402), modificada por las Enmiendas a la Ley de Seguridad Nacional de 1949 (. 63 Stat 579; 50 USC 401 y ss.). Más tarde, en 1949, como parte del Plan de Reorganización, el Consejo fue colocado en la Oficina Ejecutiva del Presidente.
https://www.whitehouse.gov/administration/eop/nsc/ consulta 3 de agosto de 2015.

[213] Public Law 107–296, 107th Congress, 25 de noviembre de 2002
http://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf consulta: 6 de agosto de 2015.

[214] Sitio web oficial del Departamento de Seguridad Nacional http://www.dhs.gov/mission consulta: 6 de agosto de 2015.

Figura 18: Estructura del Departamento de Seguridad Nacional de Estados Unidos



Fuente: Departamento de Seguridad Nacional de Estados Unidos.[215]

El encaje de esta nueva estructura en el sistema de seguridad nacional aconsejó al **Presidente** Obama solicitar, en febrero de 2009, un estudio de armonización de las responsabilidades del personal del Consejo Nacional de Seguridad y del

[215] Sitio web oficial del Departamento de Seguridad Nacional. http://www.dhs.gov/xlibrary/photos/orgchart-web.png consulta: 6 de agosto de 2015.

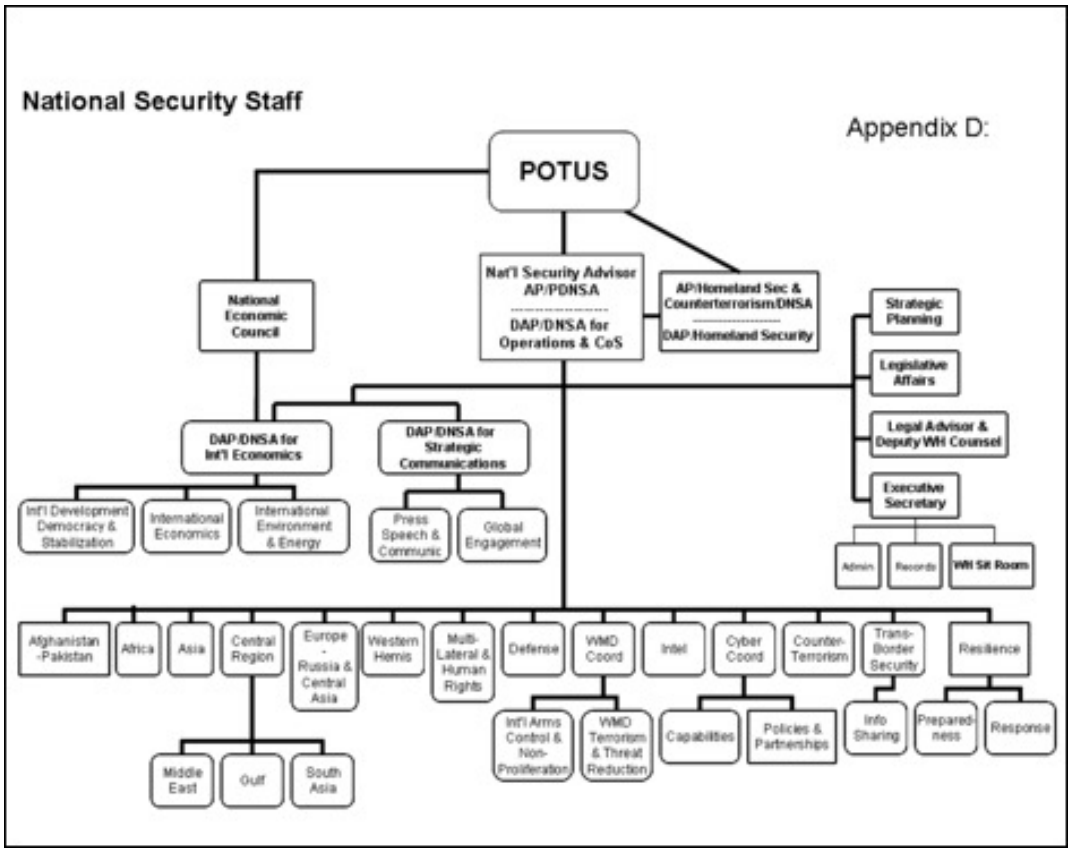
Departamento de Seguridad Nacional, al servicio del propio **Presidente** de Estados Unidos[216].

De esta forma, el 26 de mayo de 2009, la Casa Blanca emitió un comunicado oficial del Presidente Obama en el que explicó un nuevo enfoque, basado en que los desafíos del siglo XXI son cada vez menos convencionales y tienen un mayor carácter transnacional, por lo que exigen una respuesta que integre de manera efectiva todos los aspectos del poder estadounidense. De esta forma, el Presidente Obama comunicaba la plena integración del personal de la Casa Blanca en apoyo a la seguridad nacional, creando una nueva organización con responsabilidades en todas las actividades de formulación de políticas de la Casa Blanca relacionadas con asuntos internacionales, transnacionales, y de seguridad nacional. Esta estructura se colocaba bajo la dirección del Consejero de Seguridad Nacional, señalando que el Consejo Nacional de Seguridad se mantenía como foro principal para las deliberaciones interinstitucionales sobre cuestiones que afectan a la seguridad. También estableció el Presidente Obama nuevos puestos para hacer frente a los desafíos emergentes relacionados con la seguridad cibernética, el terrorismo, las armas de destrucción masiva, la seguridad transfronteriza, el intercambio de información, y la política de recuperación de las capacidades[217].

[216] OBAMA, Barack: *Presidential Study Directive*, febrero de 2009. Puede consultarse en http://fas.org/irp/offdocs/psd/psd-1.pdf consulta: 6 de agosto de 2015.

[217] OBAMA, Barack: *Declaración del Presidente sobre la organización de la Casa Blanca para la Seguridad Nacional y Contraterrorismo*. La Casa Blanca. 26 de mayo de 2009. Puede consultarse en http://fas.org/irp/news/2009/05/wh052609.html consulta: 6 de agosto de 2015.

Figura 19: Organización del *National Security Staff* de Estados Unidos



Fuente: Whittaker, Alan G.; Brown, Shannon A.; Smith, Frederick C.; y McKune, Elizabeth [218.]

3.2. REPÚBLICA POPULAR CHINA

3.2.1. Estrategia china de seguridad nacional

Señala Al-Rodhan que es prácticamente imposible intentar comprender la política exterior de China sin tener en cuenta las raíces históricas más profundas y culturales que dieron forma a la misma. La nociones de resistencia y humillación, reiteradas en el plan de estudios de la historia china, se centran en gran medida en "el siglo de

[218] WHITTAKER, Alan G.; BROWN, Shannon A.; SMITH, Frederick C.; y MCKUNE, Elizabeth: *The National Security Policy Process: The National Security Council and Interagency System*. Washington, D.C.: Industrial College of the Armed Forces, National Defense University, U.S. Department of Defense, p. 69. 15 de agosto de 2011. http://www.virginia.edu/cnsl/pdf/national-security-policy-process-2011.pdf consulta: 6 de agosto de 2015.

humillación" a principios del siglo XIX y XX. Infligido por Occidente y Japón, estas experiencias se comparten con el "Gran Salto Adelante" o la "Revolución Cultural". Estos son los discursos de los que se extrae impulso para proyectos ambiciosos como el programa espacial. Por otra parte, la relevancia de la cultura se refuerza cuando se observa la inspiración profunda y continua del Reino Medio y la visión sinocéntrica del mundo. El culto de la defensa, las enseñanzas de Sun Tzu y Confucio y la meta sin compromisos de la unificación nacional son todos los rasgos observados en la definición de las doctrinas de seguridad chinas. Menciona Al-Rodhan que, en este espíritu, en 2006 el Presidente Hu Jintao ofreció copias de seda de *El arte de la guerra* al entonces Presidente de Estados Unidos George W. Bush[219].

El referente más reciente en relación con la estrategia de seguridad nacional en China se produjo el 23 de enero de 2015, cuando la agencia oficial de noticias china Xinhua informó que el Buró Político del Comité Central del Partido Comunista de China (PCCh)[220] advirtió que el país está afrontando riesgos sin precedentes para su seguridad y debe estar atento. Algunos de estos retos y riesgos son imprevisibles, de modo que la nación debe estar alerta ante los posibles peligros, señaló una declaración emitida después de una reunión presidida por el presidente de China, Xi Jinping, quien también es secretario general del Comité Central del PCCh. Xinhua señaló que durante el encuentro se aprobó una directriz sobre la estrategia de seguridad nacional que señalaba que China protegerá su seguridad con un "modelo con características chinas". "El país defenderá con determinación sus intereses fundamentales e importantes, con la seguridad de su pueblo como la misión principal, y salvaguardará la seguridad nacional a través de la reforma y el desarrollo económico". Asimismo, China realizará contribuciones a la prosperidad global al tiempo que salvaguarda sus propios intereses, señaló la declaración. China mantendrá

[219] AL-RODHAN, Nayef: *opus citada.*

[220] Para una consulta de la estructura política de la República Popular de China puede accederse a la facilitada por la Comisión Ejecutiva sobre China del Congreso de Estados Unidos http://www.cecc.gov/chinas-state-organizational-structure consulta: 9 de agosto de 2015.

relaciones favorables con los principales países, trabajará para una vecindad segura y reforzará la cooperación con las naciones en vías de desarrollo.

Esta nota del Buró Político del Comité Central del Partido Comunista de China recordó que el país asiático tomará parte activa en la gobernación global y regional y contribuirá a la paz y el desarrollo mundiales. La reunión subrayó que los trabajos de la seguridad nacional deben de ser llevados bajo el absoluto liderazgo del PCCh con un sistema eficiente y unificado. Durante la tercera sesión plenaria celebrada en noviembre de 2013, el Comité Central del PCCh decidió crear una comisión de seguridad nacional encabezada por el mandatario chino. En la primera reunión tras la fundación de la comisión en abril de 2014, Xi pidió una "perspectiva general de la seguridad nacional".

Finaliza Xinhua señalando que en diciembre de 2014, un nuevo borrador de la ley de seguridad nacional comenzó su lectura ante la Asamblea Popular Nacional (APN), la máxima legislatura china, y que reemplazará a la anterior, que entró en vigor en 1993, y que ha sido rebautizada como Ley de Contraespionaje en concordancia con su contenido. Durante la reunión de este viernes, los miembros del comité también revisaron un informe general de trabajo presentado por el Comité Permanente de la APN, el Consejo de Estado, el Comité Nacional de la Conferencia Consultiva Política del Pueblo Chino (CCPPCh, máximo cuerpo asesor político), el Tribunal Popular Supremo y la Fiscalía Popular Suprema[221].

Shannon Tiezzi analiza esta comunicación del Buró Político del Partido Comunista de China, por el que se adopta el esquema de una estrategia de seguridad nacional, subrayando el sentido de urgencia que transmite esta nueva estrategia que, sin entrar en detalles, advirtió de la situación "impredecible" y los peligros "sin precedentes" que enfrenta China, tanto en el interior como en el extranjero, destacando que "la seguridad nacional debe estar bajo el liderazgo absoluto de mando eficiente y unificado del

[221] XINHUA: *Liderazgo chino advierte de riesgos sin precedentes para seguridad nacional*. 23 de enero de 2015. http://spanish.xinhuanet.com/china/2015-01/23/c_133942602.htm consulta: 8 de agosto de 2015.

Partido Comunista de China". Tiezzi llama la atención sobre la no mención de los problemas de seguridad no tradicionales que enfrenta China, como los ataques cibernéticos y el terrorismo, amenazas que preocupan cada vez más a las autoridades chinas, apuntando que, aunque no se hagan públicas, esas amenazas constituirán una parte clave de la estrategia de seguridad nacional de China[222].

De otra parte, es significativa la manifestación pública de apoyo de las autoridades chinas al marco de la ONU, como presentó en Singapur el 29 de julio de 2015 en un discurso pronunciado en las Conferencias Fullerton[223], la presidenta del Comité de Relaciones Exteriores de la XII Asamblea Popular Nacional, Fu Ying, en el que señaló que "el orden internacional que China apoya y con el que se identifica es el marco de la ONU y de sus instituciones internacionales asociadas creadas a raíz de la Segunda Guerra Mundial". Fu Ying explicó que China eligió integrarse al orden internacional y ha sido muy beneficiada formando parte del mismo él, resaltando que que el orden "fue construido para mantener la paz y seguridad mundiales y para ofrecer principios y normas para relaciones justas y equitativas entre los países, lo que le da una legitimidad ampliamente reconocida". Fu Ying dijo también que el papel de China en relación con el orden internacional ha pasado del "aprendizaje y adaptación" a la "participación y beneficio" y de ahí a la "reforma y la aportación"[224].

En el ámbito de las organizaciones regionales, China tiene un papel muy activo. En este sentido, el 5 de agosto de 2015 en Kuala Lumpur, el ministro de Relaciones Exteriores de China, Wang Yi, presentó 10 nuevas propuestas para profundizar en la cooperación entre China y la Asociación de Naciones del Sureste Asiático (Asean, por

[222] TIEZZI, Shannon: *China's National Security Strategy*. The Diplomat, 24 de enero de 2015. http://thediplomat.com/2015/01/chinas-national-security-strategy/ consulta: 8 de agosto de 2015.

[223] Las Conferencias Fullerton, organizadas por el Instituto Internacional para Estudios Estratégicos de Asia y apoyadas por The Fullerton Hotel Singapur, se centran en asuntos que abarcan geoeconomía, derecho internacional, política exterior y estrategias de seguridad nacional y defensa.

[224] XINHUA, *China apoya el orden internacional de posguerra y contribuye a él*. 30 de julio de 2015. http://spanish.xinhuanet.com/2015-07/30/c_134460970.htm consulta: 7 de agosto de 2015.

sus siglas en inglés), que constituyen una declaración de intenciones de la aproximación estratégica de China en este entorno[225]:

> **Primera**, hacer todos los preparativos para el 25º aniversario de las relaciones de diálogo China-Asean el próximo año y declarar 2016 como "Año del Intercambio Educativo China-Asean".
>
> **Segunda**, formular el Plan de Acción 2016-2020 para la Implementación de la Declaración Conjunta sobre la Asociación Estratégica China-Asean para la Paz y la Prosperidad, resaltar el sentido de época moderna, la inclusividad y la perspectiva, y explorar nuevos ámbitos de cooperación.
>
> **Tercera**, establecer un grupo de trabajo para negociar y firmar el "Tratado de Buena Vecindad y Cooperación Amistosa entre China y los países de Asean para fijar su amistad con medios legales de modo que las personas de las dos partes tengan una expectativa más positiva y más optimista de las relaciones China-Asean".
>
> **Cuarta**, emprender la operación sobre capacidad de producción internacional y lograr el desarrollo económico complementario de China y Asean, así como la prosperidad común.
>
> **Quinta**, China está dispuesta a discutir y firmar el plan maestro sobre conectividad China-Asean.
>
> **Sexta**, China trabajará con Asean para garantizar el éxito del "Año de la Cooperación Marítima China-Asean".
>
> **Séptima**, China expresó su interés en promover de forma conjunta el desarrollo de las subregiones a través del establecimiento del Mecanismo de Cooperación y Diálogo del Río Lancang-Mekong.
>
> **Octava**, China pide la pronta firma del protocolo para el Tratado sobre la Zona Desnuclearizada del Sureste de Asia y la parte china mantiene una actitud positiva respecto de la firma del protocolo.
>
> **Novena**, China espera reforzar la cooperación con Asean en defensa y seguridad, da la bienvenida a que los ministros de Defensa de los 10 Estados de Asean y a su secretario general para que asistan a la reunión de ministros de Defensa China-Asean.
>
> **Décima**, China y Asean deben trabajar juntas para salvaguardar la paz y la estabilidad en el Mar Meridional de China mediante el manejo adecuado de las disputas, el mantenimiento de la paz y el impulso a la cooperación.

3.2.2. El Libro Blanco "Estrategia Militar de China", mayo 2015

La Oficina de Información del Consejo de Estado publicó, el 26 de mayo de 2015, un libro blanco denominado "Estrategia Militar de China"[226]. Esta publicación se articula

[225] XINHUA, *Canciller chino presenta 10 nuevas propuestas para cooperación China-Asean*. 6 de agosto de 2105. http://spanish.xinhuanet.com/2015-08/06/c_134485118.htm consulta 7 de agosto de 2015.

[226] Consejo de Estado de la República Popular China, *China's Military Strategy*. Se puede acceder al texto completo en idioma inglés en http://www.chinadaily.com.cn/china/2015-05/26/content_20820628.htm consulta: 7 de agosto de 2015.

en un prefacio y seis capítulos: I. Situación de la Seguridad Nacional. II. Misiones y Tareas Estratégicas de las Fuerzas Armadas de China. III. Línea Estratégica de Defensa Activa IV. Construcción y Desarrollo de las Fuerzas Armadas de China. V. Preparación para la Lucha Militar. VI. Cooperación Militar y de Seguridad.

El prefacio del libro blanco destaca que la construcción de una fuerte defensa nacional y unas potentes fuerzas armadas es una tarea estratégica de la modernización de China y una garantía de seguridad para el desarrollo pacífico de China. Subordinada a servir al objetivo estratégico nacional, la estrategia militar de China es una guía general para el diseño, el desarrollo y el empleo de las fuerzas armadas del país. Señala el prefacio que en este nuevo punto de partida histórico, las fuerzas armadas de China se adaptan a los nuevos cambios en el entorno de la seguridad nacional, siguen decididamente el objetivo del Partido Comunista de China (PCCh) para construir un ejército fuerte, ponen en práctica la directriz estratégica militar de defensa activa, aceleran la modernización de las fuerzas de defensa, salvaguardan los intereses de soberanía, seguridad y desarrollo de China, y proporcionan una garantía para lograr el objetivo estratégico nacional de los "dos centenarios", y para la realización del “Sueño Chino”[227] de lograr el gran rejuvenecimiento de la nación china.

Del primer capítulo, dedicado a la situación de la seguridad nacional, puede destacarse la visión de que China se enfrenta a mayores desafíos en materia de seguridad nacional y de estabilidad social. Con el crecimiento de los intereses nacionales de China, su seguridad nacional es más vulnerable a las turbulencias, el terrorismo, la piratería, los graves desastres naturales internacionales y regionales y las epidemias, y la seguridad de los intereses en el extranjero en materia de energía

[227] SHAN Ding, *Conferencia del Encargado de Negocios de la Embajada de China en Uruguay*, Ding Shan, en la Universidad ORT de Uruguay, 4 de diciembre de 2013. “Los objetivos del Sueño Chino, llamados también Metas de Dos Centenarios, consisten en duplicar el Producto Interno Bruto y el Ingreso Promedio del Pueblo en 2020, cuando se cumple el primer centenario del Partido Comunista, en base de las cifras de 2010, materializando la construcción integral de una sociedad modestamente acomodada y transformando el país en uno socialista moderno, próspero, poderoso, democrático, civilizado y armonioso a mediados de este siglo cuando se funde 100 años de la República”. http://uy.china-embassy.org/esp/whkjs/t1105987.htm consulta: 7 de agosto de 2015.

y recursos, líneas marítimas estratégicas de comunicación, así como de instituciones, personal y activos en el exterior.

El segundo capítulo de la Estrategia Militar de China, asigna las siguientes cometidos estratégicos a las fuerzas armadas: 1. Hacer frente a una amplia gama de situaciones de emergencia y de amenazas militares, salvaguardando de manera efectiva la soberanía y la seguridad del territorio chino, terrestre, aéreo y marítimo. 2. Salvaguardar resueltamente la unificación de la patria. 3. Garantizar la seguridad y los intereses de los nuevos dominios de China. 4. Velar por la seguridad de los intereses de China en el extranjero. 5. Mantener la disuasión estratégica y llevar a cabo un contraataque nuclear. 6. Participar en la cooperación de seguridad regional e internacional y mantener la paz regional y mundial. 7. Fortalecer los esfuerzos en las operaciones contra la infiltración, el separatismo y el terrorismo a fin de mantener la seguridad política de China y la estabilidad social. 8. Llevar a cabo tareas tales como rescates de emergencia y operaciones de socorro, protección de los derechos y los intereses, labores de vigilancia, así como el apoyo para el desarrollo económico y social nacional.

En relación al tercer capítulo del libro blanco, se apunta que el concepto estratégico de defensa activa es la esencia del pensamiento estratégico militar del **PCCh**. De la práctica de las guerras revolucionarias, las fuerzas armadas populares han desarrollado un conjunto completo de los conceptos estratégicos de defensa activa, que se reduce a la adhesión a la unidad de defensa estratégica y la ofensiva operacional y táctica; la adhesión a los principios de la defensa, la defensa propia y la huelga después de la preventiva; y la adhesión a la postura de que "No vamos a atacar a menos que nos atacan, pero seguramente vamos a contraatacar en caso de ataque.”

Es en este capítulo dedicado a la defensa activa donde se incorporan los elementos más distintivos de los principios de seguridad y militares chinos. De esta forma, se señala que para implementar la directriz estratégica militar de defensa activa en la nueva situación, las fuerzas armadas de China deben cumplir los siguientes principios:

1. Estar subordinadas y al servicio del objetivo estratégico nacional, en un enfoque holístico de la seguridad nacional, prevenir las crisis, disuadir de los conflictos y ganar las guerras.

2. Fomentar una postura estratégica favorable para el desarrollo pacífico de China, favoreciendo la coordinación política, militar, económica y diplomática.

3. Lograr un equilibrio entre la protección de los derechos y el mantenimiento de la estabilidad, salvaguardar la soberanía territorial nacional y los derechos e intereses marítimos, y mantener la seguridad y la estabilidad a lo largo de la periferia de China;

4. Tomar la iniciativa estratégica en la lucha militar.

5. Emplear estrategias y tácticas que ofrezcan flexibilidad y movilidad, perseguir la eficacia de las operaciones conjuntas, y hacer un uso integrado de todos los medios y métodos operativos.

6. Preparar los escenarios más complejos y difíciles.

7. Potenciar las ventajas políticas únicas de las fuerzas armadas populares, mantener el liderazgo absoluto del PCCh sobre los militares, acentuar el cultivo del espíritu de lucha, hacer cumplir una disciplina estricta, mejorar la profesionalidad y la fuerza de las tropas, construir relaciones más estrechas entre el gobierno y las fuerzas armadas, así como entre el pueblo y el ejército, y aumentar la moral de los oficiales y soldados.

8. Utilizar la potencia global del concepto de la guerra popular.

9. Ampliar activamente la cooperación militar y de seguridad, profundizar las relaciones militares con las grandes potencias, los países vecinos y otros países en desarrollo, y promover el establecimiento de un marco regional para la seguridad y la cooperación.

El cuarto capítulo, dedicado al desarrollo de las fuerzas armadas de China, contempla el desarrollo de la fuerza en cuatro espacios de seguridad críticos:

1. La mentalidad tradicional que la tierra es de mayor valor que el mar debe ser abandonada. Los mares y océanos tienen un gran impacto en la paz duradera, la estabilidad y el desarrollo sostenible de China. Es necesario que China desarrolle una estructura de la fuerza militar marítima moderna para convertirse en una potencia marítima.

2. China se mantendrá al tanto de los procesos desarrollados en el espacio exterior, frente a las amenazas de seguridad y los desafíos en ese dominio, asegurando sus activos espaciales para servir al desarrollo económico y social del país, y mantener la seguridad del espacio exterior.

3. El ciberespacio se ha convertido en un nuevo pilar del desarrollo económico y social, y un nuevo campo de la seguridad nacional. Dado que la competencia estratégica internacional en el ciberespacio aumenta, un buen número de países están desarrollando sus fuerzas militares cibernéticas. Siendo una de las principales víctimas de los ataques de hackers, China se enfrenta a graves amenazas de seguridad a su infraestructura cibernética. Con el mayor peso del ciberespacio en la seguridad militar, China acelerará el desarrollo de una fuerza cibernética para prevenir crisis, garantizar la seguridad de la red y la información nacional, y mantener la seguridad nacional y la estabilidad social.

4. La fuerza nuclear es un pilar estratégico para salvaguardar la soberanía y la seguridad nacional. China siempre ha seguido la política de un no primer uso de armas nucleares y se adhiere a una estrategia nuclear de autodefensa que es de naturaleza defensiva. China

> siempre ha mantenido su capacidad nuclear en el nivel mínimo requerido para disuadir a otros países de usar o amenazar con la utilización del arma nuclear contra China.

En el quinto capítulo del libro blanco, dedicado a la preparación para la lucha militar, además de elementos clásicos como el entrenamiento y la mejora de la integración operativa, se impulsan áreas como la mejora de las capacidades para las operaciones de la lucha de sistemas contra sistemas, basados en los sistemas de información; así como la preparación para las operaciones militares que no sean de guerra, lo que incluye la adecuación de los sistemas de mando de respuesta a emergencias militares a los mecanismos de gestión de emergencias estatales.

Por último, el sexto capítulo de la estrategia militar, dedicado a la cooperación, contempla la continuación de las relaciones con países no alineados, el incremento de los intercambios y cooperación con los militares rusos en el marco de la asociación estratégica integral de coordinación entre China y Rusia; el fomento de un nuevo modelo de relación militar con las fuerzas armadas de Estados Unidos; el incremento de la cooperación con los países vecinos, Europa, Latinoamérica y África. En el escenario regional se continuará impulsando la cooperación estratégica en seguridad y defensa en la Organización de Cooperación de Shanghai, y se seguirá participando en los diálogos multilaterales y mecanismos de cooperación, como los Ministros de Defensa de la Asociación de Naciones del Sudeste Asiático (ASEAN), el Foro Regional de la ASEAN, el Diálogo Shangri-La, El Diálogo International de Defensa de Jakarta y el Simposio Naval del Pacífico Occidental, impulsando eventos multilaterales como el Foro de Xiangshan en China, tratando de establecer un nuevo marco para la seguridad y la cooperación para la paz, la estabilidad y la prosperidad en la región Asia-Pacífico. En el campo de la participación en misiones internacionales, China continuará participando en misiones ONU y observará estrictamente los mandatos del Consejo de Seguridad de las Naciones Unidas.

La percepciones de diferentes analistas tras la publicación del libro blanco de 2015, "Estrategia Militar de China", son diversas. Nicolas Morisset, tras destacar el cambio que supone el impulso de la proyección marítima china expresada en el libro blanco,

señala que si China está emergiendo como un garante de la estabilidad regional, no hay que olvidar que se trata del principal factor desestabilizador de la zona[228].

Esta modificación de la política del Consejo de Estado de China, para su transformación en potencia naval, es interpretada por Brice Pedroletti en clave de prioridad de protección de sus intereses en el extranjero y de sus nacionales distribuidos en todos los continentes Señala Pedroletti que este documento, presentado por Pekín como un acto de transparencia, tiene muy presente las disputas entre Estados Unidos y China en el Mar de la China Meridional, donde los proyectos en arrecifes y la recuperación de tierras realizadas en atolones por Beijing han sido objeto de una intensa campaña de denuncia por Washington[229].

La publicación del libro blanco de la defensa de Japón[230], el 21 de julio de 2015, muestra que la estrategia de seguridad nacional china no es percibida del mismo modo por otros actores cuyos intereses entran en ocasiones en fricción, e incluso en abierta colisión. De este modo, la sección de este documento dedicada a la política de defensa de China[231], señala que a pesar de que existen grandes expectativas hacia China para aceptar y cumplir con las normas internacionales, y desempeñar un papel activo de modo cooperativo en asuntos regionales y globales, existen disputas entre China y otros países sobre cuestiones tales como los desequilibrios comerciales, los tipos de cambio y los derechos humanos, y que mientras que China aboga por el “desarrollo pacífico”[232], sus acciones en particular sobre cuestiones marítimas entran en conflicto

[228] MORISSET, Nicolas: *Le Livre Blanc de la défense 2015 de la Chine*. Conflictualités et médiations, Université catholique de l’Ouest, 2 de junio de 2015. https://conflictualitemediation.wordpress.com/2015/06/02/le-livre-blanc-de-la-defense-2015-de-la-chine/ consulta: 8 de agosto de 2015.

[229] PEDROLETTI, Brice: *La marine, instrument de l’ambition planétaire de la Chine*. Le Monde, 28 de mayo de 2012. http://www.lemonde.fr/asie-pacifique/article/2015/05/28/la-marine-instrument-de-l-ambition-planetaire-de-la-chine_4642388_3216.html# consulta: 8 de agosto de 2015.

[230] Ministerio de Defensa de Japón: *Defensa 2015*. http://www.mod.go.jp/e/publ/w_paper/2015.html consulta: 8 de agosto de 2015.

[231] ibíd. Parte I, Capítulo I, Sección III. pp.1-2. http://www.mod.go.jp/e/publ/w_paper/pdf/2015/DOJ2015_1-1-3_1st_0730.pdf consulta: 8 de agosto de 2015.

[232] El término "desarrollo pacífico" de China comenzó a utilizarse en 2004. De acuerdo con un documento que el entonces consejero de Estado Dai Bingguo presentó el 11 de marzo de 2011, se

con los intereses de otros actores y son incompatibles con el orden jurídico internacional vigente.

3.2.3. La Ley de Seguridad Nacional de China, julio 2015

La nueva Ley de Seguridad Nacional fue aprobada el 1 de julio de 2015 por el máximo órgano legislativo de China, el Comité Permanente de la Asamblea Popular Nacional (APN), entrando en vigor el mismo día al ser firmada por el presidente chino Xi Jinping[233].

Aunque la Ley de Seguridad Nacional de China se aprobó con posterioridad a la publicación de la Estrategia Militar de China, que fue aprobada el 26 de mayo de 2015, estos dos documentos se encuentran alineados y este libro blanco de la estrategia militar desarrolla elementos que se encuentran en la Ley de Seguridad Nacional.

Señala la agencia oficial de noticias china Xinhua que esta Ley de Seguridad Nacional destaca la seguridad cibernética y demanda el establecimiento de un sistema de gestión de crisis coordinada y eficiente. Esta ley cubre un amplio espectro de temas que incluyen la defensa, finanzas, ciencia y tecnología, cultura y religión. La primera ley de seguridad nacional de China entró en vigor en 1993 y regulaba principalmente el trabajo de las agencias de seguridad nacional, ocupadas en su mayor parte de contraespionaje. Su nombre se cambió a Ley de Contraespionaje en noviembre de 2014.

La seguridad nacional queda definida en la nueva ley como una "condición en la que el gobierno de un país, su soberanía, unidad e integridad territorial, el bienestar de su pueblo, el desarrollo sostenible de su economía y sociedad y otros grandes intereses

---

define el "desarrollo pacífico" de China cuando la naturaleza del desarrollo es pacífico, independiente, científico, cooperativo y común co el de otros países. Ibídem. p.1.

[233] Se puede consultar una traducción en idioma inglés y el original en idioma chino en China Copyright and Media; The law and policy of media in China , Ed. Rogier Creemers: *National Security Law of the People's Republic of China,* 2 de julio de 2015 https://chinacopyrightandmedia.wordpress.com/2015/07/01/national-security-law-of-the-peoples-republic-of-china/ consulta: 9 de agosto de 2015.

están relativamente seguros y no se encuentran sujetos a amenazas internas o externas".

La agencia de noticias oficial Xinhua, apunta que un elemento clave de la nueva ley es una cláusula de soberanía en el ciberespacio. China hará que las tecnologías fundamentales de internet e información, las infraestructuras y los sistemas de información y datos en sectores importantes sean "seguros y controlables", según la ley. Se establecerá un sistema nacional de protección de internet y de la información para aumentar la capacidad de salvaguardar la seguridad cibernética y de información y reforzar la investigación innovadora, el desarrollo y la aplicación de internet y tecnología de la información.

Apunta también Xinhua que la nueva ley también se compromete a crear un sistema de gestión de crisis coordinado y eficiente bajo el liderazgo centralizado, y a publicar la información relacionada con las crisis de seguridad[234].

Stratfor y Luo, estiman que esta pieza legislativa es la más complete de China de la legislación de seguridad nacional hasta la fecha. Cubre temas de seguridad política; seguridad militar; seguridad económica y financiera; seguridad social y cultural; seguridad nuclear, seguridad ecológica, entre otras. La versión final de la ley deja claro que el liderazgo del país considera que sus intereses de seguridad que se extiende mucho más allá de las fronteras físicas de la China continental, llegando a las profundidades del mar, en el espacio exterior, y quizás lo más importante, en el ciberespacio. Además, describe las funciones y responsabilidades de la Asamblea Popular Nacional y los diferentes poderes del Estado; y en el ámbito específico de la seguridad nacional, articula los elementos clave del sistema de seguridad nacional,

[234] XINHUA: *China adopta nueva ley de seguridad nacional*. 1 de julio de 2105. http://spanish.xinhuanet.com/china/2015-07/01/c_134372895.htm consulta: 9 de agosto de 2015.

como la obtención de inteligencia, evaluación de riesgos, realización de pruebas de seguridad nacional, y la respuesta a situaciones de emergencia[235].

3.2.4. Estructura de seguridad nacional en China

Ya se ha apuntado en la comunicación del Buró Político del Comité Central del Partido Comunista de China de 23 de enero de 2015, el diseño de una estructura centralizada del control integral del Partido Comunista de China en los aspectos relativos a la seguridad nacional[236].

Además, como se ha señalado, la Ley de Seguridad Nacional describe las funciones y responsabilidades de la Asamblea Popular Nacional y los diferentes poderes del Estado; y en el ámbito específico de la seguridad nacional, articula los elementos clave del sistema de seguridad nacional.

Tiezzi opina que China continuará reformando su estructura burocrática para dirigir la seguridad nacional, señalando que después de tomar el poder, el presidente Xi Jinping, tomó rápidamente el control sobre los asuntos de seguridad nacional. La creación de una nueva comisión de seguridad nacional, encabezada por el propio Xi Jinping, se anunció en el tercer pleno del 18 Comité Central del Partido Comunista Chino, en noviembre de 2013. De esta forma, el presidente Xi Jinping lliderará directamente la seguridad política de China, la seguridad económica y la seguridad nacional[237].

Precisamente en este tercer pleno del 18 Comité Central del Partido Comunista Chino, se señalaba entre los asuntos a discutir en la sesión plenaria que “es necesario fundar

[235] STRATFORD, Timothy P. y LUO, Yan: *China’s New National Security Law*. The National Law Review, Covington & Burling LLP, 7 de julio de 2015. http://www.natlawreview.com/article/china-s-new-national-security-law consulta: 9 de agosto de 2015.

[236] XINHUA: *Liderazgo chino advierte de riesgos sin precedentes para seguridad nacional*. *opus citada.*

[237] Tiezzi, Shannon: *opus citada.*

un Consejo de Seguridad Nacional, mejorar el régimen de seguridad nacional y la estrategia de seguridad nacional y garantizar con firmeza la seguridad nacional"[238].

Posteriormente, en este mismo documento del tercer pleno se señala lo siguiente acerca del establecimiento del Consejo de Seguridad Nacional: "La seguridad nacional y la estabilidad social constituyen la premisa de la reforma y el desarrollo. Tan sólo cuando el Estado sea seguro y la sociedad estable, se puede promover constantemente la reforma y el desarrollo. En la actualidad, nuestro país se enfrenta a una presión doble: para con el exterior, salvaguardar la soberanía, la seguridad y los intereses de desarrollo nacionales, y para con el interior, defender la seguridad política y la estabilidad social, ya que aumentan visiblemente tanto los factores de riesgo previsible como los difícilmente previstos. Mientras tanto, nuestros regímenes y mecanismos de trabajo relacionado con la seguridad no pueden adaptarse a las necesidades de defender la seguridad del Estado y es necesario construir una plataforma poderosa que planee en conjunto los trabajos de seguridad nacional. El establecimiento del Consejo de Seguridad Nacional y el fortalecimiento de la dirección concentrada y unificada sobre el trabajo de seguridad nacional se han convertido en algo prioritario"[239].

Posteriormente se señalaba en las conclusiones del tercer pleno que "las principales atribuciones del Consejo de Seguridad Nacional son elaborar y ejecutar estrategias de seguridad nacional, promover el fomento de la legalidad referente a la seguridad nacional, elaborar principios y políticas para el trabajo de seguridad nacional y estudiar y resolver los importantes problemas surgidos en el trabajo de seguridad nacional"[240].

---

[238] *Documentos de la III Sesión Plenaria del XVIII Comité Central del Partido Comunista de China*, p. 7. 9-12 de noviembre de 2013. http://www.politica-china.org/imxd/noticias/doc/1389789646Documentos_de_la_III_Sesion_Plenaria_del_XVIII_Comite_Central_del_Partido_Comunista_de_China.pdf consulta: 9 de agosto de 2015.

[239] *ibídem*. p. 56.

[240] *ibídem*.

Zhao Kejin[241], experto en política exterior de China en el Centro Carnegie-Tsinghua de Política Global, analiza diversos aspectos del Consejo de Seguridad Nacional de China en el marco de la nueva Ley de Seguridad Nacional de China, señalando que el primer objetivo que se establece en la Comisión de Seguridad Nacional de China (CNSC)[242]es para ayudar a asegurar el éxito de la profundización de las reformas económicas, políticas y sociales que se están llevando a cabo en toda China. El segundo objetivo de la CNSC es establecer un sistema de seguridad nacional unificado. En tercer lugar, la CNSC fue creada para apoyar a los líderes y los objetivos políticos del Partido Comunista, que supervisa la seguridad del país, así como los asuntos militares y diplomáticos. El nuevo Consejo de Seguridad Nacional depende del partido, en lugar del gobierno nacional, y por tanto se espera que siga las directrices del Partido Comunista de China.

En cuanto a las principales tareas, del Consejo de Seguridad Nacional, señala en la misma publicación Kejin que la CNSC tiene tres tareas principales. La primera consiste en asesorar al Politburó, que supervisa el Partido Comunista, y los más altos niveles de liderazgo en materia de estrategia y seguridad. La segunda es llevar a cabo la coordinación estratégica entre los diferentes departamentos, y unificar estos departamentos en el partido, el gobierno, los militares y la sociedad. La tercera tarea de la CNSC es llevar a cabo la gestión de crisis y gestión de riesgos, tanto a las amenazas de seguridad internas como externas. Estima Kejin que en el futuro, la dirección política global para la seguridad nacional de China probablemente será determinado por el Politburó, y la aplicación concreta de estas políticas corresponderán a cada uno de los departamentos. La coordinación general, así como

[241]Puede consultarse el perfil profesional de Zhao Kejin en lhttp://carnegietsinghua.org/experts/?fa=622 consulta: 9 de agosto de 2015.

[242] En esta publicación se utiliza indistintamente la denominación Comisión de Seguridad Nacional de China y Consejo de Seguridad Nacional de China.

la determinación de planes específicos y la gestión de crisis, se llevarán a cabo por la CNSC[243].

Un aspecto interesante en relación al concepto y a la evolución del Consejo de Seguridad Nacional de China, es la evolución que señala Kejin cuando explica que de Mao Zedong a Deng Xiaoping la política de seguridad nacional estaba condicionada por la experiencia política de estos líderes en base a sus experiencias personales y las lecciones que habían aprendido en la guerra; pero a partir de la década de los noventa, y especialmente después de la muerte de Deng Xiaoping, China afronta nuevos retos de seguridad nacional, en particular en lo que respecta a Taiwán. En este contexto, algunos funcionarios chinos propusieron el establecimiento de un consejo de seguridad nacional. Bajo la dirección del renombrado erudito Wang Daohan, instituciones como el Instituto de Estudios Internacionales de Shanghai comenzó a estudiar esta propuesta, con un enfoque en la estructura del Consejo de Seguridad Nacional de Estados Unidos. En este escenario, en septiembre de 2000, se utilizó el modelo de Estados Unidos para formar el Grupo Dirigente Central para la Seguridad Nacional, un organismo informal para la deliberación y la coordinación dentro del Partido Comunista, que posteriormente evolucionó hasta el establecimiento formal del Consejo de Seguridad Nacional en noviembre de 2013[244].

Kejin también subraya las diferencias entre los consejos de seguridad nacional de Estados Unidos y de China. En los Estados Unidos, el Consejo Nacional de Seguridad sirve como órgano asesor personal del presidente. Está presidido formalmente por el presidente y se utiliza para coordinar las políticas entre los distintos organismos y departamentos gubernamentales. Las reuniones celebradas por el Consejo de Seguridad Nacional son atendidos regularmente por el vicepresidente, consejero de seguridad nacional, y varios funcionarios del gabinete. Por el contrario, el Consejo de Seguridad Nacional de China es una institución del Partido Comunista de China, y se

[243] KEJIN, Zhao: *China's National Security Commission*. Carnegie-Tsinghua Center for Global Policy, 14 de julio de 2015. http://carnegietsinghua.org/2015/07/09/china-s-national-security-commission/id7i consulta: 9 de agosto de 2015.

[244] *Ibídem*.

dirige directamente por el presidente Xi Jinping, a la vez presidente del Politburó. De esta forma en China este consejo es una agencia de coordinación administrativa, A diferencia de su homólogo de Estados Unidos (pero similar a su equivalente ruso), que supervisa varios departamentos. El Consejo de Seguridad Nacional de China es un organismo interministerial, que además coordina los esfuerzos de la Asamblea Popular Nacional y la Conferencia Consultiva del Pueblo Chino[245].

3.3. FEDERACIÓN DE RUSIA

El tercer gran actor político del que se analiza su estrategia nacional de seguridad es la Federación de Rusia. El concepto de seguridad en Rusia se encuentra muy ligado a las ideas desarrolladas por Mackinder y la "tierra corazón"; de este modo Rusia percibe su seguridad basada en el espacio geopolítico definido por el territorio continental, en el entendimiento que es la zona clave para conservar el poder y mantener el control de otros espacios geopolíticos adyacentes.

Esta región cardial o área pivote se define por Asia Central y Europa Oriental, y se encuentra rodeada de una franja intermedia donde se encuentran los ámbitos terrestre y marítimo. La teoría establece que en esa zona el poder terrestre tendría una mayor ventaja frente al dominio marítimo por su inaccesibilidad por mar, el aprovechamiento de los rápidos medios de comunicación terrestres y por la explotación de los recursos del área. Se afirma que el actor que lograra conquistarla sería una potencia mundial.

Rusia posee un corpus legislativo integrado relacionado con la seguridad nacional, destacando documentos de estrategia de seguridad, relaciones exteriores, doctrina militar y ciberseguridad.

Figura 20: Documentos políticos y de doctrina de seguridad de la Federación de Rusia

Constitución
1993: Constitución de la Federación de Rusia. 12-12-1993.

[245] *Ibídem*.

Seguridad Nacional
1997: Concepto de Seguridad Nacional de la Federación de Rusia. 17-12-1997.
2000: Concepto de Seguridad Nacional de la Federación de Rusia. 10-1-2000.
2009: La Seguridad Nacional de la Federación de Rusia hasta 2020. 12-5-2009.
Política Exterior
2008: El Concepto de la Política Exterior de la Federación de Rusia. 12-7-2008.
2000: El Concepto de la Política Exterior de la Federación de Rusia. 28-6-2000.
Seguridad de la Información
2000: Doctrina de Seguridad de Información de la Federación de Rusia. 9-9-2000.
Doctrina Militar
1993: Disposiciones fundamentales de la Doctrina Militar de la Federación de Rusia.
2000: La Doctrina militar de la Federación de Rusia.
2010: La Doctrina Militar de la Federación de Rusia. 5-2-2010.
2014: La Doctrina Militar de la Federación de Rusia hasta 2020. 26-12-2014

Fuente: Actualización sobre la base de la proporcionada por Institute for Defence Studies and Analyses[246].

3.3.1. La Estrategia de Seguridad Nacional de Rusia para el año 2020

El 12 de mayo de 2009, el presidente de la Federación de Rusia aprobó por el decreto presidencial 537 la Estrategia de Seguridad Nacional de la Federación de Rusia para el año 2020[247].

[246] En el sitio web de "Institute for Defence Studies and Analyses" pueden consultarse versiones en inglés de estos documentos: *Russian Foreign Policy Documents and Military Doctrines* en el enlace http://www.idsa.in/eurasia/resources.html consulta: 15 de agosto de 2015.

[247] El texto de la Estrategia de Seguridad Nacional se publica en el sitio web del Consejo de Seguridad de Rusia: http://www.scrf.gov.ru en http://www.scrf.gov.ru/documents/99.html (en ruso). Se

En el sitio web del Kremlin se explica que el objetivo de la Estrategia de Seguridad Nacional es consolidar los esfuerzos de las autoridades federales y regionales, y las organizaciones y los ciudadanos de Rusia para garantizar la seguridad nacional del país. El documento enumera las prioridades nacionales estratégicos de Rusia y proporciona las líneas generales de la situación de seguridad nacional. La estrategia es el documento básico para la planificación de la seguridad nacional y la base para la cooperación entre las autoridades gubernamentales, grupos públicos y organizaciones con el objetivo de proteger los intereses nacionales y garantizar la seguridad personal, pública y la seguridad del Estado. Se señala que los trabajos en la estrategia comenzaron en 2004 para sustituir el Concepto de Seguridad Nacional[248].

La definición de la seguridad nacional cobra un aspecto muy amplio y transversal en este documento, lo que se puede apreciar en los capítulos en que se articula: I. Disposiciones Generales. II. Rusia y el mundo moderno: Situación y tendencias de desarrollo. III. Los intereses nacionales de la Federación Rusa y prioridades nacionales estratégicas. IV. Garantizar la seguridad nacional: 1. La defensa nacional; 2. El Estado y la seguridad pública; 3. Mejora de la calidad de vida de los ciudadanos rusos; 4. El crecimiento económico; 5. La ciencia, la tecnología y la educación; 6. Salud; 7. Cultura; 8. La ecología de los sistemas de vida y gestión ambiental; 9. La estabilidad estratégica y la asociación estratégica equitativa. V. Organización, fundamentos jurídicos normativos e informativos para la ejecución de la Estrategia. VI. Los principales indicadores del estado de la seguridad nacional[249].

El primer artículo de esta Estrategia de Seguridad Nacional comienza describiendo la situación de Rusia, señalando que Rusia ha superado las consecuencias de la crisis política y socio-económica sistémica de finales del siglo XX; frenado la degradación

puede accede a una traducción en idioma ingles en http://rustrans.wikidot.com/russia-s-national-security-strategy-to-2020 consulta: 15 de agosto de 2015.

[248] Sitio web oficial Kremlin: *Dmitry Medvedev signed an Executive Order on Russia's National Security Strategy through to 2020*. http://archive.kremlin.ru/eng/text/news/2009/05/216230.shtml consulta: 15 de agosto de 2015.

[249] *Estrategia de Seguridad Nacional de la Federación de Rusia para el año 2020. opus citada*.

de la calidad de vida de los ciudadanos rusos; resistido las presiones del nacionalismo, el separatismo y el terrorismo internacional; impedido el descrédito en el modo constitucional de gobierno; conservado su soberanía e integridad territorial; y restaurado el potencial del país para mejorar su competitividad y defender sus intereses nacionales como un actor clave dentro de la evolución de las relaciones internacionales multipolares[250].

En este escenario, se describe en el tercer artículo la Estrategia de Seguridad Nacional 2020 como un sistema de prioridades estratégicas, objetivos y medidas con respecto a la política interior y exterior, que determinan el grado de la seguridad nacional y el nivel de desarrollo estable a largo plazo del Estado, basada en la interdependencia con el Concepto a Largo Plazo de Desarrollo Socioeconómico de la Federación de Rusia para 2020[251].

En el artículo 10 de la estrategia se apuntan los riesgos más probables, señalando que el impacto negativa en la seguridad de los intereses nacionales de Rusia vendrá por la probable repetición del uso unilateral de la fuerza en las relaciones internacionales; los desacuerdos entre los principales participantes en la política mundial; la amenaza de la proliferación de armas de destrucción masiva y de su uso por los terroristas; e igualmente por el incremento de la actividad ilícita en los dominios cibernéticos y biológicos, en el ámbito de la alta tecnología[252].

También se definen los intereses nacionales de la Federación de Rusia a largo plazo en el artículo 21 de la estrategia: el desarrollo de la democracia y la sociedad civil, y la mejora de la competitividad de la economía nacional; asegurar la solidez del sistema constitucional, la integridad territorial y la soberanía de la Federación Rusa; la transformación de la Federación de Rusia en una potencia mundial, cuya actividad está dirigida a apoyar la estabilidad estratégica y las relaciones de asociación

[250] *Ibídem*, artículo 1.
[251] *Ibídem,* artículo 3.
[252] *Ibídem,* artículo 10.

mutuamente beneficiosas en el mundo multipolar. Este artículo es complementario con el 23 donde se definen las principales prioridades de seguridad nacional de la Federación de Rusia: la defensa nacional y la seguridad de la sociedad y del Estado[253].

Un aspecto especialmente significativo de la Estrategia de Seguridad Nacional de la Federación de Rusia para el año 2020 se encuentra en el artículo 112, que cierra el documento. Se indican en este artículo los principales indicadores con el fin de evaluar el nivel del estado de la seguridad nacional: el nivel de desempleo (como proporción de la población económicamente activa); el coeficiente decil (la correlación entre los ingresos de la parte superior e inferior al 10% de la población); la tasa de crecimiento de los precios al consumidor; el nivel de la deuda pública interna y externa en porcentaje del Producto Interior Bruto; el nivel de apoyo fiscal para la salud, la cultura, la educación y la ciencia en porcentaje del PIB; el nivel de renovación anual de los armamentos, militares y equipo especializado; el nivel de incorporación de cuadros militares y de ingeniería técnica[254].

La incorporación de indicadores del nivel de seguridad nacional no es una práctica habitual en las estrategias nacionales de seguridad, lo que denota una preocupación por un desarrollo armónico de la estrategia y de la legislación derivada de la misma, disponiendo de unas claras referencias de aquellos elementos que nos indiquen su grado de cumplimiento. De otra parte, los indicadores señalados tienen un carácter marcadamente económico, lo que es consistente con el enfoque integral del documento, que ofrece constantes referencias a la importancia de la economía en la seguridad nacional.

En este contexto, señalan Dimitrakopoulou y Liaropoulos que en la Estrategia de Seguridad Nacional de la Federación de Rusia para el año 2020, en el sector económico, las amenazas son específicas y tienen un lugar prominente. Por una parte, Rusia necesita aumentar su productividad y mejorar el nivel de industrialización en ciertas regiones. De otro lado, la dependencia de la economía rusa en la exportación

[253] *Ibídem,* artículos 21 y 23.
[254] *Ibídem,* artículo 112.

de materias primas y la participación de actores extranjeros son reconocidas como amenazas a los intereses nacionales de Rusia. La crisis financiera de 2008-2009 puso de manifiesto las debilidades estructurales y el hecho de que la economía rusa es cada vez más dependiente de las importaciones de recursos energéticos. Los recuerdos de la época de Yeltsin, cuando la terapia de choque resultó en la privatización ilegal, un aumento de la delincuencia y el empobrecimiento de más de la mitad de la población, se encuentran fuertemente arraigados en la conciencia colectiva de la sociedad rusa. En este escenario se aprecia la gran importancia que se otorga en la seguridad nacional a la prosperidad y la estabilidad[255].

Javier Morales incide en este aspecto al señalar la innovación que supone en la estrategia el enfoque en la mejora de la calidad de vida de los ciudadanos, que en el Concepto de Seguridad Nacional 2000 fue apenas esbozado. De este modo, las amenazas que se perciben en este dominio incluyen la crisis financiera mundial; la competencia por los recursos escasos, como materias primas, energía, agua y alimentos; la delincuencia y la corrupción; y también problemas de salud como las nuevas epidemias a gran escala y la extensión del SIDA, la tuberculosis, la drogadicción y el alcoholismo. Apunta Morales que, aunque ya había habido referencias sobre estos problemas sociales en anteriores documentos de seguridad nacional, en esta estrategia se incluyen como una prioridad dentro del concepto de desarrollo sostenible, en un reconocimiento de la relación entre el estatus internacional de Rusia y el bienestar de su población[256].

Manutscharjan abunda en esta interconexión de la economía y el bienestar, señalando que aunque la Estrategia de Seguridad Nacional para el año 2020 pone gran énfasis

[255] DIMITRAKOPOULOU, Sophia y LIAROPOULOS, Andrew: *Russia's National Security Strategy to 2020: A Great Power in the Making?* Caucasian Review of International Affairs, Vol. 4 (1) – Winter 2010, p. 40. http://www.cria-online.org/Journal/10/Done_Russias_National_Security_Strategy_To_2020_A_Great_Power_In_The_Making_Dimitrakopoulou_Liaropoulos.pdf consulta: 18 de agosto de 2015.

[256] MORALES, Javier: *Russia's New National Security Strategy: Towards a 'Medvedev Doctrine'?* Real Instituto Elcano, ARI 135/2009, 25 de septiembre de 2009. http://www.realinstitutoelcano.org/wps/wcm/connect/0558db804fb4cfd6a6f7ff8bf7fc5c91/ARI135-2009_Morales_Russia_New_National_Security_Strategy_Medvedev.pdf?MOD=AJPERES&CACHEID=0558db804fb4cfd6a6f7ff8bf7fc5c91 consulta: 18 de agosto de 2015.

en las amenazas militares, el Kremlin se encuentra realmente alarmado por las amenazas no militares, debido principalmente al impacto de la crisis económica y financiera global en la paz social del país. De hecho, apunta Manutscharjan que otro dato que se desprende de la estrategia es el temor a la ruptura de la Federación de Rusia, con peligros tales como el nacionalismo, el separatismo, la xenofobia, el extremismo, y radicalismo religioso. Esta interacción entre la economía y la seguridad nacional se relaciona con la postura rusa que no descarta la necesidad de utilizar fuerzas militares en las controversias que surjan sobre el control de la energía y los recursos, no sólo en Oriente Medio sino también en Mar del Barents, el Ártico, la región del Caspio y Asia Central[257].

Apunta Giles que el factor económico es presentado por las autoridades rusas como el enfoque principal de la nueva Estrategia, en comparación con documentos estratégicos anteriores que daban preponderancia a otros factores de corte más militar. Señala además Giles que la nueva estrategia es un documento optimista, confiado y firme, declarando claramente los desafíos, pero evitando la sensación de fatalidad y hostilidad que impregnaba las versiones anteriores, como cuando en el documento del Concepto de Seguridad 2000 las descripciones de amenazas directas y los medios para contrarrestarlas ocupaban casi todo el documento. En cambio la versión de 2009 también se ocupa de la protección de los intereses nacionales del Estado, pero de un modo más integrado y amplio[258].

[257] MANUTSCHARJAN, Aschot: *Russia's National Security Strategy until 2020*. Konrad-Adenauer-Stiftung, Ed.: Dr. Gerhard Wahlers Berlín, 31 de Agosto de 2009, p.159-162. http://www.kas.de/wf/en/33.17407/ consulta: 18 de agosto de 2015.

[258] GILES, Keir: *Russia's National Security Strategy to 2020*. NATO Defense College, Research Division, junio 2009. http://www.conflictstudies.org.uk/files/rusnatsecstrategyto2020.pdf consulta: 18 de agosto de 2015.

3.3.2. La Doctrina Militar de la Federación de Rusia hasta el 2020

El 26 de diciembre de 2014 el presidente ruso, Vladimir Putin, aprobó una nueva doctrina militar, tras las doctrinas militares que se adoptaron en 1993, 2000 y 2010[259].

En esta doctrina militar, se señala que las tareas fundamentales de la política militar de la Federación de Rusia se determinan por el presidente de la Federación de Rusia, de conformidad con la legislación federal, la Estrategia Nacional de Seguridad de la Federación de Rusia hasta el 2020, y la doctrina actual Militar. La política militar de la Federación de Rusia está dirigida a la prevención de una carrera armamentista, la disuasión y la prevención de conflictos militares, y la mejora de la organización militar, las formas y los métodos de la utilización de las fuerzas armadas y otras tropas, y también a los medios ofensivos, con el propósito de defender y salvaguardar la seguridad de la Federación de Rusia y también los intereses de sus aliados[260].

Figura 21: Principales peligros definidos en la Doctrina Militar de la Federación de Rusia hasta 2020.

Peligros definidos en la Doctrina Militar de la Federación de Rusia hasta 2020.
Principales peligros militares externos
a) el deseo de dotar a la OTAN con funciones globales en violación de las normas del derecho internacional y el traslado de la infraestructura militar de los países miembros de la OTAN cerca de las fronteras de la Federación de Rusia, incluso mediante la ampliación del bloque;
b) la desestabilización de estados y regiones, que socavan la estabilidad estratégica;
c) el despliegue de tropas de estados extranjeros en los territorios de los Estados contiguos a Rusia y sus aliados, y en aguas adyacentes;
d) la creación y el despliegue de sistemas estratégicos de defensa antimisiles y la violación de la correlación de fuerzas de misiles nucleares, así como la militarización del espacio ultraterrestre y el despliegue de sistemas estratégicos de armas de precisión no nucleares;
e) las reivindicaciones territoriales en contra de la Federación de Rusia y sus aliados y la injerencia en sus asuntos internos;
f) la proliferación de armas de destrucción masiva, misiles y tecnologías de misiles, y el aumento en el número de estados que poseen armas nucleares;

[259] *The Military Doctrine of the Russian Federation, approved by Russian Federation Presidential Edict on 5 February 2010.* The School of Russian and Asian Studies, 20 de febrero de 2010 http://www.sras.org/military_doctrine_russian_federation_2010

[260] *Ibídem*. Artículo 17.

g) la violación de los acuerdos internacionales de los estados individuales, así como el incumplimiento de los tratados internacionales celebrados con anterioridad en materia de limitación y reducción de armamento;
h) el uso de la fuerza militar en los territorios de los estados contiguos a la Federación de Rusia en violación de la Carta de la ONU y otras normas del derecho internacional;
i) la presencia de conflictos armados y su escalada en los territorios de los estados contiguos a la Federación de Rusia y sus aliados;
j) la propagación del terrorismo internacional;
k) la aparición de focos de tensión interétnica o religiosa, la actividad de grupos radicales armados en la frontera de la Federación de Rusia y las de sus aliados, las reivindicaciones territoriales y el crecimiento del separatismo y el extremismo violento en distintas partes del mundo.
Principales peligros militares internos
a) los intentos de cambiar la estructura constitucional de la Federación Rusa por la fuerza;
b) el debilitamiento de la soberanía y la violación de la unidad y la integridad territorial de la Federación de Rusia;
c) la perturbación del funcionamiento de los órganos de poder del Estado, de instalaciones del Estado y militares, y la infraestructura de información de la Federación de Rusia.

Fuente: La Doctrina Militar de la Federación de Rusia hasta el 2020[261].

Señala Rajorshi Roy que esta nueva doctrina ofrece una visión de los principales problemas de seguridad percibidos por el Kremlin y la forma en que quieren hacerles frente; y contrariamente a la percepción popular, el documento destaca por su enfoque más bien cauteloso, aunque destaca la determinación de Rusia para proteger los intereses estratégicos fundamentales. Mientras que el núcleo de la nueva doctrina no ha experimentado grandes cambios, es de resaltar que se analizan las diferencias fundamentales que existen entre las percepciones entre Rusia y Occidente. Esto incluye un cambio notable desde el debilitamiento de la confrontación ideológica de la doctrina de 2010 hacia el aumento de la competencia global actual y las tensiones debidas a los valores y patrones de desarrollo diferentes. También aboga por la redistribución gradual y surgimiento de nuevos centros económicos y políticos

[261] *Ibídem*, artículo 8.

globales. Todo esto lo valora Roy en la sensación de Moscú de una confrontación prolongada en medio de la reconfiguración del equilibrio global de poder[262].

Vladimir Isachenkov destaca de esta nueva doctrina la definición de la acumulación de capacidades militares de la OTAN cerca de la frontera rusa como la principal amenaza militar y planteó la posibilidad de utilizar por primera vez las armas convencionales de precisión como un elemento de disuasión estratégica, señalando que la OTAN negó rotundamente ser una amenaza para Rusia, acusando por su parte a Rusia de socavar la seguridad europea; todo ello en un escenario de tensión por la situación en Ucrania[263].

La mención a la OTAN en este contexto ya aparecía en el artículo 17 de la mencionada Estrategia de Seguridad Nacional de 2009, cuando señalaba que un aspecto determinante de las relaciones con la OTAN sigue siendo el hecho de la previsión de ampliar la infraestructura militar de la alianza de las fronteras de Rusia, y los intentos de dotar a la OTAN con funciones globales que van en contra de las normas del derecho internacional, lo que Rusia manifiesta es inaceptable[264].

3.3.3. El Consejo de Seguridad Nacional de Rusia

El sitio web oficial del Kremlim ofrece información específica acerca del Consejo de Seguridad Nacional de Rusia[265], señalando que la seguridad nacional es un término que abarca la seguridad de la persona, la sociedad y el Estado frente a las amenazas internas y externas, afectando a áreas prioritarias tales como la seguridad del Estado,

---

[262] ROY, Rajorshi: *Russia's New Military Doctrine: An Overview*. Institute for Defence Studies and Analyses, 16 de abril de 2015. http://www.idsa.in/idsacomments/RussiasNewMilitaryDoctrine_rroy_160415.html consulta: 15 de agosto de 2015.

[263] Vladimir Isachenkov: *New Russian military doctrine says NATO top threat.* Associated Press, The Washington Times, 26 de diciembre de 2014. http://www.washingtontimes.com/news/2014/dec/26/new-russian-military-doctrine-says-nato-top-threat/ consulta: 15 de agosto de 2015.

[264] *Estrategia de Seguridad Nacional de la Federación de Rusia para el año 2020. opus citada*, artículo 17.

[265] Sitio web oficial Kremlin: *President of Russia, Security Council* http://archive.kremlin.ru/eng/articles/institut04.shtml consulta: 15 de agosto de 2015.

la seguridad pública, la seguridad socioeconómica y la seguridad en los ámbitos de la defensa, la información, los militares y los asuntos internacionales. Debido a la necesidad de constante análisis y la planificación estratégica en relación con los problemas de seguridad, así como la redacción de las decisiones presidenciales, se creó en 1992 el Consejo de Seguridad. El Consejo de tiene como misión elaborar propuestas de políticas en defensa de los intereses vitales de los individuos, la sociedad y el Estado en contra de las amenazas internas o externas. El Consejo también colabora en la determinación de una política estatal uniforme en materia de seguridad y ayuda a garantizar la capacidad del presidente para llevar a cabo sus deberes constitucionales en la defensa de los derechos humanos y civiles, así como la soberanía de Rusia, la independencia y la integridad territorial.

El Consejo de Seguridad está presidido por el Presidente de Rusia, de acuerdo con la Constitución de la Federación de Rusia de 1993[266].

La Ley Federal "Sobre la Seguridad", de conformidad con el artículo 83 de la Constitución de la Federación de Rusia, define el estatuto del Consejo de Seguridad de Rusia, sus objetivos, funciones, composición y organización de sus actividades[267].

Figura 22: Misiones del Consejo de Seguridad de la Federación de Rusia.

Misiones principales del Consejo de Seguridad de la Federación de Rusia
1. Determinar los intereses vitales para la sociedad y el Estado e identificar las amenazas internas y externas a la seguridad.
2. Elaborar las principales áreas de la estrategia para salvaguardar la seguridad de la Federación Rusa y organizar la preparación de programas específicos federales para garantizarla.
3. Preparar recomendaciones para el presidente de la Federación de Rusia en materia de política interior y exterior.
4. Preparar las decisiones sobre la prevención y la gestión de situaciones de emergencia de tipo sociopolítico, económico, militar, ecológico, y otras.

[266] Constitución de Rusia, capítulo 4, artículo 83, g. http://www.constitution.ru/en/10003000-05.htm consulta: 15 de agosto de 2015.

[267] Sitio web oficial Kremlin:: *Dmitry Medvedev signed Federal Law On Security*, 28 de octubre de 2010. http://en.kremlin.ru/events/president/news/9941 consulta: 15 de agosto de 2015.

5. Preparar propuestas para el presidente de la Federación de Rusia sobre la introducción, ampliación o levantamiento de un estado de excepción.
6. Elaborar propuestas sobre la coordinación de las actividades de los órganos federales del poder ejecutivo.
7. Elaborar propuestas de reforma de órganos existentes o la creación de otros nuevos para salvaguardar la seguridad de las personas, la sociedad y el Estado.

Fuente: Estatuto del Consejo de Seguridad de la Federación de Rusia [268].

El Presidente de la Federación de Rusia preside el Consejo y nombra a sus miembros. Los miembros con carácter permanente son el primer ministro de la Federación Rusa; el jefe de gabinete de la Oficina Ejecutiva Presidencial; el ministro de Interior; el ministro de Relaciones Exteriores; la presidenta del Consejo de la Federación; el presidente de la Duma Estatal; el secretario del Consejo de Seguridad; el secretario adjunto del Consejo; el director del Servicio de Inteligencia Exterior; y el ministro de Defensa. Otros miembros del Consejo son los enviados plenipotenciarios presidenciales a los Distritos Federales del Volga, Central, Crimea, Noroeste, Norte del Cáucaso, Siberia, Lejano Oriente, Sur, y Urales, el jefe del Estado Mayor General de las Fuerzas Armadas; el director del Servicio Federal de Control de Drogas; el ministro de Justicia; el gobernador de San Petersburgo; el ministro de Situaciones de Emergencia; el ministro de Finanzas; el alcalde de Moscú; el viceprimer ministro de la Federación; y el fiscal general[269]

El secretario del Consejo de Seguridad, que responde directamente ante el Presidente, supervisa la labor del Consejo y su Oficina. El Consejo de Seguridad organiza su trabajo en comisiones interinstitucionales, que se reúnen en diferentes formatos y pueden ser permanentes o temporales[270]. Con el fin de aportar su experiencia académica para el trabajo del Consejo, existe un Consejo científico

[268] *Estatuto del Consejo de Seguridad de la Federación de Rusia*. Puede consultarse una version en idioma ingles en http://fas.org/irp/world/russia/docs/edict_1024.htm consulta: 15 de agosto de 2015.

[269] Puede accederse a la composición del Consejo de Seguridad de la Federación de Rusia en http://en.kremlin.ru/structure/security-council/members consulta: 15 de agosto de 2015.

[270] En el sitio web del Kremlin puede accederse a una referencia datada de las reuniones del Consejo de Seguridad, ofreciendo un resumen de los asuntos tratados y los participantes en la reunión. http://en.kremlin.ru/events/security-council consulta: 15 de agosto de 2015.

compuesto por representantes de la Academia de Ciencias de Rusia, academias especializadas de la ciencia y de instituciones educativas, así como otros académicos y expertos[271].

Señala Giles, que en la Estrategia de Seguridad Nacional de la Federación de Rusia para el año 2020 se avanza un cambio en el proceso de toma de decisiones estratégicas en Rusia, estableciendo las reglas básicas para asegurar enfoques coherentes y unificados a los objetivos estratégicos de Rusia, potenciando la labor de la supervisión del Consejo de Seguridad liderado por el presidente de la Federación[272].

Conclusiones del Capítulo 3

Estados Unidos, China y Rusia han llevado a cabo procesos complejos de planeamiento en el ámbito de la seguridad. El modelo estadounidense ha inspirado tanto a China como a Rusia, países que, no obstante, mantienen diferencias en cuanto a las soluciones organizativas de las que se dotan para hacer frente a los retos que afectan a la seguridad nacional.

Estados Unidos ha sido el país pionero al confeccionar la primera estrategia de seguridad nacional, en 1987, en el marco de una reforma integral de la seguridad y la defensa en el país que duró cuatro años y en la que intervino el Senado y la Cámara de Representantes de modo conjunto, dando lugar al Acta Goldwater-Nichols, que generó las bases del planeamiento estratégico moderno en Estados Unidos, inspirado en una serie de pensadores estratégicos, que adaptaron el modelo de Maquiavelo de la "razón de Estado" y de la búsqueda de raíces del "fenómeno guerra" de Clausewitz.

Los pensadores contemporáneos estadounidenses también han influido en el diseño del pensamiento estratégico actual y la planificación estratégica en el ámbito de la seguridad nacional. En especial, el pensamiento de Brzezinski, que fue además consejero de Seguridad Nacional entre 1977 y 1981, ha influido de forma notoria en el

[271] Sitio web oficial Kremlin: *President of Russia, Security Council, opus citada.*

[272] GILES, Keir: *Russia's National Security Strategy to 2020*, *opus citada.*

diseño estratégico estadounidense. Otros pensadores como Fukuyama, Huntington, y Alvin y Heidi Toffler, han orientado este pensamiento estratégico estadounidense contemporáneo.

China se ha inspirado en otras corrientes de pensamiento a la hora de conformar su estrategia de seguridad, como señala Al-Rodhan al afirmar que es prácticamente imposible intentar comprender la política exterior de China sin tener en cuenta las raíces históricas más profundas y culturales que dieron forma a la misma. La nociones de resistencia y humillación, reiteradas en el plan de estudios de la historia china, se centran en gran medida en "el siglo de humillación" a principios del siglo XIX y XX. Infligido por Occidente y Japón, estas experiencias se comparten con el "Gran Salto Adelante" o la "Revolución Cultural". Por otra parte, la relevancia de la cultura se refuerza cuando se observa la inspiración profunda y continua del Reino Medio y la visión sinocéntrica del mundo. El culto de la defensa, las enseñanzas de Sun Tzu y Confucio y la meta sin compromisos de la unificación nacional son rasgos observados en la definición de las doctrinas de seguridad chinas. Como menciona Al-Rodhan, en este espíritu, en 2006 el Presidente Hu Jintao ofreció copias de seda de *El arte de la guerra* al entonces Presidente de Estados Unidos George W. Bush.

China ha desarrollado un corpus de seguridad nacional muy completo, que cuenta con la estrategia de seguridad nacional, el libro blanco “Estrategia Militar de China”, y una ley de seguridad nacional.

En cuanto a las estructuras y modelos de organización de la seguridad nacional, destaca en China el Consejo de Seguridad Nacional, que reconocen las autoridades Chinas se inspira en el estadounidense, aunque se observan importantes diferencias. En los Estados Unidos, el Consejo Nacional de Seguridad sirve como órgano asesor del presidente y se utiliza para coordinar las políticas entre los distintos organismos y departamentos gubernamentales. Por el contrario, el Consejo de Seguridad Nacional de China es una institución del Partido Comunista de China, dirigido por el presidente chino, a la vez presidente del Politburó. De esta forma en China este consejo es una agencia de coordinación administrativa, A diferencia de su homólogo de Estados

Unidos que supervisa varios departamentos. El Consejo de Seguridad Nacional de China es un organismo interministerial, que además coordina los esfuerzos de la Asamblea Popular Nacional y la Conferencia Consultiva del Pueblo Chino.

El tercer gran actor político del que se analiza su estrategia nacional de seguridad es la Federación de Rusia. El concepto de seguridad en Rusia se encuentra muy ligado a las ideas desarrolladas por Mackinder y la “tierra corazón”; de este modo Rusia percibe su seguridad basada en el espacio geopolítico definido por el territorio continental, en el entendimiento que es la zona clave para conservar el poder y mantener el control de otros espacios geopolíticos adyacentes, en una región cardial o área pivote definida por Asia Central y Europa Oriental.

La seguridad en Rusia tiene una tradición que ha llevado a que tenga un corpus legislativo integrado relacionado con la seguridad nacional, destacando documentos de estrategia de seguridad, relaciones exteriores, doctrina militar y ciberseguridad.

La Estrategia de Seguridad Nacional de la Federación de Rusia para el año 2020, aprobada en mayo de 2009, y la Doctrina Militar de la Federación de Rusia hasta el 2020, de diciembre de 2014, son los textos estratégicos que diseñan la percepción rusa de la seguridad, de sus intereses nacionales, de las amenazas y riesgos a los que se enfrenta Rusia, así como definen las líneas estratégicas que permiten una capacidad de protección y respuesta en defensa de los intereses nacionales.

Al igual que Estados Unidos y China, Rusia también ha conformado un Consejo de Seguridad Nacional, que está presidido por el Presidente de Rusia, de acuerdo con la Constitución de la Federación de 1993. La Ley Federal "Sobre la Seguridad", de conformidad con el artículo 83 de la Constitución de la Federación de Rusia, define el estatuto del Consejo de Seguridad de Rusia, sus objetivos, funciones, composición y organización de sus actividades.

Del estudio de estos tres grandes actores políticos, con intereses globales en materia de seguridad se desprenden las siguientes conclusiones: 1. Las estrategias nacionales de seguridad, iniciadas por Estados Unidos, se han convertido en el modelo de

documento maestro del que se desprende la planificación de la seguridad nacional. 2. Estas estrategias nacionales de seguridad obedecen a un esquema similar, en primer lugar se presenta la percepción nacional del escenario global; posteriormente se definen los intereses nacionales; a continuación se analizan las amenazas y riesgos contra los intereses nacionales en distintos ámbitos; después se enuncian las líneas estratégicas que el estado desarrollará para proteger los intereses nacionales y para recuperar la situación anterior en el caso de que se haya producido una agresión; por último, las estrategias generan unas estructuras que permiten gestionar la seguridad nacional. 3. La integración de los intereses nacionales es total, en especial destaca la importancia de la capacidad económica como referente transversal de la seguridad. 4. Los tres países se han dotado de un consejo de seguridad nacional que asesora al presidente de la nación. 5. Se ha establecido una jerarquía de los niveles de la seguridad que ha generado diferentes organismos con responsabilidades en esta materia. 6. Los aspectos militares, aunque de gran importancia se encuentran integrados en las estrategias nacionales de seguridad y responden a lo definido en estos documentos en este ámbito. 7. Las estrategias nacionales de seguridad se desarrollan mediante estrategias sectoriales, como es el caso de las estrategias nacionales de ciberseguridad.

CAPÍTULO 4. INICIATIVAS INTERNACIONALES EN EL ÁMBITO DEL PLANEAMIENTO DE LA CIBERSEGURIDAD

Tras haber analizado las estrategias nacionales de seguridad de Estados Unidos, la República Popular China y la Federación de Rusia, para enmarcar los principales modelos nacionales de seguridad, en el capítulo cuarto se han estudiado las iniciativas internacionales en el ámbito del planeamiento de la ciberseguridad, referidas a la Unión Europea, la Organización de las Naciones Unidas, la Organización del Tratado del Atlántico Norte y la Organización para la la Seguridad y la Cooperación en Europa. Se han elegido estas cuatro organizaciones por ser las principales con responsabilidades en el ámbito de la ciberseguridad en diferentes niveles, global y regionales.

La Unión Europea se ha tomado como referencia principal en el ámbito internacional, ya que España, como Estado miembro, se encuentra obligada en el cumplimiento de la normativa comunitaria, debiendo trasponer la legislación pertinente. Además, España forma parte de sus estructuras de seguridad, defensa y ciberseguridad.

4.1. UNIÓN EUROPEA

4.1.1. La Política Exterior y de Seguridad Común (PESC) y La Política Común de Seguridad y Defensa (PCSD) de la UE

4.1.1.1. La Política Exterior y de Seguridad Común (PESC) de la UE

El Tratado de Lisboa ha modificado los dos textos fundamentales de la Unión Europea: el Tratado de la Unión Europea (TUE) y el Tratado constitutivo de la Comunidad Europea, documento éste último que ha pasado a denominarse Tratado de Funcionamiento de la Unión Europea (TFUE)[273].

[273] Se ha utilizado para este capítulo diferentes apartados de la publicación: VILLALBA FERNÁNDEZ, ANÍBAL: “El Tratado de Lisboa y la Política Común de Seguridad y Defensa”, en Panorama

En el ámbito de la Política Exterior y de Seguridad Común, la entrada en vigor del Tratado de Lisboa ha supuesto el comienzo de un proceso destinado a favorecer que la Unión Europea tenga una estructura más armónica y le permita afrontar de modo más eficaz los retos en su acción exterior.

La personalidad jurídica de la UE, que es introducida en el art. 47 del Tratado de Lisboa, constituye un aspecto de gran relevancia. El art. 37 señala que la Unión podrá celebrar acuerdos con uno o varios Estados u organizaciones internacionales en los ámbitos comprendidos en el capítulo relativo a la PESC. Esta personalidad jurídica única de la Unión robustecerá su capacidad de interlocución, convirtiéndola en un actor más eficaz a escala internacional y un socio más visible para otros países y organizaciones internacionales.

La conformación de la personalidad jurídica de la Unión Europea constituye un aspecto de importante calado, que permite a la Unión celebrar acuerdos con Estados u organizaciones internacionales en los ámbitos de la PESC. Esta personalidad jurídica única de la Unión ha robustecido su capacidad de interlocución, convirtiéndola en un actor más eficaz a escala internacional y un socio más visible para otros países y organizaciones internacionales.

Esta personalidad jurídica, no obstante, no conlleva un tratamiento diferente en el proceso de toma de decisiones en la UE. La unanimidad continúa siendo indispensable para cualquier decisión que permita a la Unión la firma de un documento contractual con implicaciones en seguridad o defensa, según se recoge en los arts. 31 y 38 del Tratado de Lisboa.

Todo ello ajustándose a los criterios de consenso, pragmatismo y flexibilidad para favorecer los principios que el Tratado de Lisboa recoge en su art. 21 al señalar que "La acción de la Unión en la escena internacional se basará en los principios que han

---

Estratégico 2009/2010, pp. 151-184. Ministerio de Defensa; Instituto Español de Estudios Estratégicos y Real Instituto Elcano. Madrid, marzo 2010.

inspirado su creación, desarrollo y ampliación y que pretende fomentar en el resto del mundo: la democracia, el Estado de Derecho, la universalidad e indivisibilidad de los derechos humanos y de las libertades fundamentales, el respeto de la dignidad humana, los principios de igualdad y solidaridad y el respeto de los principios de la Carta de las Naciones Unidas y del Derecho internacional".

De esta forma, la Política Exterior y de Seguridad Común cobra una nueva dimensión tras la entrada en vigor del Tratado de Lisboa. Un cambio significativo en la nueva arquitectura de la UE es la supresión de la estructura de "pilares", que había sido introducida por el Tratado de Maastricht.

El estímulo que el Tratado de Lisboa ofrece a la PESC quiere permitir que la Unión Europea siga progresando en su objetivo de ser un actor integral en la escena internacional. De esta forma, se han modificado estructuras, creado instrumentos, simplificado procedimientos, potenciado capacidades y flexibilizado mecanismos, así como se ha definido una poderosa estructura que se espera permita a la UE desarrollar su potencial en los campos de la política internacional y la seguridad.

El Tratado de Lisboa ha introducido cambios significativos en el plano institucional de la Unión, con el objetivo de impulsar la Política Exterior y de Seguridad Común. A continuación se analizan los efectos en las principales instituciones y órganos de la UE en lo que afecta a la Política Exterior y de Seguridad Común.

El Consejo Europeo

Con el Tratado de Lisboa, el Consejo Europeo pasa a ser una institución independiente. Antes del Tratado de Lisboa, el Consejo Europeo no era una institución, sino la forma que adoptaba el Consejo cuando se reunía a nivel de Jefes de Estado y de Gobierno y de Presidente de la Comisión.

El Consejo Europeo fija los principios y orientaciones generales de la PESC y aprueba, a iniciativa propia o del Consejo, las Estrategias comunes (arts. 13. 1 y 2 del TUE - Niza). Al Consejo Europeo le corresponde asimismo la decisión de abrir la vía a una

Defensa común (art. 17 TUE - Niza). El Consejo Europeo se constituye finalmente en instancia de apelación suprema en caso de que un Estado se oponga a una decisión que pueda adoptarse por mayoría cualificada (art. 23.2 TUE - Niza).

Aunque el Tratado de Lisboa prevé que el Consejo Europeo pueda decidir por unanimidad que una decisión del Consejo que normalmente requiera unanimidad pueda ser aprobada por mayoría cualificada, o solicitar al Alto Representante que ejerza su derecho de iniciativa para obtener el mismo resultado, se exceptúan las decisiones que tengan repercusiones en el ámbito militar o de la defensa (art. 31.4 del TUE - Lisboa).

Con el Tratado de Lisboa el Consejo Europeo elige por mayoría cualificada a su Presidente, cuyo mandato es de dos años y medio, prorrogable una vez. Una de las funciones del Presidente del Consejo Europeo es la de asumir, de acuerdo con su rango y condición, la representación exterior de la Unión en los asuntos de PESC, sin perjuicio de las atribuciones del AR.

Es responsabilidad del Consejo Europeo nombrar por mayoría cualificada, con la aprobación del Presidente de la Comisión, al Alto Representante de la Unión para Asuntos Exteriores y Política de Seguridad. El Consejo Europeo podrá poner fin a su mandato por el mismo procedimiento (art. 18 TUE - Lisboa). Si un acontecimiento internacional así lo exige, el Presidente del Consejo Europeo convocará una reunión extraordinaria para definir las líneas estratégicas de la política de la Unión ante dicho acontecimiento (art. 26 TUE - Lisboa).

El Consejo

El Consejo está compuesto por un representante de cada Estado miembro con rango ministerial, facultado para comprometer al Gobierno de dicho Estado miembro (art. 16 TUE - Lisboa). Su funcionamiento está regulado por su Reglamento Interno[274] (RI, que deberá ser modificado con la entrada en vigor del Tratado de Lisboa). Entre las

[274] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:285:0047:0071:ES:PDF

formaciones del Consejo, hasta la entrada en vigor del Tratado de Lisboa, destacaba la de Asuntos Generales y Relaciones Exteriores (CAGRE).

El CAGRE abarcaba dos ámbitos principales de actuación (art. 2.2 del RI):

- La preparación y seguimiento de las reuniones del Consejo Europeo, incluida la coordinación necesaria de todos los trabajos preparatorios, la coordinación general de las políticas, las cuestiones institucionales y administrativas, los asuntos horizontales que afecten a varias políticas de la Unión y cualquier asunto que le encomiende el Consejo Europeo.
- El conjunto de la actuación exterior de la Unión, la PESC incluida la PESD, el comercio exterior, la cooperación para el desarrollo y la ayuda humanitaria.

Hasta la entrada en vigor del Tratado de Lisboa, la Presidencia del Consejo se ejercía por rotación por cada Estado miembro durante un período de seis meses. Con el Tratado de Lisboa este esquema cambia: aunque el turno de Presidencias del Consejo desempeñadas por los Estados miembros se mantiene se exceptúa del mismo el ámbito de la PESC, en que la mayoría de funciones hasta ahora atribuidas a la Presidencia pasan al AR, que presidirá el Consejo de Asuntos Exteriores, contribuirá con sus propuestas a elaborar la PESC y se encargará de ejecutar las decisiones adoptadas por el Consejo Europeo y el Consejo (art. 27.1 TUE - Lisboa).

El CAGRE pasa a dividirse en dos formaciones distintas:

- *El Consejo de Asuntos Generales* (CAG), que es presidido por un representante del Estado miembro que ejerza la Presidencia rotatoria y tiene como funciones velar por la coherencia de los trabajos de las diferentes formaciones del Consejo, preparar las reuniones del Consejo Europeo y garantizar su actuación subsiguiente, en contacto con el Presidente del Consejo Europeo y la Comisión (art.16. 6 del TUE - Lisboa).
- *El Consejo de Asuntos Exteriores* (CAE), que pasa a ser presidido por el AR, y que elaborará la acción exterior de la Unión atendiendo a las líneas estratégicas

definidas por el Consejo Europeo y velará por la coherencia de la acción de la Unión (art.16. 6 del TUE - Lisboa).

Conviene señalar además que el Art. 21. 3 TUE - Lisboa señala que “La Unión velará por mantener la coherencia entre los distintos ámbitos de su acción exterior y entre éstos y sus demás políticas. El Consejo y la Comisión, asistidos por el Alto Representante de la Unión para Asuntos Exteriores y Política de Seguridad, garantizarán dicha coherencia y cooperarán a tal efecto”.

El trío de Presidencias

Se encuentra previsto en el art. 2.4 del Reglamento Interno que establece que “cada 18 meses, las tres Presidencias entrantes prepararán, en estrecha cooperación con la Comisión y una vez realizadas las consultas adecuadas, un proyecto de programa de actividades del Consejo para ese período. Las tres Presidencias presentarán conjuntamente el proyecto de programa como mínimo un mes antes de que comience el período correspondiente para que lo confirme el CAGRE”.

El Proyecto de Decisión del Consejo Europeo anejo al Tratado de Lisboa señala en su art. 1 que la Presidencia del Consejo, con excepción de la formación de Asuntos Exteriores, será desempeñada por grupos predeterminados de tres Estados miembros durante un período de dieciocho meses. Estos grupos se formarán por rotación igual de los Estados miembros, atendiendo a su diversidad y a los equilibrios geográficos en la Unión. Cada miembro del grupo ejercerá por rotación, durante un período de seis meses, la presidencia de todas las formaciones del Consejo, con excepción de la formación de Asuntos Exteriores. Los demás miembros del grupo asistirán a la Presidencia en todas sus responsabilidades con arreglo a un programa común.

El Parlamento Europeo

El Parlamento Europeo (PE) es consultado y regularmente informado por la Presidencia y por la Comisión sobre el desarrollo de la PESC. El PE realiza preguntas y recomendaciones al Consejo. El PE mantiene un debate anual sobre los progresos

en la aplicación de la PESC (art. 21 TUE - Niza). Además el AR debe asegurarse de que el PE y los Estados miembros están plenamente informados de la aplicación de una cooperación reforzada en el campo de la PESC (art. 27d TUE - Niza).

En la práctica, el PE tiene mayor influencia de la que pudiera parecer en materia de PESC, a través de su participación en la aprobación el Presupuesto, que incluye el montante global atribuido a la PESC, así como de las comparecencias ante el Plenario, ante la Comisión de Asuntos Exteriores y ante las Subcomisiones de Derechos Humanos y de Defensa.

En cuanto al papel del PE en el Tratado de Lisboa, la Declaración 14 aneja al mismo señala que las disposiciones correspondientes a la PESC no confieren nuevos poderes de iniciativa a la Comisión ni amplían la función del Parlamento Europeo. En estas circunstancias, el PE debería simplemente consultado e informado por el Alto Representante en los aspectos principales de la PESC y de la PCSD.

No obstante, el Parlamento ve reforzados indirectamente sus poderes en este ámbito pues es necesario su consentimiento para el nombramiento del AR en su condición de Vicepresidente de la Comisión, y sigue pudiendo aprobar una moción de censura contra la Comisión, lo que afectaría al AR en su condición de miembro de la misma.

Además, se pasa de un debate anual a dos debates sobre la PESC y se incluye expresamente a la PCSD en los mismos. Finalmente, el PE podrá dirigir preguntas no sólo al Consejo, sino también al AR/VP, que será la persona encargada, en lugar de la Presidencia, de consultar con él periódicamente acerca de los aspectos principales y las opciones fundamentales de la PESC (incluida la PCSD), de informarle de la evolución de dichas políticas y de velar por que se tengan debidamente en cuenta sus opiniones.

La Comisión Europea

La Comisión Europea se encuentra plenamente ligada a los trabajos de la PESC (art. 27 TUE - Niza). Tiene derecho de iniciativa en materia de PESC (pero no exclusivo

como en materia comunitaria, sino compartido con los Estados miembros, de acuerdo con el art. 22 TUE - Niza) y comparte además con el Consejo la responsabilidad de velar por la coherencia del conjunto de la acción exterior de la Unión (art. 3 TUE - Niza). También comparte con la Presidencia la responsabilidad de mantener regularmente informado al PE sobre el desarrollo de la política exterior y de seguridad (art. 21 TUE - Niza).

Con el Tratado de Lisboa el derecho de iniciativa de la Comisión en materias PESC desaparece, pues es el AR en calidad de tal quién podrá hacer propuestas al Consejo en este campo (art. 18. 2 TUE - Lisboa). En todo caso y en virtud del art. 17.1 TUE - Lisboa, salvo en materia de PESC y de los demás casos previstos por los Tratados, la Comisión asumirá la representación exterior de la Unión.

El Tribunal de Justicia de la Unión Europea y el Tribunal de Cuentas

El Tribunal de Justicia de la Unión Europea y el Tribunal de Cuentas no tienen competencias en materia de PESC. El art 24 del TUE - Lisboa establece que el Tribunal de Justicia de la Unión Europea no tendrá competencia respecto de las disposiciones relativas a la PESC, con la salvedad de su competencia para controlar el respeto del artículo 40 del Tratado sobre cooperaciones reforzadas y para controlar la legalidad de determinadas decisiones contempladas en el art. 275 del Tratado de Funcionamiento de la Unión Europea en relación con el establecimiento de medidas restrictivas frente a personas físicas o jurídicas.

Alto Representante de la Unión para Asuntos Exteriores y Política de Seguridad Común

Una de las principales novedades en materia de PESC que introduce el Tratado de Lisboa es la nueva figura del Alto Representante para Asuntos Exteriores y Política de Seguridad / Vicepresidente de la Comisión. Al ser el AR también uno de los Vicepresidentes de la Comisión, encargado en ella de las relaciones exteriores y de la acción exterior de la Unión, su nombramiento como tal está sometido a las reglas que se aplican a la Comisión y por tanto a la aprobación del PE.

El AR se encuentra al frente de la PESC, preside el Consejo de Asuntos Exteriores y vela por la coherencia de la acción exterior de la Unión (art. 18 TUE - Lisboa). Cuando la Unión haya definido una posición común sobre un tema incluido en el orden del día del Consejo de Seguridad de las Naciones Unidas, los Estados miembros que sean miembros de éste pedirán que se invite al AR a presentar la posición de la Unión (art. 34 TUE - Lisboa).

El AR tiene capacidad de propuesta o iniciativa en materia de PESC/PCSD (arts. 30 y 42 TUE - Lisboa). Además, en los casos que requieran una decisión rápida, el AR puede convocar, de oficio o a petición de un Estado miembro, una reunión extraordinaria del Consejo en un plazo de 48 horas o, en caso de absoluta necesidad, en un plazo más breve (art. 30 TUE - Lisboa). Finalmente, el AR representará a la Unión en las materias concernientes a la PESC, dirigirá el diálogo político con terceros en nombre de la Unión y expresará la posición de la Unión en las organizaciones internacionales y en las conferencias internacionales (art. 27 TUE - Lisboa).

El Tratado de Lisboa creó el *Servicio Europeo de Acción Exterior (SEAE)*, en el que se apoya el AR para el ejercicio de su mandato. Este servicio trabaja en colaboración con los servicios diplomáticos de los Estados miembros y esta compuesto por funcionarios de la Secretaría General del Consejo y de la Comisión y por personal en comisión de servicios de los servicios diplomáticos nacionales. Este SEAE constituyó la primera prioridad de la primera Alta Representante Catherine Ashton[275].

Comité de los Representantes Permanentes de los Estados miembros (COREPER)

Un Comité compuesto por los representantes permanentes de los Estados miembros se encarga de preparar los trabajos del Consejo y de realizar las tareas que éste le

[275] ASHTON, CATHERINE. "*La ambición de actuar*". El Mundo. 22 de diciembre de 2009. http://www.elmundo.es/elmundo/2009/12/22/union_europea/1261454578.html

confíe. El COREPER está presidido por el representante permanente o el representante permanente adjunto del Estado que ejerza la Presidencia del Consejo.

Por lo que se refiere al Tratado de Lisboa el proyecto de Decisión del Consejo Europeo aneja al Tratado, relativa al ejercicio de la Presidencia del Consejo, señala que la presidencia del COREPER será ejercida por un representante del Estado miembro que presida el Consejo de Asuntos Generales.

Comité Político y de Seguridad (COPS)

Sin perjuicio del papel que corresponde al COREPER, el Comité Político y de Seguridad (COPS), en su formación de Embajadores Representantes en el COPS o en la de Directores Políticos, seguirá la situación internacional en los asuntos relativos a la PESC y contribuirá a definir la política mediante la emisión de dictámenes dirigidos al Consejo, bien a instancias de éste bien a iniciativa propia. En este aspecto, el Tratado de Lisboa añade también la iniciativa del AR.

Asimismo, el COPS debe supervisar la ejecución de las políticas acordadas, sin perjuicio de las competencias de la Presidencia, la Comisión y el AR. El COPS ejerce, bajo la responsabilidad del Consejo, y del AR tras la entrada en vigor del Tratado de Lisboa, el control político y la dirección estratégica de las operaciones de gestión de crisis. El Tratado de Lisboa contempla que la presidencia del COPS sea desempeñada por un representante del Alto Representante.

La red de Corresponsales europeos

La red de Corresponsales europeos, que fue establecida en el marco de la Cooperación Política Europea, está compuesta por los jefes de los Departamentos de PESC de los Estados miembros. Prestan apoyo a los Directores Políticos y son los puntos de contacto entre las capitales de los Estados miembros, para cuyo fin

gestionan la red COREU. Tiene también por misión acompañar a los Ministros de Asuntos Exteriores en sus reuniones informales en formato Gymnich[276].

El Tratado de Lisboa abandona la tipología de la PESC que distinguía ente Estrategias comunes, posiciones comunes y acciones comunes para referirse de modo general a "decisiones", aunque en la práctica la diferencia es limitada ya que la nueva denominación no afecta sustancialmente al proceso de toma de decisiones y porque la nueva tipología sigue el modelo anterior.

Así, se habla de:

- Decisiones del Consejo Europeo que determinen los intereses estratégicos de la Unión, fijen sus objetivos y definan las orientaciones generales de la PESC, incluidos los asuntos que tengan repercusiones en el ámbito de la defensa (art. 26 TUE – Lisboa). Estas decisiones corresponden a las estrategias comunes del TUE - Niza.
- Decisiones que definan el enfoque de la Unión sobre un asunto concreto de carácter geográfico o temático (art. 29 TUE – Lisboa). Estas decisiones corresponden a las posiciones comunes del TUE - Niza.
- Decisiones necesarias para la ejecución de acciones operativas de la Unión (art. 28 TUE – Lisboa). Estas decisiones corresponden a las acciones comunes del TUE - Niza.

En cuanto a la información y consulta recíproca entre Estados miembros, éstos se consultarán en el seno del Consejo Europeo y del Consejo sobre cualquier cuestión de política exterior y de seguridad que revista un interés general, materializando los llamados enfoques comunes (art. 32 TUE - Lisboa).

[276] El "Gymnich", que se celebra una vez por semestre, toma su nombre del castillo alemán donde se celebró la primera reunión de este tipo (1974) entre ministros de Asuntos Exteriores de la Unión Europea, presidida en aquel momento por Alemania. Esta reunión informal, en el sentido que permite un intercambio libre y profundo entre participantes, no da lugar a conclusiones propiamente dichas, pero permite preparar las posiciones de la diplomacia europea para los meses que siguen.

4.1.1.2. La Política Común de Seguridad y Defensa (PCSD) de la UE

Uno de los instrumentos de la Política Exterior y de Seguridad Común (PESC) de la UE que conoció mayor desarrollo en la década de 2000 a 2010 fue la Política Europea de Seguridad y Defensa (PESD), que se conviertió tras el Tratado de Lisboa en Política Común de Seguridad y Defensa (PCSD).

La PESD tuvo su origen en el nivel de frustración que se generó tras la falta de capacidad europea para actuar sobre el terreno durante la crisis de la desintegración de Yugoslavia, y en particular en el conflicto de Bosnia y Herzegovina.

Con el antecedente de la Cumbre franco-británica de Saint Malo en diciembre de 1998 en que ambos países decidieron dar impulso a la PESD, en el Consejo Europeo de Colonia en diciembre de 1999 se definieron los objetivos en materia de desarrollo de capacidades militares de gestión de crisis, y en el Consejo Europeo de Feira en junio de 2000 en materia de capacidades civiles.

El Consejo Europeo de Niza en diciembre de 2000 incorporó las funciones de gestión de crisis de la Unión Europea Occidental (UEO) a la UE, creó estructuras permanentes en la Secretaría General del Consejo especializadas en cuestiones de PESD y definió las relaciones de la UE y los países terceros en materia de defensa.

En el Consejo Europeo de Laeken en diciembre de 2001 la PESD se declaró operativa y en el Consejo Europeo de Sevilla en junio de 2002 la UE amplió los ámbitos de actuación de la PESD a la lucha contra el terrorismo. En el Consejo Europeo de Copenhague en diciembre de 2002 concluyó un acuerdo con la OTAN conocido como “Berlín Plus”, que facilita a la UE recurrir a capacidades, órganos de planeamiento y estructuras de mando de la OTAN.

Javier Solana, Alto Representante de la UE para la PESC desde octubre de 1999 a diciembre de 2009, señala que la Unión se adelantó a su tiempo en 1999 en relación a la PESD. Apunta Solana que la naturaleza integral y multifuncional de la aproximación de la UE a la seguridad constituyó una novedad. De esta forma, la UE

continúa siendo la única organización capaz de utilizar una amplia variedad de instrumentos que favorezcan la estabilidad, tanto para prevenir una situación de crisis, como para restaurar la paz y reconstruir las instituciones después de un conflicto. Estas capacidades de la UE, complementadas por las herramientas políticas tradicionales de los Estados Miembros, constituyen el valor añadido de la UE, que permite combinar ayuda humanitaria, apoyo para la reconstrucción de las instituciones y buen gobierno en países en desarrollo, con las capacidades de gestión de crisis y asistencia técnica y financiera, sin olvidar las clásicas herramientas diplomáticas como el diálogo político y la mediación.

Solana afirma que el propósito de la UE en materia PESD es promover la paz y la seguridad en el mundo, siendo la razón de ser de las operaciones la gestión de crisis, la seña de identidad una aproximación holística y la característica clave la flexibilidad. De esta forma, la Unión aspira a ofrecer soluciones diseñadas específicamente para las complejas necesidades en materia de seguridad. Todo ello teniendo en cuenta que los conflictos actuales demuestran que una solución de carácter militar no es ni la única ni la mejor solución, en particular durante la fase de estabilización de una crisis. No obstante, la UE ofrece una combinación de recursos civiles y militares que pueden ser utilizados de forma conjunta o separada.

Además, señala Solana que la UE actúa de modo autónomo o en cooperación con otros y que aunque es en el propio interés de la Unión promover estabilidad en los espacios adyacentes a la UE, la acción de la Unión no se circunscribe a este escenario, ya que la UE es un actor global con responsabilidades en la esfera internacional. De este modo, la comunidad política que es la Unión quiere continuar colaborando en la mejora del bien común, basándose en la democracia, la libertad y el imperio de la ley[277].

[277] SOLANA, Javier. *"Ten years of European Security and Defence Policy"*. ESDP newsletter. European Security and Defence Policy 1999-2009. Octubre 2009. http://www.consilium.europa.eu/uedocs/cmsUpload/ESDP%20newsletter%20-%20Special%20issue%20ESDP@10.pdf

Abundando en esta sensación, el General Bentégeat, Presidente del Comité Militar de la UE, estima que se ha conformado un sentimiento colectivo de confianza en la eficacia de la PESD, basado en resultados concretos y alimentado por el desarrollo constante y sostenido de las capacidades militares colectivas, de la cadena de mando, de los conceptos y procedimientos operativos, y de una reacción ágil en la intervención.

De otra parte, Bentégeat señala tres desafíos para continuar el progreso. En primer lugar y más importante, acelerar la integración de la capacidad de la UE en el exterior lo que requiere que la planificación y la gestión de crisis se encuentren totalmente integrados, tanto en Bruselas como sobre el terreno. En segundo término, la crisis económica no debe limitar la capacidad de acción ni la autonomía de la Unión. Por último, la UE debe reforzar los mecanismos de cooperación con otros organismos como la ONU, la OTAN y la Unión Africana[278].

Otros actores estiman también necesario avanzar en la relación con la OTAN en el campo de gestión de crisis, aunque señalan que las soluciones aportadas por la PESD en este ámbito reflejan la superación de los mecanismos establecidos en el acuerdo "Berlín Plus", que se basaba en una concepción ya superada de división del trabajo entre la OTAN en el plano puramente militar y la UE en el campo de la gestión de crisis de corte humanitario[279].

En este ámbito, algunos analistas apuntan al desarrollo de soluciones integrales como la creación de una estructura civil y militar de planificación estratégica para las operaciones y misiones PCSD, integrada por un comité político y de seguridad, un

[278] BENTÉGEAT, Henri. "*Nous avons développé un sentiment de confiance dans l'efficacité de la PESD"*. ESDP newsletter. European Security and Defence Policy 1999-2009. Octubre 2009.

[279] ASAMBLEA DE LA UNIÓN EUROPEA OCCIDENTAL. "*The EU-NATO Berlin Plus agreements*". Factsheet Nº 14. Noviembre 2009. http://www.assembly-weu.org/en/documents/Fact%20sheets/14E_Fact_Sheet_Berlin_Plus.pdf?PHPSESSID=ad7ba3060e75d20eca30f2c9c9daaedd

comité militar, personal militar y una célula civil y militar con un centro de operaciones[280].

El Tratado de Lisboa modifica el nombre de la Política Europea de Seguridad y Defensa (PESD), que pasa a llamarse Política Común de Seguridad y Defensa (PCSD), alineando así su denominación con las demás políticas comunes. De modo general, el Tratado de Lisboa en el campo de la seguridad y la defensa afecta a la armonización de la estructura institucional, lo que debería facilitar las relaciones entre instituciones clave como el Consejo y la Comisión respecto a la Política Común de Seguridad y Defensa[281].

Es muy significativo el preámbulo del Tratado de Lisboa, que recoge la voluntad de los Estados miembros de la Unión Europea para desarrollar una Política Exterior y de Seguridad Común que incluya la definición progresiva de una política de defensa común que podría conducir a una defensa común, reforzando así la identidad y la independencia europeas, con el fin de fomentar la paz, la seguridad y el progreso en Europa y en el mundo.

De esta forma, la PCSD ha venido a impulsar un salto de calidad en el campo de la seguridad y la defensa, estableciendo instrumentos para facilitar que la Unión genere y exporte seguridad, como elemento indispensable de la Política Exterior y de Seguridad Común (PESC).

Cooperación Estructurada Permanente

[280] PÉREZ DE LAS HERAS, BEATRIZ Y CHURRUCA MUGURUZA, CRISTINA. "Las capacidades civiles y militares de la UE: estado de la cuestión y propuestas de cara a la Presidencia Española 2010". Fundación Alternativas. Documento de Trabajo 41/2009. http://www.falternativas.org/opex/documentos-opex/documentos-de-trabajo/las-capacidades-civiles-y-militares-de-la-ue-estado-de-la-cuestion-y-propuestas-de-cara-a-la-presidencia-espanola-2010

[281] MÖLLING, CHRISTIAN. "*ESDP After Lisbon: More Coherent and Capable?*". Center for Security Studies (CSS), Zurich, Suiza. Vol. 3, Nº 28, febrero 2008. http://www.isn.ethz.ch/isn/Digital-Library/Publications/Detail/?ots591=0C54E3B3-1E9C-BE1E-2C24-A6A8C7060233&lng=en&id=46839

Una novedad relevante es que, de acuerdo con el art. 42.6 del TUE - Lisboa los Estados miembros que cumplan criterios más elevados de capacidades militares y que hayan suscrito compromisos más vinculantes en la materia para realizar las misiones más exigentes establecerán una Cooperación Estructurada Permanente (CEP) en el marco de la Unión. Esta fórmula nace con el ánimo de mejorar las capacidades de defensa para fortalecer la habilidad de la Unión Europea para reaccionar ante las crisis[282].

El artículo 46 establece que los Estados miembros que deseen participar en la CEP y que reúnan los criterios y asuman los compromisos en materia de capacidades militares que figuran en el Protocolo sobre la CEP notificarán su intención al Consejo y al AR. En un plazo de tres meses a partir de la notificación, el Consejo, tras escuchar al AR, se pronunciará por mayoría cualificada. Cualquier Estado miembro que, con posterioridad, desee participar en la CEP notificará su intención al Consejo y al AR. El Consejo, tras consultar al AR, por mayoría cualificada en votación en la que sólo participarán los Estados miembros participantes en la CEP, adoptará una decisión por la que se confirme la participación del Estado miembro de que se trate, que cumpla los criterios y asuma los compromisos previstos en el mencionado Protocolo.

También se contempla la posibilidad de la salida voluntaria de un Estado miembro de la CEP, o la suspensión de su participación en caso de que ya no cumpla los criterios o no pueda asumir los compromisos.

Sven Biscop alerta de los riesgos que presenta un desequilibrio en la puesta en práctica de la Cooperación Estructurada Permanente. Si bien una vanguardia de países comprometidos podría probablemente lograr una mayor cohesión y mejorar la expectativa de resultados a corto plazo, las consecuencias de dejar fuera a otras naciones podría obscurecer políticamente esta iniciativa. De hecho, podría incluso

[282] CONSEJO DE LA UNIÓN EUROPEA. "*Diez años de PESD: Retos y Oportunidades*". Declaración Ministerial del 2974 Consejo de Relaciones Exteriores. 17 de noviembre de 2009. http://www.consilium.europa.eu/uedocs/cms_Data/docs/pressdata/en/gena/111253.pdf

llevar a crear a crear una división de Estados miembros en la puesta en práctica de medidas de la Política Común de Seguridad y Defensa[283].

La conclusión es que la CEP es un mecanismo que permite participar en el desarrollo de las capacidades de la Europa de la defensa, facilitando el impulso de procesos que de otra forma serían muy complicados para generar consensos. No obstante, la CEP debe ser inclusiva y facilitar en lo posible la incorporación progresiva de aquellos Estados miembros que lo deseen.

Cooperaciones Reforzadas

El artículo 20 del TUE - Lisboa, señala que los Estados miembros que deseen instaurar entre sí una Cooperación Reforzada en el marco de las competencias no exclusivas de la Unión podrán hacer uso de las instituciones de ésta y ejercer dichas competencias aplicando las disposiciones pertinentes de los Tratados.

Las Cooperaciones Reforzadas se permitirán en cualquiera de los ámbitos del Tratado, entre ellos la Política Común de Seguridad y Defensa. En cualquier caso, la decisión de autorizar una Cooperación Reforzada será adoptada por el Consejo como último recurso, cuando haya llegado a la conclusión de que los objetivos perseguidos por dicha cooperación no pueden ser alcanzados en un plazo razonable por la Unión en su conjunto, y a condición de que participen en ella al menos nueve Estados miembros.

Además, El Consejo y la Comisión velarán por la coherencia de las acciones emprendidas en el marco de una cooperación reforzada, así como la coherencia de dichas acciones con las políticas de la Unión, cooperando a tal efecto, según se recoge en el art. 334 del Tratado de Funcionamiento de la UE.

Estas salvaguardias encajan con la preocupación manifestada durante el proceso político que ha conducido al Tratado de Lisboa. En este sentido, iniciativas como la

[283] BISCOP, SVEN. *"Permanent Structured Cooperation and the future of ESDP"*. Egmont Paper 20. Royal Institute for International relations. http://www.egmontinstitute.be/paperegm/ep20.pdf

propuesta por Pierre Lellouche de avanzar en la defensa común en torno a un núcleo de "cooperación reforzada" compuesto por un grupo de seis naciones formado por Francia, Reino Unido, Alemania, España, Italia y Polonia, preocupó en diferentes ámbitos por el riesgo de ignorar el potencial de otros Estados miembros, aunque el propio Lellouche señalaba que los demás países podrían unirse al grupo de "pioneros" en cualquier momento[284].

Un aspecto interesante en el desarrollo de las C*ooperaciones Reforzadas* en los ámbitos de seguridad y defensa es su relación con la *Cooperación Estructurada Permanente*, ya que este último mecanismo es la primera vez que se recoge en un texto de la Unión, y aunque las inquietudes generadas su puesta en práctica, como por ejemplo que los Estados miembros que participen en la Cooperación Estructurada Permanente decidan establecer una misión de mutuo acuerdo en nombre de la UE, han sido articuladas en el proceso de toma de decisiones de la UE, nada impide que este mismo grupo de países pudiera tomar decisiones como el establecimiento de una misión *ad hoc* fuera del ámbito de la UE, lo que podría llevar a un *de facto* conflicto institucional[285].

Ampliación del tipo de misiones PESD

El Tratado de Lisboa, atendiendo a la evolución de la PESD en los últimos años, completa las “misiones Petersberg” recogidas en el Tratado de Amsterdam, que se desglosaban en misiones humanitarias o de rescate; misiones de mantenimiento de la paz; y misiones con fuerzas de combate para la gestión de crisis, incluidas las misiones de restablecimiento de la paz.

[284] LELLOUCHE, PIERRE. “*8 propositions pour donner à l'Union une défense commune*”. Le Figaro. 31 de enero de 2008. http://www.lefigaro.fr/debats/2008/01/31/01005-20080131ARTFIG00515--propositions-pour-donner-a-l-union-une-defense-commune.php

[285] QUILLE, GERRARD. “The Lisbon Treaty and its implications for CFSP/ESDP”. Directorate-General for External Policies of the Union, European Parliament, febrero 2008. http://www.europarl.europa.eu/document/activities/cont/200805/20080513ATT28796/20080513ATT28796EN.pdf

En el art. 43 del TUE - Lisboa, se especifica que la Unión podrá recurrir a medios civiles y militares en misiones fuera de la Unión que tengan por objetivo garantizar el mantenimiento de la paz, la prevención de conflictos y el fortalecimiento de la seguridad internacional, conforme a los principios de la Carta de las Naciones Unidas, que abarcarán las actuaciones conjuntas en materia de desarme, las misiones humanitarias y de rescate, las misiones de asesoramiento y asistencia en cuestiones militares, las misiones de prevención de conflictos y de mantenimiento de la paz, las misiones en las que intervengan fuerzas de combate para la gestión de crisis, incluidas las misiones de restablecimiento de la paz y las operaciones de estabilización al término de los conflictos. Todas estas misiones podrán contribuir a la lucha contra el terrorismo, entre otras cosas mediante el apoyo prestado a terceros países para combatirlo en su territorio.

El Consejo adoptará las decisiones relativas a estas misiones, definiendo su objetivo, alcance, y las normas generales de su ejecución. El Alto Representante, bajo la autoridad del Consejo y en contacto estrecho y permanente con el Comité Político y de Seguridad, se hará cargo de la coordinación de los aspectos civiles y militares de dichas misiones.

Respecto a este tipo de misiones, el art. 44 del TUE - Lisboa señala que el Consejo podrá encomendar la realización de una misión a un grupo de Estados miembros que lo deseen y que dispongan de las capacidades necesarias para tal misión.

La gestión de la misión se acordará entre dichos Estados miembros, en asociación con el AR. Los Estados miembros que participen en la realización de la misión informarán periódicamente al Consejo acerca del desarrollo de la misma, por propia iniciativa o a petición de un Estado miembro y comunicarán de inmediato al Consejo si la realización de la misión acarrea consecuencias importantes o exige una modificación del objetivo, alcance o condiciones de la misión encomendada. En tales casos, el Consejo adoptará las decisiones necesarias.

Esta provisión, según Sophie Dagand, viene a dar carta de naturaleza a iniciativas de la UE como la misión Artemis liderada por Francia en la República Democrática del Congo en septiembre de 2004[286].

Integración de la Agencia Europea de Defensa en el Tratado.

La Agencia Europea de Defensa (AED) fue creada en 2004, y el Tratado de Lisboa la incorpora a los Tratados (artículos 42 y 45). En el compromiso que adquieren los Estados miembros para mejorar progresivamente sus capacidades militares, se señala que la AED determinará las necesidades operativas, fomentará medidas para satisfacerlas, contribuirá a definir y, en su caso, a aplicar cualquier medida oportuna para reforzar la base industrial y tecnológica del sector de la defensa, participará en la definición de una política europea de capacidades y de armamento y asistirá al Consejo en la evaluación de la mejora de las capacidades militares.

La Agencia Europea de Defensa se encuentra bajo la autoridad del Consejo y tiene como misión:

a) contribuir a definir los objetivos de capacidades militares de los Estados miembros y a evaluar el respeto de los compromisos de capacidades contraídos por los Estados miembros;

b) fomentar la armonización de las necesidades operativas y la adopción de métodos de adquisición eficaces y compatibles;

c) proponer proyectos multilaterales para cumplir los objetivos de capacidades militares y coordinar los programas ejecutados por los Estados miembros y la gestión de programas de cooperación específicos;

d) apoyar la investigación sobre tecnología de defensa y coordinar y planificar actividades de investigación conjuntas y estudios de soluciones técnicas que respondan a las futuras necesidades operativas;

[286] DAGAND, SOPHIE. "*The impact of the Lisbon Treaty on CFSP and ESDP*". European Security Review, Nº 37, marzo 2008. http://www.isis-europe.org/pdf/2008_artrel_150_esr37tol-mar08.pdf

e) contribuir a definir y, en su caso, aplicar cualquier medida oportuna para reforzar la base industrial y tecnológica del sector de la defensa y para mejorar la eficacia de los gastos militares.

Podrán participar en la Agencia Europea de Defensa todos los Estados miembros que lo deseen. El Consejo adoptará por mayoría cualificada una decisión en la que se determinará el estatuto, la sede y la forma de funcionamiento de la Agencia. Dentro de ésta se constituirán grupos específicos, formados por los Estados miembros que realicen proyectos conjuntos. En caso necesario, La Agencia desempeñará sus funciones manteniéndose en contacto con la Comisión.

Cláusula de Asistencia Mutua.

De acuerdo con el artículo 42.7 del TUE - Lisboa, si un Estado miembro es objeto de una agresión armada en su territorio, los demás Estados miembros le deberán ayuda y asistencia con todos los medios a su alcance, de conformidad con el artículo 51 de la Carta de las Naciones Unidas. Ello se entiende sin perjuicio del carácter específico de la política de seguridad y defensa de determinados Estados miembros.

Los compromisos y la cooperación en este ámbito seguirán ajustándose a los compromisos adquiridos en el marco de la OTAN, que seguirá siendo, para los Estados miembros que forman parte de la misma, el fundamento de su defensa colectiva y el organismo de ejecución de ésta.

En este aspecto, el Parlamento Europeo en su informe sobre la función de la OTAN en la arquitectura de seguridad de la UE, reconoce el papel fundamental que ha desempeñado y sigue desempeñando la OTAN en la arquitectura de seguridad en Europa; señala que para la mayoría de los Estados miembros, que también son miembros de la OTAN, la Alianza sigue siendo el fundamento de su defensa común y que la seguridad de Europa en su conjunto sigue beneficiándose del mantenimiento de la alianza transatlántica. De esta forma, considera que la futura defensa colectiva

de la UE debería organizarse en la medida de lo posible en cooperación con la OTAN[287].

El caso especial de la Cláusula de Solidaridad

El Tratado de Lisboa recoge que la Unión y sus Estados miembros actuarán conjuntamente con espíritu de solidaridad si un Estado miembro es objeto de un ataque terrorista o víctima de una catástrofe natural o de origen humano. La Unión movilizará todos los instrumentos de que disponga, incluidos los medios militares puestos a su disposición por los Estados miembros, para:

a) prevenir la amenaza terrorista en el territorio de los Estados miembros; proteger a las instituciones democráticas y a la población civil de posibles ataques terroristas; y prestar asistencia a un Estado miembro en el territorio de éste, a petición de sus autoridades políticas, en caso de ataque terrorista;

b) prestar asistencia a un Estado miembro en el territorio de éste, a petición de sus autoridades políticas, en caso de catástrofe natural o de origen humano.

Las modalidades de aplicación por la Unión de la Cláusula de Solidaridadserán definidas mediante decisión adoptada por el Consejo, a propuesta conjunta de la Comisión y del AR. Cuando dicha decisión tenga repercusiones en el ámbito de la defensa, el Consejo se pronunciará por unanimidad.

Además, se informará al Parlamento Europeo. El Consejo estará asistido por el COPS, con el apoyo de las estructuras creadas en el marco de la PCSD, y de un comité permanente encargado de garantizar dentro de la Unión el fomento y la intensificación

[287] VATANEN, ARI (Ponente): "Informe sobre la función de la OTAN en la arquitectura de seguridad de la UE", PE (2008/2197(INI)). Comisión de Asuntos Exteriores. Parlamento Europeo. 28 de enero de 2009. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A6-2009-0033+0+DOC+PDF+V0//ES

de la cooperación operativa en materia de seguridad interior. Además, el Consejo Europeo deberá evaluar de forma periódica las amenazas a que se enfrenta la Unión.

Sobre la Cláusula de Solidaridad hay que señalar que, aunque en la misma se prevea el uso de medios militares y se haga referencia a la asistencia del COPS y al apoyo de las estructuras creadas en el marco de la Política Común de Seguridad y Defensa, no forma parte de la PCSD y se encuentra separada de la parte del Tratado dedicada a la misma.

No obstante, el explícito uso de medios militares y de los mecanismos de la PCSD, así como la obligación del Consejo Europeo de evaluar las amenazas en materia de terrorismo, relacionan esta Cláusula de Solidaridad con los ámbitos de la seguridad y la defensa, lo que podría conducir al establecimiento de mecanismos de coordinación u otro tipo de pasarelas políticas y técnicas aún por explorar.

Parlamento Europeo

El Parlamento tiene derecho a supervisar la Política Común de Seguridad y Defensa y a tomar la iniciativa de dirigirse al Vicepresidente y Alto Representante (VP/AR) y al Consejo en este ámbito (artículo 36 del TUE). También ejerce su autoridad sobre el presupuesto de esta política (artículo 41 del TUE). Dos veces al año, el Parlamento celebra un debate sobre los avances en la ejecución de la PESC y de la PCSD, y aprueba dos informes: uno sobre la PESC, elaborado por la Comisión de Asuntos Exteriores, que incluye elementos relativos a la PCSD, si procede, y otro sobre la PCSD, elaborado por la Subcomisión de Seguridad y Defensa[288].

4.1.2. La Ciberseguridad en la Unión Europea

4.1.2.1 La Estrategia Europea de Seguridad

[288] KAROCK, Ulrich: La Política Común de Seguridad y Defensa, Parlamento Europeo, fichas técnicas, febrero 2015, p.2. http://www.europarl.europa.eu/ftu/pdf/es/FTU_6.1.2.pdf consulta: 6 octubre 2015.

La “Estrategia Europea de Seguridad: Una Europa segura en un mundo mejor” se redactó a instancias del Alto Representante de la UE para la Política Exterior y de Seguridad Común (PESC), Javier Solana, y fue presentada al Consejo Europeo, que la adoptó en su reunión del 12 y 13 de diciembre de 2003, en Bruselas. En este documento, el Alto Representante define los retos mundiales y las principales amenazas contra la seguridad de la Unión y clarifica los objetivos estratégicos de la UE para hacer frente a estas amenazas[289].

La estrategia de seguridad diseñada en este documento define como principales amenazas para Europa el terrorismo, del que señala que resulta indispensable una acción europea concertada contra este fenómeno, señalando la relación de sus causas especialmente con las presiones ejercidas por la modernización, la crisis cultural, social y política, y la enajenación de los jóvenes que viven en sociedades extranjeras; la proliferación de armas de destrucción masiva, que destaca como la amenaza más importante apuntando que el escenario más temible sería que un grupo terrorista adquiriera este tipo de armas; los conflictos regionales, que pueden tener un impacto directo o indirecto en los intereses europeos, independientemente de su localización geográfica; el debilitamiento de los Estados, debido a la mala gestión de los asuntos públicos y los conflictos civiles; y la delincuencia organizada, que tiene una dimensión exterior importante, ya que el tráfico de drogas, la trata de seres humanos o el tráfico de armas no se detienen en las fronteras de la Unión[290].

Para la defensa de su seguridad y la promoción de sus valores, la Unión Europea se concentra en tres objetivos estratégicos: hacer frente a las amenazas, con instrumentos como la orden de detención europea o iniciativas contra la financiación del terrorismo; la política de lucha contra la proliferación de armas, en particular reforzando los tratados internacionales y sus disposiciones en materia de comprobación; la contribución a la solución de los conflictos regionales y a reforzar a

[289] Consejo Europeo: *Estrategia Europea de Seguridad: Una Europa segura en un mundo mejor*, Bruselas, 12 de diciembre de 2013. http://www.consilium.europa.eu/uedocs/cmsUpload/031208ESSIIES.pdf consulta: 6 de octubre de 2015.

[290] *Ibídem*, pp. 3-5.

los Estados que son víctimas de una situación de debilitamiento; y el combate contra la delincuencia organizada; construir la seguridad en los países vecinos; y basar el orden internacional en un multilateralismo eficaz, del que dependen la seguridad y la prosperidad. Señala la Estrategia Europea de Seguridad que a cada una de las amenazas es necesario oponer una combinación de medios de acción, y la Unión está particularmente bien equipada para responder a situaciones que presentan aspectos múltiples, para establecer que la mejor protección para la seguridad de la Unión Europea es un mundo formado por Estados democráticos, hacia donde va encaminada la política exterior de la Unión[291].

La ciberseguridad como tal no aparece recogida en la Estrategia Europea de Seguridad de 2003 y no es hasta su revisión en 2008, en el "Informe sobre la aplicación de la Estrategia Europea de Seguridad: Ofrecer seguridad en un mundo en evolución", que analiza el grado de cumplimiento de los objetivos y revisa las amenazas, en el marco de la Política Europea de Seguridad y Defensa, en cuanto parte integrante de la Política Exterior y de Seguridad Común, que se menciona expresamente en el apartado de retos mundiales y principales amenazas, especificando que: "Las economías modernas dependen en gran medida de las infraestructuras vitales como los transportes, las comunicaciones y el suministro de energía, e igualmente de internet. La Estrategia de la UE para una sociedad de la información segura en Europa, adoptada en 2006, hace referencia a la delincuencia basada en internet. Sin embargo, los ataques contra sistemas de TI privadas o gubernamentales en los Estados miembros de la UE han dado una nueva dimensión a este problema, en calidad de posible nueva arma económica, política y militar. Se debe seguir trabajando en este campo para estudiar un planteamiento general de la UE, concienciar a las personas e intensificar la cooperación internacional" [292].

[291] *Ibídem*, pp. 6-14.

[292] Consejo Europeo: *Informe sobre la aplicación de la Estrategia Europea de Seguridad: Ofrecer seguridad en un mundo en evolución*, Bruselas, 11 de diciembre de 2008, p. 5. http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressdata/ES/reports/104637.pdf consulta: 6 de octubre de 2015.

En esta “Estrategia de la UE para una sociedad de la información segura en Europa” de 2006, se subraya que las sociedades están cambiando rápidamente hacia una nueva fase de desarrollo, en lo que viene a llamar una "sociedad de la información omnipresente", en la que las actividades cotidianas de los ciudadanos se basarán cada vez más en la utilización de las tecnologías de la información y de las comunicaciones (TIC) y en redes de comunicaciones electrónicas; la seguridad de las redes y de la información debe considerarse como un factor clave para que este desarrollo se lleve a cabo con éxito[293].

La Estrategia de la UE para una sociedad de la información segura en Europa de 2006 fue en muchos sentidos pionera de un concepto de la ciberseguridad integral. De esta forma, se señalaba que la confianza es un factor clave para el éxito de la nueva sociedad de la información; añadiendo que la confianza está relacionada con las experiencias de los usuarios y con el deber de respetar su intimidad; por consiguiente, la seguridad de las redes y de la información no debe considerarse simplemente como un aspecto técnico. De esta forma, la seguridad de las redes y de la información debe considerarse como elemento fundamental en la creación del espacio europeo de información, que contribuye al cumplimiento de la Estrategia renovada de Lisboa. Las TIC son consideradas también un elemento clave de innovación, crecimiento económico y empleo[294].

El 7 de febrero de 2013, la Comisión Europea y la Alta Representante de la UE para Asuntos Exteriores y Política de Seguridad presentaron una Comunicación conjunta al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo, y al Comité

[293] Consejo de la Unión Europea: *Una estrategia para una sociedad de la información segura en Europa*, Bruselas, 12 de diciembre de 2006, p. 9. http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/es/trans/92382.pdf consulta: 6 de octubre de 2015.

[294] *Ibídem*, p. 11.

de las Regiones titulada: “Estrategia de Ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro”[295].

Señala la Estrategia de Ciberseguridad de la UE que para que el ciberespacio siga siendo abierto y libre, deben aplicarse en línea los mismos principios, valores y normas que la UE promueve fuera de línea. Los derechos fundamentales, la democracia y el Estado de Derecho deben ser protegidos en el ciberespacio. La libertad y la prosperidad de la Unión dependen cada vez más de una Internet sólida e innovadora. Pero la libertad en línea requiere también protección y seguridad. El ciberespacio ha de ser protegido de incidentes, actividades malintencionadas y utilizaciones abusivas. A las administraciones públicas les corresponde un papel destacado en la custodia de un ciberespacio libre y seguro. Entre sus tareas figuran las de salvaguardar el acceso y la apertura, respetar y proteger los derechos fundamentales en línea y mantener la fiabilidad e interoperabilidad de Internet[296].

Con todo, la Estrategia de Ciberseguridad de la UE reconoce el liderazgo del sector privado, que posee y explota cuotas significativas de ciberespacio. Las tecnologías de la información y la comunicación se han convertido en la piedra angular del crecimiento económico en la UE y constituyen un recurso crítico del que dependen todos los sectores económicos. Actualmente reposan en ellas los complejos sistemas que permiten funcionar las economías en sectores clave tales como las finanzas, la sanidad, la energía y los transportes. Muchos modelos empresariales se basan en la disponibilidad ininterrumpida de Internet y el buen funcionamiento de los sistemas de información[297].

La UE constata que los incidentes de ciberseguridad, tanto deliberados como accidentales, están incrementándose a un ritmo alarmante y podrían llegar a perturbar

[295] Comisión Europea y la Alta Representante de la UE para Asuntos Exteriores y Política de Seguridad: *Estrategia de Ciberseguridad de la Unión Europea: Un ciberespacio abierto*, *protegido y seguro*, Bruselas, 7 de febrero de 2013. http://register.consilium.europa.eu/doc/srv?f=ST+6225+2013+INIT&l=es consulta: 6 de octubre de 2015.

[296] *Ibídem*, p. 2.

[297] *Ibídem*, p. 2.

el suministro de servicios esenciales que damos por descontados como el agua, la asistencia sanitaria, la electricidad o los servicios móviles. Las amenazas pueden tener varios orígenes, entre ellos los ataques delictivos, por motivos políticos, terroristas o patrocinados por los Estados, así como catástrofes naturales o errores no intencionados. La economía de la UE se ve afectada por actividades de ciberdelincuencia contra el sector privado y las personas. Los ciberdelincuentes recurren a métodos cada vez más complejos para introducirse en los sistemas de información, sustraer datos críticos o exigir rescates a las empresas. El aumento del espionaje económico y de las actividades alentadas por los Estados en el ciberespacio representa una nueva categoría de amenaza para las administraciones públicas y empresas de la UE. Asimismo, las autoridades de terceros países pueden emplear abusivamente el ciberespacio para ejercer vigilancia y control sobre sus propios ciudadanos[298].

La Unión Europea, en el ámbito de la ciberseguridad, se articula en torno a cinco prioridades estratégicas[299]:

1. **Lograr la ciberresiliencia**. Europa seguirá siendo vulnerable si no se dedican considerables esfuerzos a impulsar las capacidades, recursos y procedimientos públicos y privados para prevenir, detectar y gestionar los incidentes de ciberseguridad. Por ello, la Comisión ha desarrollado una política de seguridad de las redes y de la información (SRI)[300]. En 2004 se creó la Agencia Europea de Seguridad de las Redes y de la Información (ENISA)[301].

[298] *Ibídem*, p. 3.

[299] *Ibídem*, pp. 2-18.

[300] En 2001, la Comisión adoptó la Comunicación titulada Seguridad de las redes y de la información: Propuesta para un enfoque político europeo [COM(2001)298]; en 2006, adoptó una estrategia para una sociedad de la información segura [COM(2006)251]. Desde 2009, la Comisión también ha adoptado un plan de acción y una Comunicación sobre protección de infraestructuras críticas de información (PICI) [COM(2009)149, aprobado por la Resolución 2009/C 321/01 del Consejo, y COM(2011)163, aprobado por las conclusiones 10299/11 del Consejo].

[301] Reglamento (CE) nº 460/2004. https://www.boe.es/doue/2004/077/L00001-00011.pdf consulta: 6 de octubre de 2015.

Además, la Directiva marco sobre las comunicaciones electrónicas[302] exige que los proveedores de comunicaciones electrónicas gestionen adecuadamente los riesgos a que se enfrentan sus redes y notifiquen las violaciones significativas de la seguridad. Asimismo, la normativa de la UE sobre protección de datos[303] establece que los responsables del tratamiento han de prever requisitos y salvaguardias que garanticen la adecuada protección.

2. **Reducir drásticamente la ciberdelincuencia**. Los ciberdelitos son actividades de bajo riesgo que generan grandes beneficios y los delincuentes se aprovechan a menudo del anonimato de los dominios de los sitios web. La ciberdelincuencia no conoce fronteras y, habida cuenta del alcance mundial de Internet, los cuerpos de seguridad deben adoptar un enfoque transfronterizo coordinado y colaborativo para responder a esta amenaza creciente. La UE y los Estados miembros necesitan una normativa rigurosa y eficaz para luchar contra la ciberdelincuencia. El Convenio sobre la Ciberdelincuencia del Consejo de Europa[304], también denominado Convenio de Budapest, es un tratado internacional vinculante que ofrece un marco efectivo para la adopción de normas nacionales. La UE ya ha adoptado actos legislativos sobre la ciberdelincuencia, entre ellos una Directiva relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil[305].

3. **Desarrollar estrategias y capacidades de ciberdefensa vinculadas a la Política Común de Seguridad y Defensa (PCSD)**. Los esfuerzos de ciberseguridad de la UE entrañan asimismo una dimensión de ciberdefensa. Para aumentar la resiliencia de los sistemas de comunicación e información que

[302] Artículos 13 bis y 13 ter de la Directiva 2002/21/CE.

[303] Artículo 17 de la Directiva 95/46/CE; artículo 4 de la Directiva 2002/58/CE.

[304] Consejo de Europa: *Convenio sobre la Ciberdelincuencia*, Budapest, 23 de noviembre de 2001 https://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/consejo_europa/convenios/common/pdfs/Convenio_Ciberdelincuencia.pdf consulta: 6 de octubre de 2015.

[305] Directiva 2011/93/UE, que sustituye la Decisión Marco 2004/68/JAI del Consejo.

amparan los intereses de los Estados miembros en materia de defensa y seguridad nacional, el desarrollo de capacidades de ciberdefensa debería concentrarse en la detección, respuesta y recuperación frente a complejas ciberamenazas. Ante tan polifacéticas amenazas, conviene potenciar las sinergias entre los enfoques civil y militar para la protección de ciberactivos críticos. Estos esfuerzos se han de apoyar con actividades de investigación y desarrollo y una mayor cooperación entre las administraciones públicas, el sector privado y la comunidad académica de la UE. Para evitar duplicaciones, la UE examinará de qué modo pueden ella y la OTAN aunar sus esfuerzos para aumentar la resiliencia de infraestructuras críticas públicas, de defensa y de información de las que dependen los miembros de ambas organizaciones.

4. **Desarrollar recursos industriales y tecnológicos de ciberseguridad**. Europa dispone de excelentes capacidades de investigación y desarrollo, pero muchas de las empresas punteras mundiales proveedoras de productos y servicios de TIC innovadores están establecidas fuera de la UE. Europa corre el riesgo de depender excesivamente no solo de las TIC producidas en terceros países, sino también de las soluciones de seguridad desarrolladas fuera de sus fronteras. Es esencial velar por que los equipos y programas informáticos producidos en la UE y en terceros países que se utilizan en infraestructuras y servicios críticos —y cada vez más en dispositivos móviles— sean fiables y seguros y garanticen la protección de los datos personales. La UE debe sacar el máximo provecho del Programa Marco de Investigación e Innovación («Horizonte 2020»)[306].

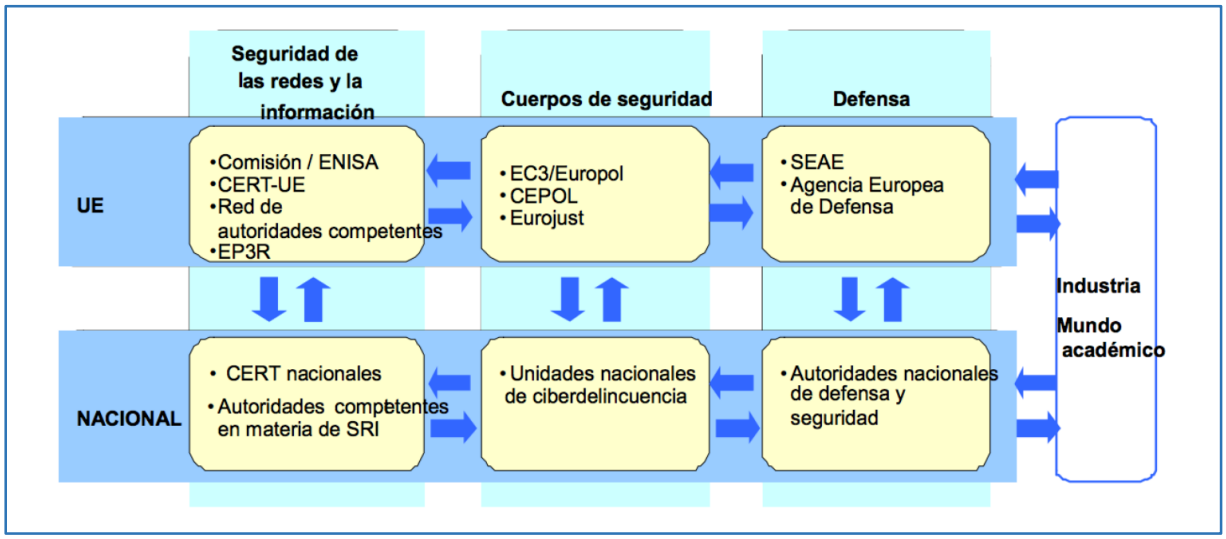
[306] «Horizonte 2020» es el instrumento financiero de ejecución de la Unión por la Innovación, la iniciativa emblemática de la Estrategia Europa 2020 destinada a garantizar la competitividad de Europa a escala mundial. El nuevo Programa Marco de Investigación e Innovación de la UE para el período 2014-2020 se inscribe en un proceso que tiene por objeto generar crecimiento y crear nuevos puestos de trabajo en Europa. http://ec.europa.eu/research/innovation-union/index_en.cfm consulta: 9 de octubre de 2015.

5. **Establecer una política internacional coherente del ciberespacio para la Unión Europea y promover los valores esenciales de la UE**. En su política internacional del ciberespacio, la UE promoverá la apertura y la libertad de Internet, alentará las actividades de elaboración de normas de conducta y aplicará el Derecho internacional existente en este campo. Asimismo, la UE tomará medidas para superar la brecha digital y participará activamente en los esfuerzos internacionales de creación de capacidades de ciberseguridad. El compromiso internacional de la Unión en este ámbito estará presidido por los valores esenciales de la UE; a saber: la dignidad humana, la libertad, la democracia, la igualdad, el Estado de derecho y el respeto de los derechos fundamentales. Para hacer frente a los problemas mundiales que plantea el ciberespacio, la UE procurará cooperar más estrechamente con organizaciones que trabajan en este campo, como el Consejo de Europa, la OCDE, las Naciones Unidas, la OSCE, la OTAN, la UA, la ASEAN y la OEA. A nivel bilateral, la cooperación con los Estados Unidos reviste especial importancia y se potenciará, en particular en el contexto del Grupo de Trabajo UE-EE.UU. sobre Ciberseguridad y Ciberdelincuencia.

Señala la Estrategia de Ciberseguridad de la Unión Europea que dada la complejidad del problema y las muchas partes que intervienen, la solución no puede consistir en una supervisión europea centralizada. Las administraciones nacionales son las que se hallan en mejores condiciones para organizar las actividades de prevención y respuesta a incidentes y ataques cibernéticos, así como para establecer contactos y redes con el sector privado y los ciudadanos a través de los procedimientos y marcos jurídicos establecidos. Al mismo tiempo, habida cuenta del carácter transfronterizo potencial o real de los riesgos, una respuesta efectiva a escala nacional requeriría a menudo la intervención de la UE. Para abordar la ciberseguridad de forma global, las actividades deben articularse en torno a tres pilares esenciales - seguridad de las

redes y la información (SRI), cuerpos de seguridad y defensa - , también regulados por diferentes marcos jurídicos[307].

Figura 23: Marco de referencia de la integración de los mecanismos de la UE y nacionales en ciberseguridad.



Fuente: Estrategia de Ciberseguridad de la Unión Europea[308].

La coordinación entre autoridades competentes en materia de seguridad de las redes y la información y mecanismos de respuesta a incidentes SRI/CERT, junto con los cuerpos de seguridad y defensa contempla tres planos de actuación, la escala nacional, la de la Unión Europea y la internacional[309].

A escala nacional

Los Estados miembros deberían disponer, ya en la actualidad o como resultado de la estrategia, de estructuras para abordar la ciberresiliencia, la ciberdelincuencia y la ciberdefensa; deben asimismo alcanzar el nivel de capacidades requerido para resolver los ciberincidentes. No obstante, dado que una serie de entidades pueden

[307] *Ibídem*, p. 19.
[308] *Ibídem.*
[309] *Ibídem*, pp. 19-20.

tener responsabilidades operativas en distintas dimensiones de la ciberseguridad y habida cuenta de la importancia que reviste la participación del sector privado, conviene lograr una coordinación óptima entre ministerios a escala nacional. Los Estados miembros deberán establecer en sus estrategias nacionales de ciberseguridad las funciones y responsabilidades de sus diversas entidades nacionales.

Debe fomentarse el intercambio de información entre entidades nacionales y con el sector privado para que este y los Estados miembros puedan tener una visión global de las diversas amenazas y comprender mejor las nuevas tendencias y las técnicas utilizadas tanto para cometer ciberataques como para reaccionar ante ellos con mayor rapidez. La elaboración de planes nacionales de cooperación en materia de SRI, que se han de activar en caso de que se produzcan ciberincidentes, facilitará a los Estados miembros la tarea de asignar claramente funciones y responsabilidades y optimizar las medidas de respuesta.

A escala de la UE

Como ocurre a escala nacional, en la UE hay distintas entidades responsables de ciberseguridad. Cabe citar, en particular, a la ENISA, Europol/EC3 y la AED, tres agencias que actúan desde la perspectiva de la SRI, los cuerpos de seguridad y la defensa, respectivamente. Estas agencias cuentan con consejos de administración en que están representados los Estados miembros y constituyen plataformas de coordinación a escala de la UE.

Se impulsarán la coordinación y la colaboración entre la ENISA, Europol/EC3 y la AED en una serie de ámbitos de interés para las tres agencias, en particular el análisis de tendencias, la evaluación de riesgos, la formación y el intercambio de mejores prácticas. Las tres han de colaborar, manteniendo al mismo tiempo sus especificidades. Estas agencias, junto con el CERT-UE, la Comisión y los Estados miembros, deberán apoyar la creación de una comunidad de especialistas técnicos y policiales de confianza en este campo. Los canales informales de coordinación y

colaboración se completarán con vínculos más estructurados. El personal militar de la UE y el equipo encargado del proyecto de ciberdefensa de la AED podrán servir de vector de coordinación en el ámbito de la defensa. El Consejo de Programación de Europol/EC3 reunirá, entre otros, a EUROJUST, CEPOL, los Estados miembros, la ENISA y la Comisión, y les ofrecerá la oportunidad de compartir sus respectivos conocimientos especializados y de comprobar que las actuaciones del EC3 se llevan a cabo en concertación, reconociéndose las aportaciones de cada parte y respetándose sus mandatos. El nuevo mandato de la ENISA permitirá que esta estreche sus relaciones con Europol y refuerce sus relaciones con la industria. Ante todo, la propuesta legislativa de la Comisión sobre la SRI establecerá un marco de cooperación a través de una red de autoridades nacionales competentes en materia de SRI y fomentará el intercambio de información entre dichas autoridades y los cuerpos de seguridad.

A escala internacional

La Comisión y la Alta Representante garantizan, junto con los Estados miembros, una actuación internacional coordinada en el ámbito de la ciberseguridad. En este marco, la Comisión y la Alta Representante defenderán los valores esenciales de la UE y promoverán una utilización pacífica, abierta y transparente de las cibertecnologías. La Comisión, la Alta Representante y los Estados miembros mantienen diálogos políticos con los socios internacionales y organizaciones internacionales tales como el Consejo de Europa, la OCDE, la OSCE, la OTAN y las Naciones Unidas.

El Consejo de la Unión Europea dio la bienvenida a la citada Estrategia mediante unas Conclusiones adoptadas el 25 de junio de 2013, en las que invita a los Estados miembros, a la Comisión y a la Alta Representante a trabajar conjuntamente

respetando las correspondientes competencias de los demás y el principio de subsidiariedad en respuesta a los objetivos estratégicos incluidos en la Estrategia[310].

Estas Conclusiones del Consejo de la UE sobre la Estrategia de Ciberseguridad de la Unión Europea aportan un elemento especialmente significativo en relación con el derecho internacional, que ha marcado la posición dela UE en diferentes foros sobre ciberseguridad. Las Conclusiones reconocen que el derecho internacional, incluidos convenios internacionales como el Convenio sobre Ciberdelincuencia del Consejo de Europa (Convenio de Budapest) y los correspondientes convenios en materia de Derecho humanitario y derechos humanos, como el Pacto Internacional de Derechos Civiles y Políticos, el Pacto internacional relativo a los derechos económicos, sociales y culturales, proporcionan un marco jurídico aplicable al ciberespacio. Por todo ello, las Conclusiones instan a procurar que dichos instrumentos sean también de aplicación en el ciberespacio; en consecuencia, la UE no defiende la creación de nuevos instrumentos jurídicos internacionales para abordar las cuestiones relacionadas con el ciberespacio[311].

En el ámbito de las tecnologías de la información y la comunicación (TIC), las citadas Conclusiones subrayan la importancia fundamental de que la UE posea un sector de las TIC y un sector de seguridad de las TIC dinámicos y que refuercen la ciberseguridad, invitando a los Estados miembros y a la Comisión a explorar y comunicar qué tipo de medidas podrían adoptarse para apoyar su desarrollo, señalando que la legislación en apoyo de la ciberseguridad debería fomentar la innovación y el crecimiento, centrándose en la protección de las infraestructuras y funciones vitales que los Estados miembros consideren esenciales, ya que la economía digital debe ser un motor esencial de crecimiento, innovación y empleo, y la

---

[310] Consejo de la Unión Europea: *Conclusiones del Consejo sobre la comunicación conjunta de la Comisión y de la Alta Representante de la Unión para Asuntos Exteriores y Política de Seguridad, titulada "Estrategia de ciberseguridad de la Unión Europea: un ciberespacio abierto, protegido y seguro"*, Bruselas, 22 de julio de 2013. http://register.consilium.europa.eu/doc/srv?f=ST+12109+2013+INIT&l=es consulta: 6 de octubre de 2015.

[311] *Ibídem*, art. 6, p. 2.

ciberseguridad es esencial para proteger la economía digital, para lo cual debe impulsarse a escala nacional la protección de infraestructuras críticas de información (CIIP)[312].

En el marco de la Política Común de Seguridad y Defensa (PCSD), las Conclusiones del Consejo de la UE en relación con su Estrategia de Ciberseguridad destacan la necesidad urgente de aplicar y hacer avanzar la PCSD para desarrollar un marco de ciberdefensa; la necesidad de mejorar las capacidades de ciberdefensa de los Estados miembros, en particular mediante el desarrollo de normas comunes; y la concienciación a través de la formación y educación en ciberseguridad, utilizando los recursos de la Escuela Europea de Seguridad y Defensa. Se señala que es prioritario alentar a los Estados miembros a desarrollar tecnologías seguras y resistentes respecto de la ciberdefensa, con una importante participación del sector privado y del mundo académico, así como reforzar los aspectos de ciberdefensa en los proyectos de investigación de la Agencia Europea de Defensa (AED). También se deberá reforzar la cooperación entre la UE y la OTAN sobre ciberdefensa, determinando las prioridades de una cooperación continua sobre ciberdefensa UE-OTAN[313].

En el ámbito internacional, las Conclusiones del Consejo de la UE, solicitan a los Estados miembros, la Comisión y Alto Representante que se esfuercen en lograr una política internacional en materia de ciberespacio de la UE coherente, de conformidad con los procedimientos pertinentes establecidos en los Tratados; reforzando su compromiso con los socios y las organizaciones internacionales clave; integrando las cuestiones de ciberseguridad en la PESC; mejorando la coordinación de las cuestiones mundiales de la ciberseguridad e integrándolas en el resto de las políticas, en particular mediante medidas de creación de confianza y de transparencia en el marco general de las relaciones con terceros países y con organizaciones internacionales; respaldando el desarrollo de capacidades en terceros países, con miras a permitir el desarrollo pleno del potencial económico y social de las TIC,

[312] *Ibídem*, art. 23, p. 5-6.

[313] *Ibídem*, art. 37, pp. 11-12.

respaldando el desarrollo de sistemas resilientes en esos países y reduciendo los riesgos cibernéticos pare las instituciones de la UE y los Estados miembros, haciendo uso al mismo tiempo de las redes y foros existentes para la coordinación política y el intercambio de información[314].

Estas Conclusiones del Consejo de la UE recogen también la normativa aplicable y específica de la Unión Europea en materia de ciberseguridad, que se incorpora en el anexo 1 de esta tesis.

4.1.2.2. Marco Político de Ciberdefensa de la UE

El Consejo de la Unión Europea decidió adoptar, el 18 de noviembre de 2014, un Marco Político de Ciberdefensa(MPCD) de la UE [315], señalando que el ciberespacio se describe a menudo como el quinto de los ámbitos de la actividad militar, tan crucial para la aplicación de la Política Común de Seguridad y Defensa (PCSD) de la Unión Europea como pueden serlo los de tierra, mar, aire y espacio. Para aplicar con éxito la PCSD se ha venido dependiendo cada vez en mayor medida de la disponibilidad y el acceso a un ciberespacio seguro. En la actualidad se requieren capacidades sólidas y resistentes en el ámbito del ciberespacio para apoyar las estructuras, misiones y operaciones de la PCSD. En las Conclusiones del Consejo Europeo sobre la PCSD de diciembre de 2013 y en las Conclusiones del Consejo sobre la PCSD de noviembre de 2013 se pedía la elaboración de un marco político de la UE para la ciberdefensa, a partir de una propuesta de la Alta Representante, en cooperación con la Comisión Europea y con la Agencia Europea de Defensa (AED)[316].

La tarea principal de este marco de actuación consiste en impulsar las capacidades de ciberdefensa que aporten los Estados miembros en el marco de la PCSD y proteger las redes de comunicación e información del Servicio Europeo de Acción Exterior

[314] *Ibídem*, art. 45, pp. 14-15.

[315] Consejo de la Unión Europea: *Marco Político de Ciberdefensa de la UE*, Bruselas, 18 de noviembre de 2014. http://data.consilium.europa.eu/doc/document/ST-15585-2014-INIT/es/pdf consulta: 10 de octubre de 2015.

[316] *Ibídem*, p. 1.

(SEAE) que tengan repercusiones sobre la PCSD. Es importante que la dimensión cibernética se aborde adecuadamente mediante ejercicios que permitan mejorar la capacidad de la UE para responder a crisis cibernéticas en el contexto de la PCSD, mejorar los procedimientos de toma de decisiones estratégicas y reforzar la arquitectura de las infraestructuras de información. El del ciberespacio es un ámbito en rápida evolución en el que las capacidades de doble uso desempeñan un papel esencial, por lo que es necesario propiciar la cooperación civil y militar y las correspondientes sinergias con estrategias cibernéticas más amplias de la UE con el fin de afrontar los nuevos retos que plantea[317].

El Marco Político de Ciberdefensa de la UE aspira a mejorar la protección de las redes de comunicación de la PCSD utilizadas por las entidades de la UE[318]. De esta forma, sin perjuicio del papel de los CERT de la UE como estructuras centrales de coordinación de la respuesta de la UE ante incidentes cibernéticos, el SEAE impulsará elaborará su propia capacidad de seguridad de las tecnologías de la información, centrándose en la prevención, detección, respuesta ante incidentes, conocimiento de la situación, intercambio de información y mecanismos de alerta temprana[319].

El Marco Político de Ciberdefensa de la UE, impulsa la cooperación internacional, en concreto con la OTAN, OSCE y ONU. Destaca la cooperación con la OTAN en lo referente a la ciberdefensa, estimulando las consultas y reuniones entre el Grupo Político-Militar y los correspondientes comités de la OTAN, con el fin de evitar duplicaciones innecesarias y a garantizar la coherencia y complementariedad de esfuerzos. Además, el SEAE y la AED, junto con los Estados miembros, deberán impulsar la cooperación en materia de ciberdefensa entre la UE y la OTAN, intercambiando información sobre gestión de crisis, operaciones militares y misiones

[317] *Ibídem*, p. 3.

[318] *Ibídem*, pp. 6-7.

[319] La protección de los sistemas de comunicación e información del SEAE y el desarrollo de capacidades de seguridad en tecnologías de la información son responsabilidades de la Dirección de Gestión de Recursos (DGR) del SEAE. El Estado Mayor de la Unión Europea (EMUE), la Dirección de Gestión de Crisis y Planificación (CMPD) y la Capacidad Civil de Planificación y Ejecución (CPCC) proporcionarán recursos adicionales y apoyo.

civiles; evitarán los solapamientos en el desarrollo de capacidades de ciberdefensa; mejorarán la cooperación en relación en formación y educación sobre ciberdefensa; utilizarán el acuerdo de enlace de la AED con el Centro de Excelencia para la Ciberdefensa Cooperativa de la OTAN (CCDCOE); reforzarán la cooperación entre el CERT de la UE y los órganos pertinentes de la UE encargados de la ciberdefensa y el NIRC (Capacidad de respuesta ante incidentes informáticos de la OTAN) con el fin de mejorar el conocimiento de las situaciones, el intercambio de información, los mecanismos de alerta temprana y la previsión de amenazas que pudieran afectar a ambas organizaciones[320].

Señala Fojón Chamorro que una de las prioridades estratégicas de la UE en materia de ciberdefensa es la colaboración con la Alianza Atlántica. Entre las acciones desarrolladas destaca que la EDA ha asumido el rol de observador en el proyecto Multinational Cyber Defence Education and Training (MNCDE&T) –liderado por Portugal– del Programa de Defensa Inteligente de la Alianza. Igualmente, el Mando Aliado de Transformación y la Agencia de Comunicaciones e Información de la OTAN han aceptado un rol de observador en el proyecto CyberRanges liderado por la EDA. Además, se está trabajando para que el EU-CERT y NCIRC alcancen un acuerdo para el intercambio de información técnica y mejorar el proceso de gestión de incidencias. Igualmente, la EDA ha participado como observador en los últimos ciberejercicios –Cyber Coalition y LockedShields– ejecutados por la Alianza. No obstante, Fojón Chamorro apunta que para construir un sistema de ciberdefensa en el seno de UE será necesario algo más que ciberjercicios, adiestramiento y colaboración. Los logros en el plano institucional deberán ir acompañados de: una determinante involucración de los Estados Miembros, una definición clara de las competencias –dejando a un lado sus desavenencias– de los actores europeos implicados, el desarrollo de capacidades de ciberdefensa operativas y planes de actuación coherentes[321].

---

[320] *Ibídem*, p. 12.

[321] FOJÓN CHAMORRO, Enrique: *La ciberdefensa en la Unión Europea*, Real Instituto Elcano, Madrid, 25 de junio de 2015. http://www.blog.rielcano.org/reto-la-ciberdefensa-la-union-europea/ consulta: 11 de octubre de 2015.

El Parlamento Europeo, recogió el avance que supone el Marco Político de Ciberdefensa de la Unión Europea, en su informe sobre la aplicación de la Política Común de Seguridad y Defensa. De esta forma, hace hincapié en la importancia de lograr un nivel común de ciberseguridad entre los Estados miembros con el fin de progresar de forma adecuada en la cooperación en ciberdefensa y de reforzar las capacidades en lo tocante a los ciberataques y al ciberterrorismo, y espera que este plan de acción marque el punto de partida de una integración más sistemática de las cuestiones de ciberdefensa en las estrategias de seguridad nacional de los Estados miembros, así como una toma de conciencia de las bazas de la ciberdefensa a escala de las instituciones de la UE; recuerda que se requiere más claridad y un marco jurídico adecuado, habida cuenta de la dificultad que entraña atribuir la autoría de los ciberataques y de la necesidad de dar una respuesta proporcionada y necesaria en todos los contextos[322].

Un aspecto interesante, que destacan Röhrig y Smeaton, en referencia a la ciberdefensa de la UE, es que aunque la percepción pública es que la protección cibernética es principalmente una cuestión tecnológica más que humana, los factores humanos están emergiendo rápidamente como una prioridad, desplazando a cuestiones tecnológicas. De esta forma, un enfoque de defensa cibernética en la educación, la formación y los ejercicios es vital si se quiere alcanzar una capacidad de defensa cibernética operativa adecuada. De esta forma, el énfasis de la política de ciberdefensa de la UE en educación y formación es compartido por estos autores, que estiman que el conocimiento y la experiencia de los pueblos es un requisito fundamental para una cultura europea de defensa cibernética[323].

---

[322] Parlamento Europeo: *Informe sobre la aplicación de la política común de seguridad y defensa (en base al Informe anual del Consejo al Parlamento Europeo sobre la Política Exterior y de Seguridad Común)*, Comisión de Asuntos Exteriores, Ponente: Arnaud Danjean, Bruselas, 19 de marzo de 2015.

[323] RÖHRIG, Wolfgang y SMEATON, Rob: *Cyber security and cyber defence in the European Union: Opportunities, synergies and challenges*, Cyber Security Review, 2015. http://www.cybersecurity-review.com/articles/cyber-security-and-cyber-defence-in-the-european-union consulta: 11 de octubre de 2015.

4.1.2.3. Las Cláusulas de Solidaridad y de Defensa Mutua en el ámbito de la ciberseguridad y la ciberdefensa

Patryk Pawlak ha realizado un novedoso análisis en relación con la invocación y aplicación de la Cláusula de Solidaridad y la Cláusula de Defensa Mutua en el ámbito de la ciberseguridad y la ciberdefensa en la Unión Europea[324]. Señala Pawlak que frente a las crisis complejas, la Unión Europea (UE) ha realizado esfuerzos significativos[325] para mejorar sus capacidades de respuesta, incluyendo la adopción de la Política Integrada de Respuesta a Crisis de la UE (IPCR) y la transformación del Centro de Supervisión y de Información (MIC) en el Centro de Coordinación de Respuestas a Emergencias (ERCC) en 2013. Estas cláusulas de solidaridad y defensa mutua fueron introducidas en el Tratado de Lisboa - los artículos 222 TFUE y 42 (7) TEU respectivamente - para fortalecer la cooperación entre Instituciones de los Estados miembros y de la UE en caso de una crisis o agresión armada respectivamente. La Cláusula de Solidaridad va más allá mediante la creación de una obligación de todos los Estados miembros Unidos para actuar de forma conjunta y para ayudar a otros miembros de la UE en casos de desastres y crisis que excedan sus capacidades de respuesta individual. Si bien la disposición del Tratado relativo a la Cláusula de Solidaridad se ha complementado con directrices más detalladas de empleo, la Cláusula de Defensa Mutua sigue siendo un concepto teórico y su aplicación todavía tiene que ser establecida[326].

La posibilidad de el empleo de la Cláusula de Solidaridad para mitigar el daño de un ataque cibernético aparece en la Estrategia de Ciberseguridad de la UE de febrero de 2013. De acuerdo con la Estrategia, en su apartado 3.2. “Apoyo de la UE ante

---

[324] PAWLAK, Patryk: *Cybersecurity and cyberdefence EU Solidarity and Mutual Defence Clauses*. Servicio de Investigación Parlamentario Europeo, PE 559.488, Bruselas, junio de 2015. http://www.europarl.europa.eu/RegData/etudes/BRIE/2015/559488/EPRS_BRI(2015)559488_EN.pdf consulta: 8 de octubre de 2015.

[325] NIMARK, Agnieszka y PAWLAK, Patryk: *Upgrading the Union’s response to disasters*. http://www.iss.europa.eu/uploads/media/Brief_45_Crisis_response.pdf consulta: 10 de octubre de 2015.

[326] PAWLAK, Patryk: *Cybersecurity and cyberdefence EU Solidarity and Mutual Defence Clauses*. *Opus citada*, p. 2.

incidentes y ataques cibernéticos graves", se señala que "Si el incidente parece estar relacionado con el ciberespionaje o con un ataque promovido por un Estado, o afecta a la seguridad nacional, las autoridades policiales y de defensa nacionales deberán alertar a sus homólogos de que sufren un ataque y se hallan en condiciones de defenderse. Entonces se activarán mecanismos de alerta temprana y, en caso necesario, procedimientos de gestión de crisis o de otros tipos. Un incidente o ataque cibernético de especial gravedad podría ser motivo suficiente para que un Estado miembro invocara la Cláusula de Solidaridad de la UE (artículo 222 del Tratado de Funcionamiento de la Unión Europea)"[327].

Además, las Conclusiones del Consejo de la UE, de junio de 2013, sobre esta comunicación conjunta de la Comisión y de la Alta Representante de la Unión para Asuntos Exteriores y Política de Seguridad, que presenta la Estrategia de Ciberseguridad de la UE, invitan a los Estados miembros a tener en cuenta los problemas ligados a la ciberseguridad a la luz de los trabajos en curso sobre la cláusula de solidaridad[328].

Por otra parte, el Marco Político de Ciberdefensa de la UE establece que "Por último, los objetivos de la ciberdefensa deberán hallarse mejor integrados en los mecanismos de gestión de crisis de la Unión. Para abordar los efectos de las crisis cibernéticas, pueden aplicarse, según proceda, las disposiciones pertinentes del Tratado de la Unión Europea y del Tratado de Funcionamiento de la Unión Europea". Para mencionar específicamente a pie de página los artículos 222 del TFUE y 42.7 del TUE, teniendo en cuenta debidamente el art. 17 del TUE, referidos a la Cláusula de Solidaridad y a la Clausula de Defensa Mutua[329].

---

[327] Comisión Europea y la Alta Representante de la UE para Asuntos Exteriores y Política de Seguridad: *Estrategia de Ciberseguridad de la Unión Europea: Un ciberespacio abierto*, *protegido y seguro*. *Opus citada*, p. 21.

[328] Consejo de la Unión Europea: *Conclusiones del Consejo sobre la comunicación conjunta de la Comisión y de la Alta Representante de la Unión para Asuntos Exteriores y Política de Seguridad, titulada "Estrategia de ciberseguridad de la Unión Europea: un ciberespacio abierto, protegido y seguro". Opus citada, pp. 8-9.*

[329] Consejo de la Unión Europea: *Marco Político de Ciberdefensa de la UE*. *Opus citada*, p.3.

La activación de la Cláusula de Solidaridad o la Cláusula de Defensa Mutua en caso de un ataque cibernético requiere una involucración en el proceso de los niveles político y estratégico. Además, la gestión multinacional de una crisis en el ámbito del ciberespacio también requiere que los expertos y técnicos trabajan en paralelo para prevenir, detectar, responder y hacer frente a las consecuencias de los ataques cibernéticos. Pawlak señala los siguientes grupos de actores que pueden estar involucrados en estos procesos[330]:

- En el caso de la Cláusula de Solidaridad: un Equipo Nacional de Respuesta a Emergencias Informáticas (CERT) - también conocido como Equipo de Respuesta a la Seguridad de la Información Informática (CSIRT) - y / u otros organismos designados dentro de las estructuras nacionales, incluidos las fuerzas y cuerpos de seguridad, así como el sector privado. Los CERTs o CSIRTs son los proveedores de seguridad primaria en cada país y los principales activos en la respuesta a los ataques cibernéticos. Para fortalecer su capacidad de respuesta, muchos CERTs han establecido redes regionales o globales como FIRST (Foro de Respuesta a Incidentes y Equipos de Seguridad) o APCERT (Asia Pacífico CERT)[331].

- En el caso de la Cláusula de Defensa Mutua: un Mando Nacional de Ciberseguridad o un Equipo Nacional de Respuesta a Emergencias Informáticas de carácter militar (milCERT). En respuesta a un número creciente de ciberataques y un uso potencial de capacidades cibernéticas en un conflicto militar, un creciente número de países han desarrollado o están desarrollando actualmente su doctrinas de ciberdefensa y sus capacidades militares en el

[330] PAWLAK, Patryk: *Cybersecurity and cyberdefence EU Solidarity and Mutual Defence Clauses*. *Opus citada*, pp. 7-8.

[331] Se puede acceder a más información sobre FIRST (Forum for Incident Response and Security Teams) en http://www.first.org/ y sobre APCERT en http://www.apcert.org/ consulta: 11 de octubre de 2015.

ciberespacio. Señala Pawlak que tal división es una simplificación y una división clara civil y militar podría ser difícil de mantener en una crisis compleja.

El Parlamento Europeo, por su parte, ha atendido en tres ocasiones aspectos relacionados con las Cláusulas de Solidaridad y de Defensa Mutua en el ámbito del ciberespacio[332]:

- El 22 de noviembre de 2012, el Parlamento Europeo acordó una Resolución sobre los aspectos políticos y operativos de las Cláusulas de Defensa Mutua y Solidaridad de la UE. En lo que respecta a la Cláusula de Defensa Mutua señala, en su artículo 13, que considera que los ataques aún no siendo armados, como por ejemplo los ciberataques contra infraestructuras críticas, que se dirigen para causar graves daños y la interrupción de un Estado miembro y que se identifiquen procedentes de una entidad externa podrían incluirse en la cláusula, si la seguridad del Estado miembro se ve amenazada de manera significativa por sus consecuencias, respetando el principio de proporcionalidad. En relación a la Cláusula de Solidaridad, incluye en su artículo 20 a los ataques en el ciberespacio[333].
- También el 22 de noviembre de 2012, el Parlamento Europeo emitió una Resolución, en este caso específica sobre ciberseguridad y defensa. En su artículo 3, insta a la Comisión y al Alto Representante de la Unión para Asuntos Exteriores y Política de Seguridad a considerar la posibilidad de un ataque cibernético grave contra un Estado miembro en su próxima propuesta sobre las disposiciones para la aplicación de la cláusula de solidaridad (artículo 222 del TFUE); tiene, además, la opinión de que a pesar de los ataques cibernéticos que ponen en peligro la seguridad nacional todavía tienen que ser definido por

[332] PAWLAK, Patryk: *Cybersecurity and cyberdefence EU Solidarity and Mutual Defence Clauses*. *Opus citada*, p. 8.

[333] Parlamento Europeo: *Resolución sobre las Cláusulas de Defensa Mutua y Solidaridad de la UE: Dimensiones políticas y operacionales*, 22 de noviembre de 2012. http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2012-0456&language=EN&ring=A7-2012-0356 consulta: 11 de octubre de 2015.

una terminología común, podrían ser cubiertos por la cláusula de defensa mutua (artículo 42.7 TUE), sin perjuicio del principio de proporcionalidad[334].

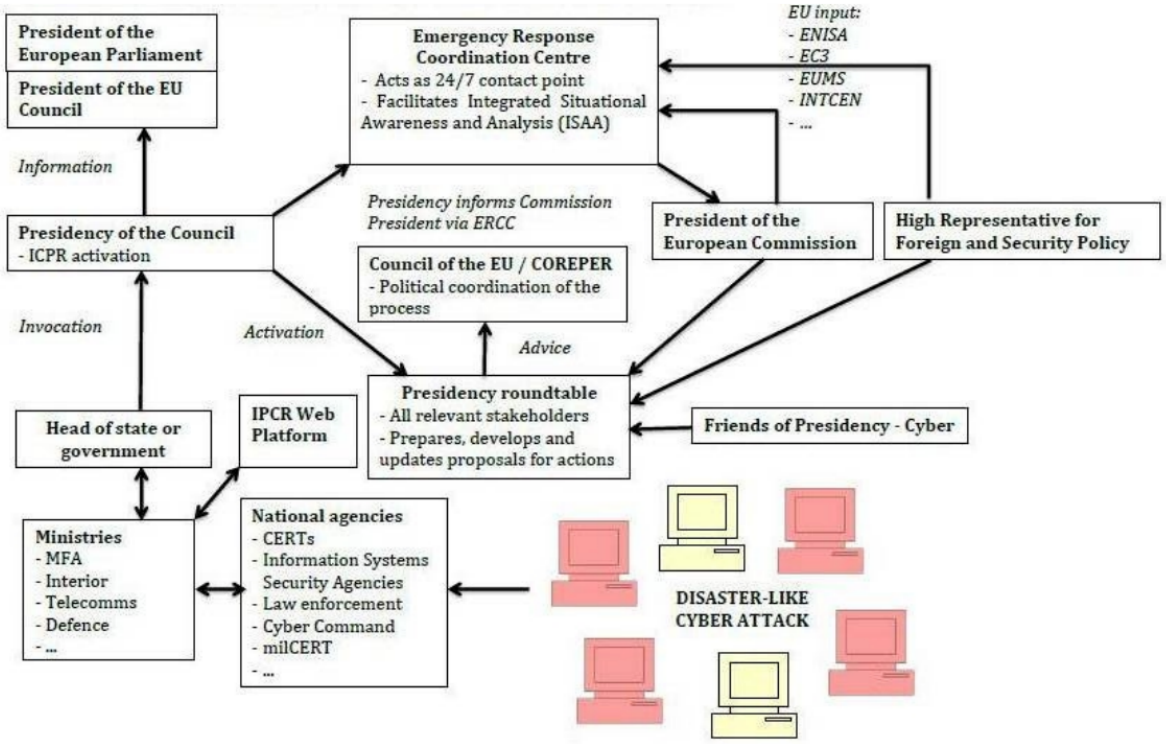
- El 12 de marzo de 2015, el Parlamento Europeo adoptó una resolución sobre sobre el Informe anual de la Alta Representante de la UE en la que hace hincapié en el potencial aún no explotado de varias cláusulas del Tratado de Lisboa, entre ellas el artículo 42 del Tratado UE (la Cláusula de solidaridad), y el artículo 222 del TFUE (Cláusula de Defensa Mutua), y solicita a la Vicepresidenta de la Comisión y Alta Representante promover activamente estos instrumentos y su aplicación, al tiempo que alienta a los Estados miembros a hacer uso de ellos[335].

Pawlak propone un sistema de gestión de crisis en relación a los posibles efectos de un ciberataque que permite visualizar las relaciones entre los diferentes organismos y actores de la Unión Europea en el caso de que sea invocada la Cláusula de Solidaridad:

[334] Parlamento Europeo: *Resolución sobre Ciberseguridad y Defensa*, 22 de noviembre de 2012. http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2012-0457&language=EN&ring=A7-2012-0335 consulta: 11 de octubre de 2015.

[335] Parlamento Europeo: *Resolución sobre el Informe anual de la Alta Representante de la Unión Europea para Asuntos Exteriores y Política de Seguridad al Parlamento Europeo*, Estrasburgo, 12 de marzo de 2015. http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P8-TA-2015-0075&language=EN&ring=A8-2015-0039 consulta: 11 de octubre de 2015.

Figura 24: Gestión de los efectos de un ciberataque utilizando la Cláusula de Solidaridad



Fuente: Ciberseguridad y ciberdefensa en la UE: Clausulas de Solidadridad y Defensa Mutua[336].

4.2. LA CIBERSEGURIDAD EN ORGANIZACIONES Y FOROS INTERNACIONALES

4.2.1. Naciones Unidas

El tema de la seguridad de la información apareció en la agenda de la ONU cuando la Federación Rusa presentó en 1998 un proyecto de resolución en la Primera Comisión de la Asamblea General de la ONU. Este proyecto fue aprobado por la Asamblea General en su Resolución A/53/70 (1998). En esta Resolución 53/70, la Asamblea General recordaba sus resoluciones sobre la función de la ciencia y la tecnología en

[336] PAWLAK, Patryk: *Cybersecurity and cyberdefence EU Solidarity and Mutual Defence Clauses*. *Opus citada*, p. 10.

el contexto de la seguridad internacional, en las cuales se reconocía que los avances científicos y tecnológicos pueden tener aplicaciones civiles y militares y que hay que mantener y fomentar el progreso científico y tecnológico en bien de las aplicaciones civiles[337].

En la actualidad, en el ámbito de la Asamblea General de las Naciones Unidas se está llevando a cabo un debate institucional para determinar qué normas son de aplicación en el ciberespacio para regular el comportamiento de los Estados y garantizar la paz y la seguridad internacional. Hasta la fecha se han aprobado por consenso varias Resoluciones sobre los desarrollos en el ámbito de las tecnologías de la información en el contexto de la seguridad internacional.

Además, en el 2010 se creó un Grupo de Expertos Gubernamentales que ha elaborado informes con recomendaciones sobre la cooperación internacional, la aplicación del derecho internacional en el ciberespacio y la importancia de la construcción de capacidades. España fue seleccionada para participar en el Grupo de Expertos Gubernamentales de Naciones Unidas (GGE), en su cuarta edición. Este GGE está integrado por 20 miembros y en él están representados los países considerados más avanzados en ciberseguridad (Estados Unidos, Reino Unido, Alemania, Francia, Rusia, China, Israel, Japón y Corea, entre otros). El objetivo de este GGE es reflexionar sobre cómo deben aplicarse las normas de derecho internacional, relativas a la paz y seguridad en el ciberespacio. El Grupo presentó un Informe final al Secretario General de la ONU, que fue distribuido en julio de 2015[338].

Este informe final se recoge que:

---

[337] A/RES/53/70. Los avances en la informatización y las telecomunicaciones en el contexto de la seguridad internacional. 79a sesión plenaria de la Asamblea General de Naciones Unidas. 4 de diciembre de 1998. http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/53/70&referer=http://www.un.org/disarmament/topics/informationsecurity/&Lang=S consulta: 2 de noviembre de 2015.

[338] Naciones Unidas: *Informe del Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional*. Nueva York, 22 de julio de 2015. http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174&referer=http://www.un.org/disarmament/topics/informationsecurity/&Lang=S consulta: 2 de noviembre de 2015.

1. Las tecnologías de la información y las comunicaciones (TIC) brindan inmensas oportunidades y su importancia para la comunidad internacional es cada vez mayor. Sin embargo, existen tendencias preocupantes que generan riesgos para la paz y la seguridad internacionales. Para reducir estos riesgos, es esencial que exista una cooperación eficaz entre los Estados.

2. Los Estados deben colaborar para evitar la aplicación de prácticas perjudiciales en la esfera de las TIC y no permitir deliberadamente que su territorio sea utilizado para hechos internacionalmente ilícitos.

3. También se abogó por que se incrementara el intercambio de información y la asistencia para entablar acciones penales por el uso de las TIC con fines terroristas y delictivos.

4. Un Estado no debería realizar o apoyar de forma deliberada actividades en la esfera de las TIC que dañaran intencionadamente infraestructuras fundamentales o dificultaran de otro modo su utilización y funcionamiento.

5. Los Estados también deberían tomar las medidas apropiadas para proteger sus infraestructuras fundamentales frente a las amenazas relacionadas con las TIC.

6. Asimismo, los Estados no deberían dañar los sistemas de información de los equipos autorizados de respuesta a emergencias de otro Estado ni utilizar esos equipos para participar en una actividad internacional malintencionada.

7. Los Estados deberían alentar la divulgación responsable de las vulnerabilidades de las TIC y adoptar las medidas pertinentes para garantizar la integridad de la cadena de suministro y evitar la proliferación de técnicas e instrumentos malintencionados en la esfera de las TIC o funciones ocultas y dañinas.

8. Si bien los Estados tienen la responsabilidad A/70/174 15-12404 3/20 primordial de garantizar un entorno de TIC seguro y pacífico, la cooperación internacional mejoraría si el sector privado, el mundo académico y la sociedad civil participaran de manera adecuada.

9. La creación de capacidades es fundamental para la cooperación y el

fomento de la confianza.

10. La existencia de principios jurídicos internacionales establecidos, entre ellos los principios de humanidad, necesidad, proporcionalidad y distinción son aplicables al ciberespacio.

Además, en 2015, España ha propuesto en el marco de Naciones Unidas un informe nacional en el que se señala que España considera que los Estados Miembros de las Naciones Unidas deben seguir sus esfuerzos de negociación, tanto en el ámbito de Naciones Unidas como en el resto de formatos multilaterales de carácter regional, para alcanzar consensos en cuatro ámbitos de actuación con el objetivo de reforzar la seguridad en la esfera de la información y las telecomunicaciones a nivel global[339]:

11. **Medidas de fomento de la confianza**: Estas medidas se deben adoptar tanto en el ámbito de organismos internacionales y regionales como de manera bilateral entre Estados. Las medidas de fomento de la confianza pueden desarrollarse en una primera fase a través del intercambio de información sobre estrategias nacionales, mejores prácticas e información sobre incidentes y amenazas o creación de puntos de contacto nacionales, entre otras. En una segunda fase, dichas medidas, de carácter más cooperativo, tendrían como objeto último fomentar la transparencia entre los Estados en materia de ciberseguridad y las capacidades de neutralización de eventuales ataques detectados provenientes de terceros países.

12. **Derecho Internacional**: España considera que los Estados, tanto en el ámbito de Naciones Unidas como en otros formatos regionales, deben seguir reflexionando sobre cómo interpretar y aplicar los principios y normas del derecho internacional en el ciberespacio, especialmente los relativos a la amenaza o uso de la fuerza, al derecho humanitario y a la protección de los derechos y libertades fundamentales de las personas.

13. **Cooperación internacional**: Se debe reforzar la cooperación

[339] Naciones Unidas: *Informe de España relativo a RES 69/28 "Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional"* https://unoda-web.s3.amazonaws.com/wp-content/uploads/2015/08/SpainISinfull.pdf consulta: 2 de noviembre de 2015.

internacional para hacer frente a las amenazas y riesgos en el ciberespacio, mejorando los canales de comunicación, estableciendo mecanismos de coordinación de CERTs, realizando ejercicios conjuntos, etc. Se deben promover, agilizar y reforzar los mecanismos de cooperación judicial y policial para prevenir y perseguir los crímenes cometidos en el ciberespacio con rapidez y eficacia.

14. **Desarrollo de capacidades**: Se debe seguir promoviendo el desarrollo de capacidades en los países que lo necesiten, tanto bilateralmente como en el marco de organismos internacionales, preferentemente de carácter regional. En este contexto, los Estados donantes pueden también prestar asistencia a los Estados beneficiarios para el desarrollo de leyes nacionales que establezcan normas de seguridad cibernética uniformes para las diversas agencias gubernamentales de los mismos; vigilar los sistemas de redes de información que estén en desarrollo y poder detectar y analizar las actividades no autorizadas o eventuales ataques. Por otra parte, es preciso promover en aquellos Estados que soliciten ayuda que sus gobiernos tomen medidas para mejorar la cooperación entre las organizaciones nacionales competentes en materia ciberseguridad y para que las responsabilidades de estas organizaciones sea clara, a fin de contrarrestar los ataques cibernéticos que pueden afectar a la seguridad de terceros Estados.

4.2.2. Organización del Tratado del Atlántico Norte

La OTAN es una de las organizaciones pioneras en el diseño de políticas y estructuras de ciberseguridad[340].

Aunque la OTAN siempre ha protegido a sus sistemas de comunicación e información, la Cumbre de Praga de 2002 fue la que primero incorporó la defensa cibernética en la agenda política de la Alianza, recogiendo en su declaración la decisión de “fortalecer

[340] OTAN: *Ciberseguridad*. 1 de septiembre de 2015. http://www.nato.int/cps/en/natohq/topics_78170.htm consulta: 26 de octubre de 2015. En este informe la OTAN presenta un recorrido por las diferentes iniciativas de ciberseguridad de la Alianza.

nuestras capacidades para la defensa de los ataques cibernéticos"[341].

Los líderes aliados reiteraron la necesidad de proporcionar protección adicional a estos sistemas de información en la Cumbre de Riga en 2006, recogiendo en su declaración que se debe "trabajar para desarrollar una capacidad de la OTAN de red habilitada para compartir información, datos e inteligencia de forma fiable, segura y sin demora en las operaciones de la Alianza, al tiempo que se mejora la protección de nuestros sistemas de información clave contra ataques cibernéticos"[342].

Después de los ataques cibernéticos contra las instituciones públicas y privadas de Estonia en abril y mayo de 2007, los Ministros de Defensa de la Alianza acordaron en junio de 2007 impulsar medidas políticas para en el ámbito de la ciberseguridad. Como resultado, la OTAN aprobó su primera Política de Defensa Cibernética en enero de 2008 y que definía los tres pilares básicos de su política respecto al ciberespacio[343]:

- Subsidiariedad: la ayuda se proporciona únicamente ante una petición, y en caso de no haberla se aplica el principio de responsabilidad exclusiva de cada país soberano.
- No duplicación: evitar duplicaciones innecesarias de estructuras o capacidades a nivel internacional, regional y nacional.
- Seguridad: una cooperación basada en la confianza, teniendo en cuenta lo sensible que puede ser la información de los sistemas a la que se debe ofrecer acceso, y sus posibles vulnerabilidades.

En 2008 se creó el Centro de Excelencia para la Cooperación de la Ciberdefensa en Tallín, donde posteriormente se desarrollaría lo que se conoce como el "Manual de

[341] OTAN: *Declaración de la Cumbre de Praga*. 21 de noviembre de 2002. http://www.nato.int/docu/pr/2002/p02-127e.htm consulta: 26 de octubre de 2015.

[342] OTAN: *Declaración de la Cumbre de Riga*. 29 de noviembre de 2006. http://www.nato.int/docu/pr/2006/p06-150e.htm consulta: 26 de octubre de 2015.

[343] THEILER, Olaf: *Nuevas amenazas: el ciberespacio*. Revista de la OTAN, 11, 2011. http://www.nato.int/docu/review/2011/11-september/Cyber-Threads/ES/index.htm consulta: 26 de octubre de 2015.

Tallín", donde se realiza un estudio en profundidad de la situación jurídica del ciberespacio en el ámbito de la seguridad internacional[344].

La OTAN aprobó un nuevo Concepto Estratégico en la Cumbre de Lisboa en 2010, donde se trataba de forma específica la ciberseguridad y la ciberdefensa[345]:

- Artículo 12: Los ataques cibernéticos son cada vez más frecuentes, más organizados y es más costoso el daño que infligen a las administraciones gubernamentales, empresas, economías y, potencialmente, también al transporte y redes de abastecimiento y otras infraestructuras críticas; pudiendo llegar a un umbral que amenace la prosperidad, seguridad y estabilidad, tanto nacionales como euroatlántica. El origen de tales ataques puede deberse a militares, servicios de inteligencia extranjeros, criminales organizados, y grupos terroristas y extremistas.
- Artículo 19: Desarrollar aún más nuestra capacidad de prevenir, detectar, defenderse y recuperarse de ataques cibernéticos, mediante el uso del proceso de planificación de la OTAN para mejorar y coordinar las capacidades nacionales de ciberdefensa, favoreciendo una protección cibernética centralizada en la OTAN, y una mejor integración de la conciencia de ciberdefensa, alerta y respuesta.

En la Cumbre de Chicago, en mayo de 2012, los líderes aliados reafirmaron su compromiso para mejorar las defensas cibernéticas de la Alianza colocando las redes de la OTAN bajo protección centralizada, y estableciéndose la NCIA (NATO Communications and Information Agency) en la que se integran las agencias existentes relacionadas con las tecnologías de la información y comunicaciones[346].

[344] Centro de Excelencia para la Cooperación de la Ciberdefensa de la OTAN: *Tallinn Manual*. https://ccdcoe.org/tallinn-manual.html consulta: 27 de octubre de 2015.

[345] OTAN: *Declaración de la Cumbre de Lisboa*. 20 de noviembre de 2010. http://www.nato.int/cps/en/natolive/official_texts_68828.htm consulta: 27 de octubre de 2015.

[346] OTAN: *Declaración de la Cumbre de Chicago*. 20 de mayo de 2012. http://www.nato.int/cps/en/natohq/official_texts_87593.htm?selectedLocale=en consulta: 27 de octubre de 2015.

En la Política de Defensa Reforzada aprobada por los Ministros de Defensa en junio de 2014 y en la Declaración adoptada en la Cumbre de Gales en septiembre de 2014, se recuerda que la principal responsabilidad de la OTAN es defender sus propias redes y que la asistencia a los aliados debe abordarse de acuerdo a los principios de solidaridad y destacando la responsabilidad de los aliados de desarrollar las capacidades relevantes para la protección de sus redes nacionales. El comunicado de Gales, prioriza además, en su artículo 64, dos aspectos para favorecer una respuesta defensiva en un escenario de crisis colectiva: mejorar la robustez y la disposición de las fuerzas terrestres de la Alianza, y también la ciberdefensa[347].

4.2.3. Organización para la Seguridad y la Cooperación en Europa

La Organización para la Seguridad y la Cooperación en Europa (OSCE) señala que el mundo de hoy no podría funcionar sin las tecnologías de la información y la comunicación (TIC), y dado este escenario, la ciberseguridad se reconoce cada vez más como uno de los principales puntos de discusión sobre la seguridad y la estabilidad internacionales en el siglo XXI. La OSCE estima que tiene un papel importante que desempeñar, especialmente en lo referente a la construcción de la confianza entre los Estados en la región, lo que la OSCE considera especialmente relevante en un área geopolítica donde el potencial de error de percepción y el riesgo de escalada en una crisis constituye una preocupación creciente[348].

Apunta Ziolkowski que la OSCE es una organización con una gran experiencia y una historia de éxito en lo que respecta al desarrollo de las medidas de fomento de la confianza (Confidence Building Measures, CBM) en el área de las armas convencionales. Desde 2011, la OSCE ha demostrado un enfoque integral de la seguridad cibernética, habiendo centrado previamente sus actividades en los aspectos individuales de la ciberseguridad, como la lucha contra la ciberdelincuencia y el uso de internet con fines terroristas. El 26 de abril de 2012, a raíz de una resolución de la

[347] OTAN: *Declaración de la Cumbre de Gales*. 5 de septiembre de 2014. http://www.nato.int/cps/en/natohq/official_texts_112964.htm consulta: 27 de octubre de 2015.
[348] OSCE: *Cyber/ICT security*. 12 de febrero de 2014. http://www.osce.org/node/106324 consulta: 27 de octubre de 2015.

Asamblea Parlamentaria de 2011, el Consejo Permanente de la OSCE estableció un grupo de trabajo oficioso de composición abierta bajo los auspicios del Comité de Seguridad de la organización para elaborar un conjunto de proyectos de medidas de fomento de la confianza para mejorar la cooperación interestatal, la transparencia, la previsibilidad y la estabilidad, y para reducir los riesgos de error de percepción, la escalada, y los conflictos que puedan derivarse de la utilización de las TIC[349].

Los Estados participantes en la OSCE decidieron adoptar, en diciembre de 2013, un conjunto inicial de medidas de fomento de la confianza de la OSCE para reducir los riesgos de conflictos derivados del uso de las tecnologías de la información y la comunicación. Esta iniciativa se centra en una serie de medidas de transparencia y permite el intercambio voluntario de información y la comunicación entre los Estados en varios niveles, incluyendo la formulación de políticas y el nivel de la seguridad nacional de los Estados, todo ello de manera voluntaria y en la medida que los Estados estimen apropiada[350].

Figura 25: Medidas de fomento de la confianza de la OSCE en el ámbito de la ciberseguridad.

1. Los Estados participantes presentarán, de manera voluntaria, su postura nacional sobre diversos aspectos relacionados con las amenazas nacionales y transnacionales contra las TIC y en el uso de las mismas. El alcance de dicha información será determinado por las partes que la faciliten.
2. Los Estados participantes fomentarán la cooperación entre sus organismos nacionales competentes en la materia e intercambiarán información relacionada con la seguridad de las TIC y en el uso de las mismas.
3. Los Estados participantes mantendrán consultas con objeto de reducir los riesgos de percepción errónea, y de posible aparición de tensiones o conflictos políticos o militares que pudieran derivarse del uso de las TIC, así como para proteger las infraestructuras críticas de las

[349] Ziolkowski, Katharina: *Confidence Building Measures for Cyberspace – Legal Implications*. Centro de Excelencia para la Cooperación de la Ciberdefensa de la OTAN, Tallín 2013, pp. 20-21. https://ccdcoe.org/publications/CBMs.pdf consulta: 27 de octubre de 2015.

[350] OSCE: *Decisión nº 1106, Conjunto inicial de medidas de la OSCE para el fomento de la confianza, destinadas a reducir los riesgos de conflicto dimanantes del uso de las tecnologías de la información y la comunicación*. 975ª sesión plenaria, Diario CP Nº 975, punto 1 del orden del día, 3 de diciembre de 2013. http://www.osce.org/es/pc/109650?download=true consulta: 27 de octubre de 2015.

TIC, nacionales e internacionales.
4. Los Estados participantes intercambiarán información acerca de las medidas que hayan adoptado para velar por un Internet abierto, interoperable, seguro y fiable.
5. Los Estados participantes usarán la OSCE como plataforma de diálogo.
6. Se alienta a los Estados a que dispongan de una normativa nacional moderna y eficaz con miras a facilitar la cooperación bilateral y el intercambio de información, incluidos los organismos y las fuerzas de orden público, a fin de luchar contra el uso de las TIC con fines terroristas o delictivos.
7. Los Estados intercambiarán información acerca de su organización, sus estrategias, sus políticas y programas nacionales que sean pertinentes a la seguridad de las TIC.
8. Los Estados participantes nombrarán un punto de contacto para facilitar las comunicaciones y el diálogo pertinentes sobre la seguridad de las TIC y en el uso de las mismas.
9. Los Estados proporcionarán una lista de terminología nacional relacionada con la seguridad de las TIC. A largo plazo, se procurará elaborar un glosario consensuado.
10. Los Estados intercambiarán opiniones haciendo uso de las plataformas y mecanismos de la OSCE.
11. Los Estados participantes, representados por los expertos nacionales que ellos designen, se reunirán por lo menos tres veces al año, en el marco del Comité de Seguridad.

Fuente: OSCE: Decisión nº 1106[351].

La OSCE quiere ser más ambiciosa y tras estas once medidas de fomento de la confianza se encuentra estudiando el impulso del desarrollo de un segundo conjunto de medidas de fomento de la confianza, según ha señalado el Embajador Daniel Baer, Representante Permanente de Estados Unidos ante la OSCE y presidente del grupo de trabajo informal de medidas de fomento de la confianza en el ámbito de la ciberseguridad[352].

[351] *Ibídem*.
[352] OSCE: *Confidence building measures to enhance cybersecurity in focus at OSCE meeting in Vienna*. Viena, 7 de noviembre de 2014. http://www.osce.org/cio/126475 consulta: 27 de octubre de 2015.

Conclusiones del Capítulo 4

En el ámbito de la **Unión Europea**, se ha estudiado la Política Exterior y de Seguridad Común (PESC) de la UE y su derivada, la Política Común se Seguridad y Defensa (PCSD) tras el Tratado de Lisboa. Se ha analizado posteriormente la "Estrategia Europea de Seguridad: Una Europa Segura en un mundo mejor", para estudiar a continuación la "Estrategia de Ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro". En el ámbito de la ciberseguridad, la Unión Europea también se ha dotado de un "Marco Político de Ciberdefensa de la UE".

En **Naciones Unidas** se está desarrollando un proceso de alto nivel en el ámbito de la ciberseguridad, para lo que se ha creado un esquema basado en informes que son elaborados por un Grupo de Expertos en el que se encuentran representados los Estados líderes en el proceso de planeamiento de la ciberseguridad. Los informes de este Grupo de Expertos se presentan al Secretario General de la ONU, quien los eleva a la Asamblea General de las Naciones Unidas, estando sus conclusiones orientadas al impacto de la seguridad en el ciberespacio en el marco de la legalidad y seguridad internacionales.

En la **OTAN** la ciberdefensa forma parte del Concepto Estratégico de la Alianza desde la Cumbre de Lisboa en 2010. En enero de 2008, se desarrolló la primera Política de Ciberdefensa. En el 2008 se creó el Centro de Excelencia para la Cooperación de la Ciberdefensa en Tallin. En la Cumbre de Chicago de 2012 se reafirmó el compromiso de mejora de la ciberdefensa de la Alianza. En la Política de Defensa Reforzada aprobada por los Ministros de Defensa en junio 2014 y en la Declaración adoptada en la Cumbre de Gales en septiembre de 2014, se recuerda que la principal responsabilidad de la OTAN es defender sus propias redes y que la asistencia a los aliados debe abordarse de acuerdo a los principios de solidaridad y destacando la responsabilidad de los aliados de desarrollar las capacidades relevantes para la protección de sus redes nacionales.

La **OSCE** ha desarrollado un sistema de trabajo en relación con la ciberseguridad favoreciendo las medidas de confianza entre sus miembros. Además, al ser un foro de

seguridad regional en el que participan Estados Unidos y Rusia, ha servido para intercambiar posiciones políticas y también técnicas.

Las conclusiones que se han obtenido al analizar los aspectos de ciberseguridad de estas organizaciones internacionales reflejan que la ciberseguridad es un ámbito de primer orden en las políticas de estas organizaciones, que han realizado un planeamiento estratégico, acorde a las misiones de la organización, y que se encuentran desarrollando en un planeamiento en cascada que aspira a favorecer adecuados niveles de seguridad en el ciberespacio para desempeñar las misiones que tienen encomendadas.

CAPÍTULO 5. DE LAS ESTRATEGIAS NACIONALES DE CIBERSEGURIDAD A LOS MODELOS DE ORGANIZACIÓN DE LA CIBERSEGURIDAD.

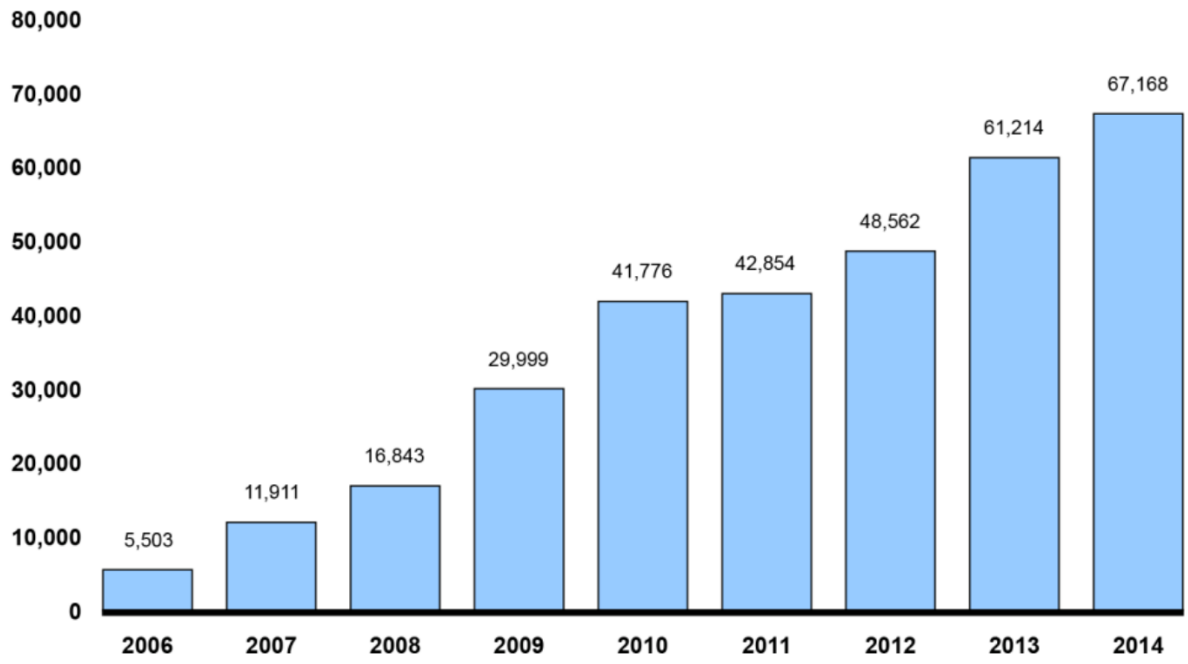
5.1. ESTADOS UNIDOS DE AMÉRICA

5.1.1. De la Estrategia Nacional de Ciberseguridad al modelo de organización

Las amenazas cibernéticas e incidentes en los sistemas de apoyo al gobierno federal y las infraestructuras críticas nacionales en Estados Unidos mantienen un ritmo creciente. Estas amenazas provienen de una variedad de fuentes y varían en función de los tipos y capacidades de los actores, su voluntad de actuar, y su motivación. Por ejemplo, las amenazas persistentes avanzadas, vectores que implican que los adversarios poseen niveles sofisticados de conocimientos y recursos significativos, suponen aumento de los riesgos. Lo que subraya aún más estos riesgos es el incremento de incidentes que podrían amenazar la seguridad nacional y la salud pública; o conducir al acceso inapropiado y la divulgación, modificación o destrucción de información confidencial. Estos incidentes pueden ser involuntarios, como una interrupción del servicio debido a un fallo en el equipo o bien debidos a un evento natural, y también intencionado, como ataque de un hacker a una red informática o sistema. En los últimos 8 años, el número de incidentes de seguridad de información

reportados por las agencias federales al US-CERT, como Capacidad de Respuesta a incidentes de Seguridad de la Información de Estados Unidos, ha aumentado de 5.503 en el año fiscal 2006 a 67.168 en el año fiscal 2014, un incremento de 1.121 por ciento, como se puede apreciar en el siguiente gráfico[353].

Figura 26: Incidentes reportados al US-CERT por agencias federales entre los años fiscales 2006 y 2014



Fuente: Análisis de GAO con información del US-CERT[354].

El informe GAO-15-290 continúa señalando que, en este escenario, el gobierno federal continúa conservando desafíos relacionados con la aplicación efectiva de las políticas de seguridad cibernética. GAO y los inspectores de la agencia de informes generales han identificado retos en un número de áreas clave relacionadas con el enfoque del gobierno en la seguridad cibernética, incluidas las relacionadas con la protección de

[353] United States Government Accountability Office: *Informe a los Comités del Congreso, High-Risk Series: An Update, GAO-15-290*, Washington D.C.,11 de febrero de 2015, p. 241. http://www.gao.gov/assets/670/668415.pdf consulta: 27 de septiembre de 2015.

[354] *Ibídem*, p. 242.

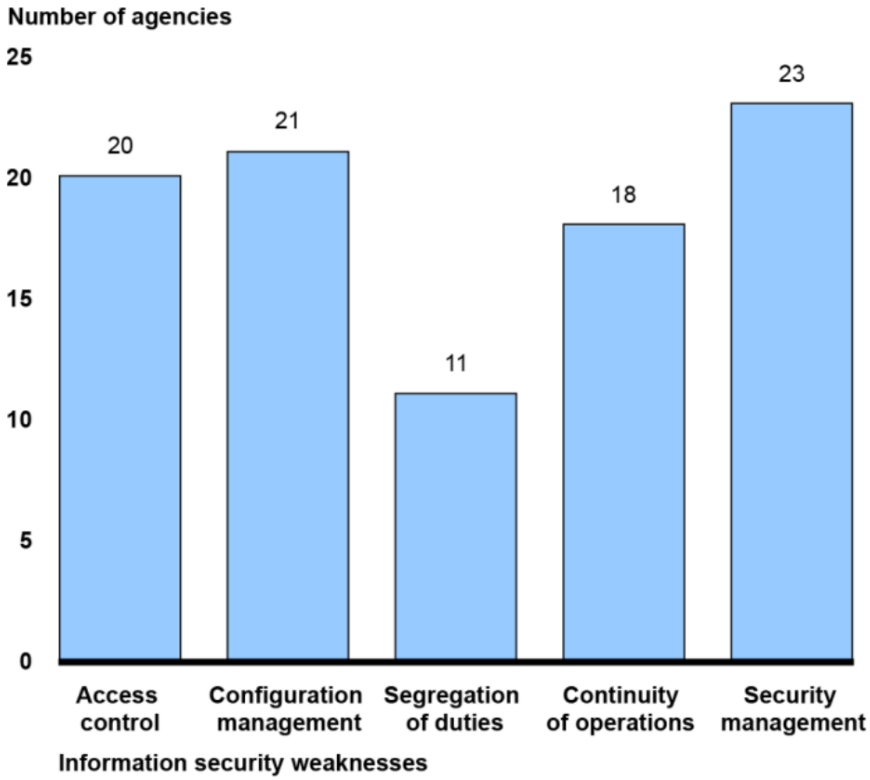
la información del gobierno y de los sistemas que la soportan, así como de las infraestructuras cibernéticas críticas del país. En el año fiscal 2014, la mayoría de las agencias tenían debilidades de la seguridad información en la mayoría de las cinco categorías de control clave: 1.- Limitación, prevención y detección del acceso inapropiado a los ordenadores . 2.- Gestión de la configuración de software y hardware. 3.- Segregación de obligaciones para asegurar que una sola persona no tiene el control sobre todos los aspectos clave de una operación relacionada con los sistemas de información. 4.- Planificación para la continuidad de las operaciones en caso de un desastre o interrupción de los flujos. 5.- Implementación de programas de gestión de seguridad de la información interdepartamentales que son fundamentales para la identificación de las deficiencias de control, la resolución de problemas, y la gestión de riesgos.

La siguiente figura muestra el volumen de agencias con debilidades en estas cinco categorías de control clave[355].

[355] Los 24 principales departamentos y agencias recogidos son los Departamentos de Agricultura; Comercio; Defensa; Educación; Energía; Salud y Servicios Humanos; Seguridad Nacional; Vivienda y Desarrollo Urbano; Interior; Justicia; Trabajo; Estado; Transporte; Hacienda; y Asuntos de Veteranos; y las Agencias de Protección del Medio Ambiente; Administración de Servicios Generales; Administración Nacional de Aeronáutica y del Espacio; Fundación Nacional de la Ciencia; Comisión Reguladora Nuclear; Oficina de Administración de Personal; Administración de Pequeñas Empresas; Administración de la Seguridad Social; y la Agencia de Estados Unidos para el Desarrollo Internacional.

.

Figura 27: Debilidades en el ámbito de la seguridad de la Información en los principales departamentos y agencias federales de Estados Unidos en el año fiscal 2014

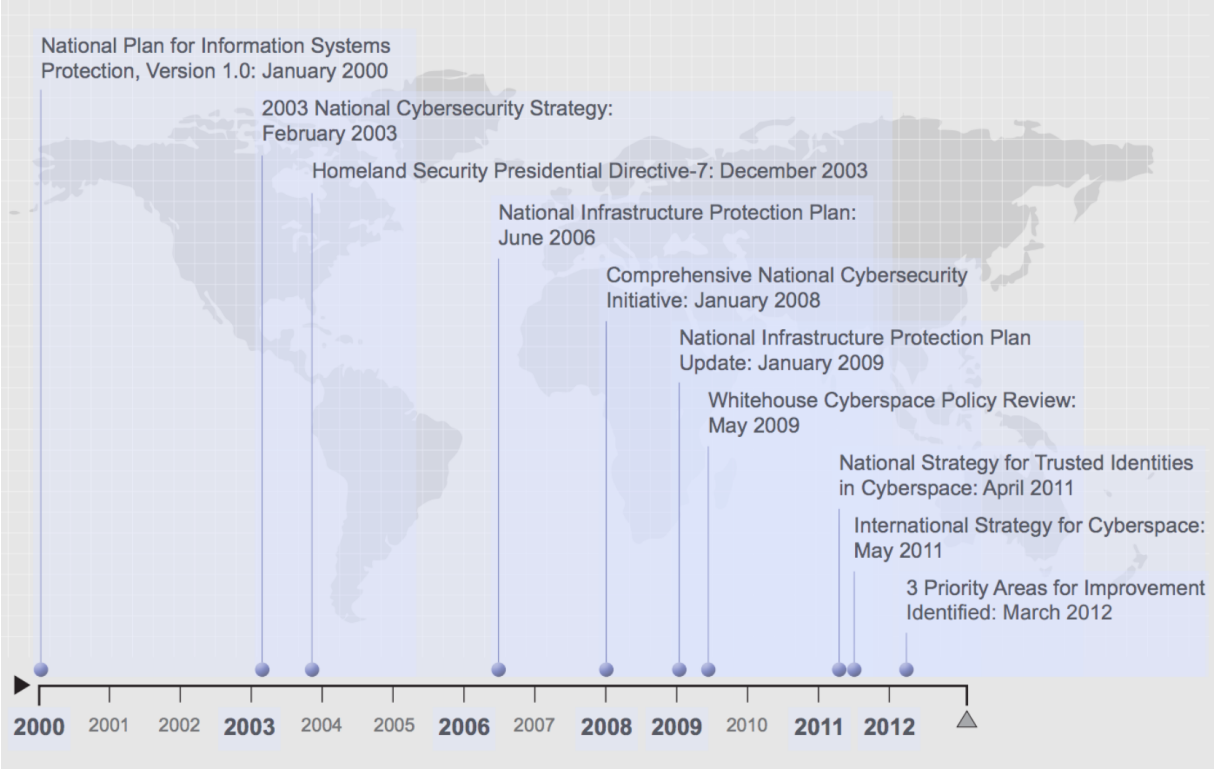


Fuente: Análisis de GAO sobre los informes financieros de departamentos y agencias a 13 de enero de 2015[356].

No existe un único documento que defina exhaustivamente la estrategia de ciberseguridad de Estados Unidos. La evolución del proceso hasta 2012 se aprecia en la siguiente figura, en la que también se integran los hitos relacionados con la protección de infraestructuras críticas.

[356] United States Government Accountability Office: *Informe a los Comités del Congreso, High-Risk Series: An Update, GAO-15-290, opus citada,* p. 244.

Figura 28: Proceso de definición de la estrategia nacional de ciberseguridad en EE.UU.



Fuente: GAO: *Cybersecurity: National Strategy, roles, and responsibilities need to be better defined and more effectively* [357].

El Plan Nacional para la Protección de Sistemas de Información se emitió en enero de 2000 por el Presidente Clinton. El plan se concibió como base de un esfuerzo más amplio para proteger los sistemas de información de la nación y los activos críticos de ataques futuros. Se centró en los esfuerzos federales para proteger infraestructuras críticas basadas en sistemas informáticos y de red. Se identificaron riesgos asociados con la dependencia de Estados Unidos de ordenadores y redes de servicios críticos; reconociendo la necesidad de que el gobierno federal definiera su rol para abordar los riesgos en las infraestructuras críticas. El plan identificó hitos y elementos de acción

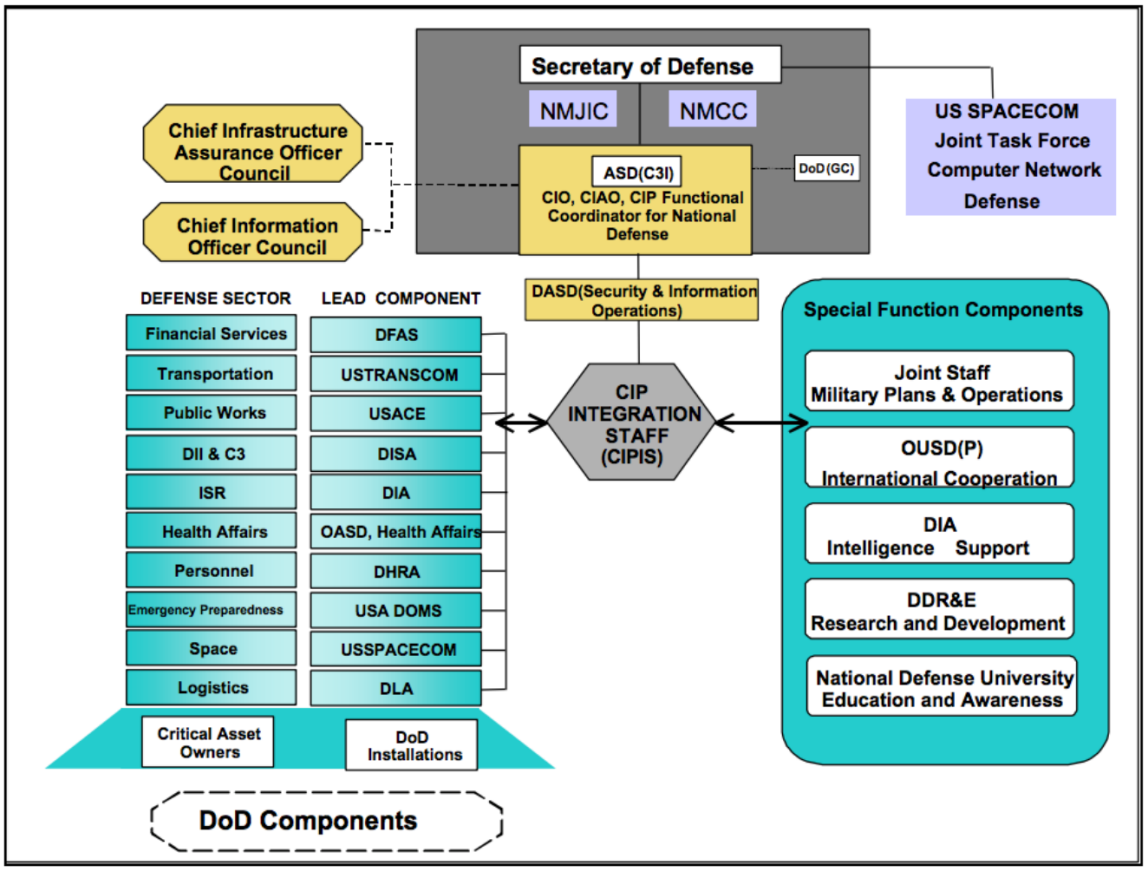
[357] United States Government Accountability Office: *Informe a los Congresistas,* Cybersecurity: National Strategy, roles, and responsibilities need to be better defined and more effectively, *GAO-13-187*, Washington D.C., febrero de 2013, p. 20. http://www.gao.gov/assets/660/652170.pdf consulta: 12 de octubre de 2015.

específicos para el desarrollo de diez programas con el objeto de hacer frente a la necesidad de prevención, preparación, detección y respuesta ante los ataques cibernéticos[358].

En el Plan Nacional para la Protección de Sistemas de Información se integra el Programa de protección de infraestructuras críticas del Departamento de Defensa, que aporta un diseño de estructura novedosa, basada en procesos horizontales, para integrar la respuesta a las agresiones que utilizan el ciberespacio.

[358] La Casa Blanca: *Defending America's Cyberspace, National Plan for Information Systems Protection, Version 1.0, An Invitation to a Dialogue*, Washington D.C., 2000. https://fas.org/irp/offdocs/pdd/CIP-plan.pdf consulta: 12 de octubre de 2015.

Figura 29: Estructura del sistema de respuesta del Departamento de Defensa en el Plan Nacional para la Protección de Sistemas de Información



Fuente: Plan Nacional para la Protección de Sistemas de Información[359].

La Estrategia Nacional para Asegurar el Ciberespacio[360] se emitió en febrero de 2003 por el Presidente George W. Bush, con el propósito de proporcionar un marco para organizar y priorizar los esfuerzos para proteger el ciberespacio. La estrategia se organizó de acuerdo a cinco prioridades nacionales:

• Un sistema de respuesta de seguridad nacional para el ciberespacio.

[359] *Ibídem*, p. 84.

[360] La Casa Blanca: *The National Strategy to Secure Cyberspace*, Washington D.C., febrero de 203. https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf consulta: 12 de octubre de 2015.

• Un programa de reducción de amenazas y vulnerabilidades para la seguridad nacional en el ciberespacio.
• Un programa de concienciación y formación sobre el impacto del ciberespacio en la seguridad nacional.
• Asegurar el ciberespacio para la acción de gobierno.
• La Cooperación de seguridad internacional en el ciberespacio y la seguridad nacional.

La Estrategia Nacional para Asegurar el Ciberespacio definió además las responsabilidades de los diferentes actores nacionales de acuerdo a estas cinco prioridades.

Figura 30: Responsabilidades para asegurar el ciberespacio en Estados Unidos

Roles and Responsibilites in Securing Cyberspace

	Priority 1	Priority 2	Priority 3	Priority 4	Priority 5
	National Cyberspace Security Response System	National Cyberspace Security Threat and Vulnerability Reduction System	National Cyberspace Security Awareness and Training Program	Securing Governments' Cyberspace	National Security and International Cyberspace Security Cooperation
Home User/Small Business		X	X		
Large Enterprises	X	X	X	X	X
Critical Sectors/ Infrastructures	X	X	X	X	X
National Issues and Vulnerabilities	X	X	X	X	
Global					X

Fuente: Estrategia Nacional para Asegurar el Ciberespacio[361].

[361] *Ibídem*, p. 9.

Aunque no se define si la estrategia de 2003 sustituye el plan de 2000 o estaba destinada a ser un documento suplementario, las prioridades la estrategia son similares a las del documento 2000. No obstante, analistas como Casey saludan esta nueva aproximación, en un escenario en el que la desaceleración de la economía de Estados Unidos había afectado de manera significativa a la alta tecnología y a las industrias de telecomunicaciones. Dado que el terrorismo y la guerra habían elevado la preocupación y estimulado la conciencia sobre la necesidad de aumentar la seguridad de la información, esta estrategia de 2003 favorece la incorporación de recursos adicionales para la ciberseguridad[362].

La Iniciativa Integral Nacional de Ciberseguridad (CNCI) se emitió en 2008, por el Presidente George W. Bush. Este documento clasificado presentaba un conjunto de 12 proyectos destinados a salvaguardar los sistemas de información del poder ejecutivo mediante la reducción de las vulnerabilidades potenciales, la protección contra intentos de intrusión y la anticipación a futuras amenazas. El Presidente Obama actualizó esta Iniciativa en 2009, tras identificar la ciberseguridad como uno de los más graves desafíos la seguridad económica y nacional. Poco después de asumir el cargo, el Presidente Obama ordenó una revisión exhaustiva de los esfuerzos federales para defender la información de Estados Unidos y la infraestructura de comunicaciones y el desarrollo de un enfoque integral para asegurar la infraestructura digital de Estados Unidos. En mayo de 2009, el Presidente Obama aceptó las recomendaciones del análisis de las políticas del ciberespacio, incluyendo la selección de un Coordinador de Ciberseguridad en el Poder Ejecutivo con acceso regular al Presidente de Estados Unidos. También se actualizaron los doce proyectos de la Iniciativa Integral Nacional de Ciberseguridad[363]:

[362] CASEY, Tim: *Research on Topics in Information Security. The National Strategy to Secure Cyberspace: an In-depth Review,* Global Information Assurance Certification (GSEC), SANS Institute, 2003. http://www.giac.org/paper/gsec/2875/national-strategy-secure-cyberspace-in-depth-review/104847 consulta: 12 de octubre de 2015.

[363] La Casa Blanca: *The Comprehensive National Cybersecurity Initiative*, 2009 https://www.whitehouse.gov/sites/default/files/cybersecurity.pdf

15. Administrar la red federal de empresas como una única empresa de la red con conexiones seguras a Internet.
16. Implementar un sistema de detección de intrusiones de sensores en esta empresa federal.
17. Desplegar sistemas de prevención de intrusiones en toda la empresa federal.
18. Coordinar y redirigir los esfuerzos de investigación y desarrollo (I + D).
19. Conectar los actuales centros de operaciones de ciberseguridad para mejorar la percepción de la situación.
20. Desarrollar e implementar un plan de todo el Gobierno en contrainteligencia cibernética.
21. Aumentar la seguridad de las redes clasificadas.
22. Ampliar la educación en ciberseguridad.
23. Definir y desarrollar estrategias y programas de tecnología duradera que impliquen un salto cualitativo.
24. Definir y desarrollar estrategias y programas perdurables de disuasión.
25. Desarrollar un enfoque múltiple para la gestión global de riesgo.
26. Definir el papel federal para extender la seguridad cibernética en dominios de infraestructuras críticas.

Dado que esta Iniciativa Integral Nacional de Ciberseguridad se emitió en las postrimerías de la presidencia de George W. Bush y que recién tomada posesión Barack Obama como Presidente de Estados Unidos procedió a su revisión, este interregno produjo numerosa literatura en el ámbito de la ciberseguridad, favorecida por la transición de un documento clasificado como "top secret" a otro sin clasificación. En este sentido, se recomienda la lectura del informe de Rollins y Henning "Iniciativa Integral Nacional de Ciberseguridad: Consideraciones sobre Autoridades Legales y Política"[364].

[364] ROLLINS, John y HENNING, Anna C.: *Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations*, Informe al Congreso, 10 de marzo de 2009.

Además de esta revisión de la CNCI, el Presidente Obama publicó en mayo de 2009 la Revisión de la Política sobre el Ciberespacio[365]. En este documento, se establecen los objetivos a corto y a medio plazo para la ciberseguridad en Estados Unidos.

Figura 31: Plan de Acción a corto plazo de la Revisión de la Política sobre el Ciberespacio

Plan de Acción a corto plazo
1. Nombrar a un responsable encargado de coordinar la ciberseguridad nacional para coordinar el desarrollo interinstitucional de estrategias y políticas relacionadas con la ciberseguridad.
2. Preparar la aprobación del Presidente de una estrategia nacional actualizada para asegurar los flujos de información y la infraestructura de las comunicaciones.
3. Designar la ciberseguridad como una de las prioridades clave de la administración del Presidente y establecer métricas de rendimiento.
4. Designar un responsable para garantizar la privacidad y las libertades civiles en el ámbito de la ciberseguridad en la dirección del Consejo de Seguridad Nacional.
5. Establecer mecanismos para llevar a cabo análisis jurídicos en el ámbito de la ciberseguridad y formular una orientación política unificada coherente.
6. Iniciar una campaña nacional de sensibilización y educación para promover la concienciación en ciberseguridad.
7. Desarrollar el marco internacional de políticas de ciberseguridad.
8. Preparar un plan de respuesta a incidentes de seguridad cibernética.
9. En colaboración con otras entidades de la Oficina Ejecutiva del Presidente, desarrollar un marco para la investigación y el desarrollo de las estrategias para mejorar la ciberseguridad.

https://www.whitehouse.gov/files/documents/cyber/Congressional%20Research%20Service%20-%20CNCI%20-%20Legal%20Authorities%20and%20Policy%20Considerations%20(March%202009).pdf consulta: 12 de octubre de 2015.

[365] La Casa Blanca: *Cyber Space Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, Washington D.C., mayo de 2009. https://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf consulta: 12 de octubre de 2015.

10. Construir una visión de gestión de identidades basadas en la ciberseguridad y la estrategia que se dirige a la privacidad y la libertades intereses civiles, aprovechando las tecnologías de privacidad de mejora de la Nación.

Fuente: Revisión de la Política sobre el Ciberespacio[366].

Figura 32: Plan de Acción a medio plazo de la Revisión de la Política sobre el Ciberespacio

Plan de Acción a medio plazo
1. Mejorar el proceso para la resolución de discrepancias entre las agencias respecto a las interpretaciones de la ley y la aplicación de la política y las autoridades responsables.
2. Use el marco de evaluación del programa de la Oficina de Administración y Presupuesto para garantizar los objetivos de ciberseguridad.
3. Ampliar el apoyo a los programas y la investigación y el desarrollo.
4. Desarrollar una estrategia para ampliar y capacitar la fuerza de trabajo, en el ámbito de la ciberseguridad en el gobierno federal.
5. Determinar el mecanismo más eficiente para mantener los indicadores estratégicos, el conocimiento de la situación, y la información en las capacidades de respuesta a incidentes.
6. Desarrollar un conjunto de escenarios de amenaza y el control de las decisiones en la gestión de riesgos, planificación de la recuperación, y la priorización de la I + D.
7. Desarrollar un proceso entre el gobierno y el sector privado para contribuir a prevenir, detectar y responder a incidentes cibernéticos.
8. Desarrollar mecanismos de intercambio de información relacionada con la seguridad cibernética en relación con la privacidad y la propiedad de la información.
9. Desarrollar soluciones para capacidades de comunicaciones de emergencia en desastres naturales, crisis o conflictos, al tiempo que se garantiza la neutralidad de la red.
10. Ampliar el intercambio de información sobre incidentes de red y vulnerabilidades con aliados clave.
11. Fomentar la colaboración investigación y tecnológica.
12. Definir de estándares nacionales e internacionales.

[366] *Ibídem*, p. 37.

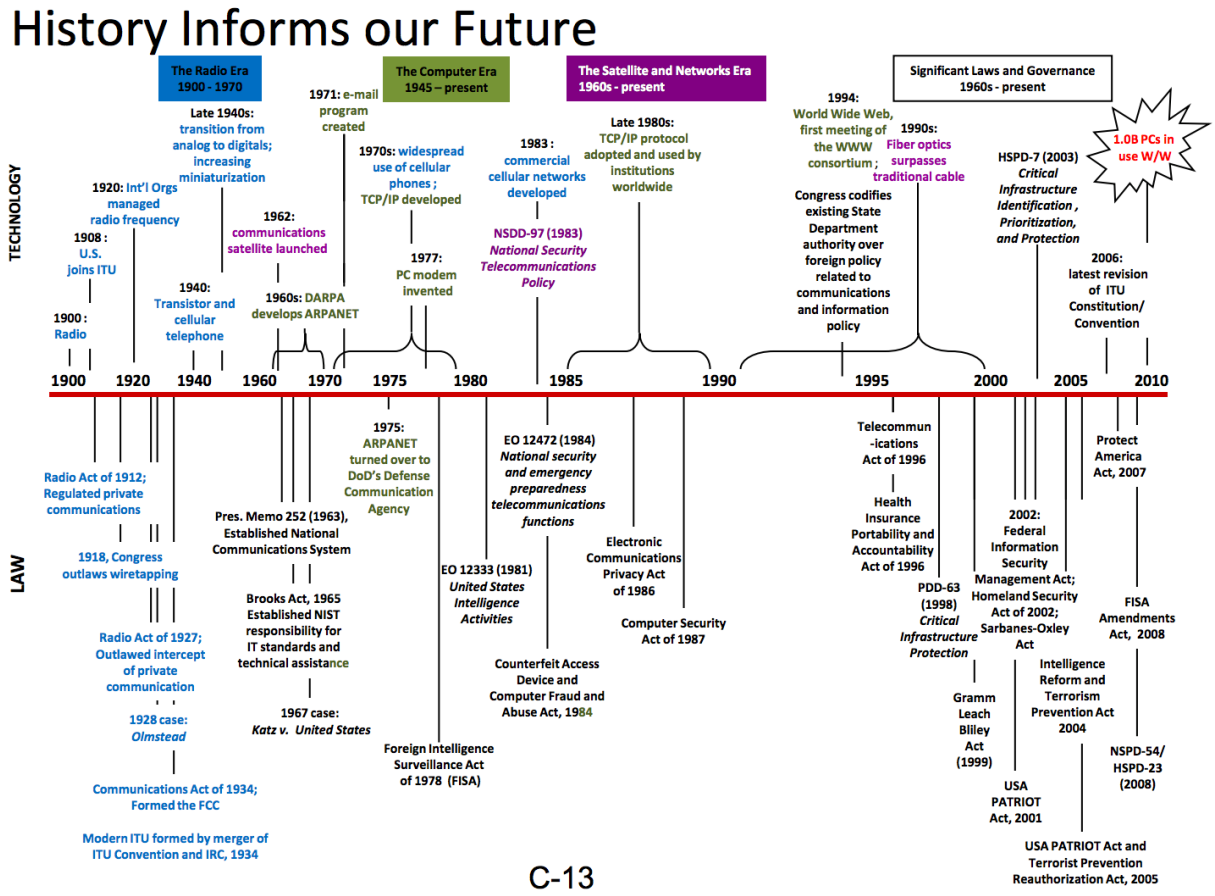
13. Mejorar la confianza en las transacciones en línea y la privacidad.
14. Mejorar las estrategias de contratación pública en innovación, seguridad y servicios.

Fuente: Revisión de la Política sobre el Ciberespacio[367].

La Revisión de la Política sobre el Ciberespacio presenta además un interesante gráfico que incorpora los hitos más significativos en el ámbito de la tecnología y el desarrollo legislativo aplicable desde 1900 a 2010. La historia de las comunicaciones electrónicas en los Estados Unidos incorpora los esfuerzos del gobierno para regular, administrar o responder a las cuestiones que presentan estos nuevos medios de comunicación, incluidos los problemas de seguridad. La evolución de estos procesos ha dado lugar a un mosaico de leyes y estructuras de gobierno en relación con la seguridad y la capacidad de recuperación de la información y las comunicaciones.

[367] *Ibídem*, p. 38.

Figura 33: Comparativa del desarrollo tecnológico en las comunicaciones y la evolución legislativa en Estados Unidos de 1900 a 2010.



Fuente: Revisión de la Política sobre el Ciberespacio[368].

La Estrategia Nacional de Identidades de Confianza en el Ciberespacio (NSTIC), aprobada por el Presidente Obama en abril de 2011, establece diferentes medidas para que los ciudadanos y el sector privado colaboren para elevar el nivel de confianza asociado con la identidad de los individuos, organizaciones, redes, servicios y dispositivos, que intervienen en las transacciones en línea[369].

[368] *Ibídem*, C-12 y C-13.

[369] La Casa Blanca: *National Strategy for Trusted Identities in Cyberspace: Enhancing Online Choice, Efficiency, Security, and Privacy*, Washington D.C., abril de 2011. https://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf consulta: 12 de octubre de 2015.

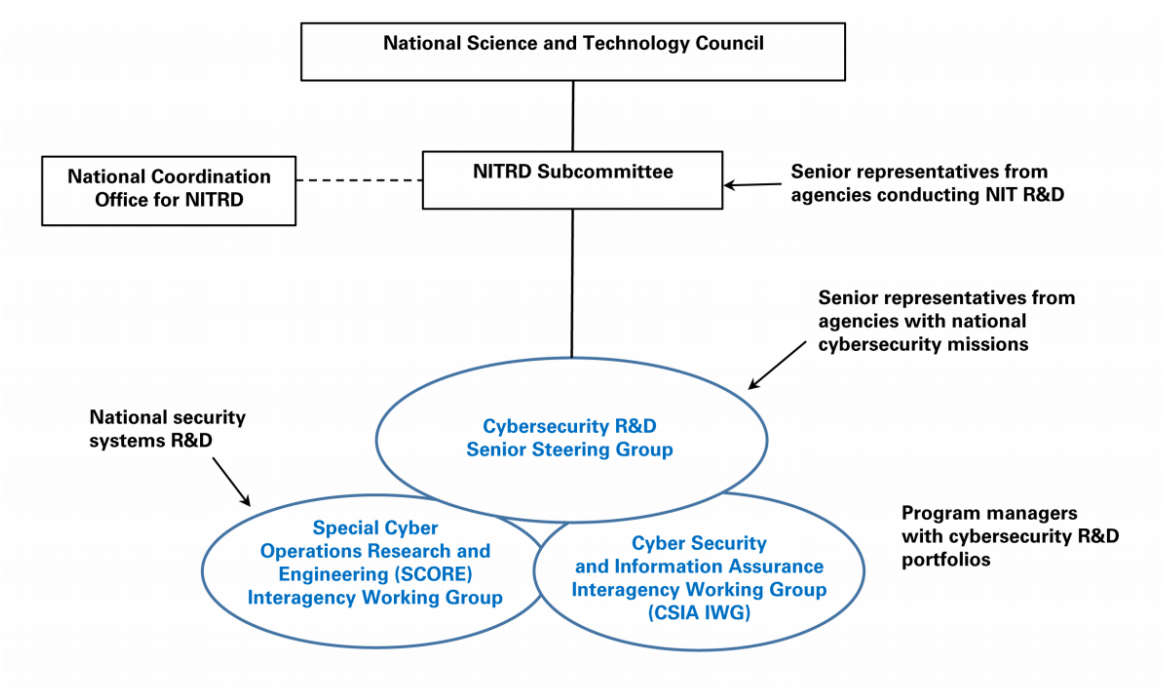
La NSTIC fue, en general, acogida favorablemente por empresas y particulares. Señala Alex Howard que los gobiernos se enfrentan ahora a decisiones complejas en su manera de abordar cuestiones de identidad, dada la creciente integración de la tecnología en la vida cotidiana de los ciudadanos. De esta forma, la estrategia aborda las tendencias clave que son cruciales para el crecimiento del sistema operativo de Internet: identidad en línea, privacidad y seguridad[370].

El Plan Estratégico de Investigación y Desarrollo en Ciberseguridad, de diciembre de 2011, se conforma en respuesta a las recomendaciones relacionadas con la I + D en la Casa Blanca, expuestas en el Examen de las Políticas del Ciberespacio. De esta forma, en el Plan Estratégico se recoge el modo en el que las actividades de I + D pueden contribuir a combatir los desafíos de ciberseguridad críticos en áreas de prioridad nacional, como la salud, la energía, los servicios financieros y la defensa[371].

[370] HOWARD. Alex: *A Manhattan Project for online identity*: *A look at the White House's National Strategy for Trusted Identities in Cyberspace*. O'Reilly Radar, 4 de mayo de 2011. http://radar.oreilly.com/2011/05/nstic-analysis-identity-privacy.html consulta: 13 de octubre de 2015.

[371] Oficina Ejecutiva del Presidente y Consejo Nacional de Ciencia y Tecnología: *Strategic Plan for Cybersecurity Research and, Development*, Washington D.C., diciembre de 2011. https://www.whitehouse.gov/sites/default/files/microsites/ostp/fed_cybersecurity_rd_strategic_plan_2011.pdf consulta: 13 de octubre de 2015.

Figura 34: Coordinación de la estructura de I + D en ciberseguridad en Estados Unidos



Fuente: Plan Estratégico de Investigación y Desarrollo en Ciberseguridad[372].

La Estrategia Internacional para el Ciberespacio, emitida por la Casa Blanca en mayo de 2011, establece una hoja de ruta para una mejor definición y coordinación de la política internacional en relación con el ciberespacio. El objetivo de la estrategia establece que los Estados Unidos trabajarán a nivel internacional para promover un infraestructura de comunicaciones abierta, interoperable, segura y fiable, que permita el desarrollo del comercio internacional, fortalezca la seguridad internacional, y fomente la libertad de expresión y la innovación. La estrategia señala que para cumplir ese objetivo, se apoyará el Estado de derecho en el ciberespacio[373].

David P. Fidler señala que un tema recurrente en la Estrategia Internacional para el Ciberespacio es la necesidad del imperio de la ley tanto en el ámbito nacional como

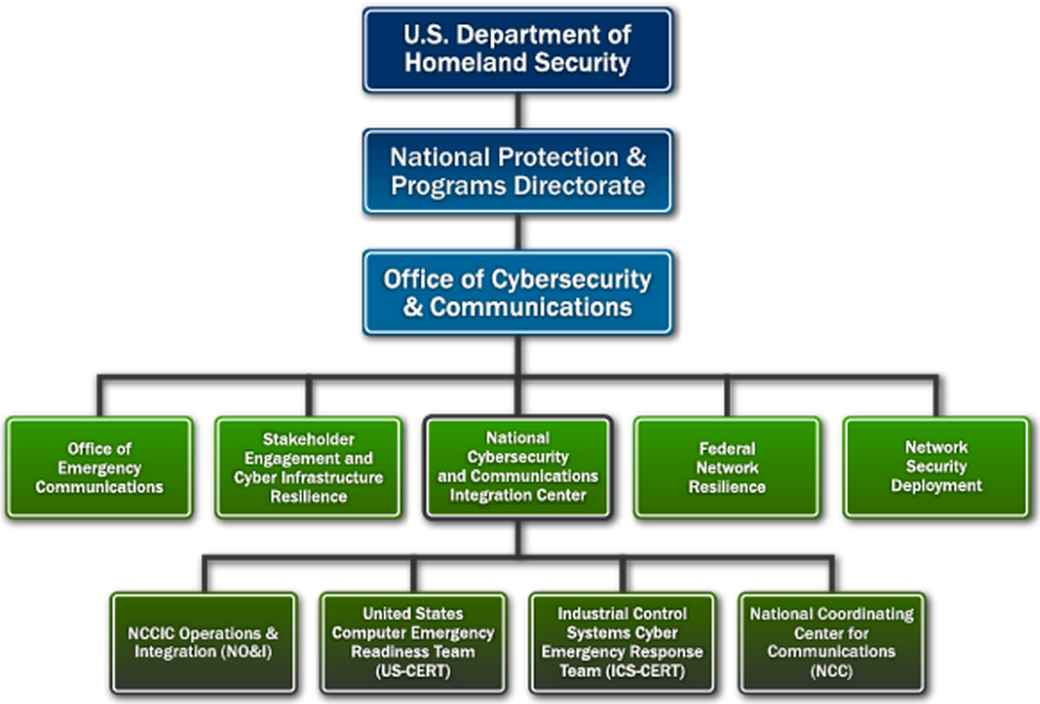
[372] *Ibídem*, p. 17.

[373] La Casa Blanca: *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, Washington D.C., mayo de 2011. https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf consulta: 13 de octubre de 2015.

en el internacional de la gobernanza del ciberespacio. El derecho internacional y los procesos legales juegan un papel crítico en la visión de la Administración Obama en relación con la prosperidad, la seguridad, y la apertura en un mundo conectado. En términos de derecho sustantivo, la Estrategia Internacional pone de manifiesto que muchos de los principios vigentes del derecho internacional, tanto en tiempo de paz como de conflicto, también se aplican en el ciberespacio. Estas normas jurídicas internacionales vigentes incluyen el respeto a los derechos civiles y políticos fundamentales de la libertad de expresión y asociación, la privacidad y la propiedad; la responsabilidad del Estado para negar refugio a los criminales; y el derecho a usar la fuerza en legítima defensa, tanto individual como colectiva, en respuesta a los ataques armados[374].

[374] FIDLER, David P.: *International Law and the Future of Cyberspace: The Obama Administration's International Strategy for Cyberspace*, American Society of International Law, Insights, volumen 15, 8 de junio de 2011. http://www.asil.org/insights/volume/15/issue/15/international-law-and-future-cyberspace-obama-administration%E2%80%99s consulta: 13 de octubre de 2015.

Figura 35: El Centro de Integración Nacional de Ciberseguridad y Comunicaciones en la estructura del DHS



Fuente: Departamento de Homeland Security[375].

5.2. LA CIBERSEGURIDAD EN LA REPÚBLICA POPULAR DE CHINA

5.2.1. La ciberseguridad en la Estrategia de Seguridad Nacional de China

La utilización de las nuevas tecnologías de la información y en especial la utilización de internet supone para las autoridades chinas un factor de importancia sobresaliente. Ya en el tercer pleno del 18 Comité Central del Partido Comunista Chino en 2013 se señalaba que frente al vertiginoso desarrollo de la tecnología y las aplicaciones de Internet, existen evidentes fallas, ya que al mismo tiempo, a medida que Internet se fortalece como medio de comunicación, la administración de los medios en la red y la

[375] Departamento de Homeland Security: *Centro de Integración Nacional de Ciberseguridad y Comunicaciones*. http://www.dhs.gov/national-cybersecurity-communications-integration-center consulta: 2 de noviembre de 2015.

administración industrial están lejos de alcanzar el desarrollo y cambio que la situación exige. Sobre todo, frente al rápido incremento de las redes de contacto sociales y de usuarios de herramientas de comunicación instantánea. Continúan los documentos de este tercer pleno señalando que la forma de reforzar el fomento de la legalidad de la red y la orientación de la opinión pública, asegurar el orden de transmisión de informaciones en la red, la seguridad estatal y la estabilidad social se ha convertido en un tema destacado, lo que necesita establecer las medidas adecuadas para asegurar el uso correcto de la red y su seguridad[376].

La Ley de Seguridad Nacional menciona específicamente la ciberseguridad en su artículo 25: "El Estado construye un sistema de protección de seguridad de las redes y de la información, que actualiza las capacidades de protección de seguridad de las redes y de la información, refuerza la innovación, la investigación, el desarrollo y la aplicación de tecnologías de las redes y de la información, se hace cargo de la seguridad y la capacidad de control de las redes principales, tecnologías de la información, infraestructuras críticas, sistemas de información y datos en áreas importantes; fortalece la gestión de redes; previene y reprime de acuerdo a la ley sanciones contra los ataques en línea, el hacking, el robo de secretos en la red, la difusión de información ilegal o perjudicial, y otros actos ilegales y criminales utilizando las redes; salvaguarda la seguridad de la soberanía nacional y el desarrollo de los intereses en el ciberespacio"[377].

Este artículo de la Ley de Seguridad Nacional, que arroga al Estado amplias responsabilidades en el control y seguridad de las redes, es el referente de máximo nivel legislativo chino del que se desprenden las diferentes piezas legislativas relacionadas con la ciberseguridad.

[376] *Documentos de la III Sesión Plenaria del XVIII Comité Central del Partido Comunista de China*, pp. 55-56. *opus citada*.

[377] China Copyright and Media; The law and policy of media in China , Ed. Rogier Creemers: *opus citada.*

El 6 de julio de 2015, solo cinco días más tarde de la aprobación de la Ley de Seguridad Nacional, la Asamblea Popular Nacional de China dio a conocer el proyecto de texto de Ley de Ciberseguridad, poniendo a disposición pública el texto para comentarios[378].

En este sentido, es de destacar la posibilidad que se ha ofrecido a cualquier persona o institución para hacer comentarios al proyecto de Ley de Ciberseguridad, según se recoge en una traducción no oficial de la organización "China Law Translate", que señala que la 15ª sesión del Comité Permanente de la 12 ª Asamblea Popular Nacional realizó la revisión inicial de esta "Ley de Seguridad Cibernética de la República Popular de China (Proyecto)" en junio de 2014 y que este proyecto de Ley se facilita en la página web del Congreso Nacional del Pueblo chino para la incorporación de comentarios públicos. El período de consulta concluyó el 5 de agosto de 2015[379].

El proyecto de Ley de Ciberseguridad consta de 68 artículos en siete capítulos: Capítulo 1, Disposiciones Generales; Capítulo II, Red de Seguridad de Estrategia, Planificación y Promoción; Capítulo III, Red de Operaciones de Seguridad;; Capítulo IV, Red de Información sobre Seguridad; Capítulo V, El monitoreo, alertas tempranas, y la respuesta de emergencia; Capítulo VI, Responsabilidad Legal; Capítulo VII, Disposiciones Complementarias.

Del primer capítulo puede destacarse la declaración inicial que señala en el artículo 1: "Esta ley se formula a fin de garantizar la seguridad de la red, para preservar la soberanía del ciberespacio, la seguridad nacional y el interés público de la sociedad, para proteger los derechos e intereses legítimos de los ciudadanos, personas jurídicas y otras organizaciones, y para promover el sano desarrollo de los derechos

[378] Council on Foreign Relations: *Cybersecurity Law of the People's Republic of China*, 6 de julio de 2015. http://www.cfr.org/internet-policy/cybersecurity-law-peoples-republic-china/p36788 consulta: 11 de agosto de 2015.

[379] CHINA LAW TRANSLATE: *Cybersecurity Law (Draft),* 6 de julio de 2015. http://chinalawtranslate.com/cybersecuritydraft/?lang=en consulta: 11 de agosto de 2015. Se ha podido acceder directamente a la página web de la APN (www.npc.gov.cn) y formular observaciones, y también se han podido enviar comentarios al Comité Nacional de Trabajo Legal del Congreso Pueblo (Pekín, Triciclos, Qianmen West Road # 1, 100805).

económicos e informatización social". El resto de los artículos de este primer capítulo profundizan en las atribuciones y responsabilidades que se arroga el Estado en el campo de la ciberseguridad: el Estado tiene la responsabilidad de la seguridad de la red; asegura un comportamiento civilizado en la red; establece la formulación de normas; combate la delincuencia informática; adopta las medidas para la respuesta a incidentes de seguridad de la red; protege los derechos de los ciudadanos, personas jurídicas y otras organizaciones para utilizar las redes de acuerdo con la ley; garantiza la circulación legal, ordenada y libre de información de la red; y promueve la construcción de un ciberespacio pacífico, seguro, abierto y cooperativo[380].

En el segundo capítulo del proyecto de Ley de Ciberseguridad se delimitan responsabilidades para diferentes organismos en materia de ciberseguridad en China, siendo el Estado responsable de formular la estrategia de seguridad de la red, estableciendo los requisitos básicos y principales objetivos nacionales para garantizar la seguridad de la red, estimulando el desarrollo de tecnologías de seguridad, y avanzando medidas políticas para preservar la seguridad de la red con la participación de toda la sociedad. Este capítulo señala también que todos los niveles de la administración deberán organizar y llevar a cabo la concienciación de la seguridad en la red, mencionando específicamente que los medios de comunicación deberán dirigir actividades concienciación de seguridad en la red dirigidas a la opinión pública[381].

El capítulo tercero, recoge que para satisfacer las necesidades de la seguridad nacional y la investigación penal, se podrá solicitar a los operadores de red que proporcionan la asistencia y el soporte tecnológico necesario de conformidad con las leyes y reglamentos. En cuanto a la seguridad de las infraestructuras críticas, se señalan en este capítulo las responsabilidades estatales en la protección de las redes de información básicas que prestan servicios como el correo; la radio; la televisión; las industrias de los sectores de la energía, el transporte, la conservación del agua, las finanzas; y las áreas de servicio público como la electricidad, agua, gas y servicio

[380] *Ibídem,* artículos 1-10.

[381] *Ibídem,* artículos 11-16.

médico, entre otros. También se señala que los operadores de infraestructuras críticas deberá almacenar información personal de los ciudadanos, y otros datos significativos, en el territorio continental de la República Popular de China.[382]

El capítulo cuarto regula en qué condiciones deben realizarse por los operadores de red la recolección y el uso de información personal de los ciudadanos, que deberán respetar los principios de legalidad y la necesidad, indicando explícitamente los objetivos, medios y el alcance de la recopilación o el uso de la información, así como la obtención del consentimiento de la persona cuyos datos se reunieron. De esta forma, se señala que los operadores de red no deben recopilar información personal de los ciudadanos sin relación con los servicios que prestan; no deben violar las disposiciones de las leyes, reglamentos administrativos o los acuerdos bilaterales para recoger o utilizar información personal de los ciudadanos[383].

El capítulo quinto, dedicado a las alertas tempranas y respuesta ante emergencias delimita las responsabilidades para la coordinación general de los departamentos pertinentes para fortalecer la recopilación, análisis y presentación de informes los esfuerzos de información de seguridad de red y la información de alerta temprana. En caso de emergencias repentinas o accidentes de seguridad que se produzcan como consecuencia de los incidentes de seguridad de la red, se tramitará de conformidad con lo dispuesto en las leyes pertinentes, tales como la "Ley de Respuesta a Emergencias de la República Popular China". Además, para cumplir con la necesidad de proteger la seguridad nacional y el orden público social y responder a incidentes importantes de seguridad social, se podrán adoptar las medidas temporales que restrinjan la utilización de las comunicaciones de red en ciertas regiones[384].

En cuanto a las responsabilidades legales que se recogen en el capítulo sexto, se encuentran orientadas en su mayor parte a los operadores de redes, aunque también se señalan a los proveedores de productos y servicios de red, previendo carencias en

[382] *Ibídem,* artículos 17-33.
[383] *Ibídem,* artículos 14-43.
[384] *Ibídem,* artículos 44-50.

las tareas de protección de seguridad de red; instalación de programas maliciosos; recolección de información del usuario sin su consentimiento; el robo o el uso de otros medios ilegales para obtener y comerciar de manera ilegal con la información personal de los ciudadanos; pudiéndose ordenar una suspensión temporal de las operaciones, una suspensión del negocio para establecer las correcciones pertinentes, el cierre de los sitios web, la revocación de los permisos de operaciones relevantes, o la cancelación de licencias comerciales[385].

El séptimo y último capítulo del proyecto de Ley de Ciberseguridad, de disposiciones complementarias, además de recoger las definiciones de los diferentes elementos recogidos en esta pieza legislativa, establece una provisión referente a la protección de seguridad de la información de la red militar, cuya responsabilidad en la formulación de medidas se encarga a la Comisión Militar Central[386].

Diferentes analistas internacionales han apuntado su preocupación por un proyecto legislativo sobre la ciberseguridad en China, que consideran arroga poderes al Estado que entran en colisión con los derechos de los ciudadanos y de las empresas operadoras de servicios de red.

De esta forma, señala Gillian Wong que China ha lanzado un proyecto de ley de seguridad cibernética que busca reforzar la capacidad de Pekín para protegerse contra las ciberamenazas y proteger los datos de los usuarios chinos, a la vez que reforzar los controles a través de Internet, apuntando que esta ley es una prioridad para este año, lo que refleja la urgencia de la cuestión en la agenda de seguridad nacional de la administración del presidente Xi Jinping. Continúa Wong señalando que China, que a menudo es acusada de utilizar la guerra cibernética contra otros Estados, expresa que es una víctima de este tipo de ataques. Este proyecto de ley permite expresamente a las autoridades chinas cortar el acceso a Internet durante las emergencias de seguridad pública, medidas que, señala Wong, ya han utilizado. las autoridades chinas durante los disturbios en Uigur y en otras zonas de minorías étnicas tibetanas. Por

[385] *Ibídem,* artículos 51-64.

[386] *Ibídem,* artículos 65-68.

último, Wong opina que los requerimientos para establecer los controles de seguridad cibernética, así como los sistemas de alerta y medidas de respuesta a emergencias, ponen de relieve que Pekín carecía de una política coherente para responder a las amenazas de ciberseguridad[387].

Harold Thibault escribe que poco después de asumir el cargo, el presidente chino Xi Jinping, dio la responsabilidad de la gestión de Internet a un nuevo y potente organismo, la Administración del Ciberespacio en China, colocando en su dirección a un alto cargo especializado en propaganda, Lu Wei[388]. Señala Thibault que, a nivel internacional, el Sr. Lu está tratando de imponer el concepto de "ciber-soberanía". En este sentido, el proyecto de ley sobre la seguridad cibernética impone ciertas normas que pueden ser desfavorables para las empresas extranjeras. El texto da fuerza de ley en el bloqueo del acceso a Internet en algunas partes del país cuando se encuentre en peligro la "estabilidad social". Una medida que, continúa Thibault, de hecho ya se ha utilizado, en particular durante los incidentes violentos en Xinjiang y en las áreas tibetanas, pero que ahora tendrá una legitimidad legal[389].

Por parte de las autoridades chinas, conscientes de las críticas que el **proyecto de ley de ciberseguridad** ha generado en el ámbito internacional, se han desarrollado unas acciones de difusión informativa, principalmente a través de la agencia oficial de noticias Xinhua.

Señala Xinhua, recogiendo fuentes oficiales chinas, que con la aprobación de una nueva ley sobre seguridad nacional y otro proyecto de ley sobre seguridad cibernética, China intensificará su defensa contra los cada vez más numerosos ciberdelitos. El ciberespacio se ha convertido en "un nuevo pilar para el desarrollo económico y social,

---

[387] WONG, Gillian: *China to Get Tough on Cybersecurity*. The Wall Street Journal, 9 de julio de 2015. http://www.wsj.com/articles/china-to-get-tough-on-cybersecurity-1436419416 consulta: 13 de agosto de 2015.

[388] Se puede acceder a una biografía profesional de Lu Wei en NETmundial Initiative https://www.netmundial.org/lu-wei consulta: 13 de agosto de 2015.

[389] THIBAULT, *Harold: Chine : bientôt des policiers chez les géants du Web*. Le Monde, 7 de agosto de 2015. http://www.lemonde.fr/economie/article/2015/08/07/chine-bientot-des-policiers-chez-les-geants-du-web_4715681_3234.html consulta: 13 de agosto de 2015.

y un nuevo campo de la seguridad nacional", de acuerdo con un libro blanco publicado en mayo sobre la estrategia militar china. Con una seria necesidad de disponer de una ley que garantizase sistemáticamente las medidas legales para proteger el ciberespacio y a sus usuarios, la nueva ley de seguridad nacional se centró principalmente en la ciberseguridad. El borrador de 68 artículos de la ley de ciberseguridad, se crea con el objetivo de proteger al público y no perjudicar su libertad, como aseguran los medios de comunicación occidentales. Aunque Internet en cierto sentido no tiene fronteras, la ciberseguridad sí las tiene. La red es un aspecto importante de la infraestructura de la nación. Dentro de China, está sujeta a la soberanía del país. China respeta la soberanía de otros países en el terreno de la ciberseguridad y espera que los demás respeten la suya en reciprocidad. A fin de evitar que la red sea aprovechada como un instrumento de propaganda que ponga en riesgo la estabilidad social, el proyecto de ley estipula que el servicio de Internet ha de suspenderse para responder a "emergencias graves" que puedan constituir amenazas para la seguridad pública. Frente a esa realidad, la legislatura china proclama que la seguridad cibernética no sólo trata de la seguridad y el desarrollo de una nación, sino que también se relaciona con los intereses inmediatos de cada usuario de la red. Desde que China se conectó a Internet en 1994, la red ha cambiado profundamente la forma de vida y de hacer negocios del país. China alberga la mayor población de internautas del mundo, pero todavía está rezagada en el desarrollo de la tecnología de Internet. China también ha sido víctima de ciberataques. La baja concienciación pública ha provocado grandes pérdidas en las propiedades financieras y personales. Cerca del 32 por ciento de los 332 millones de chinos que usan el pago por móvil han sido objeto de intentos de estafas como el phising y otros timos en línea, con las pérdidas multiplicándose por cuatro en 2014 en términos interanuales. El **presidente chino, Xi Jinping, quien también encabeza al grupo directivo central para seguridad en Internet y la informatización del país**, afirmó el año pasado que "el

ciberespacio ha de estar limpio y ordenado", y además, "dónde no haya seguridad en Internet no habrá seguridad nacional"[390].

En otra publicación relacionada, Xinhua recoge citando también fuentes oficiales, que China está trabajando en su primera ley de seguridad cibernética, diseñada para proteger al público, no para minar su libertad, como dicen algunos periodistas occidentales. El proyecto de ley aclara que proteger la soberanía y seguridad cibernéticas es una norma internacional indiscutible. Aunque internet en cierto sentido no tiene fronteras, la seguridad de internet tiene límites. Como la regulación de internet es una convención internacional, China tiene derecho a supervisar tanto a las compañías chinas como a las extranjeras que hacen negocios en línea en China. Cuando las compañías, sin importar su ubicación, ofrezcan productos o servicios en China, deben guiarse por las leyes y regulaciones chinas, de acuerdo con el principio territorial consagrado en las leyes internacionales. China sigue en una etapa temprana en la legislación relacionada con internet, aunque cuenta con el mayor número de usuarios de la red en el mundo, 700 millones de personas. Los países desarrollados, como Estados Unidos, prestan mucha atención a la seguridad cibernética, poseen un sistema jurídico y procedimientos de supervisión de seguridad de internet para garantizar su seguridad cibernética, que se ha convertido en un nuevo dominio de la seguridad nacional. China está aprendiendo actualmente de Estados Unidos en legislación de seguridad cibernética. La protección de la ciberseguridad no se logrará con una sola ley. Se necesita de un sistemático orden legal y regulaciones subordinadas. Quienes se precipitan a criticar la "irrazonable" forma en que China protege la ciberseguridad deben ser pacientes y dar tiempo al país en desarrollo más grande del mundo para mejorar su sistema legal. Las empresas extranjeras que buscan entrar al mercado de China, pero no quieren ver un mejor sistema legal chino y siempre recurren a tácticas de acusación para presionar a China, deben reflexionar

[390] XINHUA: *Voz de China: Seguridad cibernética es prioritaria para China*, 10 de julio de 2015. http://spanish.xinhuanet.com/china/2015-07/10/c_134400659.htm consulta: 11 de agosto de 2015.

si son ciudadanos que acatan la ley en su propio país, ¿entonces por qué no han de hacerlo en China?[391].

5.2.2. Las responsabilidades en la estructura de ciberseguridad en China

Como reconocen las propias autoridades chinas, la estructura del sistema de ciberseguridad en China está conformándose en la actualidad. Del proyecto de ley de ciberseguridad principalmente y también de otros documentos referenciados se ha elaborado una tabla con los organismos y sus responsabilidades en materia de ciberseguridad.

Figura 36: Responsabilidades de ciberseguridad en China

ORGANISMOS	RESPONSABILIDADES
Presidente de la República Popular de China	Preside el grupo directivo central para la seguridad en Internet y la informatización del país[392].
Consejo de Estado	Establecimiento de medidas de seguridad para la infraestructura de información crítica[393].
Administración del Ciberespacio de China[394]	- Planeamiento, coordinación, supervision y gestión integral de la seguridad en la red[395]. - Formular catálogo de equipos de red críticos y productos especializados de seguridad de red, y promover el reconocimiento recíproco de las certificaciones de seguridad[396]. - Inspeccionar a operadores de infraestructuras críticas[397].

[391] XINHUA: *Ley sobre seguridad cibernética de China busca proteger al público no minar su libertad*, 25 de julio de 2015. http://spanish.xinhuanet.com/2015-07/25/c_134445095.htm consulta: 11 de agosto de 2015.

[392] XINHUA: *China eyes Internet power*, 8 de marzo de 2014. http://news.xinhuanet.com/english/special/2014-03/08/c_133171308.htm consulta: 13 de Agosto de 2015. Este grupo se creó el 27 de febrero de 2014 por el Comité Permanente del Buró Político del Partido Comunista del Comité Central de China, que también creó el comité de la seguridad del Estado y el grupo directivo central para profundizar en la reforma integral del país.

[393] CHINA LAW TRANSLATE: *Cybersecurity Law (Draft), opus citada*, artículo 25.

[394] Sitio web de la Administración del Ciberespacio de China http://www.cac.gov.cn/english/ consulta: 13 de agosto de 2015.

[395] CHINA LAW TRANSLATE: *Cybersecurity Law (Draft), opus citada*, artículo 6.

[396] *Ibídem,* artículo 19.

[397] *Ibídem,* artículo 30.

	- Coordinar los departamentos con responsabilidades en infraestructuras críticas[398]. - Supervisar la seguridad de la red en cuanto a contenidos para que se ajusten a la legislación, solicitando de los operadores su bloqueo tanto si vienen del interior o exterior de China[399]. - Coordinar los informes de seguridad de la red y la información de alerta temprana[400]. - Coordinar los planes y las respuestas de emergencia de seguridad de la red[401].
Ministerio de Industria y Tecnología de la Información	Protección de la seguridad de la red, supervisión y gestión de esfuerzos[402].
Organizaciones de comercio de la red	Fortalecer la autodisciplina en la industria, formular normas de comportamiento de seguridad y estimular el desarrollo de la industria[403].
Departamentos del Consejo de Estado de telecomunicaciones, radio y televisión, energía, transporte, conservación del agua, y finanzas	Compilar los planes de seguridad de red que afecten a la seguridad nacional, las principales industrias de la economía nacional y la vida del pueblo, organizando su ejecución[404]. Orientar y supervisar el trabajo operativo de protección de seguridad para la infraestructura de información crítica[405].
Departamento Administrativo del Consejo de Estado para la normalización	Organizar la formulación y revisión de las normas industriales relevantes para la gestión de seguridad de la red, así como la seguridad de los productos de red, servicios y operaciones[406].
Consejo de Estado y gobiernos de las provincias, regiones autónomas y municipios	- Confección de planes integrales; apoyo a las industrias de tecnología clave de seguridad de red; apoyo a la investigación de tecnología de seguridad; protección de los derechos de propiedad intelectual de las instituciones que participen en programas de innovación de tecnología de seguridad de red del Estado[407]. - Para cumplir con la necesidad de proteger la seguridad nacional y el orden público social y responder a incidentes importantes de seguridad social, el Consejo de Estado, o de los

[398] *Ibídem,* artículo 33.

[399] *Ibídem,* artículo 43.

[400] *Ibídem,* artículo 44.

[401] *Ibídem,* artículo 46.

[402] *Ibídem,* artículo 6. Responsabilidad que es extensiva a otros departamentos pertinentes del Consejo de Estado en el ámbito de sus competencias. La protección a nivel de condado o superior será determinada por los reglamentos estatales pertinentes.

[403] *Ibídem,* artículo 8.

[404] *Ibídem,* artículo 12.

[405] *Ibídem,* artículo 26.

[406] *Ibídem,* artículo 13.

[407] *Ibídem,* artículo 14.

	gobiernos de las provincias, regiones autónomas y municipios con la aprobación por el Consejo de Estado, podrán adoptar medidas temporales relativas a las comunicaciones de red en ciertas regiones, como su restricción[408].
Operadores de red	1. Formular sistemas de gestión de la seguridad interna; 2. Adoptar las medidas para prevenir los virus informáticos, ataques de red, intrusiones de red y otras acciones que pongan en peligro la seguridad de la red; 3. Adoptar las medidas para la grabación y el seguimiento del estado de las operaciones de la red y los incidentes de seguridad; 4. Realizar clasificación de datos, copias de seguridad y cifrado[409]; 5. Elaborar planes de respuesta de emergencia[410].
Operadores de infraestructuras críticas de información	1. Establecimiento y control de los responsables de la gestión de seguridad; 2. Formación de los empleados; 3. Copias de seguridad de sistemas y bases de datos relevantes; 4. Planes de respuesta de emergencia para incidentes de seguridad de la red y organización de simulacros[411]; 5. Evaluación anual de seguridad[412].
Comisión Militar Central	Protección de la seguridad de la información en la red militar[413].

Fuente: elaboración propia sobre diversa legislación china.

5.3. RUSIA

5.3.1. La ciberseguridad en la estructura de seguridad nacional de Rusia

La Estrategia de Seguridad Nacional de la Federación de Rusia para el año 2020 recoge en varios artículos aspectos relacionados con la ciberseguridad[414]:

[408] *Ibídem,* artículo 50.

[409] *Ibídem,* artículo 17.

[410] *Ibídem,* artículo 21.

[411] *Ibídem,* artículo 28.

[412] *Ibídem,* artículo 32.

[413] *Ibídem,* artículo 67.

[414] *Estrategia de Seguridad Nacional de la Federación de Rusia para el año 2020, opus citada.*

En el artículo 10 se mencionan entre los riesgos más probables los relacionados con el incremento de la actividad ilícita en el dominio cibernético, en el ámbito de la alta tecnología.

El artículo 108 apunta la importancia de avanzar en el desarrollo en áreas de la tecnología de la información y las comunicaciones; desarrollar e introducir tecnologías de seguridad de la información en los sistemas de gobierno y administración militar, sistemas de gestión de productos ecológicamente peligrosos e instalaciones de importancia crítica.

El artículo 109 trata de la prevención de las amenazas a la seguridad de la información en el mediante la mejora de la seguridad de los sistemas de información y telecomunicaciones en infraestructuras críticas; y mediante la creación de un sistema unificado de apoyo a los sistemas de información y telecomunicaciones para el sistema de la seguridad nacional.

También se integran en el artículo 61 estos factores cuando se señala que con el fin de contrarrestar las amenazas a la seguridad económica, las fuerzas de seguridad nacional, en cooperación con las instituciones de la sociedad civil tienen por objeto apoyar la política socio-económica del Estado, que se dirige al desarrollo de las industrias de la información y las telecomunicaciones tecnologías, los recursos de tecnología informática, electrónica, equipos de telecomunicaciones y programación.

El Presidente de la Federación de Rusia aprobó el 24 de Julio de 2013 los "Principios básicos para la política del Estado en el campo de la seguridad de la información en el ámbito internacional para el año 2020"[415].

El marco legal de los principios básicos incluye la Constitución de la Federación Rusa, los tratados y acuerdos de la Federación en el ámbito de la seguridad internacional de

[415] *Basic Principles for State Policy of the Russian Federation in the field of International Information Security in 2020*. Se puede consultar una traducción no oficial facilitada por la Embajada de la Federación de Rusia en el Gran Ducado de Luxemburgo en http://en.ambruslu.com/wp-content/uploads/2013/09/state-policy.doc consulta 20 de agosto de 2015.

la información, las leyes federales, los actos jurídicos del Presidente de Rusia y del Gobierno, así como otros instrumentos jurídicos de la Federación[416].

Estos principios básicos constituyen un documento de planificación estratégica de Rusia y emanan de la Estrategia de Seguridad Nacional de la Federación de Rusia para el año 2020, aprobada por decreto de su Presidente de fecha 12 de mayo de 2009, así como de otros documentos de planificación estratégica, en especial la Doctrina de Seguridad de Información de la Federación de Rusia de 9 de septiembre de 2000 [417] y el Concepto de la Política Exterior de la Federación de Rusia de 12 de febrero de 2013.[418]

La intención declarada en estos principios es promover la política exterior de Rusia para alcanzar la concordia y los intereses mutuos en el proceso de internacionalización del entorno global de información. Todo ello enmarcado en la premisa de que en la sociedad moderna, las tecnologías de la información y las comunicaciones constituyen la clave que determina el nivel de desarrollo social y político y la situación de la seguridad nacional. Los principios básicos se han diseñado para definir las principales amenazas en el ámbito de la seguridad de la información en el contexto internacional, la meta, los objetivos y las prioridades de la política estatal de la Federación de Rusia

[416] *Ibídem*, artículo 3.

[417] La Doctrina de Seguridad de Información de la Federación de Rusia fue uno de los primeros documentos emitidos por el Consejo de Seguridad del presidente Vladimir Putin y generó destacada controversia por intentar legitimar el control sobre los medios de comunicación. Translation and Analysis of the Doctrine of Information Security of the Russian Federation: Mass Media and the Politics of Identity; Carman, Douglas; Pacific Rim Law & Policy Journal 339 (2002). En: https://digital.law.washington.edu/dspace-law/bitstream/handle/1773.1/757/16_11PacRimL%26PolyJ339%282002%29.pdf?sequence=1 consulta 20 de agosto de 2015.

[418] Puede consultarse este documento en su versión en idioma inglés, facilitado por el Ministerio de Asuntos Exteriores de la Federación Rusa, en el enlace: http://www.mid.ru/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/869c9d2b87ad8014c32575d9002b1c38?OpenDocument consulta 20 de agosto de 2015.

en el ámbito de la seguridad de la información internacional, así como los mecanismos para su aplicación[419].

Los principios básicos definidos en el documento son: a) Promover en el ámbito internacional las iniciativas rusas para establecer el sistema internacional de seguridad de la información, lo que incluye un mejor apoyo legal y organizativo, entre otros aspectos. b) El desarrollo de programas intergubernamentales en el campo de la seguridad de la información internacional, así como otros programas estatales. c) Fomentar la cooperación interinstitucional en la ejecución de la política estatal de la Federación de Rusia en el ámbito de la seguridad de la información internacional. d) Lograr y mantener la paridad tecnológica con las principales potencias del mundo a través de un mayor uso de las tecnologías de la información y las comunicaciones en la economía real[420].

Es destacable la descripción que en el documento se hace de la seguridad de la información internacional, que se define como tal condición para el espacio de información global que impida cualquier posibilidad de violación de los derechos de la persona, la sociedad y el Estado en la esfera de la información, así como el impacto destructivo e ilegal en los elementos de la infraestructura nacional de la información crítica[421].

Esta definición de la seguridad de la información internacional en estos principios básicos para el año 2020, recoge una tendencia que venía mostrándose en otros documentos sobre la política pública de Rusia en el ciberespacio, en especial en el "Proyecto de Convención sobre Seguridad de la Información Internacional" de 24 de septiembre de 2011.[422]

---

[419] *Basic Principles for State Policy of the Russian Federation in the field of International Information Security in 2020, opus citada, artículos 2 y 20.*

[420] *Ibídem*, artículo 5.

[421] *Ibídem*, artículo 7.

[422] Ministerio de Relaciones Exteriores de la Federación de Rusia: *Convention on International Information Security (Concept).* Disponible en: http://www.mid.ru/bdomp/ns-

Este Proyecto de Convención señala en su artículo 5.5 que cada Estado tiene el derecho de legislar según normas soberanas y gobernar su espacio de información de acuerdo con sus leyes nacionales[423]. De esta forma, la soberanía del Estado y de sus leyes se aplicarían a la infraestructura de la información que se encontrara en el territorio del Estado o que cayera bajo su jurisdicción.

Esta posición de Rusia sobre la naturaleza, el potencial y el uso del ciberespacio difieren significativamente del consenso occidental. De este modo, la "soberanía en internet" es un área clave de desacuerdo. Rusia apoya de modo firme la idea del control nacional de todos los recursos ligados a internet que se alojan en el interior de las fronteras físicas del Estado, así como del concepto asociado de aplicación de la legislación local, como recoge el mencionado artículo 5.5 del Proyecto de Convención sobre Seguridad de la Información Internacional.

Esta aproximación a la seguridad de la información internacional ha sido valorada por diferentes analistas como un intento de las autoridades rusas de controlar los flujos informativos, aduciendo razones de seguridad nacional.

En particular, Rusia tiene profundas preocupaciones sobre el principio de intercambio incontrolado de información en el ciberespacio, y favorece la relevancia del control no solo de la infraestructura sino también del contenido en las fronteras nacionales. La circulación de la información que representa una amenaza percibida para la sociedad o el Estado, y la soberanía de la "internet nacional", son preocupaciones clave de seguridad en Rusia, según apunta Giles[424].

---

osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/7b17ead7244e2064c3257925003bcbcc!OpenDocument consulta: 20 de Agosto de 2015.

[423] *Ibídem*, artículo 5.5.

[424] GILES, Keir: *Russia's Public Stance on Cyberspace Issues*, p. 63, Conflict Studies Research Centre Oxford, UK; 4th International Conference on Cyber Conflict; C. Czosseck, R. Ottis, K. Ziolkowski (Eds.), Publicado a través de NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), Tallinn, junio 2012. Disponible en: http://www.ccdcoe.org/publications/2012proceedings/2_1_Giles_RussiasPublicStanceOnCyberInformationWarfare.pdf consulta: 20 de agosto de 2015.

Esta aproximación se encuentra en oposición con la postura, entre otros, de Estados Unidos, como expresó la Secretaria de Estado Hillary Clinton en diciembre de 2011, cuando dijo que países como Rusia deseaban que cada gobierno pudiera establecer sus propias reglas para el uso de internet, lo que que no sólo socava los derechos humanos y el libre flujo de información, sino también la interoperabilidad de la red. Añadiendo Clinton que los gobiernos que impulsan esta agenda quieren crear barreras nacionales en el ciberespacio y que este enfoque sería un desastre para la libertad en internet [425].

Abundando en esta percepción diferente a la postura rusa, se utiliza de modo habitual el principio fundamental de que el ciberespacio permanece abierto a la innovación y al libre intercambio de ideas, información y expresión, según afirmó el Secretario de Asuntos Exteriores del Reino Unido William Hague en la Conferencia Internacional de Londres sobre el Ciberespacio, celebrada el uno y dos de noviembre de 2011[426].

Giles incide, en el estudio mencionado, en que la diferencia clave entre las posturas de Rusia y Occidente en relación a la ciberseguridad, es la percepción de Rusia del contenido como amenaza[427].

En este sentido, es muy ilustrativo el estudio conjunto realizado por el Instituto de Asuntos de Seguridad de la Información de la Universidad Estatal de Moscú (IISI) y el Centro de Investigación de Estudios de Conflicto de Oxford (CSRC), que interpretan en paralelo los artículos del mencionado Proyecto de Convención sobre Seguridad de la Información Internacional[428].

---

[425] CLINTON, Hillary: *Remarks by Hillary Rodham Clinton at Conference on Internet Freedom*, The Hague, Netherlands, 8 de diciembre de 2011. Disponible en: http://iipdigital.usembassy.gov/st/english/texttrans/2011/12/20111209083136su0.3596874.html#axzz3jNXkemIm consulta: 20 de agosto de 2015.

[426] HAGUE, William: London Conference on Cyberspace: Chair's statement, 2 de noviembre de 2011. Disponible en: https://www.gov.uk/government/news/london-conference-on-cyberspace-chairs-statement consulta: 20 de agosto de 2015.

[427] GILES, Keir: *Russia's Public Stance on Cyberspace Issues*, p. 64. *Opus citada*.

[428] Institute for Information Security Issues, Moscow State University & Conflict Studies Research Centre, Oxford: *Russia's "Draft Convention on International Information Security" A Commentary*, abril

Es de destacar que, en este significativo estudio conjunto, los comentarios de las dos instituciones académicas ofrecen interpretaciones tan divergentes sobre el mismo texto que se pone de manifiesto la separación conceptual de las visiones rusa y occidental. En especial en lo referente a las amenazas y al encaje de los contenidos en el ciberespacio dentro de ellas, como se refleja en el apartado de la amenaza de utilizar contenido para influir en las esferas social y humanitaria, en referencia al artículo 4 del Proyecto de Convención sobre las amenazas más importantes para la paz y seguridad internacionales en el espacio informativo[429].

En este sentido, la Universidad Estatal de Moscú intenta responder a las críticas específicas estadounidenses que, según ellos, tratan de presentar el Proyecto de Convención como un documento que perjudica el ejercicio de los derechos humanos en beneficio del control gubernamental sobre el contenido. De esta forma, se citan las declaraciones de la diplomática estadounidense Michele Markof: "Las autoridades de algunos Estados consideran el libre intercambio de ideas sobre Internet inaceptable desde el punto de vista cultural y político, o lo perciben como una amenaza para la estabilidad política"[430].

En la estela de esta afirmación, los académicos rusos apuntan que la cuestión del uso de contenido, con el fin de influir en la esfera social y humanitaria, se aplica íntegramente a las normas y tradiciones de un solo Estado, incluyendo al espacio de la información. De este modo, un Estado, basándose en su soberanía y actuando en nombre de sus ciudadanos, puede determinar que un contenido específico conlleva algunos elementos negativos para el Estado y puede entonces limitar su propagación con la legislación apropiada. Los académicos rusos señalan que las prohibiciones y restricciones a la información de incitar al odio interétnico, interracial e interreligioso; o promover el odio, la discriminación o la violencia contra cualquier individuo o grupo de

---

de 2012. Disponible en: http://www.conflictstudies.org.uk/files/20120426_CSRC_IISI_Commentary.pdf consulta: 20 de agosto de 2015.

[429] *Ibídem,* pp. 3-5.

[430] *Ibídem,* p. 4, señalando la fuente: Diario ruso "Kommersant" de 8 de febrero de 2012.

individuos, utilizando como pretexto factores como la raza, el color de piel, el origen nacional o étnico, o la fe son legítimas y se practican por la comunidad internacional[431].

Para reforzar este argumento, los académicos rusos señalan el Artículo 19 del Pacto Internacional de Derechos Civiles y Políticos, que establece que el ejercicio de la libertad de expresión puede estar sujeto a ciertas restricciones: (a) Asegurar el respeto a los derechos o a la reputación de los demás; (b) Para la protección de la seguridad nacional o del orden público o la salud o la moral públicas[432]. Además, se señala aplicable el artículo 10 del Convenio de la Unión Europea para la Protección de los Derechos Humanos (libertad de expresión), que establece que "toda persona tiene derecho a la libertad de expresión", pero "el ejercicio de estas libertades, que entrañan deberes y responsabilidades, podrá ser sometido a ciertas formalidades, condiciones, restricciones o sanciones previstas por la ley que sean necesarias en una sociedad democrática, en interés de la seguridad nacional, la integridad territorial o la seguridad pública, la prevención de desórdenes o delitos, para la protección de la salud o la moral, para la protección de la reputación o de los derechos ajenos, para impedir la divulgación de informaciones confidenciales o para garantizar la autoridad y la imparcialidad del poder judicial"[433].

Destaca además Giles, dos importantes áreas de divergencia conceptual de este estudio conjunto, la mención de terrorismo y la cuestión del acceso al espacio de la información de un Estado extranjero[434].

En este estudio conjunto se ponen de manifiesto las diferencias conceptuales en la comprensión de la naturaleza de "terrorismo" entre Rusia y otros Estados, lo que

---

[431] *Ibídem,* pp. 4-5.

[432] El *Pacto Internacional de Derechos Civiles y Políticos* puede consultarse en el Boletín Oficial del Estado en https://www.boe.es/diario_boe/txt.php?id=BOE-A-1977-10733 consulta: 20 de Agosto de 2015.

[433] El *Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales* puede consultarse en el Boletín Oficial del Estado en https://www.boe.es/buscar/doc.php?id=BOE-A-1979-24010 consulta: 20 de agosto de 2015.

[434] GILES, Keir: *Russia's Public Stance on Cyberspace Issues*, p. 66. *Opus citada*.

proporciona una capa adicional de complejidad e indeterminación a la ya enturbiada percepción de lo que constituye terrorismo cibernético o ciberterrorismo.

Es interesante acceder a las interpretaciones sobre el terrorismo en el ámbito cibernético de estos académicos de la Universidad Estatal de Moscú y de los investigadores del Centro de Investigación de Estudios de Conflicto de Oxford, en el mencionado estudio conjunto, ya que ofrece la oportunidad de evaluar la diferente percepción conceptual sobre la base de la interpretación de un mismo texto, el Proyecto de Convención sobre Seguridad de la Información Internacional, que hace referencia al terrorismo en cinco artículos de los 14 que componen el cuerpo principal de su articulado:

Figura 37: Referencias al terrorismo en el ciberespacio en el Proyecto de Convención sobre Seguridad de la Información Internacional de Rusia.

Proyecto de Convención sobre Seguridad de la Información Internacional de Rusia **Referencias al terrorismo en el ciberespacio**
Artículo 4. Las principales amenazas a la paz y la seguridad internacionales en el espacio de la información. 5) El uso del espacio de información internacional por las estructuras gubernamentales y no gubernamentales, organizaciones, grupos e individuos, con fines terroristas, extremistas o delictivos.
Artículo 5. Principios fundamentales para garantizar la de Seguridad de la Información Internacional. 18) Cada Estado Parte tiene como objetivo mantener un equilibrio entre los derechos humanos fundamentales y la neutralización efectiva del uso terrorista del espacio de información.
Artículo 8. El uso del espacio de información con fines terroristas. Los Estados Parte reconocen la posibilidad de que el espacio de la información pueda ser utilizado para la realización de actividades terroristas.
Artículo 9. Principales medidas para prevenir el uso del espacio de información con fines terroristas Para evitar el uso del espacio de la información con fines de terrorismo, los Estados Parte deberán: 1) adoptar medidas para prevenir el uso del espacio de la información con fines terroristas y reconocer la necesidad de esfuerzos conjuntos decisivos en este sentido; 2) esforzarse por desarrollar los enfoques uniformes para deshabilitar los recursos de Internet de índole terrorista; 3) Reconocer la necesidad de establecer y ampliar el intercambio de información sobre posibles ataques informáticos, en las señales, hechos, métodos y medios de la utilización de Internet con fines terroristas, y sobre los objetivos y actividades de las organizaciones terroristas en el espacio de información, así como la necesidad de intercambiar experiencias y mejores prácticas sobre el control de los recursos de Internet, encontrar y controlar el contenido de los sitios web de carácter terrorista, llevar a cabo investigaciones penales por los expertos en informática en este ámbito, y la regulación legal y la organización de actividades para la prevención del uso del espacio de la información con fines terroristas;

4) adoptar las medidas de carácter legislativo o de otra índole que sean necesarias para permitir que las fuerzas del orden puedan llevar a cabo las actividades pertinentes de investigación y otras encaminadas a prevenir y reprimir las actividades terroristas en el espacio de la información y en la eliminación de las consecuencias de las mismas, así como penalizar a las personas y organizaciones culpables de dichas actividades; 5) tomar las medidas necesarias de carácter legislativo o de otro tipo que garanticen el acceso legal a partes específicas de la infraestructura de información y comunicación en el territorio del Estado Parte, que estén jurídicamente implicadas para ser empleadas para la comisión de actividades terroristas en el espacio de la información o involucradas en este tipo de actividades en otros lugares, para la comisión de actividades que conduzcan a actos terroristas, o para las actividades de las organizaciones terroristas o grupos o individuos terroristas.
Artículo 12. Cooperación entre los Estados Parte. 2) Los Estados Parte, sobre la base de la voluntariedad y la reciprocidad, el intercambio de mejores prácticas en la prevención, investigación jurídica, así como la liquidación de las consecuencias de los delitos, incluidos los relacionados con el terrorismo, que implica el espacio de información.

Fuente: Proyecto de Convención sobre Seguridad de la Información Internacional[435].

Además, la propuesta rusa en el Proyecto de Convención incluye una definición del "terrorismo en el espacio de la información", como el uso de los recursos y / o la actividad de información que les afecten en el espacio de información a los efectos de terrorismo[436].

Los académicos de la Universidad Estatal de Moscú desarrollan, en su comentario sobre estos artículos, una postura cuyo punto de partida, al comentar el artículo 4[437], recoge la posición del Grupo de Expertos Gubernamentales en el Campo de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional, que señalan que “En la actualidad los terroristas en su mayoría dependen de estas tecnologías para comunicarse, recabar información, reclutar, organizar, promover sus ideas y acciones, y solicitar financiación, pero con el tiempo podrían adoptar el uso de los sistemas de Información y Telecomunicaciones (TIC) para el ataque. Hasta el momento, hay pocos indicios de intentos terroristas para comprometer o inhabilitar la

[435] Ministerio de Relaciones Exteriores de la Federación de Rusia: *Convention on International Information Security (Concept), opus citada.*

[436] *Ibídem*, artículo 2, términos y definiciones.

[437] Institute for Information Security Issues, Moscow State University & Conflict Studies Research Centre, Oxford: *Russia’s “Draft Convention on International Information Security” A Commentary, opus citada, pp. 3-5.*

infraestructura de las TIC o la ejecución de operaciones de uso de las TIC, aunque pueden intensificarse en el futuro"[438].

Esta posición, sostenida también en la actualidad por el grupo de expertos gubernamentales en ciberseguridad de Naciones Unidas, que señalan en el informe de 2013 que "Los grupos terroristas utilizan las TIC para comunicarse, recabar información, reclutar, organizar, planificar y coordinar los ataques, la promoción de sus ideas y acciones y solicitar financiación. Si estos grupos adquirieran herramientas ofensivas, podrían llevar a cabo actividades disruptivas contra los sistemas de Información y Telecomunicaciones."[439], sirve también a los académicos rusos de punto de partida al analizar el artículo 8, relativo al uso del espacio de información con fines terroristas, para señalar que "Dada la magnitud de las posibles consecuencias de las acciones de los recursos de Internet (y las actividades terroristas en el espacio de la información) la adopción de esta disposición es esencial. Esto plantea la cuestión del desarrollo de métodos para supervisar y filtrar el contenido del correspondiente recurso de Internet (para la búsqueda y recopilación de pruebas). De esta forma, habrá que desarrollar criterios para clasificar un recurso de Internet como un recurso de carácter terrorista"[440]. Esta aproximación del IISI de la Universidad Estatal de Moscú, abunda en lo ya apuntado sobre la prioridad rusa de establecer el control del contenido en las redes.

En cuanto al artículo 9 del Proyecto de Convención, relativo a las principales medidas para prevenir el uso del espacio de información con fines terroristas, el IISI de la

---

[438] *Informe a la Asamblea General de las Naciones Unidas del Grupo de Expertos Gubernamentales en el Campo de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional*. A/65/20 de 30 de julio de 2010. Disponible en http://www.unidir.org/files/medias/pdfs/final-report-eng-0-189.pdf consulta: 21 de agosto de 2015.

[439] *Informe a la Asamblea General de las Naciones Unidas del Grupo de Expertos Gubernamentales en el Campo de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional. A/68/98 de 24 de junio de 2013*. Disponible en http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98 consulta: 21 de agosto de 2015.

[440] Institute for Information Security Issues, Moscow State University & Conflict Studies Research Centre, Oxford: *Russia's "Draft Convention on International Information Security" A Commentary, opus citada, pp. 21-22.*

Universidad Estatal de Moscú hace referencia igualmente a lo esencial de adoptar esta posición, debido a la magnitud de las posibles consecuencias, señalando además que la adopción de algunas de las medidas propuestas ya se encuentra en el Convenio sobre la Ciberdelincuencia del Consejo de Europa [441], conocido como Convenio de Budapest[442], en concreto en el preámbulo y en el Artículo 2 sobre Derecho procesal [443]. Apuntando además que el Convenio sobre la Ciberdelincuencia no contiene normas relativas a actividades terroristas.

Otro aspecto de relevancia, que evidencia la diferente percepción entre la posición rusa y la occidental, es la relativa a la cuestión del **acceso al espacio de la información de un Estado extranjero**. Ha sido precisamente esta divergencia conceptual la que ha tenido mayor peso específico para que la Federación de Rusia no haya suscrito el Convenio sobre la Ciberdelincuencia, pese a los motivos que favorecen la adhesión rusa a este Convenio de Budapest[444].

El artículo 32 del Convenio sobre la Ciberdelincuencia del Consejo de Europa, que trata del acceso transfronterizo a los datos informáticos almacenados, señala que cualquier Estado podrá, sin autorización de otro Estado, acceder a los datos informáticos almacenados de libre acceso al público independientemente de la localización geográfica de esos datos; así como acceder a los datos informáticos almacenados situados en otro Estado, o recibir a través de un sistema informático

[441] *Ibídem, p. 23.*

[442] Consejo de Europa: *Convenio sobre la Ciberdelincuencia;* Budapest, 23 de noviembre de 200*1*. Disponible en: http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/ETS_185_spanish.PDF

[443] El Convenio sobre la Ciberdelincuencia, recoge en su Capítulo II, Medidas que deberán adoptarse a nivel nacional, al hablar de Derecho penal sustantivo, en su Título I, Delitos sobre la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos en su Artículo 2, Acceso ilícito, que cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno el acceso deliberado e ilegítimo a todo o parte de un sistema informático.

[444] ORJI, Uchenna Jerome: *Russia and the Council of Europe Convention on Cybercrime. Computer and Telecommunications,* Law Review, Vol.18 Issue 1, 2012.

situado en su territorio, si se obtiene el consentimiento legal y voluntario de la persona autorizada para divulgarlos a través de ese sistema informático[445].

Señala Giles que la frase clave que impulsa a las objeciones de Rusia es "sin autorización de otro Estado", ya que en opinión de Rusia, se trata de una intromisión intolerable en el principio de la soberanía nacional, añadiendo que además, la gama de opciones cubierta por el consentimiento legal y voluntario de la persona autorizada para divulgarlos es fuente de preocupación, al incluir a individuos y organizaciones diferentes del Estado[446]. Ilustra Giles estas reservas rusas con la mención de un informe en un periódico oficial que subraya la "dudosa prestación de los servicios especiales extranjeros para invadir nuestro espacio cibernético y llevar a cabo sus operaciones especiales, sin notificación a nuestros servicios de inteligencia"[447].

Es en este escenario, donde el Proyecto de Convención sobre Seguridad de la Información Internacional intenta limitar esta aproximación occidental. De esta forma, se recogen restricciones en diferentes artículos y provisiones, como en el artículo 3, que limita la aplicación de la Convención en aquellos casos en que las acciones en cuestión se establezcan dentro de la infraestructura de información de un Estado, ciudadano o corporación bajo la jurisdicción de ese Estado, y los efectos de esas acciones sólo sean sentidos por los ciudadanos y las empresas bajo la jurisdicción de ese Estado; el artículo 4, que limita la difusión de información a través de las fronteras nacionales, cuando atente contra los principios y normas del derecho internacional o la legislación nacional; o el artículo 5, que subraya la no injerencia en los asuntos internos de otros Estados[448].

Este "Proyecto de Convención sobre Seguridad de la Información Internacional", continúa constituyendo la primera prioridad de la Federación de Rusia en relación a la

[445] Consejo de Europa: *Convenio sobre la Ciberdelincuencia, opus citada, artículo 32.*

[446] GILES, Keir: *Russia's Public Stance on Cyberspace Issues*, p. 67. *Opus citada*.

[447] *Ibídem*, p. 66; GILES cita a T. BORISOV: "Virtual'nyy mir zakryt", Rossiyskaya Gazeta, 12 de noviembre de 2010.

[448] Ministerio de Relaciones Exteriores de la Federación de Rusia: *Convention on International Information Security (Concept), opus citada, artículos 3, 4 y 5.*

seguridad en el ciberespacio, como se recoge en los “Principios básicos para la política del Estado en el campo de la seguridad de la información en el ámbito internacional para el año 2020”, que señala las prioridades en relación a la seguridad de la información:

Figura 38: Prioridades de la Federación de Rusia en relación a la seguridad de la información.

Prioridades de la Federación de Rusia en relación a la seguridad de la información
1. Promover a nivel internacional la iniciativa rusa para desarrollar y adoptar el Convenio sobre la Seguridad de la Información Internacional por los Estados Miembros de las Naciones Unidas.
2. Garantizar las iniciativas rusas, en el Grupo de Expertos Gubernamentales de las Naciones Unidas sobre los avances en el campo de la Información y telecomunicaciones en el contexto de la seguridad internacional.
3. Impulsar la cooperación con los Estados Miembros de la Organización de Cooperación de Shanghai, la Comunidad de Estados Independientes, la Organización del Tratado de Seguridad Colectiva, la Cooperación Económica Asia-Pacífico, los Estados BRICS, los Estados miembros del G8 y G20, entre otros.
4. Avanzar en la iniciativa rusa de internacionalizar la gestión de la información y de la red de telecomunicaciones Internet, impulsando el papel de la Unión Internacional de Telecomunicaciones.
5. Mejorar la estructura organizativa y de personal, así como la coordinación de la actividad de los órganos ejecutivos federales en este ámbito.
6. Facilitar el progreso de la comunidad de expertos de Rusia para apoyar las iniciativas de Rusia en el establecimiento de un sistema internacional de seguridad de la información.
7. Crear un entorno para la conclusión de los tratados y acuerdos internacionales sobre la cooperación en el campo de la seguridad de la información internacional.
8. Impulsar el Acuerdo de la Organización de Cooperación de Shanghai sobre la cooperación en el campo de la prestación de la seguridad de la información internacional.

9. Aprovechar el potencial científico y de investigación de los expertos de las Naciones Unidas y de otras organizaciones internacionales para avanzar en las iniciativas de Rusia en el establecimiento de un sistema internacional de seguridad de la información.

Fuente: Principios básicos para la política del Estado en el campo de la seguridad de la información en el ámbito internacional para el año 2020[449].

5.3.2. Los aspectos militares de la ciberseguridad en Rusia

En 2012, el entonces primer ministro de Rusia Vladimir Putin publicó un artículo en el que abogaba por potenciar la seguridad nacional en Rusia, realizando un énfasis especial en la mejora de las capacidades militares rusas. En relación con la ciberseguridad y las tecnologías de la información, señalaba Putin que la capacidad militar de un país en el ciberespacio, jugará un gran papel en la determinación de la naturaleza de un conflicto armado. En un futuro se desarrollarán sistemas de armas basados en nuevos principios, lo que junto a las armas nucleares, proporcionarán nuevos instrumentos para el logro de objetivos políticos y estratégicos. Continúa Putin señalando que estos sistemas de armas de alta tecnología serán comparables a las armas nucleares, pero serán más "aceptables" en términos de ideología política y militar, lo que llevará a que el equilibrio estratégico de fuerzas nucleares disminuya su importancia[450].

Señala Amit Kumar que este artículo mencionado de Vladimir Putin, antes de volver a ocupar el cargo de presidente de Rusia el 7 de mayo de 2012, refleja el impulso de las reformas en materia militar en Rusia, que se convirtieron en las de mayor calado. De esta forma, estos planes de modernización de las fuerzas armadas de Rusia y la industria de defensa se consideraban fundamentales para asegurar Rusia lugar que

[449] *Basic Principles for State Policy of the Russian Federation in the field of International Information Security in 2020*, *opus citada.*

[450] PUTIN, Vladimir: *Being strong: National security guarantees for Russia*. Rossiiskaya Gazeta, 20 de febrero de 2012. http://archive.premier.gov.ru/eng/events/news/18185/ consulta: 15 de Agosto de 2015.

le corresponde en la comunidad de naciones, y para garantizar la seguridad y el prestigio de Rusia[451].

En la estela de esta corriente política, la Doctrina Militar de la Federación de Rusia hasta el 2020 menciona como primera tarea de Rusia en la disuasión y la prevención de conflictos militares, la evaluación y predicción de la evolución de la situación político-militar a nivel mundial y regional, así como el estado de las relaciones interestatales en el ámbito político-militar, con base en la utilización de los sistemas técnicos modernos y tecnologías de la información[452].

5.3.3. La estructura de ciberseguridad de la Federación de Rusia

Menciona Jeffrey Carr, un artículo de marzo de 2011 en Finansovaya Gazeta, una publicación del Ministerio de Finanzas de Rusia, que elabora un esquema sobre la estructura de nivel superior del Sistema de Protección Integral de la Información (KSZI). De acuerdo al artículo mencionado, este sistema consta de dos organizaciones: el Servicio Federal de Control Técnico y Exportación (FSTEC), subordinado al Ministerio de Defensa y el Servicio Federal de Seguridad (FSB), dependiente del presidente ruso. El FSTEC certifica equipo técnico y emite licencias, para organizaciones privadas y gubernamentales, para trabajar con información clasificada. El FSB emite licencias para el trabajo con material criptográfico, y controla la difusión de este material, incluyendo el equipo técnico y de software. La Ley Federal Nº 40-FZ, del Servicio Federal de Seguridad, asigna la responsabilidad general al FSB para la protección de la seguridad de información de Rusia y de su infraestructura, incluyendo las telecomunicaciones críticas e Internet[453], colocando al FSB por encima

[451] KUMAR, Amit: Russian Military Reforms: An Evaluation. Institute for Defence Studies and Analyses, 23 de mayo de 2013. http://www.idsa.in/~idsa/issuebrief/RussianMilitaryReforms_amitk_230513.html consulta: 17 de agosto de 2015.

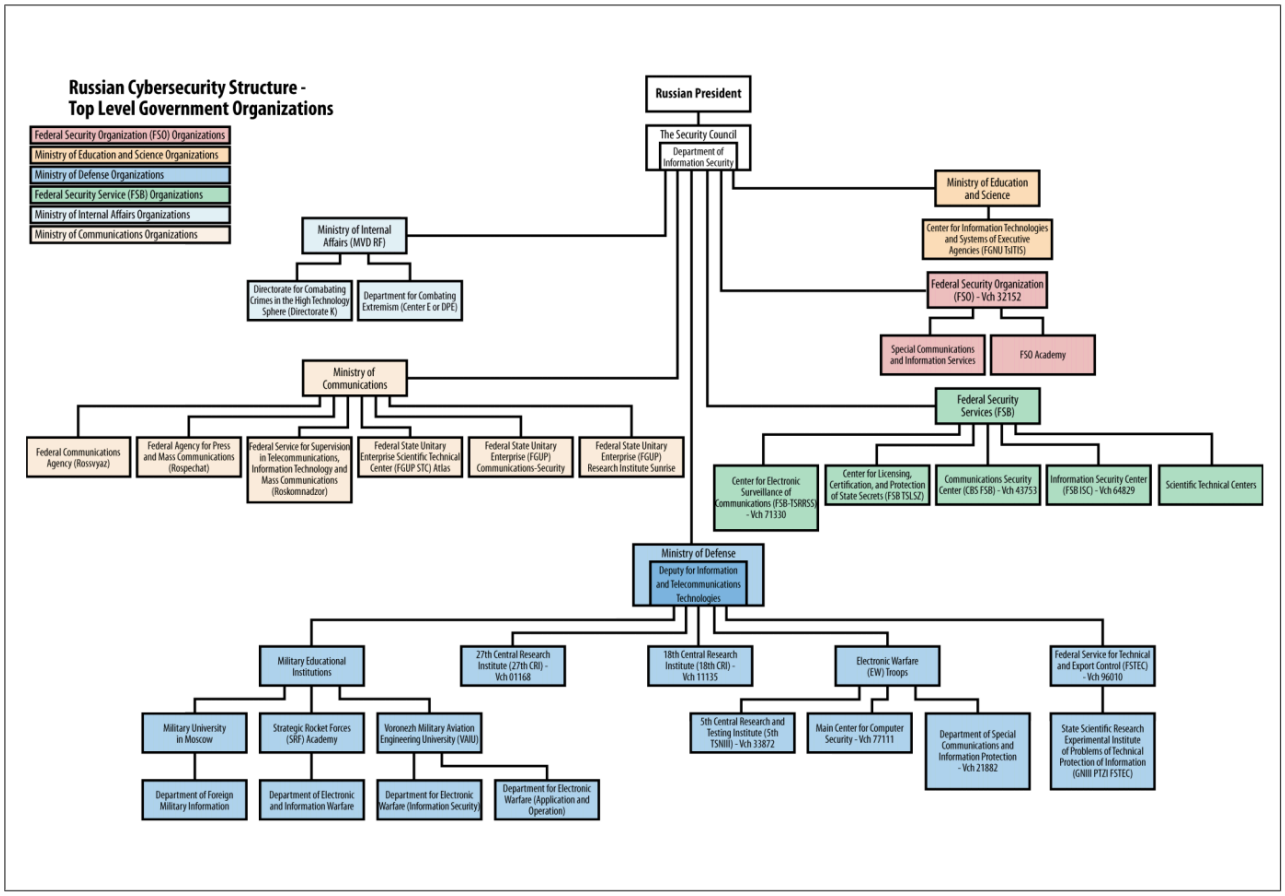
[452] *The Military Doctrine of the Russian Federation, opus citada.* Artículo 19.

[453] Puede accederse a una traducción no oficial en idioma inglés de la Ley Federal Nº 40-FZ, del Servicio Federal de Seguridad de la Federación de Rusia, realizada por el Consejo de Europa de 24 de febrero de 2102 CDL-REF(2012)011 en http://www.legislationline.org/download/action/download/id/3708/file/RF_law_fed_security_service_1999_am2011_en.pdf consulta: 18 de agosto de 2015.

del Ministerio de Defensa en la cadena del KSZI. De hecho, la autoridad del FSB sobre la infraestructura criptográfica de Rusia es casi absoluta e incluso la Academia Rusa de Criptografía, una prestigiosa institución académica, está subordinada al FSB. El Decreto Presidencial de Rusia Nº 351 identifica una organización adicional fundamental para el sector ruso de Internet, la Organización Federal de Seguridad (FOE), también subordinada al presidente de Rusia; este Decreto No. 351 encarga a la FOE tareas relacionadas con el desarrollo de las conexiones seguras a Internet para el gobierno ruso que faciliten el tránsito de información clasificada[454].

[454] CARR, Jeffrey: *Inside Cyber Warfare, Russian cyber security structure*, p. 220. O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472, segunda edición, diciembre 2011.

Figura 39: Estructura de ciberseguridad de la Federación de Rusia



Fuente: CARR: Inside Cyber Warfare, Russian cyber security structure[455].

5.4. La situación de la ciberseguridad en los países de la Unión Europea

Tras el estudio de los modelos más complejos de los casos de Estados Unidos, China y Rusia, que sirven para ilustrar los procesos de generación de políticas de seguridad y estrategias nacionales de seguridad y de ciberseguridad, y constituyen las referencias primarias en las que se han inspirado otros países, se va a presentar la situación de la ciberseguridad en los países de la Unión Europea.

A continuación se van a presentar los resultados de un estudio comparativo en relación a la legislación y capacidades de los países de la Unión Europea en el ámbito de la

[455] *Ibídem,* p. 221.

ciberseguridad, que se estima ilustra la situación y permite obtener conclusiones acerca del estado de la cuestión, lo que podrá ser utilizado posteriormente para poder proponer posteriormente un modelo español.

Este informe incorpora de modo integral diferentes parámetros pertinentes para comprender la situación de la ciberseguridad en la Unión Europea, ofreciendo una visión global del estado de los marcos políticos y estratégicos actuales, así como las estructuras y capacidades nacionales en el ámbito de la ciberseguridad, con los datos actualizados a 1 de enero de 2015. Se analizan cinco bloques: fundamentos legales para la ciberseguridad; capacidades operativas; asociaciones público-privadas; planes de ciberseguridad en sectores específicos; y educación en ciberseguridad[456].

Fundamentos legales para la ciberseguridad.

Los gobiernos deben promulgar y mantener al día un marco jurídico y político global, basado en una estrategia de ciberseguridad nacional sólida. Este marco debe ser construido sobre los siguientes principios clave:

Figura 40: Principios clave de los fundamentos legales para la ciberseguridad

Priorización basada en el riesgo: Las ciberamenazas tienen diversos grados de gravedad. El establecimiento de una jerarquía de prioridades, sobre la base de una evaluación objetiva del riesgo, es un punto de partida eficaz desde el que garantizar que las protecciones cibernéticas se centran en aquellas áreas donde el potencial de daño es mayor.
Tecnológicamente neutral: Los requerimientos específicos o políticas que exigen el uso de determinada tecnología socavan la seguridad mediante la restricción de la evolución de controles de seguridad y buenas prácticas.

[456] BSA - The Software Alliance: *EU Cybersecurity Dashboard. A Path to a Secure European Cyberspace*. Washington D.C., 2015. http://cybersecurity.bsa.org/assets/PDFs/study_eucybersecurity_en.pdf consulta: 21 de octubre de 2015.

Factible: Una carga excesiva en la supervisión del gobierno de los operadores privados, o la intervención reguladora desproporcionadamente intrusiva en la gestión operativa de la ciberseguridad puede resultar contraproducente.
Flexible: La gestión del riesgo cibernético es un cruce de disciplinas y cada actor se enfrenta a distintos retos con necesidades únicas.
Respetuoso de la privacidad y las libertades civiles: Los requisitos de seguridad deben estar debidamente equilibrados con la necesidad de protección de la privacidad y las libertades civiles. Asegurar que los requisitos y obligaciones proporcionadas, no representan más intrusiones en los derechos fundamentales que lo estrictamente necesario.

Fuente: BSA - The Software Alliance: *EU Cybersecurity Dashboard. A Path to a Secure European Cyberspace*[457].

Capacidades operativas.

Es importante establecer entidades y organismos con capacidades operativas y responsabilidades en la gestión de la ciberseguridad. Los gobiernos deben establecer estas estructuras para facilitar la prevención de incidentes de seguridad cibernética y para garantizar una respuesta adecuada a los mismos. Un componente central debe ser el establecimiento de la seguridad operativa de tecnologías de información y comunicaciones, y el establecimiento de equipos de emergencia y respuesta a incidentes (CERT).

Asociaciones público-privadas

Es crucial generar confianza y trabajar en asociación. Ningún país o gobierno puede abordar la ciberseguridad de forma aislada. La colaboración con organizaciones no gubernamentales, entidades privadas, así como con los socios internacionales y aliados es un componente crucial de un enfoque eficaz para seguridad cibernética. La asociación con el sector privado es fundamental, ya que la mayor parte de la infraestructura es propiedad de este sector. La cooperación también mejora la eficacia

[457] *Ibídem*, p. 3.

de la gestión de riesgos mediante el adecuado intercambio de información. También es crucial la cooperación internacional en un ámbito global.

La educación en ciberseguridad.

El impulso de la educación y la conciencia sobre los riesgos asociados a la ciberseguridad es clave. Las personas, además de los procesos y la tecnología, son primordiales para garantizar la seguridad cibernética. Incluso la mejor tecnología será ineficaz si no se usa adecuadamente. La conciencia, la sensibilización, la educación y la formación favorecen el cumplimiento de las prioridades, principios, políticas, procesos y programas de cualquier estrategia de ciberseguridad.

Estos cinco aspectos: fundamentos legales para la ciberseguridad; capacidades operativas; asociaciones público-privadas; planes de ciberseguridad en sectores específicos; y educación en ciberseguridad, son los que se utilizan para efectuar el análisis del estado de la ciberseguridad en los diferentes países de la Unión Europea.

Figura 41: Marco legal de los países de la Unión Europea en materia de ciberseguridad

✔ Yes ✖ No ◑ Partial

#	QUESTION	Austria	Belgium	Bulgaria	Croatia	Cyprus	Czech Republic	Denmark	Estonia	Finland	France
	LEGAL FOUNDATIONS										
1.	Is there a national cybersecurity strategy in place?	✔	✔	✖	✖	✔	✔	✖	✔	✔	✔
2.	What year was the national cybersecurity strategy adopted?	2013	2012	–	–	2013	2011	–	2014	2013	2011
3.	Is there a critical infrastructure protection (CIP) strategy or plan in place?	✔	◑	◑	✖	✖	✔	✖	✔	✔	✖
4.	Is there legislation/policy that requires the establishment of a written information security plan?	✖	✖	✖	✖	✖	✔	◑	✔	◑	✖
5.	Is there legislation/policy that requires an inventory of "systems" and the classification of data?	✔	✔	✔	✔	◑	✔	✔	✔	✔	✔
6.	Is there legislation/policy that requires security practices/ requirements to be mapped to risk levels?	✔	✔	✔	✔	✖	✔	✔	✔	✔	✔
7.	Is there legislation/policy that requires (at least) an annual cybersecurity audit?	✔	✖	✖	✖	✖	◑	✖	✔	✔	✖
8.	Is there legislation/policy that requires a public report on cybersecurity capacity for the government?	◑	✖	✖	◑	✖	✔	✖	✔	✔	✖
9.	Is there legislation/policy that requires each agency to have a chief information officer (CIO) or chief security officer (CSO)?	✖	✖	✖	✖	✖	✖	✖	✖	✖	✔
10.	Is there legislation/policy that requires mandatory reporting of cybersecurity incidents?	✖	◑	✖	✖	✔	✔	✖	✔	✖	✖
11.	Does legislation/policy include an appropriate definition for "critical infrastructure protection" (CIP)?	✔	✔	✔	✖	✖	✔	✔	✔	✔	✖
12.	Are requirements for public and private procurement of cybersecurity solutions based on international accreditation or certification schemes, without additional local requirements?	✔	◑	N/A	N/A	N/A	◑	✔	✔	✔	◑

Germany	Greece	Hungary	Ireland	Italy	Latvia	Lithuania	Luxembourg	Malta	Netherlands	Poland	Portugal	Romania	Slovakia	Slovenia	Spain	Sweden	United Kingdom
✔	✖	✔	✖	✔	✔	✔	✔	✖	✔	✔	Draft	✔	✔	✖	✔	✖	✔
2011	–	2013	–	2014	2014	2011	2013	–	2013	2013	–	2013	2008	–	2013	–	2011
✔	✔	◑	✖	✔	✖	◑	✖	◑	✔	✔	✖	✔	✔	✔	✔	✔	✔
✖	◑	✔	✖	✖	✖	✖	✖	◑	◑	✖	✖	✖	◑	✖	✖	✔	◑
✔	✔	✔	✖	✔	✔	✔	◑	◑	✔	✔	✔	✔	✔	✔	✔	✔	✔
✔	✖	✔	✖	✔	✔	✔	✖	✖	✔	✔	✔	✔	✔	✔	✔	✔	✔
Draft	✖	✖	✖	✖	✔	◑	◑	◑	◑	✖	◑	✖	✖	◑	◑	✖	✖
Draft	✖	✔	✖	✔	✖	◑	✖	✖	✔	✖	◑	✖	◑	✖	✖	✖	◑
✖	✖	✖	✖	✖	✔	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✔	✖
✔	✖	✖	✖	✖	✔	✔	✖	✔	✖	✔	✖	◑	✖	✔	✖	✖	✖
✔	✔	✔	✖	✔	✔	✔	✔	✔	✔	✔	✖	✔	✔	✔	✔	✔	✔
✔	✔	✔	N/A	✔	◑	◑	◑	N/A	✔	◑	N/A	◑	✖	N/A	✔	✔	◑

Fuente: : BSA - The Software Alliance: *EU Cybersecurity Dashboard. A Path to a Secure European Cyberspace*[458].

[458] *Ibídem*, pp. 8-9.

Las conclusiones[459] de este estudio del marco jurídico de la ciberseguridad en los países de la Unión Europea recogen que los políticos tienen un papel fundamental para garantizar que tanto las entidades públicas como las privadas se encuentran bien equipadas para enfrentar los desafíos de seguridad cibernética de un mundo cada vez más conectado.

Un componente clave de este marco legal es la estrategia nacional de ciberseguridad, fundamental para la gestión de los riesgos nacionales asociados al uso del ciberespacio. Una sólida estrategia de ciberseguridad debe ser un documento vivo, desarrollado e implementado en colaboración con los sectores público y privado. Esta estrategia debe contener los principios y las prioridades claramente articulados que reflejen los valores sociales, las tradiciones y los principios jurídicos.

En este sentido, se estima que existe la necesidad de seguir mejorando dentro de la UE. Solamente 19 de los 28 Estados miembros tienen una estrategia nacional de ciberseguridad y en algunos casos estas estrategias son demasiado generales y no incorporan mecanismos para su aplicación. Además, la mayoría de los países no han revisado sus estrategias de ciberseguridad. De otra parte, no se han producido progresos significativos en el desarrollo legislativo de estas estrategias de ciberseguridad.

Los resultados de este estudio muestran que más de la mitad de los Estados miembros de la UE aún no han pasado por un proceso de evaluación para planificar la protección de sus activos más importantes. Una vez identificadas estas infraestructuras críticas, su resistencia cibernética debería ser evaluada con el fin de identificar y abordar sus vulnerabilidades.

En cuanto a la implantación obligatoria de la notificación de incidentes, la mayoría de los países europeos parecen seguir siendo reacios a introducir estas prácticas. Muchos temen que un requisito obligatorio para notificar incidentes pueden ser menos eficaz que el intercambio de información basado en la confianza mutua y la

[459] *Ibídem*, pp. 4-5.

colaboración en curso. De hecho, si tuviera que imponerse un régimen de notificación de incidentes, la mayoría de los Estados miembros reconocen que solamente los incidentes que tuvieran un impacto significativo o que causaran un grave riesgo de daño debían estar sujetos a estas notificaciones obligatorias. El intercambio de información eficaz, sin embargo, requiere protección de la información, con los apropiados requisitos de clasificación, lo que es reconocido por casi todos los Estados miembros de la UE.

Figura 42: Capacidades operativas de los países de la Unión Europea en materia de ciberseguridad

✔ Yes ✖ No ◑ Partial

#	QUESTION	Austria	Belgium	Bulgaria	Croatia	Cyprus	Czech Republic	Denmark	Estonia	Finland	France
	OPERATIONAL ENTITIES										
1.	Is there a national computer emergency response team (CERT) or computer security incident response team (CSIRT)?	✔	✔	✔	✔	✖	✔	✔	✔	✔	✔
2.	What year was the computer emergency response team (CERT) established?	2008	2008	2008	2009	–	2011	2009	2008	2014	2008
3.	Is there a national competent authority for network and information security (NIS)?	◑	✔	✔	✔	◑	✔	✔	✔	✔	✔
4.	Is there an incident reporting platform for collecting cybersecurity incident data?	✔	✔	✔	✔	✖	✔	✔	✔	✔	✔
5.	Are national cybersecurity exercises conducted?	✔	✔	✔	◑	◑	◑	✔	✔	✔	✔
6.	Is there a national incident management structure (NIMS) for responding to cybersecurity incidents?	✔	✖	◑	✖	✖	✔	◑	◑	✖	✖

Germany	Greece	Hungary	Ireland	Italy	Latvia	Lithuania	Luxembourg	Malta	Netherlands	Poland	Portugal	Romania	Slovakia	Slovenia	Spain	Sweden	United Kingdom
✔	✔	✔	◑	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
2012	2009	2013	–	2014	2006	2006	2011	2002	2012	2008	2008	2011	2009	2010	2008	2003	2014
✔	✔	✔	✖	✔	✔	✔	◑	✔	◑	◑	✔	✔	✔	✔	✔	✔	✔
✔	✔	✔	✖	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
✔	✔	◑	✔	✔	✔	◑	◑	◑	✔	◑	◑	◑	✔	◑	◑	✔	✔
✖	✖	✔	✖	✔	✔	◑	◑	✖	✔	✔	◑	◑	✖	✖	✔	◑	✔

Fuente: : BSA - The Software Alliance: *EU Cybersecurity Dashboard. A Path to a Secure European Cyberspace*[460].

Deben establecerse capacidades de respuesta a incidentes para gestionar los eventos más importantes y significativos que ponen en peligro la confidencialidad, integridad o disponibilidad de redes de información y sistemas a nivel nacional. Los equipos de respuesta a emergencias informáticas (CERT) y los equipos de respuesta a incidentes de seguridad informática (CSIRT) juegan un papel crucial en la mejora de resiliencia cibernética. Estos organismos pueden ofrecer servicios de respuesta a incidentes a las víctimas de los ataques; compartir información relativa a vulnerabilidades y

[460] *Ibídem*, pp. 8-9.

amenazas con los principales actores en el gobierno, sector privado y en algunos casos con el público en general; y ofrecer otras formas de ayudar a mejorar la seguridad informática y de red. Es positivo resaltar que la mayoría de los Estados miembros de la UE tienen los CERT operativos, sólo Chipre e Irlanda aún no han implementado completamente estas capacidades. La mayoría de los países también han establecido las autoridades nacionales competentes para la red y la seguridad de información[461].

Figura 43: Asociaciones público-privadas de los países de la Unión Europea en materia de ciberseguridad

✔ Yes ✖ No ◑ Partial

# QUESTION	Austria	Belgium	Bulgaria	Croatia	Cyprus	Czech Republic	Denmark	Estonia	Finland	France
PUBLIC PRIVATE PARTNERSHIPS										
1. Is there a defined public private partnership (PPP) for cybersecurity?	✔	◑	◑	◑	◑	✖	✖	◑	◑	✖
2. Is industry organised (i.e. business or industry cybersecurity councils)?	✔	✔	◑	✖	✖	✖	✔	◑	✔	✖
3. Are new public private partnerships in planning or underway (if so, which focus area)?	✔	–	✖	✖	✖	◑	✖	✖	✖	◑

Germany	Greece	Hungary	Ireland	Italy	Latvia	Lithuania	Luxembourg	Malta	Netherlands	Poland	Portugal	Romania	Slovakia	Slovenia	Spain	Sweden	United Kingdom
✔	✖	◑	✖	◑	✖	✖	✖	◑	✔	✖	◑	✖	✖	✖	✔	◑	✔
✔	✖	◑	✔	◑	✖	◑	✖	✖	✔	◑	✖	◑	◑	◑	✔	◑	✔
✔	✖	✖	✖	◑	◑	◑	◑	✖	–	✖	✖	✔	✖	✖	–	✖	–

Fuente: : BSA - The Software Alliance: *EU Cybersecurity Dashboard. A Path to a Secure European Cyberspace*[462].

La asociación efectiva entre lo público y el sector privado es realmente significativa porque entidades no gubernamentales gestionan y operan numerosas infraestructuras críticas, incluyendo aquellos que controlan el transporte, la salud, banca y energía. Si bien se reconoce la importancia de la cooperación en Europa, existe una amplia

[461] *Ibídem*, pp. 5-6.

[462] *Ibídem*, pp. 8-9.

diversidad nacional en sus enfoques y en los niveles de madurez la cooperación entre ambos sectores. Cinco países - Austria, Alemania, Países Bajos, España y el Reino Unido - están liderando el camino al haber establecido alianzas público-privadas formales para la ciberseguridad. Por otro lado, las asociaciones público-privadas para ciberseguridad son inexistentes, se encuentran en un estadio muy restringido, o aún permanecen en una fase muy temprana de desarrollo en la mayoría de los Estados miembros de la Unión Europea[463].

Figura 44: Planes de ciberseguridad en sectores específicos en los países de la Unión Europea

✔ Yes ✖ No ◑ Partial

#	QUESTION	Austria	Belgium	Bulgaria	Croatia	Cyprus	Czech Republic	Denmark	Estonia	Finland	France
	SECTOR SPECIFIC CYBERSECURITY PLANS										
1.	Is there a joint public private sector plan that addresses cybersecurity?	✔	✖	✖	◑	◑	✖	✖	✖	◑	✔
2.	Have sector specific security priorities been defined?	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖
3.	Have any sector cybersecurity risk assessments been conducted?	✖	✖	✖	✖	✖	✔	✖	✖	✖	✖

Germany	Greece	Hungary	Ireland	Italy	Latvia	Lithuania	Luxembourg	Malta	Netherlands	Poland	Portugal	Romania	Slovakia	Slovenia	Spain	Sweden	United Kingdom
✖	✖	◑	✖	✖	✖	✖	✖	✖	✔	✖	✖	✖	✖	✖	✔	✖	✔
✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	◑	✖	◑
✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖

Fuente: : BSA - The Software Alliance: *EU Cybersecurity Dashboard. A Path to a Secure European Cyberspace*[464].

España y el Reino Unido son los países que lideran la implementación de planes sectoriales específicos en el ámbito de la ciberseguridad entre los Estados miembros de la Unión Europea. Es significativo que solamente la República Checa ha llevado a cabo un análisis de riesgos en algún sector específico relacionado con la ciberseguridad. En general, los países de la Unión Europea no han desarrollado la

[463] *Ibídem*, p. 6.

[464] *Ibídem*, pp. 8-9.

planificación adecuada en la planificación específica en sectores relacionados con la ciberseguridad.

Figura 45: La educación en ciberseguridad en los países de la Unión Europea

✔ Yes ✖ No ◑ Partial

# QUESTION	Austria	Belgium	Bulgaria	Croatia	Cyprus	Czech Republic	Denmark	Estonia	Finland	France
EDUCATION										
1. Is there an education strategy to enhance cybersecurity knowledge and increase cybersecurity awareness of the public from a young age?	✔	◑	◑	✖	✖	✔	✖	✔	✔	✔

Germany	Greece	Hungary	Ireland	Italy	Latvia	Lithuania	Luxembourg	Malta	Netherlands	Poland	Portugal	Romania	Slovakia	Slovenia	Spain	Sweden	United Kingdom
◑	✖	✔	◑	✔	✔	✔	✔	✖	✔	✔	✖	✔	✔	✖	✔	✖	✔

Fuente: : BSA - The Software Alliance: *EU Cybersecurity Dashboard. A Path to a Secure European Cyberspace*[465].

Los datos del informe reflejan que la educación en ciberseguridad se encuentra incorporada en gran medida en los Estados miembros de la Unión Europea. Este es un aspecto transversal de la ciberseguridad que debe impregnar los sectores público y privado, aunque los gobiernos y otros actores tienen recorrido para incorporar aspectos de la cultura de ciberseguridad en la sociedad.

Por parte de la Unión Europea se han desarrollado diversas iniciativas, como la celebración del mes de la ciberseguridad. El Mes Europeo de Ciberseguridad (ECSM) es una campaña de promoción de la UE que promueve la seguridad cibernética entre los ciudadanos y los defensores del cambio en la percepción de los ciberamenazas, mediante la difusión de datos e información de ciberseguridad, la puesta en valor de

[465] *Ibídem*, pp. 8-9.

la necesidad de educación en este ámbito, así como el intercambio de buenas prácticas[466].

Una reciente iniciativa de la Unión Europea, que comenzó en octubre de 2015, es la creación de una base de datos con una lista de cursos disponibles y programas de certificación vinculados a la red y a la seguridad de la Información. La página web permite a los representantes de las instituciones educativas a añadir al mapa cursos, programas y cursos de capacitación[467].

5.4.1. Reino Unido

El Reino Unido dispone de una estrategia de ciberseguridad, formulada en 2011. Dispone también de un sólido marco legal en materia de ciberseguridad y dos equipos de respuesta a emergencias informáticas (CERT). El CERTUK apoya principalmente a operadores de infraestructuras críticas, mientras el GovCertUK apoya a las agencias gubernamentales. Otros órganos relacionados con la ciberseguridad son el Consejo de Seguridad Nacional, y la Oficina de Seguridad Cibernética y Protección de la Información. El Reino Unido también posee un sistema bien desarrollado de asociaciones público-privadas. Este enfoque de colaboración se encuentra también apoyado por su Estrategia de Ciberseguridad. El Centro para la Protección de la Infraestructura Nacional (CPNI), tiene un rol significativo en el impulso del intercambio de información[468].

La Estrategia de Ciberseguridad del Reino Unido, que lleva por título “La protección y la promoción del Reino Unido en un mundo digital”, pone en valor la revolución que ha supuesto para la sociedad el uso de Internet y su impulso para el crecimiento económico; además de constituir un elemento "democratizador", en donde el uso de

[466] Unión Europea: *Mes Europeo de Ciberseguridad*. https://cybersecuritymonth.eu/ consulta: 21 de octubre de 2015.

[467] Unión Europea: *Mapa educativo en ciberseguridad*. https://cybersecuritymonth.eu/references/universities consulta: 21 de octubre de 2015.

[468] BSA - The Software Alliance: *United Kingdom, Country Report.* Washington D.C., 2015. http://cybersecurity.bsa.org/assets/PDFs/country_reports/Cs_unitedkingdom.pdf consulta: 21 de octubre de 2015.

la tecnología alimenta el flujo de innovación y productividad. El capitulo 1 describe los antecedentes del crecimiento del mundo en red y la inmensa y los beneficios sociales y económicos que está ofreciendo; para apuntar a continuación la dependencia del ciberespacio, que trae nuevas amenazas. El capítulo 2 describe estas amenazas, señalando que las redes trascienden los límites nacionales. El capítulo 3 establece la visión del Gobierno del Reino Unido para la ciberseguridad en 2015[469].

Figura 46: Objetivos del Reino Unido en ciberseguridad para 2015

<table>
<tr><td colspan="3">El objetivo es que en 2015 el Reino Unido pueda alcanzar un nivel económico y social de alto nivel en un vibrante, resistente y seguro ámbito en el ciberespacio, donde sus acciones, guiadas por un núcleo de valores inspirados en la libertad, la equidad, la transparencia y el imperio de la ley, permitan mejorar la prosperidad, la seguridad nacional y una sólida sociedad.</td></tr>
<tr><td colspan="3">Para alcanzar esta visión en 2015 el Reino Unido quiere:</td></tr>
<tr><td>Objetivo 1:
El Reino Unido debe hacer frente a la delincuencia en el ciberespacio y ser uno de los lugares seguros en el mundo para hacer negocios en ciberespacio</td><td>Objetivo 2:
El Reino Unido debe ser más resistente a los ataques cibernéticos y más capaz de proteger sus intereses en el ciberespacio</td><td>Objetivo 3:
El Reino Unido debe haber ayudado a conformar un proceso abierto, estable y vibrante en el ciberespacio que la población del Reino Unido pueda utilizar con seguridad y que apoye las sociedades abiertas</td></tr>
<tr><td colspan="3">Objetivo 4:
El Reino Unido debe obtener los conocimientos, habilidades y capacidades transversales que necesita para respaldar sus objetivos de seguridad en el ciberespacio</td></tr>
</table>

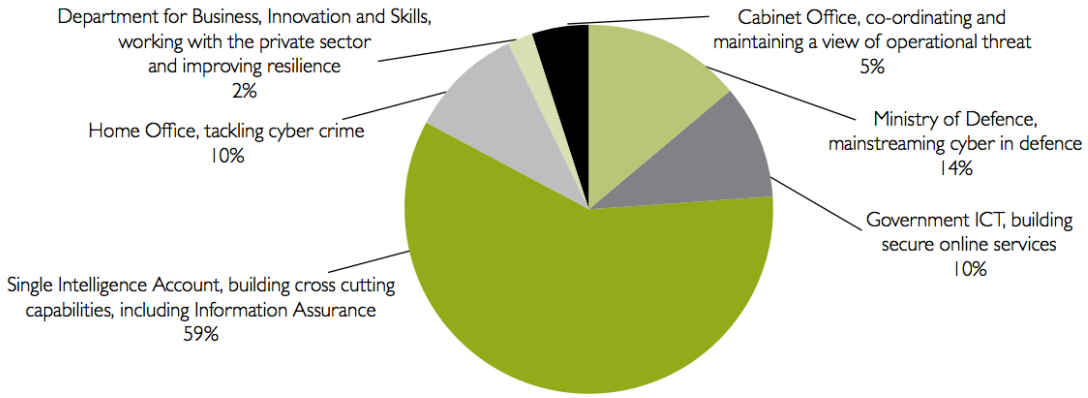
Fuente: *The UK Cyber Security Strategy. Protecting and promoting the UK in a digital world*[470].

[469] Gobierno del Reino Unido, Cabinet Office: *The UK Cyber Security Strategy. Protecting and promoting the UK in a digital world*. Londres, noviembre de 2011, p. 7. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf consulta: 22 de octubre de 2015.

[470] *Ibídem*, p. 8.

El Reino Unido efectúa en su Estrategia de Ciberseguridad una explicación de sus inversiones en materia de ciberseguridad nacional en el Programa Nacional de Ciberseguridad.

Figura 47: Inversión en el Programa Nacional de Ciberseguridad (2011-2015)



Fuente: Estrategia de Ciberseguridad del Reino Unido[471].

Además, el Ministerio de Defensa del Reino Unido ha seleccionado a un consorcio de empresas de tecnologías de la información y comunicaciones, que opera bajo el nombre de ATLAS, para transformar la infraestructura de la información de Defensa. El consorcio debe integrar los cientos de sistemas TIC antiguos en una sola red, lo que permitirá a los usuarios acceder a la información en movilidad. Según el acuerdo de cuatro años, el consorcio –formado por CGI, Fujitsu y Airbus, y liderado por HP– debe ofrecer servicios de comunicaciones, tanto en el lugar de trabajo como en movilidad, basados en la nube para 200.000 usuarios TIC[472].

[471] Ibídem, p. 25.

[472] Consultancy.UK: *IT firms lead mega project at UK Ministry of Defence*, 20 de agosto de 2015. http://www.consultancy.uk/news/2464/it-firms-lead-mega-project-at-uk-ministry-of-defence consulta: 21 de octubre de 2015.

Esta medida no sólo se suma a la intensa actividad británica en ciberseguridad, sino que además se une a la investigación llevada a cabo por el CEBR (Centro para la Investigación Económica y de Negocio), en la que han calculado el coste que supone el cibercrimen en el Reino Unido, el cual asciende a 34.000 millones de libras al año. De este montante, el CEBR estima que 18.000 millones se deben a la pérdida de ingresos tras ciberataques mientras que los otros 16.000 millones corresponden a la prevención de amenazas[473].

Figura 48: Ecosistema de empresas de ciberseguridad en el Reino Unido

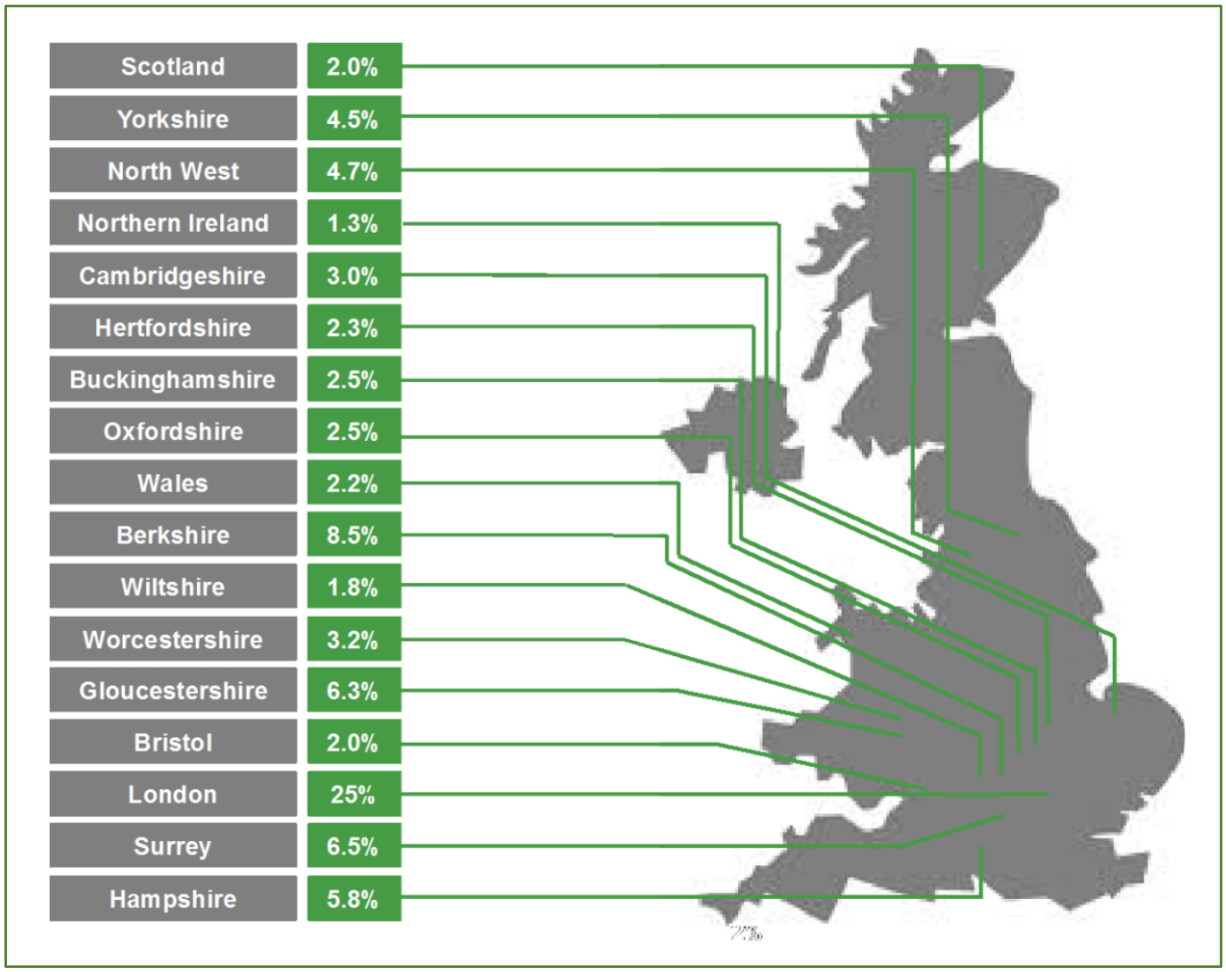
Fuente: Pierre Audoin Consultants[474].

[473] Revista SIC, Ciberseguridad, Seguridad de la Información y Privacidad: *El Ministerio de Defensa de Reino Unido confía el acceso seguro a sus redes al consorcio ATLAS*. nº 116, septiembre de 2015, p. 10.

[474] Pierre Audoin Consultants: *Competitive analysis of the UK cyber security sector.* Reino Unido, 29 de julio de 2013, p. 25. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/259500/bis-13-1231-competitive-analysis-of-the-uk-cyber-security-sector.pdf consulta: 2 de noviembre de 2015.

El sector de las empresas de ciberseguridad en el Reino Unido es muy dinámico, existiendo unas 600 compañías de relevancia. Casi tres cuartas partes de las 600 empresas (73%) son compañías de servicios de pequeña entidad, siendo significativamente mucho menor el número de las empresas orientadas al producto[475].

Figura 49: Empresas de ciberseguridad en el Reino Unido



Fuente: Pierre Audoin Consultants[476].

5.4.2. Francia

Francia dispone de una estrategia de ciberseguridad nacional desde 2011. Esta estrategia se encuentra muy orientada a la defensa nacional al nivel superior de la

[475] *Ibídem,* pp. 27-29.
[476] *Ibídem,* p. 30.

seguridad nacional. La Agencia Nacional de la Seguridad de los Sistemas de Información (ANSSI) es la autoridad dedicada a la seguridad de la información y cuenta con el equipo de respuesta a incidentes de ciberseguridad nacional, CERT-FR. La estrategia de seguridad cibernética contiene recomendaciones para llevar a cabo una estrecha cooperación con el sector privado, aunque estos aspectos no han sido desarrollados significativamente. ANSSI ha publicado medidas específicas dedicadas al sector de la ciberseguridad, constituyendo uno de los países más avanzados de la UE en adoptar un enfoque integral orientado a la gestión de la seguridad cibernética[477].

En la "Estrategia de Francia para la defensa y seguridad de los sistemas de información", se comienza haciendo referencia al Libro Blanco Francés de Defensa y Seguridad Nacional de 2008, apuntando que entre las principales amenazas que Francia tendrá que hacer frente en los próximos quince años, se encuentran ciberataques contra infraestructuras nacionales a gran escala. Esta observación llevó a la decisión del Gobierno francés de fortalecer significativamente capacidades de ciberdefensa nacionales. La creación de la Agencia Nacional de la Seguridad de los Sistemas de Información (ANSSI) en 2009 fue el primer paso de este proceso[478].

La estrategia de ciberseguridad francesa se basa en cuatro objetivos:

1. **Convertirse en una potencia mundial en ciberdefensa.** Para mantener su independencia estratégica, Francia debe asegurar que pertenece al círculo íntimo de las naciones líderes en el área de la ciberdefensa.

2. **Salvaguardar la capacidad de Francia para tomar decisiones mediante la protección de la información relacionada con su soberanía.** Las autoridades gubernamentales y los actores de gestión de crisis deben disponer de los recursos

[477] BSA - The Software Alliance: *France, Country Report.* Washington D.C., 2015. http://cybersecurity.bsa.org/assets/PDFs/country_reports/cs_france.pdf consulta: 2 de noviembre de 2015.
[478] Primer Ministro de Francia: *Information systems defence and security France's strategy.* París, febrero de 2011. http://www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_Information_system_defence_and_security_-_France_s_strategy.pdf consulta: 2 de noviembre de 2015.

para comunicarse en cualquier situación y en total confidencialidad. Garantizar la confidencialidad de la información que circula en estas redes requiere productos de seguridad propios, lo que exige la experiencia para diseñarlos y optimizar sus métodos de desarrollo y producción.

3. **Fortalecer la ciberseguridad de las infraestructuras nacionales críticas.** La sociedad es cada vez más dependiente de los sistemas de información y de las redes, en particular de Internet. Un ataque con éxito sobre una sistema de información crítico francés o Internet podría tener graves consecuencias económicas o personales. El Estado debe trabajar para garantizar y mejorar la seguridad de estos sistemas críticos, en estrecha colaboración con los fabricantes y operadores de equipos.

4. **Garantizar la seguridad en el ciberespacio.** Las amenazas a los sistemas de información afectan simultáneamente los servicios públicos, privados, empresas y ciudadanos. Los servicios públicos deben operar de manera ejemplar y mejorar la protección de sus sistemas de información y los datos asociados. En cuanto a la lucha contra el delito cibernético, Francia promoverá el fortalecimiento de la la legislación vigente y la cooperación judicial internacional.

Para cumplir estos objetivos, se han identificado siete áreas de actuación.

Figura 50: Áreas de actuación para la protección de los sistemas de información

1. Poseer la capacidad de anticipación y análisis para la toma apropiada de decisiones.
2. Detectar y bloquear ataques; alertar y apoyar a las víctimas potenciales.
3. Mejorar y mantener las capacidades en los planos científico, técnico, e industrial, con el objetivo de mantener la independencia.
4. Proteger los sistemas de información del Estado y los de los operadores de infraestructuras críticas, para garantizar una mejor capacidad de recuperación nacional.
5. Adaptar la legislación francesa para incorporar los avances tecnológicos.
6. Desarrollar iniciativas de colaboración internacional en las áreas de seguridad de los sistemas de información, ciberdefensa y lucha contra la delincuencia informática.

7. Mejorar la comprensión por parte de la sociedad de la magnitud de los desafíos relacionados con los sistemas de seguridad de la información.

Fuente: Estrategia de Francia para la defensa y seguridad de los sistemas de información[479].

Francia ha publicado el 15 de octubre de 2015 la "Estrategia Nacional Francesa para la Seguridad del Ámbito Digital", destinada a apoyar la transición digital de la sociedad francesa. Esta estrategia ha sido coordinado por el trabajo interdepartamental de ANSSI sus objetivos se han consolidado por el Secretario de Estado para lo Digital y por el Secretario General de la Defensa y la Seguridad Nacional. Esta Estrategia Nacional para la seguridad de la tecnología digital dispone cinco objetivos: garantizar la soberanía nacional; ofrecer respuesta contra los actos de ciberdelincuencia; informar al público en general; hacer de la seguridad digital una ventaja competitiva para las empresas francesas; y fortalecer la presencia de Francia en el extranjero. Esta estrategia espera una respuesta colectiva en el ámbito de la confianza digital, conducente a la estabilidad del Estado, el desarrollo económico y la protección de los ciudadanos[480].

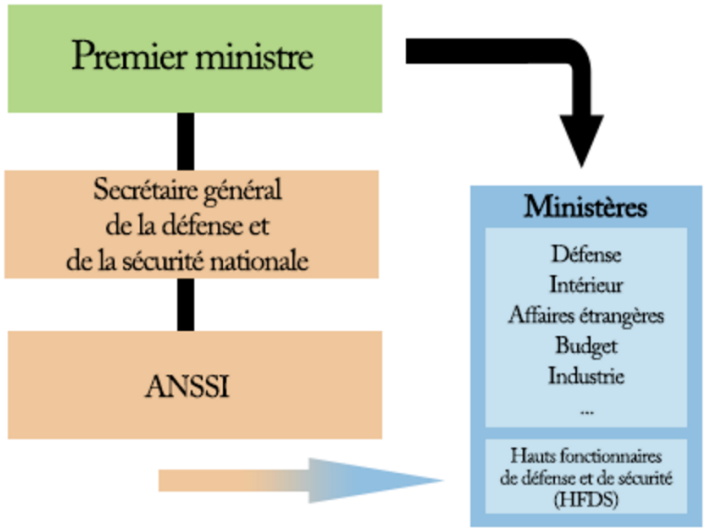
El Primer Ministro de Francia, Manuel Valls, escribe que Francia está plenamente comprometida en la transición digital. Con una gran población ampliamente conectada y una economía digital en sostenido crecimiento, Francia dispone de talentos y ventajas a la vanguardia de la innovación europea y mundial. El mundo digital es también un espacio de competición y enfrentamiento. Competencia desleal y espionaje, desinformación y propaganda, terrorismo y criminalidad encuentran en el ciberespacio un nuevo ámbito de expresión. La estrategia nacional francesa para la seguridad del ámbito digital debe apoyarse en particular sobre la formación y sobre la cooperación internacional, y debe ser respaldada por el conjunto de la comunidad

[479] *Ibídem.*
[480] Agencia Nacional de la Seguridad de los Sistemas de Información (ANSSI): *Stratégie nationale pour la sécurité du numérique*. París, 15 de octubre de 2015. http://www.ssi.gouv.fr/actualite/la-strategie-nationale-pour-la-securite-du-numerique-une-reponse-aux-nouveaux-enjeux-des-usages-numeriques/ consulta: 2 de noviembre de 2015.

nacional: el Gobierno, las administraciones, las colectividades territoriales, las empresas y más ampliamente sobre todo nuestros compatriotas. Responder a los retos en torno a la seguridad del mundo digital es un factor clave del éxito colectivo[481].

La seguridad de la información cae dentro de las responsabilidades de cada ministro en el área de la que es responsable. El Ministro está asistido por un alto funcionario de defensa y seguridad (HFDS) cuyos poderes son definidos por el código de la defensa. El Ministro correspondiente designa un funcionario de seguridad de los sistemas de información (FSSI), que, por lo general, se coloca bajo la autoridad del HFDS. Este FSSI coordina la política de seguridad de los sistemas de información y establece los controles necesarios.

Figura 51: Organización de la Ciberseguridad en Francia



Fuente: Agencia Nacional de la Seguridad de los Sistemas de Información (ANSSI)[482].

[481] Primer Ministro de Francia: *Estrategia Nacional Francesa para la Seguridad del Ámbito Digital*. París, 15 de octubre de 2015. http://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_es.pdf consulta: 2 de noviembre de 2015.

[482] Agencia Nacional de la Seguridad de los Sistemas de Información (ANSSI): *Organisation Ministérielle*. http://www.ssi.gouv.fr/agence/cybersecurite/ssi-en-france/organisation-ministerielle/ consulta: 2 de noviembre de 2015.

Además del CERT Gubernamental Nacional (CERT-FR), Francia dispone de otros equipos de respuesta a incidentes de ciberseguridad.

Figura 52: Organizaciones CERT en Francia incorporadas a la alianza FIRST

le CERT-FR est le CSIRT dédié au secteur de l'administration française
le CERT-DEVOTEAM est un CSIRT commercial français
le Cert-IST est un CSIRT dédié au secteur de l'Industrie, des Services et du Tertiaire (IST). Il a été créé à la fin de l'année 1998 par quatre partenaires : Alcatel, le CNES, ELF (Total) et France Télécom (Orange)
le CERT LA POSTE est le CSIRT du groupe La Poste, pour ses services internes et ses clients
le CERT-LEXSI(Laboratoire d'EXpertise en Sécurité Informatique) est un CSIRT commercial français
le CERT-RENATER est le CERT dédié à la communauté des membres du GIP RENATER (Réseau National de télécommunications pour la Technologie, l'Enseignement et la Recherche)
le CERT-societegenerale est le CSIRT dédié au groupe Société Générale
le CERT-XMCO est un CSIRT commercial français
le CSIRT-BNP Paribas est le CSIRT dédié au groupe BNP Paribas
Orange-CERT-CC est le CERT interne de l'opérateur de télécommunication Orange
le CERT-SOLUCOM est un CSIRT commercial français
le CERT Crédit Agricole est le CSIRT dédié au groupe Crédit Agricole
Airbus Cybersecurity and Computer Emergency Response Team est un CSIRT commercial européen
CERT Banque de France est le CSIRT interne de la Banque de France
CSIRT ATOS est un CSIRT commercial français
Airbus Group CERT (ou AiG CERT) est le CSIRT du groupe Airbus

Fuente: Agencia Nacional de la Seguridad de los Sistemas de Información (ANSSI)[483].

5.4.3. Alemania

Alemania tiene una estrategia integral de seguridad cibernética, adoptada en 2011 y complementada por un sólido marco legal en el ámbito de la ciberseguridad. La existencia de la Oficina Federal para la Seguridad de la Información (BSI), a cargo de

[483] Agencia Nacional de la Seguridad de los Sistemas de Información (ANSSI): *Les CERT Français*. http://www.ssi.gouv.fr/agence/cybersecurite/ssi-en-france/les-cert-francais/ consulta: 2 de noviembre de 2015.

la gestión de la seguridad informática y las comunicaciones para el gobierno alemán, demuestra que ciberseguridad es tratada en un nivel gubernamental elevado. Alemania también tiene una red de emergencias informáticas equipos de respuesta (CERT), con el CERT nacional, CERT-BUND, que trabaja en estrecha colaboración con los dos de nivel estatal y los CERT no gubernamentales. Por otra parte, el país ha bien desarrollado asociaciones público privadas, como la Alianza para la Ciberseguridad y la asociación UP KRITIS, y las políticas nacionales y el marco jurídico reflejan este enfoque en la cooperación[484].

La Estrategia de Ciberseguridad para Alemania señala que en los últimos años los ataques contra infraestructuras de información se han convertido en cada vez más frecuentes y complejos, mientras que al mismo tiempo los autores son más profesionales. Estos ataques cibernéticos se ejecutan tanto desde Alemania como desde el extranjero. Dado el carácter abierto y la extensión del ciberespacio es posible utilizar sistemas vulnerables para llevar a cabo un ataque. En vista del desarrollo de la tecnología de malware, las posibilidades de responder en caso de ataque son bastante limitadas. A menudo los ataques no dan ninguna pista sobre la identidad del atacante. Delincuentes, terroristas y espías utilizan el ciberespacio como un lugar para su actividades y no se detienen en las fronteras estatales. La Estrategia señala además, que detrás este tipo de ataques pueden encontrarse también operaciones militares[485].

La Estrategia de Ciberseguridad apunta que garantizar la seguridad cibernética, hacer cumplir los derechos y la protección de información crítica de las infraestructuras requieren mayores esfuerzos por parte del Estado, tanto a nivel nacional como en la cooperación con los socios internacionales. Dadas las responsabilidades compartidas

---

[484] BSA - The Software Alliance: *Country Report, Germany*. http://cybersecurity.bsa.org/assets/PDFs/country_reports/cs_germany.pdf consulta: 21 de octubre de 2015.

[485] Ministerio Federal de Interior de Alemania: *Cyber Security Strategy for Germany*. Berlín, febrero de 2011, p. 3. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CyberSecurity/Cyber_Security_Strategy_for_Germany.pdf?__blob=publicationFile consulta: 21 de octubre de 2011.

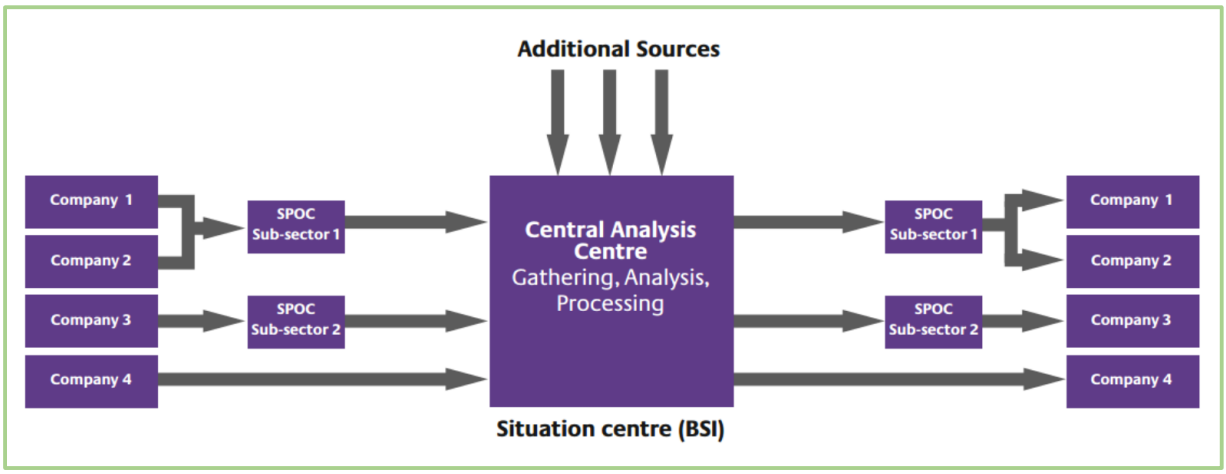
del Estado, la industria y la sociedad, una estrategia de seguridad cibernética sólo tendrá éxito si todos los actores colaboran y cumplen sus responsabilidades. Lo mismo se aplica al contexto internacional. Dado que los sistemas TIC están interconectados en redes globales, las incidencias en las infraestructuras de información de otros países también pueden afectar indirectamente a Alemania. Por esta razón, el fortalecimiento de la seguridad cibernética también requiere la aplicación de las normas internacionales de conducta, reglas y normas. Se significa que solamente una combinación de medidas de política interna y externa será apropiada para afrontar el problema[486].

Con la actual Estrategia de Ciberseguridad, el Gobierno Federal adapta las medidas a las amenazas actuales sobre la base de las estructuras establecidas por el plan de implementación de protección de infraestructuras críticas (CIP). Se señala que el suministro fiable de los servicios que estas infraestructuras transmiten es una condición previa fundamental para el desarrollo económico del país, el bienestar de nuestra sociedad y la estabilidad política. De esta forma, tanto el Gobierno Federal como la comunidad empresarial consideran la protección de las infraestructuras críticas una tarea nacional clave, porque la seguridad nacional está cada vez más afectada por la seguridad las TIC. En este sentido, el plan CIP está haciendo una contribución importante para la provisión confiable de servicios vitales a través de una protección adecuada de las tecnologías de información y comunicaciones[487].

[486] *Ibídem*, p. 4.

[487] Ministerio Federal de Interior de Alemania*: CIP Implementation Plan of the National Plan for Information Infrastructure Protection*. Berlín, 2005. http://www.bmi.bund.de/SharedDocs/Downloads/EN/Broschueren/2009/kritis.pdf;jsessionid=B0B3D978E9BA15DA303E89BF20F7CDA7.2_cid373?__blob=publicationFile consulta: 21 de octubre de 2015.

Figura 53: Estructura de comunicaciones del plan de implementación de protección de infraestructuras críticas



Fuente: Plan de implementación de protección de infraestructuras críticas de Alemania[488].

En este escenario, el Gobierno Federal ha establecido específicamente diez áreas estratégicas en el ámbito de la ciberseguridad:

1. La protección de infraestructuras críticas de información.

La protección de las infraestructuras críticas de información es la principal prioridad de seguridad cibernética. El sector público y el privado deben crear una base estratégica y organizativa mejorada para una coordinación más estrecha basada en un intensivo intercambio de información. Con este fin, la cooperación establecida por el plan de implementación de protección de infraestructuras críticas.

2. Los sistemas informáticos seguros en Alemania.

La protección de infraestructuras requiere una mayor seguridad con respecto a los sistemas informáticos utilizados por los ciudadanos y las pequeñas y medianas empresas. Los usuarios necesitan apropiado y información

[488] *Ibídem*, p. 29.

consistente sobre los riesgos relacionados con el uso de los sistemas informáticos y en la seguridad medidas que pueden tomar para usar el ciberespacio de una manera segura.

3. El fortalecimiento de la seguridad informática en la administración pública.

Las autoridades estatales tienen que servir de referencia para la seguridad de datos. Se va a crear una red segura en la administración federal. Los recursos deben utilizarse apropiadamente en el nivel central y el local. La cooperación operativa con los Lander federales debe incrementarse, particularmente con respecto a los CERT.

4. Centro Nacional de Respuesta Cibernética

Para optimizar la cooperación operativa entre todas las autoridades estatales y mejorar la coordinación de las medidas de protección y respuesta de incidentes TIC se crea un Centro Nacional de Respuesta Cibernética. Se deben observar rigurosamente las funciones y competencias de todas las autoridades legales involucradas en la base de acuerdos de cooperación, Oficina Federal de Seguridad de la Información (BSI), Oficina Federal para el Protección de la Constitución (BfV), y Oficina Federal de Protección Civil y Asistencia para Desastres (BBK). En este Centro Nacional de Respuesta Cibernética deben cooperar la Oficina Federal de Policía Criminal (BKA), la Policía Federal (BPOL), la Oficina de Aduanas Criminológica (ZKA), el Servicio Federal de Inteligencia (BND), la Bundeswehr y las autoridades supervisoras de los operadores de infraestructuras críticas, participando los diferentes organismos en este centro en el marco de sus funciones y competencias estatutarias. El Centro de Respuesta Cibernética presentará recomendaciones al Consejo Nacional de Ciberseguridad. En caso de crisis, el Centro Nacional de Respuesta Cibernética informará directamente al personal de gestión de crisis

encabezado por el Secretario de Estado responsable en el Ministerio Federal de Interior.

5. Consejo Nacional de Ciberseguridad.

La identificación y eliminación de las causas estructurales de las crisis se consideran un importante herramienta de prevención para la ciberseguridad. Por esta razón se quiere intensificar la cooperación dentro del Gobierno Federal y entre los sectores público y privado, estableciendo un Consejo Nacional de Ciberseguridad. En este Consejo participarán la Cancillería Federal y el Secretario de Estado de la Oficina Federal de Relaciones Exteriores, el Ministerio Federal del Interior, el Ministerio Federal de Defensa, el Ministerio Federal de Economía y Tecnología, el Ministerio Federal de Justicia, el Ministerio de Hacienda Federal, el Ministerio Federal de Educación e Investigación y los representantes de los Lander federales. En ocasiones específicas participarán adicionalmente otros ministerios y representantes de los sectores público y privado. El Consejo Nacional de Ciberseguridad se encuentra en el nivel político y estratégico.

6. El control eficaz del delito también en el ciberespacio.

Debe fortalecerse las capacidades de las agencias de aplicación de la ley, la Oficina Federal de Información y Seguridad, y el sector privado en la lucha contra el delito cibernético, así como en relación a la protección contra el espionaje y sabotaje, Para mejorar el intercambio de conocimiento se crearán instituciones conjuntas con la industria. Se apoyarán además las iniciativas internacionales que faciliten este objetivo.

7. Acción coordinada eficaz para garantizar la seguridad cibernética en Europa y en el resto del mundo.

La seguridad del ciberespacio sólo puede lograrse a través de herramientas coordinadas a nivel nacional e internacional. A nivel de la UE se apoyarán las iniciativas legislativas en este sentido y se colaborará con organizaciones como las Naciones Unidas, la OSCE, el Consejo de Europa, la OCDE y la OTAN.

8. El uso de tecnologías de la información fiables y de confianza.

Se va a continuar e intensificar la investigación sobre la seguridad de las tecnologías de la información y comunicaciones y sobre la protección de infraestructuras críticas. Además se fortalecerá la soberanía tecnológica de Alemania, a la vez que se trabajará con socios y aliados, especialmente en Europa. Alemania está a favor de la diversidad en la tecnología.

9. Desarrollo de personal en las autoridades federales.

Dada la importancia estratégica de la seguridad cibernética, ha de examinarse como una prioridad dotar con el personal adicional necesario a las autoridades en interés de la ciberseguridad. Se incentivará el intercambio de personal entre las autoridades federales y se establecerán nuevas medidas de formación, lo que mejorará la cooperación interministerial.

10. Herramientas para responder a los ataques cibernéticos.

Si el Estado quiere estar plenamente preparado para los ataques cibernéticos, debe desarrollar un conjunto de herramientas, en cooperación con las autoridades estatales competentes. Si es necesario, se examinará la necesidad de disponer de facultades legales adicionales, a nivel federal o de los Lander, en un proceso en el que deben ser incorporadas las empresas.

De otra parte, el Bundestag alemán ha aprobado la Ley de Seguridad Informática, la cual se caracteriza por imponer medidas a las grandes empresas estratégicas, como

es el caso de las energéticas o las financieras asociadas a las infraestructuras críticas, con el objetivo de proteger sus sistemas de información ante ataques perpetrados por hackers como los que han sufrido algunas estructuras nacionales. De este modo, las compañías habrán de reportar cualquier tipo de anomalía al BSI, pues en el caso de no hacerlo deberán enfrentarse a sanciones de hasta 100.000 euros en caso de negligencia. Además, el BSI ampliará también el centro internacional para la seguridad, cuya principal tarea será evaluar los informes de violaciones cibernéticas en las infraestructuras críticas. Además, al Servicio Federal de Inteligencia (BND) se le permitirá el acceso a los datos extranjeros enlazados a firmas de malware[489].

Conclusiones del Capítulo 5

En este capítulo se han analizado las estrategias de seguridad y los modelos organizativos nacionales derivados de estas estrategias de diversos países. Los casos de Estados Unidos, China y Rusia continúan ofreciendo referencias y modelos –al igual que lo hicieron al tratar las estrategias nacionales de seguridad– que son analizados por el resto de países para adaptarlos a sus propias necesidades de desarrollo de estrategias nacionales de ciberseguridad, procesos de planeamiento, modelos de gobernanza de la ciberseguridad, y diseño de modelos organizativos en el ámbito de la ciberseguridad.

Estados Unidos, China y Rusia adoptan soluciones organizativas diferentes, derivadas de sus propias estrategias nacionales de ciberseguridad y de la cultura de seguridad de cada uno de estos Estados. No obstante, estos tres actores políticos comparten una clara definición de niveles en el ámbito de la ciberseguridad: político estratégico, operacional y táctico / técnico. Además, los tres países tienen definido un esquema de respuesta a incidentes de ciberseguridad coherente y bien estructurado.

Se han estudiado a continuación los países de la Unión Europea, utilizando cinco bloques de parámetros: fundamentos legales para la ciberseguridad; capacidades

[489] Revista SIC, Ciberseguridad, Seguridad de la Información y Privacidad: *Alemania endurece el castigo a las negligencias en infraestructuras críticas*. nº 116, septiembre de 2015, p. 10.

operativas; asociaciones público-privadas; planes de ciberseguridad en sectores específicos; y educación en ciberseguridad.

El proceso normativo y de planeamiento de la ciberseguridad de los países de la UE en el ámbito de la ciberseguridad es dispar. Aunque 19 de los 28 países de la Unión Europea han desarrollado una estrategia de ciberseguridad nacional, no se han producido en la mayor parte de estos países progresos significativos en el desarrollo legislativo de estas estrategias de ciberseguridad. Además, más de la mitad de los países de la UE aún no han desarrollado un proceso de evaluación para planificar la protección de sus infraestructuras críticas, paso previo para evaluar las vulnerabilidades de carácter cibernético. En cuanto a la capacidad CERT, solamente dos países no han desarrollado aún estas capacidades. Además, la mayoría de los países de la UE han establecido autoridades nacionales competentes para la red y la seguridad de la información.

En cuanto al Reino Unido, Francia y Alemania, los tres países de referencia tienen establecidas estrategias nacionales de ciberseguridad; han desarrollado en diferentes niveles planes que desarrollan la estrategia de ciberseguridad; tienen establecidos los niveles político estratégico, operacional y táctico / técnico; cuentan con un organismo específico en el nivel operacional a modo de centro o agencia nacional para la ciberseguridad; y los tres países han establecido un CERT Gubernamental Nacional de referencia CERT-FR en Francia, CERT-BUND en Alemania, y dos en el caso de Reino Unido: CERTUK para operadores de infraestructuras críticas y GovCERTUK para las agencias gubernamentales.

CAPÍTULO 6. EL PLANEAMIENTO DE CIBERSEGURIDAD EN ESPAÑA.

6.1. LA LEY DE SEGURIDAD NACIONAL

España se ha dotado de una Ley de Seguridad Nacional, donde se define la Seguridad Nacional como la acción del Estado dirigida a proteger la libertad, los derechos y bienestar de los ciudadanos, a garantizar la defensa de España y sus principios y valores constitucionales, así como a contribuir junto a los socios y aliados a la seguridad internacional en el cumplimiento de los compromisos asumidos[490].

El preámbulo de la Ley de Seguridad Nacional señala que la seguridad constituye la base sobre la cual una sociedad puede desarrollarse, preservar su libertad y la prosperidad de sus ciudadanos, y garantizar la estabilidad y buen funcionamiento de sus instituciones. De esta forma, la legislación española así lo reconoce e interpreta, y contiene instrumentos normativos que, partiendo del marco diseñado por la Constitución, regulan los aspectos fundamentales que han venido permitiendo a los poderes públicos cumplir con sus obligaciones en esta materia. Así, las normas aplicables a los estados de alarma, excepción y sitio, a la Defensa Nacional, a las Fuerzas y Cuerpos de Seguridad, a la protección de la seguridad ciudadana, a la protección de infraestructuras críticas, a la protección civil, a la acción y el servicio exterior del Estado o a la seguridad privada, regulan, junto con la legislación penal y los tratados y compromisos internacionales en los que España es parte, distintos aspectos de la seguridad.

Continúa el preámbulo de la Ley de Seguridad Nacional señalando que la regulación se basa en la asignación de competencias a las distintas autoridades y Administraciones Públicas, y se articula en un modelo tradicional y homologable con

[490] Gobierno de España; *Proyecto de Ley de Seguridad Nacional*, Boletín Oficial de las Cortes Generales, Senado, 31 de julio de 2015, art. 3. http://www.senado.es/legis10/publicaciones/pdf/senado/bocg/BOCG_T_10_574.PDF consulta: 23 de septiembre de 2015.

los países de nuestro entorno, que se ha demostrado válido hasta ahora y que ha permitido hacer frente a las necesidades de seguridad de una sociedad abierta, libre y democrática como la española. Sin embargo, en el mundo actual, y en el entorno más previsible para el futuro, los actores y circunstancias que ponen en peligro los niveles de seguridad, se encuentran sujetos a constante mutación, y es responsabilidad de los poderes públicos dotarse de la normativa, procedimientos y recursos que le permitan responder con eficacia a estos desafíos a la seguridad.

Se señala a continuación en este preámbulo que, en este contexto aparece el campo de la Seguridad Nacional como un espacio de actuación pública nuevo, enfocado a la armonización de objetivos, recursos y políticas ya existentes en materia de seguridad. Lo que no había sido aún objeto de una regulación normativa integral. Este esfuerzo de integración reviste tanta mayor importancia cuanto que la Seguridad Nacional debe ser considerada un objetivo compartido por las diferentes Administraciones, estatal, autonómica y local, los órganos constitucionales, en especial las Cortes Generales, el sector privado y la sociedad civil, dentro de los proyectos de las organizaciones internacionales de las que formamos parte.

Por otro lado, el preámbulo de la Ley de Seguridad Nacional apunta que la realidad demuestra que los desafíos para la Seguridad Nacional que afectan a la sociedad revisten en ocasiones una elevada complejidad, que desborda las fronteras de categorías tradicionales como la defensa, la seguridad pública, la acción exterior y la inteligencia, así como de otras más recientemente incorporadas a la preocupación por la seguridad, como el medio ambiente, la energía, los transportes, el ciberespacio y la estabilidad económica. De esta forma, la dimensión que adquieren ciertos riesgos y amenazas, su acusada transversalidad, o la combinación de estos rasgos con su naturaleza abierta e incierta, como sucede en las situaciones de interés para la Seguridad Nacional definidas por la presente ley, son factores que indican claramente que toda respuesta que implique a los distintos agentes e instrumentos de la Seguridad Nacional se verá reforzada y resultará más eficiente si se realiza de forma coordinada.

En este escenario, se señala que el superior interés nacional requiere mejorar la coordinación de las diferentes Administraciones Públicas, buscando marcos de prevención y respuesta que ayuden a resolver los problemas que plantea una actuación compartimentada, organizando a diversos niveles y de manera integral, la acción coordinada de los agentes e instrumentos al servicio de la Seguridad Nacional.

Finaliza el preámbulo explicando que la ley se dicta con el propósito de responder a la demanda, expresada por los agentes de la Seguridad Nacional integrados en las Administraciones Públicas, por el sector privado y por la sociedad en general. También se señala que la Ley de Seguridad Nacional no afecta a la regulación de los distintos agentes e instrumentos que ya son objeto de normas sectoriales específicas, sino que facilita su inserción armónica en el esquema de organización general, establecido por la Estrategia de Seguridad Nacional, de 31 de mayo de 2013, bajo la denominación de Sistema de Seguridad Nacional, y liderado por el Presidente del Gobierno[491].

La citada ley señala que los órganos competentes en materia de Seguridad Nacional son: las Cortes Generales; el Gobierno; el Presidente del Gobierno; los Ministros; el Consejo de Seguridad Nacional; y los Delegados del Gobierno en las Comunidades Autónomas y en las ciudades con Estatuto de Autonomía de Ceuta y Melilla[492].

6.2. EL SISTEMA DE SEGURIDAD NACIONAL

El Sistema de Seguridad Nacional, se define en la Ley de Seguridad Nacional como el conjunto de órganos, organismos, recursos y procedimientos, integrados en una estructura, que permite a los órganos competentes en materia de Seguridad Nacional ejercer sus funciones. En este Sistema de Seguridad Nacional se integran los componentes fundamentales siguiendo los mecanismos de enlace y coordinación que determine el Consejo de Seguridad Nacional, actuando bajo sus propias estructuras y

[491] *Ibídem*, preámbulo.

[492] *Ibídem*, art. 12.

procedimientos. En función de las necesidades, podrán asignarse cometidos a otros organismos y entidades, de titularidad pública o privada[493].

La estructura del Sistema de Seguridad Nacional incluye al Presidente del Gobierno, que dirige el Sistema asistido por el Consejo de Seguridad Nacional; al Departamento de Seguridad Nacional, que ejerce las funciones de Secretaría Técnica y órgano de trabajo permanente del Consejo de Seguridad Nacional y de sus órganos de apoyo; los órganos de apoyo del Consejo de Seguridad Nacional, con la denominación de Comités Especializados u otra que se determine, que ejercen las funciones asignadas por el Consejo de Seguridad Nacional en los ámbitos de actuación previstos en la Estrategia de Seguridad Nacional, o cuando las circunstancias propias de la gestión de crisis lo precisen[494].

Al Sistema de Seguridad Nacional le corresponde evaluar los factores y situaciones que puedan afectar a la Seguridad Nacional, recabar y analizar la información que permita tomar las decisiones necesarias para dirigir y coordinar la respuesta ante las situaciones de crisis contempladas en esta ley, detectar las necesidades y proponer las medidas sobre planificación y coordinación con el conjunto de las Administraciones Públicas, con el fin de garantizar la disponibilidad y el correcto funcionamiento de los recursos del Sistema[495].

Uno de los organismos del Sistema de Seguridad Nacional que cobra un protagonismo especial es el Consejo de Seguridad Nacional, que tiene condición de Comisión Delegada del Gobierno para la Seguridad Nacional, y 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 le atribuye

[493] *Ibídem*, art. 18.
[494] *Ibídem*, art. 20.
[495] *Ibídem*, art. 19.

la Ley de Seguridad Nacional y los que puedan asignársele por reglamento que se desarrolle[496].

Figura 54: Composición del Consejo de Seguridad Nacional

Forman parte del Consejo
Presidente del Gobierno
Vicepresidentes del Gobierno
Ministro de Asuntos Exteriores y de Cooperación
Ministro de Justicia
Ministro de Defensa
Ministro de Hacienda y Administraciones Públicas
Ministro del Interior
Ministro de Fomento
Ministro de Industria, Energía y Turismo
Ministro de Presidencia
Ministro de Economía y Competitividad
Ministro de Sanidad, Servicios Sociales e Igualdad
Director del Gabinete de la Presidencia del Gobierno
Secretario de Estado de Asuntos Exteriores
Jefe de Estado Mayor de la Defensa
Secretario de Estado de Seguridad
Secretario de Estado-Director del Centro Nacional de Inteligencia
Podrán formar parte del Consejo
En función de los asuntos a tratar, los titulares de los demás departamentos ministeriales y las autoridades autonómicas afectadas en la toma de decisiones y actuaciones a desarrollar por parte del Consejo
Los titulares de los órganos superiores y directivos de la Administración General del Estado, de los organismos públicos, de las Comunidades Autónomas y de las ciudades con Estatuto de Autonomía, así como las autoridades de la Administración Local, serán convocados a las reuniones del Consejo cuando su contribución se considere necesaria, y en todo caso cuando los asuntos a tratar afecten a sus respectivas competencias
Personas físicas o jurídicas cuya contribución se considere relevante a la vista de los asuntos a tratar en el orden del día
Será convocado al Consejo
Director del Departamento de Seguridad Nacional

Fuente: Ley de Seguridad Nacional[497].

[496] *Ibídem*, art. 17.

[497] *Ibídem*, art. 21.

Las funciones asignadas al Consejo de Seguridad Nacional son; a) Dictar las directrices necesarias en materia de planificación y coordinación de la política de Seguridad Nacional. b) Dirigir y coordinar las actuaciones de gestión de situaciones de crisis. c) Supervisar y coordinar el Sistema de Seguridad Nacional. d) Verificar el grado de cumplimiento de la Estrategia de Seguridad Nacional y promover e impulsar sus revisiones. e) Promover e impulsar la elaboración de las estrategias de segundo nivel que sean necesarias y proceder, en su caso, a su aprobación, así como a sus revisiones periódicas. f) Organizar la contribución de recursos a la Seguridad Nacional. g) Aprobar el Informe Anual de Seguridad Nacional antes de su presentación en las Cortes Generales. h) Acordar la creación y el fortalecimiento de los órganos de apoyo necesarios para el desempeño de sus funciones. i) Impulsar las propuestas normativas necesarias para el fortalecimiento del Sistema de Seguridad Nacional. j) Realizar las demás funciones que le atribuyan las disposiciones legales y reglamentarias que sean de aplicación[498].

6.3. LA ESTRATEGIA DE SEGURIDAD NACIONAL EN ESPAÑA.

La Ley de Seguridad Nacional señala que la Estrategia de Seguridad Nacional es 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, quien la somete a la aprobación del Consejo de Ministros, y se revisará cada cinco años o cuando lo aconsejen las circunstancias cambiantes del entorno estratégico. Una vez aprobada, la Estrategia de Seguridad Nacional será presentada en las Cortes Generales[499].

La Política de Seguridad Nacional es una política pública en la que bajo la dirección del Presidente del Gobierno y la responsabilidad del Gobierno, participan todas las Administraciones Públicas, de acuerdo con sus respectivas competencias, y la

[498] *Ibídem*, art. 21.

[499] *Ibídem*, art. 4.

sociedad en general, para responder a las necesidades de la Seguridad Nacional. Los principios básicos que orientarán la política de Seguridad Nacional son la unidad de acción, anticipación, prevención, eficiencia, sostenibilidad en el uso de los recursos, capacidad de resistencia y recuperación, coordinación y colaboración[500].

La ciberseguridad en la Estrategia Española de Seguridad de 2011

La primera Estrategia Española de Seguridad (EES) se aprobó por el Consejo de Ministros el 24 de junio de 2011[501]. En el resumen ejecutivo de la EES 2011se recoge que garantizar la seguridad de España y de sus habitantes y ciudadanos es responsabilidad esencial del Gobierno y del conjunto de las Administraciones Públicas, pero también de la sociedad, ya que la seguridad es responsabilidad de todos, que afrontamos amenazas y riesgos transversales, interconectados y transnacionales. De esta forma, preservar la seguridad requiere coordinación, tanto internacional como interna, y la contribución de la sociedad en su conjunto.

La EES 2011 señala que los límites entre la seguridad interior y la seguridad exterior se han difuminado. Las políticas nacionales en los ámbitos tradicionales de la seguridad ya no son suficientes para salvaguardarla en el siglo XXI. Sólo un enfoque integral, que conciba la seguridad de manera amplia e interdisciplinar, a nivel nacional, europeo e internacional, puede responder a los complejos retos a los que nos enfrentamos. Analizar las amenazas y riesgos a nuestra seguridad, identificar líneas de respuesta y definir mecanismos de coordinación son los objetivos centrales de esta primera Estrategia Española de Seguridad. La política de seguridad estará basada en seis conceptos básicos[502]:

- Enfoque integral de las diversas dimensiones de la seguridad.
- Coordinación entre las Administraciones Públicas y con la sociedad.

[500] *Ibídem*, art. 4.

[501] Gobierno de España: *Estrategia Española de Seguridad, una responsabilidad de todos*. Madrid, 24 de junio de 2011. http://www2.urjc.es/ceib/investigacion/publicaciones/REIB_05_01_Document03.pdf consulta: 19 de octubre de 2015.

[502] *Ibídem*, pp. 8-10.

- Eficiencia en el uso de los recursos.
- Anticipación y prevención de las amenazas y riesgos.
- Resistencia y recuperación de sistemas e instrumentos.
- Interdependencia responsable con nuestros socios y aliados.

El ciberespacio se incorpora a la EES 2011 al señalar los diferentes ámbitos en los que pueden materializarse que las amenazas y riesgos más importantes para la seguridad España, identificando: el terrestre, el marítimo, el aéreo, el espacial, el ciberespacio y el informativo. El ciberespacio se define en la EES 2011 como el "espacio virtual donde se agrupan y relacionan usuarios, líneas de comunicación, páginas web, foros, servicios de Internet y otras redes. Creado por el ser humano, es un entorno singular para la seguridad, sin fronteras geográficas, anónimo, asimétrico, que puede ser utilizado de forma casi clandestina y sin necesidad de desplazamientos. Es mucho más que la Red, pues incluye también dispositivos como los teléfonos móviles, la televisión terrestre y las comunicaciones por satélite"[503].

Las ciberamenazas aparecen recogidas en la EES 2011. Para ciudadanos y Gobiernos, el ciberespacio y las redes de información y comunicación son una fuente de nuevas posibilidades. Soportan la prestación de servicios ampliamente utilizados, como los buscadores de información, el correo electrónico, así como la gestión de muchas infraestructuras y servicios privados y un número cada vez mayor de servicios de las Administraciones Públicas. Pero precisamente este carácter crítico hace vital su protección y capacidad de resistencia y recuperación, y más preocupante su vulnerabilidad[504].

Se señala que la ciberseguridad no es un mero aspecto técnico de la seguridad, sino un eje fundamental de la sociedad y del sistema económico. Dada la cada vez mayor importancia de los sistemas informáticos en la economía, la estabilidad y prosperidad económica del país dependerá en buena medida de la seguridad del ciberespacio. Ésta puede verse comprometida por causas técnicas, fenómenos naturales o por

[503] *Ibídem*, pp. 34-36.
[504] *Ibídem*, p. 65.

ataques ilícitos. Los ciberataques son una amenaza en crecimiento con la que los posibles agresores -terroristas, crimen organizado, empresas, Estados o individuos aislados- podrían poner en dificultad infraestructuras críticas[505].

El ciberespacio es asimismo un ámbito para el espionaje por parte tanto de agentes criminales como de otros Estados. Si bien España también está expuesta, como el resto de países, a ciberataques de terroristas, otros tipos de delincuentes e incluso de otros Estados, los más comunes tienen fines comerciales. La obtención de información y de datos personales en la Red, a menudo para ser vendidos a terceros, es cada vez más preocupante. Más allá del coste económico, genera una pérdida de confianza entre los ciudadanos en los sistemas electrónicos de pago que podría tener un importante efecto desestabilizador en la economía[506].

Hay factores legales y tecnológicos que incrementan las posibilidades de que las ciberamenazas se materialicen. Entre los primeros, la ausencia de una legislación común o de seguridad global que permita una lucha más efectiva contra ellas. Tecnológicamente, Internet fue creado para ser útil y sencillo, no para ser seguro. La creciente interconexión de la Red, incluyendo necesariamente las infraestructuras, suministros y servicios críticos, incrementa los niveles de riesgos sobre éstos. El anonimato y la dificultad para rastrear los ciberataques son factores añadidos que entorpecen su neutralización. España es un nodo importante en muchas redes, por lo que garantizar la seguridad en este ámbito es de especial importancia para nuestro país. Para ello es necesario seguir impulsando la toma de conciencia y la formación sobre los riesgos, reforzando las políticas específicas y los procedimientos de seguridad en los sistemas de información y comunicaciones de ciudadanos, empresas e instituciones, y reduciendo la dependencia de la tecnología de seguridad de terceros países[507].

[505] *Ibídem*.

[506] *Ibídem*.

[507] *Ibídem*, pp. 65-66.

En relación a las líneas estratégicas de acción ligadas a la ciberseguridad, la EES 2011 señala que mejorar la seguridad en el ciberespacio pasa por fortalecer la legislación, sin poner en riesgo la privacidad, y fomentar la colaboración entre el sector público y el privado. Ya se están impulsando sistemas de certificación de carácter voluntario u obligatorio y desarrollando planes de contingencia. Además, hay que concienciar a las Administraciones Públicas, empresas y ciudadanos sobre los riesgos, mejorar la cooperación nacional e internacional y elaborar mapas de riesgos y catálogos de expertos, recursos y buenas prácticas. En esa línea, España ha fortalecido la seguridad de las infraestructuras y los servicios electrónicos de las Administraciones Públicas, dotándolas de una red de comunicaciones entre sí y con las instituciones europeas y las de otros Estados miembros[508].

La EES 2011 pone en valor que el Centro Criptológico Nacional (CCN), encuadrado en el CNI, dispone desde 2007 de su propia capacidad de respuesta para incidentes relacionados con la seguridad de la información. La herramienta principal de respuesta frente a las ciberamenazas son los Equipos de Respuesta ante Incidentes de Seguridad (CERT). El CCN-CERT elabora guías e instrucciones, ofrece soporte y coordinación y forma al personal de las Administraciones Públicas (General, Autonómica y Local). También certifica la seguridad de productos, acredita la seguridad de los sistemas, promueve el desarrollo de tecnología nacional de seguridad basada en mejores prácticas y facilita información sobre vulnerabilidades, alertas y avisos de nuevas amenazas a los sistemas de información[509].

Menciona también la EES 2011 que existen otros CERT en España, tanto nacionales como autonómicos o privados. El INTECO-CERT desarrolla servicios orientados a ciudadanos y empresas para fomentar la sensibilización y difusión de buenas prácticas en materia de seguridad de la información y de prevención y respuesta ante incidentes

[508] *Ibídem*, p. 66.

[509] *Ibídem*, p. 67.

de seguridad. El IRIS-CERT tiene como misión la protección de la RedIRIS y la red académica y de investigación nacional[510].

La Estrategia Española de Seguridad de 2011 recoge que para afianzar la seguridad nacional en el ciberespacio y en las redes de información y comunicaciones, se debe, a nivel nacional, crear más medios y coordinarlos mejor, con medidas destinadas a[511]:

- Invertir más en tecnologías de seguridad y en formación de personal especializado.
- Consolidar y ampliar las líneas de acción establecidas a este respecto en el Plan Nacional de Protección de Infraestructuras Críticas.
- Desarrollar el Esquema Nacional de Seguridad (cuyo objetivo es establecer la política de seguridad en la utilización de medios electrónicos), reforzar su aplicación y realizar auditorías que verifiquen la seguridad de los sistemas de la Administración.
- Desarrollar un mapa de riesgos y catálogos de expertos, recursos y buenas prácticas.
- Apoyar el desarrollo de empresas privadas nacionales en un sector estratégico como éste, en el que puede ser peligrosa la dependencia de empresas extranjeras.
- Impulsar una educación en seguridad en el uso del ciberespacio.
- Fomentar la formación y sensibilización acerca del desarrollo y la utilización segura de las nuevas tecnologías de la información, con iniciativas como la ya creada Oficina de Seguridad del Internauta (OSI) del INTECO.
- Promover el uso de estándares de seguridad y de la certificación de los productos y sistemas de información y comunicaciones, tanto en el ámbito público como en el privado.

[510] *Ibídem,* pp. 67-68.

[511] *Ibídem*, p. 68.

En el plano internacional, la EES 2011 estima necesario en el ámbito de la ciberseguridad[512]:

- Impulsar la cooperación para desarrollar acuerdos de control de las ciberarmas, tal y como ocurre con las nucleares.
- Luchar contra las ciberamenazas a escala europea, ampliando y consolidando los medios ya existentes[513].
- Homogeneizar la legislación penal de los Estados miembros de la UE en aspectos como el acceso ilegal al conjunto o una parte de los sistemas de información, la intromisión, interrupción, obstaculización o daño sobre un sistema de información, o la intromisión ilegal en sus datos.
- Ampliar la lucha contra la delincuencia cibernética más allá de la UE, dada la naturaleza global de las redes y sistemas de información.
- Mejorar el sistema en línea con lo avanzado por la estrategia y doctrina de la OTAN en este ámbito. Los esfuerzos aliados se han materializado en el acuerdo de un concepto y la futura elaboración de una política de ciberdefensa, así como en la creación de una Autoridad de Gestión y de un Centro de Respuesta ante Incidentes de Seguridad.

La Estrategia Española de Seguridad de 2011 se considera el primer documento que incorpora de modo integral la ciberseguridad en el esquema de la seguridad nacional, definiendo el ciberespacio como un ámbito donde pueden materializarse los riesgos y amenazas. Además, esta EES aporta líneas de acción estratégicas para afrontar los desafíos derivados de la ciberseguridad.

[512] *Ibídem*, p. 69.

[513] Se señala que En 2004 se creó la Agencia Europea de Seguridad de las Redes y de la Información (ENISA), con una doble finalidad: lograr que las redes y la información de la Unión alcancen un alto grado de seguridad y propiciar el desarrollo de una cultura de la seguridad de las redes y de la información en beneficio de toda la sociedad.

La ciberseguridad en la Estrategia de Seguridad Nacional de 2013

El 31 de mayo de 2013, el Consejo de Ministros aprobó la Estrategia de Seguridad Nacional (ESN), que sustituía a la Estrategia Española de Seguridad de 2011. Además, en ese mismo Consejo de Ministros se aprobó un Real Decreto, que modifica otro de 2011 que establecía las Comisiones Delegadas del Gobierno, con el fin de incluir entre las mismas al Consejo de Seguridad Nacional en su condición de Comisión Delegada para la Seguridad Nacional, presidido por el Presidente del Gobierno[514].

En la comunicación de la aprobación de la ESN se significa que se persevera en el enfoque integral de la Seguridad Nacional. Como instrumento de su tiempo, refleja los riesgos y amenazas que es necesario encarar en un mundo que está cambiando profunda y constantemente. En este sentido, se contempla el concepto de seguridad de una manera amplia acorde con estas transformaciones globales que afectan al Estado y a la vida diaria del ciudadano. La seguridad comprende ámbitos muy diversos y el carácter esencialmente transnacional y transversal de los riesgos y amenazas que comprometen la seguridad en nuestros días demandan respuestas completas[515].

La Estrategia de 2013 concibe la Seguridad Nacional de una forma amplia y global, por lo que incluye muy distintos ámbitos de actuación. Tradicionalmente, el concepto de Seguridad Nacional se ceñía a la defensa y la seguridad pública, pero hoy se extiende a nuevos actores y amenazas y, por ello, la Seguridad Nacional hace frente a nuevos riesgos como las ciberamenazas. En total, la Estrategia contempla hasta doce riesgos para la seguridad nacional: conflictos armados; terrorismo; ciberamenazas; crimen organizado; inestabilidad económica y financiera; vulnerabilidad energética; flujos migratorios irregulares; armas de destrucción masiva;

[514] Presidencia de Gobierno: *Aprobada la Estrategia de Seguridad Nacional de 2013*. Madrid, 31 de mayo de 2013. http://www.lamoncloa.gob.es/consejodeministros/Paginas/enlaces/310513Enlace%20%20seguridad.aspx consulta: 20 de octubre de 2015.

[515] *Ibídem.*

espionaje; emergencias y catástrofes naturales; vulnerabilidad del espacio marítimo y vulnerabilidad de las infraestructuras críticas y servicios esenciales[516].

Es significativo señalar que esta comunicación resalta que la Estrategia de Seguridad Nacional de 2013, coordinada por el Departamento de Seguridad Nacional de la Presidencia del Gobierno, es una revisión de la Estrategia aprobada en 2011 por el anterior Ejecutivo, y que cuenta con el respaldo político del principal partido de la oposición. Señala a continuación la comunicación que el objetivo del Gobierno es reforzar y hacer extensible a todos, este consenso político y social, porque se trata de una verdadera política de Estado[517].

Otra novedad es que también se proponen líneas concretas de acción estratégica y objetivos a alcanzar. La finalidad es mejorar la prevención y la capacidad de reacción ante estos nuevos riesgos y amenazas. En este sentido, señala Martín Cubel que nuestra seguridad aspira a ser transversal, flexible, con una profunda capacidad de adaptación y coordinación, que priorice acciones y respuestas multilaterales y cooperativas, capaz de diferenciar los riesgos inmediatos de aquellos otros que suscitan una perspectiva de análisis a medio y largo plazo y que inciden en nuestras opciones estratégicas y recursos, en la sociedad y en la estabilidad institucional[518].

Además, la Estrategia prevé un sistema institucional flexible para potenciar la actuación coordinada de los instrumentos existentes en el campo de la seguridad. Este sistema estará liderado por el presidente del Gobierno y se apoyará en el nuevo Consejo de Seguridad Nacional, que será un órgano colegiado del Gobierno, que

---

[516] *Ibídem.*

[517] *Ibídem.*

[518] MARTÍN CUBEL, Fernando: *ESN-2013: Propuesta de Sistema de Seguridad Nacional*. Instituto Español de Estudios Estratégicos.Documento Opinión 118/2013. 02 diciembre de 2013, pp. 3-4. http://www.ieee.es/Galerias/fichero/docs_opinion/2013/DIEEEO118-2013_Prop.SisteSegNacional_FdoMartinCubel.pdf consultado 28 de julio de 2015.

responde al Programa de Reformas del Gobierno y que nace con la vocación de administrar de una forma más eficaz y eficiente los recursos existentes[519].

Este Consejo de Seguridad Nacional estará presidido por el Presidente del Gobierno, excepto cuando S.M. el Rey asista a sus reuniones. Se reunirá periódicamente, al menos una vez cada dos meses, y cuantas veces lo demanden las circunstancias. Además de la Presidencia, el Consejo estará compuesto por los siguientes miembros: Vicepresidente del Gobierno; Ministro de Asuntos Exteriores y Cooperación; Ministro de Defensa; Ministro de Hacienda y Administraciones Públicas; Ministro de Interior; Ministro de Fomento; Ministro de Industria, Energía y Turismo; Ministro de Economía y Competitividad; Director del Gabinete de la Presidencia del Gobierno, que actuará como secretario; Secretario de Estado de Asuntos Exteriores; Jefe de Estado Mayor de la Defensa; Secretario de Estado de Seguridad; Secretario de Estado Director del Centro Nacional de Inteligencia; y Responsable del Departamento de Seguridad Nacional[520].

En lo relativo a la estructura de la Estrategia, el documento cuenta con cinco capítulos[521]:

El capítulo 1 ofrece un concepto de Seguridad Nacional integral acorde con los riesgos y amenazas actuales.

El capítulo 2 sitúa la seguridad de España en el mundo y presenta las grandes prioridades estratégicas de España como Estado diverso y plural.

El capítulo 3 identifica los principales riesgos y amenazas para la Seguridad Nacional.

---

[519] Presidencia de Gobierno: *Aprobada la Estrategia de Seguridad Nacional de 2013, opus citada.*

[520] Gobierno de España: *Real Decreto 385/2013, de 31 de mayo, de modificación del Real Decreto 1886/2011, de 30 de diciembre, por el que se establecen las Comisiones Delegadas del Gobierno*. http://www.boe.es/diario_boe/txt.php?id=BOE-A-2013-5771 consulta: 20 de octubre de 2015.

[521] Presidencia de Gobierno: *Aprobada la Estrategia de Seguridad Nacional de 2013. Opus citada.*

El capítulo 4 define los ámbitos de actuación prioritarios en materia de Seguridad Nacional a la luz de los riesgos y amenazas que nos afectan.

El capítulo 5 define el Sistema de Seguridad Nacional que potenciará la actuación coordinada de las Administraciones en un uso eficiente y racional de los recursos actuales.

En la carta de presentación de la ESN 2013, el Presidente del Gobierno escribe que a los riesgos y amenazas tradicionales se suman, en efecto, otros nuevos de naturaleza generalmente transnacional, que se interconectan y potencian su peligrosidad, a la vez que aparecen nuevos espacios abiertos que facilitan su expansión e impacto. "El ciberespacio es hoy el ejemplo más claro de un ámbito accesible, poco regulado y de difícil control, y en consonancia, la ciberseguridad es uno de los principales ámbitos de actuación de esta Estrategia" [522].

La ESN 2013 recoge que el ciberespacio es un nuevo ámbito de relación que ha proporcionado el desarrollo de las nuevas tecnologías de la información y las comunicaciones, ha diluido las fronteras, permitiendo una globalización sin precedentes, que propicia nuevas oportunidades, pero conlleva serios riesgos y amenazas. La dependencia de la sociedad del ciberespacio y su fácil accesibilidad hacen que cada vez sean más comunes y preocupantes las intromisiones en este ámbito. En buena medida, el ciberespacio es un medio para la materialización de otros riesgos y amenazas. Los ciberataques, ya sean en sus modalidades de ciberterrorismo, ciberdelito/cibercrimen, ciberespionaje o hacktivismo, se han convertido en un potente instrumento de agresión contra particulares e instituciones públicas y privadas. El bajo coste y mínimo riesgo que suponen para el atacante y su

[522] Gobierno de España: *Estrategia de Seguridad Nacional, un proyecto compartido*. Madrid, 31 de mayo de 2013.
http://www.lamoncloa.gob.es/documents/seguridad_1406connavegacionfinalaccesiblebpdf.pdf
consulta: 20 de coctubre de 2015.

fácil empleo, efectividad y accesibilidad, son factores que explican la extensión del fenómeno[523].

Continúa la Estrategia de Seguridad Nacional que los ataques ilícitos en el ámbito del ciberespacio proceden de grupos terroristas, redes de crimen organizado, empresas, Estados o individuos aislados. También la ciberseguridad se puede ver comprometida por causas técnicas o fenómenos naturales. Estas circunstancias explican que sea un objetivo prioritario garantizar la integridad, confidencialidad y disponibilidad de los sistemas que soportan la prestación de servicios ampliamente utilizados, así como la gestión de las infraestructuras críticas. La ausencia de una legislación armonizada en materia de ciberseguridad, así como el hecho de que Internet fuera diseñado como un canal de comunicación accesible, sencillo y útil, sin considerar la dimensión de su seguridad, son elementos que incrementan las posibilidades de que las ciberamenazas se materialicen. España 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[524].

En relación con los riesgos y amenazas que se ciernen sobre las infraestructuras críticas españolas, señala la ESN que su origen puede ser natural o inducido por errores humanos o fallos tecnológicos inesperados. Sin embargo, son los que se causan deliberadamente, bien por una agresión de carácter físico o por un ataque cibernético, los que revisten mayor peligrosidad, puesto que su móvil y objetivos consisten en ocasionar un daño grave a España y a sus ciudadanos[525].

En relación con la ciberseguridad, con el objetivo de garantizar un uso seguro de las redes y los sistemas de información a través del fortalecimiento de nuestras

[523] *Ibídem,* p. 26.
[524] *Ibídem,* p. 27.
[525] *Ibídem,* p. 37.

capacidades de prevención, detección y respuesta a los ciberataques, la ESN 2013 diseña seis líneas de acción estratégicas[526].

Figura 55: Líneas de acción estratégicas de la Estrategia de Seguridad Nacional de 2013 en el ámbito de la ciberseguridad

1. Incremento de la capacidad de prevención, detección, investigación y respuesta ante las ciberamenazas con apoyo en un marco jurídico operativo y eficaz. Se mejorarán los procedimientos y se impulsarán los recursos necesarios con especial énfasis en las Administraciones Públicas, las infraestructuras críticas, las capacidades militares y de defensa y todos aquellos sistemas de interés nacional.
2. Garantía de la seguridad de los sistemas de información y las redes de comunicaciones e infraestructuras comunes a todas las Administraciones Públicas. Se finalizará la implantación del Esquema Nacional de Seguridad, previsto en la Ley 11/2007, de 22 de junio, mediante el refuerzo de las capacidades de detección y la mejora de la defensa de los sistemas clasificados. Se fortalecerá la seguridad de los sistemas de información y las redes de comunicaciones que soportan las infraestructuras críticas. Se impulsará la normativa sobre protección de infraestructuras críticas con el desarrollo de las capacidades necesarias para la protección de los servicios esenciales.
3. Mejora de la seguridad y resiliencia de las Tecnologías de la Información y la Comunicación (TIC) en el sector privado a través del uso de las capacidades de los poderes públicos. Se impulsarán y liderarán actuaciones destinadas a reforzar la colaboración público-privada y la seguridad y robustez de las redes, productos y servicios de las TIC empleados por el sector industrial.
4. Promoción de la capacitación de profesionales en ciberseguridad e impulso a la industria española a través de un Plan de I+D+i.
5. Implantación de una cultura de ciberseguridad sólida. Se concienciará a los ciudadanos, profesionales y empresas de la importancia de la seguridad de la información y del uso responsable de las nuevas tecnologías y de los servicios de la sociedad del conocimiento.
6. Intensificación de la colaboración internacional. Se promoverán los esfuerzos tendentes a conseguir un ciberespacio internacional donde se alineen las iniciativas de todos los países que persiguen un entorno seguro y fiable. En todo momento se salvaguardarán los intereses nacionales.

Fuente: Estrategia de Seguridad Nacional, un proyecto compartido[527].

[526] *Ibídem,* p. 42.

[527] *Ibídem.*

6.4. LA ESTRATEGIA NACIONAL DE CIBERSEGURIDAD EN ESPAÑA.

El Consejo de Seguridad Nacional presidido por el Presidente del Gobierno, aprobó el 5 de diciembre de 2013 la Estrategia de Ciberseguridad Nacional y la Estrategia de Seguridad Marítima Nacional. Señala la comunicación del Gobierno que los trabajos, coordinados por el Departamento de Seguridad Nacional de la Presidencia del Gobierno, son fruto de un proceso de elaboración en el que han participado diversos ministerios y organismos. Estos documentos establecen la orientación estratégica para la acción coordinada y eficaz de las Administraciones Públicas en dos ámbitos que revisten una importancia crítica para la seguridad nacional[528].

Indica la comunicación del Gobierno que la Estrategia de Ciberseguridad Nacional responde a la creciente necesidad de preservar la seguridad del ciberespacio por su enorme repercusión en cuestiones que afectan a la seguridad nacional, así como a la competitividad de nuestra economía y, en general, al progreso y prosperidad de nuestra sociedad. La Estrategia delimita el entorno del ciberespacio, fija principios, objetivos y líneas de acción para el logro de la ciberseguridad nacional, y define el marco de coordinación de la política de ciberseguridad[529].

El Consejo de Seguridad Nacional decidió crear dos órganos colegiados de apoyo al presidente del Gobierno y al propio Consejo para la puesta en marcha de las nuevas Estrategias. El Gobierno estima que estos nuevos órganos contribuirán a mejorar la prevención y respuesta ante los riesgos y amenazas a la seguridad nacional en sus ámbitos respectivos, y les asignó la denominación de Consejo de Ciberseguridad Nacional y Consejo de Seguridad Marítima Nacional[530].

---

[528] Gobierno de España: *Reunión del Consejo de Seguridad Nacional*. Madrid, 5 de diciembre de 2013. http://www.lamoncloa.gob.es/presidente/actividades/Paginas/2013/051213CSN.aspx consulta: 20 de octubre de 2015.

[529] *Ibídem*.

[530] *Ibídem*.

Se decidió que la presidencia de los Consejos de Ciberseguridad Nacional y de Seguridad Marítima Nacional fuera rotatoria, y con periodicidad anual. El nivel de representación en ambos órganos se definió en los niveles de secretario de Estado o subsecretario. En el Consejo de Ciberseguridad Nacional la presidencia debe entre representantes de los Ministerios de la Presidencia, del Interior, de Industria, Energía y Turismo, de Defensa y de Asuntos Exteriores y de Cooperación[531].

También se decidió la creación de un tercer órgano colegiado dependiente del Consejo de Seguridad Nacional. Este órgano facilitará la dirección político-estratégica de aquellas situaciones de crisis que, por su transversalidad o su dimensión, desborden las capacidades de los departamentos y organismos responsables. Recibe la denominación de Comité de Situación y es el único para todos los ámbitos de la Seguridad Nacional. El Departamento de Seguridad Nacional, en su condición de Secretaría Técnica y órgano de trabajo permanente del Consejo de Seguridad Nacional, debe ejercer las funciones de Secretaría de los Consejos y brindar el soporte técnico al Comité Especializado de Situación[532].

La Estrategia de Ciberseguridad Nacional es el documento estratégico que sirve de fundamento al Gobierno de España para desarrollar las previsiones de la Estrategia de Seguridad Nacional en materia de protección del ciberespacio con el fin de implantar de forma coherente y estructurada acciones de prevención, defensa, detección, respuesta y recuperación frente a las ciberamenazas[533].

La Estrategia consta de cinco capítulos. **El primer capítulo** "**El ciberespacio y su seguridad"**, pone de manifiesto que el desarrollo de las Tecnologías de Información y Comunicación (TIC) ha generado un nuevo espacio de relación en el que la rapidez y facilidad de los intercambios de información y comunicaciones han eliminado las barreras de distancia y tiempo. El ciberespacio ha venido a difuminar fronteras,

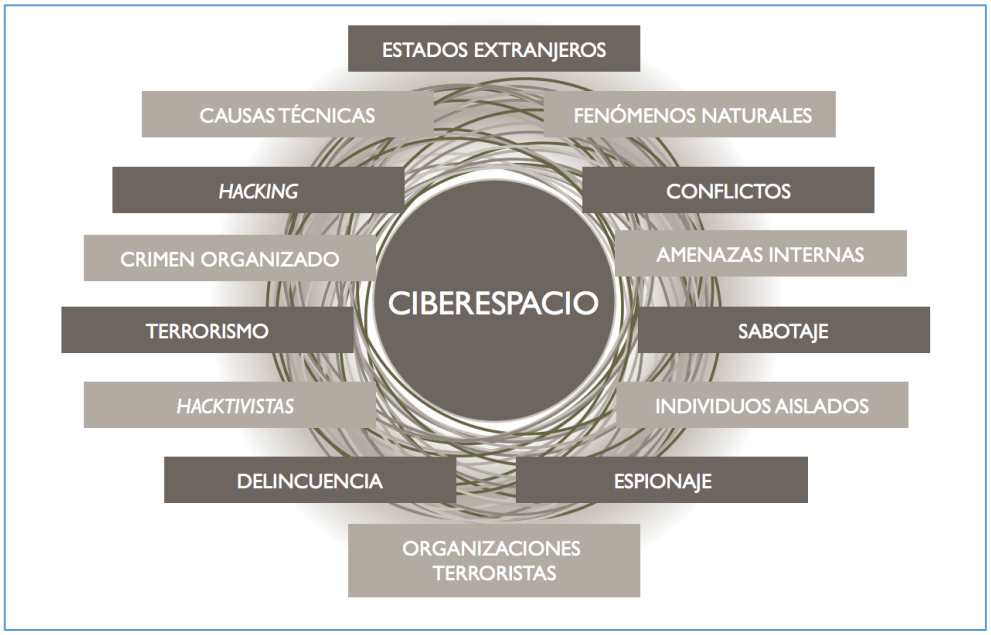
[531] *Ibídem*.

[532] *Ibídem*.

[533] Gobierno de España: *Estrategia de Ciberseguridad Nacional*. Madrid, 5 de diciembre de 2015. http://www.lamoncloa.gob.es/documents/20131332estrategiadeciberseguridadx.pdf consulta: 20 de octubre de 2015.

haciendo partícipes a sus usuarios de una globalización sin precedentes que propicia nuevas oportunidades, a la vez que comporta nuevos retos, riesgos y amenazas. El grado de dependencia de nuestra sociedad respecto de las TIC y el ciberespacio crece día a día. Conocer sus amenazas, gestionar los riesgos y articular una adecuada capacidad de prevención, defensa, detección, análisis, investigación, recuperación y respuesta constituyen elementos esenciales de la Política de Ciberseguridad Nacional[534].

Figura 56: Riesgos y Amenazas a la Ciberseguridad Nacional



Fuente: Estrategia de Ciberseguridad Nacional[535].

El **segundo capítulo "Propósito y principios rectores de la ciberseguridad en España"**, recoge que el propósito de la Estrategia de Ciberseguridad Nacional es fijar las directrices generales del uso seguro del ciberespacio, impulsando una visión integradora cuya aplicación ayude a garantizar a nuestra nación su seguridad y progreso, a través de la adecuada coordinación y cooperación de todas las

[534] *Ibídem*, p. 9.

[535] *Ibídem*, p. 11.

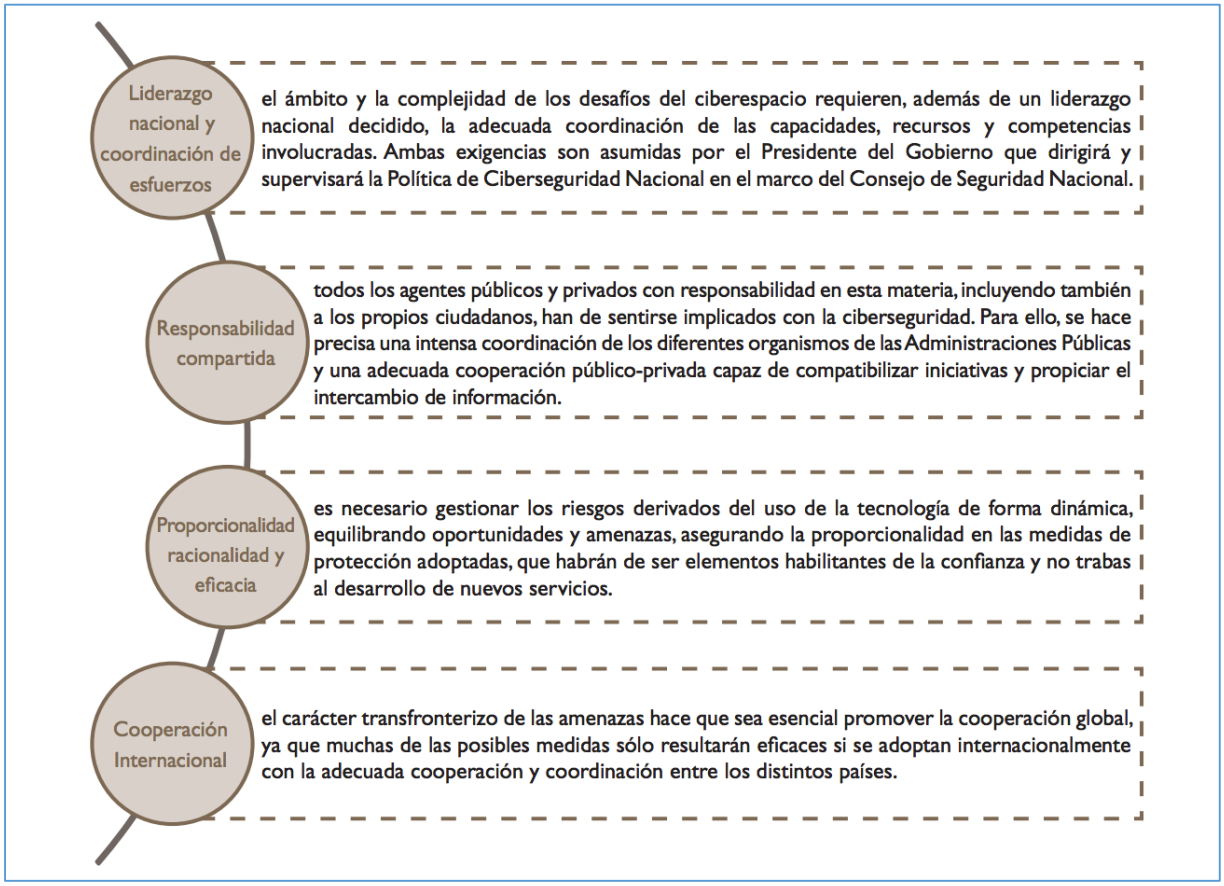
Administraciones Públicas entre ellas, con el sector privado y con los ciudadanos. Todo ello dentro del máximo respeto a los principios recogidos en la Constitución; en las disposiciones de la Carta de Naciones Unidas, relativas al mantenimiento de la paz y seguridad internacional; en coherencia con la Estrategia de Seguridad Nacional y con iniciativas desarrolladas en el marco europeo, internacional y regional[536].

Por lo que se refiere a los principios rectores de la ciberseguridad, se recogen el liderazgo nacional y la coordinación de esfuerzos; la responsabilidad compartida; la proporcionalidad, racionalidad y eficacia; y la cooperación internacional como extensión de los principios informadores de la Estrategia de Seguridad Nacional. Estos principios subrayan la necesaria planificación de desarrollo del contexto actual haciendo especial hincapié en la protección de los valores constitucionales como elemento común[537].

[536] *Ibídem*, p. 15.

[537] *Ibídem*, p. 16.

Figura 57: Principios rectores de la ciberseguridad en España



Fuente: Estrategia de Ciberseguridad Nacional[538].

En el **tercer capítulo "Objetivos de la ciberseguridad"** la Estrategia aborda, con un nivel creciente de detalle, los Objetivos de la ciberseguridad. Como objetivo global se establece lograr que España haga un uso seguro de los Sistemas de Información y Telecomunicaciones, fortaleciendo las capacidades de prevención, defensa, detección, análisis, investigación, recuperación y respuesta a los ciberataques. A este fin debe servir la Política de Ciberseguridad Nacional. Seguidamente, la Estrategia fija seis objetivos específicos.

[538] *Ibídem*, p. 16.

Figura 58: Objetivos específicos de la ciberseguridad en España

1. Para las Administraciones Públicas, garantizar que los Sistemas de Información y Telecomunicaciones utilizadas por estas poseen el adecuado nivel de seguridad y resiliencia.
2. Para las empresas y las infraestructuras críticas, impulsar la seguridad y la resiliencia de las redes y los sistemas de información usados por el sector empresarial en general y los operadores de infraestructuras críticas en particular.
3. En el ámbito judicial y policial, potenciar las capacidades de prevención, detección, respuesta, investigación y coordinación frente a las actividades del terrorismo y la delincuencia en el ciberespacio.
4. En materia de sensibilización, concienciar a los ciudadanos, profesionales, empresas y Administraciones Públicas españolas de los riesgos derivados del ciberespacio.
5. En capacitación, alcanzar y mantener los conocimientos, habilidades, experiencia y capacidades tecnológicas que necesita España para sustentar todos los objetivos de la ciberseguridad.
6. En lo que se refiere a la colaboración internacional, contribuir en la mejora de la ciberseguridad, apoyando el desarrollo de una política de ciberseguridad coordinada en la Unión Europea y en las organizaciones internacionales, así como colaborar en la capacitación de Estados que lo necesiten a través de la política de cooperación al desarrollo.

Fuente: Estrategia de Ciberseguridad Nacional[539].

El capítulo cuarto "Líneas de acción de la ciberseguridad nacional" especifica las

Para alcanzar los objetivos señalados, la Estrategia de Ciberseguridad Nacional se articula a través de ocho Líneas de Acción que con carácter interdependiente y vinculadas a los objetivos establecidos en el capítulo precedente, orienta la acción dirigida a alcanzar los objetivos expuestos[540].

[539] *Ibídem*, pp. 22-27.

[540] *Ibídem*, pp. 31-39.

Figura 59: Líneas de Acción de la Ciberseguridad Nacional

LÍNEA DE ACCIÓN		CONTENIDO
1	Capacidad de prevención, detección, respuesta y recuperación ante las ciberamenazas	Incrementar las capacidades de prevención, defensa, detección, análisis, respuesta, recuperación 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 y Telecomunicaciones que soportan 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 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 en materia de 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.

Fuente: Estrategia de Ciberseguridad Nacional[541].

[541] *Ibídem,* p. 40.

El **quinto capítulo "La ciberseguridad en el Sistema de Seguridad Nacional"** está dedicado a La ciberseguridad en el Sistema de Seguridad Nacional y establece la estructura orgánica al servicio de la ciberseguridad. Bajo la dirección del Presidente del Gobierno, la estructura se compone de tres órganos: uno ya existente, el Consejo de Seguridad Nacional, como Comisión Delegada del Gobierno para la Seguridad Nacional; y dos nuevos: el Comité Especializado de Ciberseguridad, que dará apoyo al Consejo de Seguridad Nacional prestando asistencia a la dirección y coordinación de la Política de Seguridad Nacional en materia de ciberseguridad, así como fomentando la coordinación, cooperación y colaboración entre Administraciones Públicas y entre éstas y el sector privado y el Comité Especializado de Situación, que, con apoyo del Centro de Situación del Departamento de Seguridad Nacional, gestionará las situaciones de crisis de ciberseguridad que, por su transversalidad o su dimensión, desborden las capacidades de respuesta de los mecanismos habituales. Los dos Comités Especializados actuarán de forma complementaria[542].

Figura 60: Estructura orgánica de la ciberseguridad nacional

Fuente: Estrategia de Ciberseguridad Nacional[543].

[542] *Ibídem*, pp. 4-5.

[543] *Ibídem*, p. 43.

La estructura orgánica de la ciberseguridad nacional se define como sigue[544]:

a) **Consejo de Seguridad Nacional**:

El Consejo de Seguridad Nacional configurado como Comisión Delegada del Gobierno para la Seguridad Nacional, asiste al Presidente del Gobierno en la dirección de la Política de Seguridad Nacional.

b) **Comité Especializado de Ciberseguridad**:

El Comité Especializado de Ciberseguridad dará apoyo al Consejo de Seguridad Nacional para el cumplimiento de sus funciones y, en particular, en la asistencia al Presidente del Gobierno en la dirección y coordinación de la Política de Seguridad Nacional en el ámbito de la ciberseguridad. Además, reforzará las relaciones de coordinación, colaboración y cooperación entre las distintas Administraciones Públicas con competencias en materia de ciberseguridad, así como entre los sectores públicos y privados, y facilitará la toma de decisiones del propio Consejo mediante el análisis, estudio y propuesta de iniciativas tanto en el ámbito nacional como en el internacional.

La composición del Comité Especializado de Ciberseguridad reflejará el espectro de los ámbitos de los departamentos, organismos y agencias de las Administraciones Públicas con competencias en materia de ciberseguridad, para coordinar aquellas actuaciones que se deban abordar de forma conjunta con el fin de elevar los niveles de seguridad.

En el Comité podrán participar otros actores relevantes del sector privado y especialistas cuya contribución se considere necesaria. En el cumplimiento de sus funciones el Comité Especializado de Ciberseguridad será apoyado por el

[544] *Ibídem*, p. 44-45.

Departamento de Seguridad Nacional en su condición de Secretaría Técnica y órgano de trabajo permanente del Consejo de Seguridad Nacional.

c) Comité Especializado de Situación:

El Comité Especializado de Situación será convocado para llevar a cabo la gestión de las situaciones de crisis en el ámbito de la ciberseguridad que, atendiendo a la acentuada transversalidad o dimensión e impacto de sus efectos, produzcan el desbordamiento de los límites de capacidad de respuesta eficaz por parte de los mecanismos habituales previstos, siempre respetando las competencias asignadas a las distintas Administraciones Públicas y a los efectos de garantizar una respuesta inmediata y eficaz a través de un solo órgano de dirección político-estratégica de la crisis.

El Comité Especializado de Ciberseguridad y el Comité Especializado de Situación actuarán de forma complementaria, cada uno en su ámbito de competencias, pero bajo la misma dirección estratégica y política del Consejo de Seguridad Nacional presidido por el Presidente del Gobierno.

El Comité Especializado de Situación será apoyado por el Centro de Situación del Departamento de Seguridad Nacional con el fin de garantizar su interconexión con los centros operativos implicados y dar una respuesta adecuada en situaciones de crisis, facilitando su seguimiento y control y la trasmisión de las decisiones.

Para el cumplimiento eficaz de sus funciones de apoyo al Comité Especializado de Situación, el Centro de Situación del Departamento de Seguridad Nacional podrá ser reforzado por personal especializado proveniente de los departamentos ministeriales u organismos competentes, los cuales conformarán la Célula de Coordinación específica en el ámbito de la Ciberseguridad.

Félix Arteaga y Enrique Fojón Chamorro realizan una reflexión que pone en valor la aparición de las Estrategias de Seguridad de carácter nacional en relación con la ciberseguridad, señalando que la primera de ellas incluyó en 2011 las ciberamenazas y los ciberataques entre los riesgos principales para la seguridad nacional, al igual que la vigente aprobada en 2013. La Estrategia de Ciberseguridad Nacional viene a facilitar la incorporación a la gobernanza. Del mismo modo, desde el punto de vista operativo nuestro país dispone de varios *Centros de Respuesta ante Incidencias Informáticas* (CERT) nacionales y autonómicos, un *Mando Conjunto de Ciberdefensa* de las Fuerzas Armadas, una *Dirección General de Tecnologías de la Información y Comunicación* de la Administración General del Estado y una *Oficina de Coordinación Cibernética* en el Centro Nacional de Protección de Infraestructuras Críticas. Además, el gobierno parece haber identificado la necesidad de disponer de un sector e industria de ciberseguridad de primer nivel, tal y como refleja en el Plan de Confianza en el ámbito Digital[545].

Llaman la atención Arteaga y Fojón sobre que la gobernanza tiende a consolidarse tras decidir el Gobierno, a principios de 2015, acabar con el sistema de rotación que afectaba a la dirección de la ciberseguridad y residenciar la presidencia del Consejo de Ciberseguridad en el Centro Nacional de Inteligencia (CNI). La dirección única actual bajo el CNI ofrece mejores oportunidades de gobernanza y desarrollo a la ciberseguridad que la rotación anterior por los diferentes ministerios y agencias[546].

En este sentido se manifiesta la Secretaria General del Centro Nacional de Inteligencia, al ser preguntada en una entrevista en la revista SIC por las razones por las que, en razón de su cargo de Secretario de Estado Director del CNI, sigue siendo Presidente del Consejo Nacional de Ciberseguridad, cuando en principio dicha posición iba a ser rotatoria entre CNI, Interior, Defensa, Industria y Exteriores. La

[545] ARTEAGA, Félix y FOJÓN CHAMORRO, Enrique: *En favor de una política nacional de ciberseguridad en España*. Real Instituto Elcano, 23 de marzo de 2015. http://www.realinstitutoelcano.org/wps/portal/web/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/comentario-arteaga-fojon-en-favor-de-una-politica-nacional-de-ciberseguridad-en-espana consulta: 20 de octubre de 2015.

[546] *Ibídem.*

Secretaria General del CNI manifiesta que no ha sido una decisión que haya tomado el propio CNI, sino que le correspondía adoptarla a Presidencia del Gobierno. Aclara la Secretaria General que los argumentos que se han manejado dentro del Consejo Nacional de Ciberseguridad para aconsejar la prórroga han sido, fundamentalmente, dotar de mayor estabilidad y dirección a este organismo. Había, entre las instituciones que conforman el Consejo, un consenso amplio en torno a la necesidad de una dirección única que pudiese impulsar el Plan nacional y los planes derivados que se están llevando a cabo. Sobre todo, teniendo en cuenta el estado de desarrollo de la Estrategia y la gravedad de la amenaza a la que nos enfrentamos[547].

Opinan además Arteaga y Fojón que las funciones de la nueva política sujetas a la gobernanza actual –seguridad de la información, gestión de crisis, análisis de riesgos, defensa y explotación y la resiliencia– son adecuadas para afrontar la ciberseguridad desde la perspectiva de los riesgos. Más allá de los peligros, el ciberespacio ofrece oportunidades para crear un tejido industrial innovador, empleos de calidad y capacitación tecnológica. Una visión más amplia debería desarrollar instrumentos de demanda pública, definir prioridades en I+D+i, incentivar las inversiones y crear centros de excelencia, entre otros, para que en España se pase de consumir a producir ciberseguridad[548].

6.5. EL DESARROLLO DE LA ESTRATEGIA NACIONAL DE CIBERSEGURIDAD.

María del Mar López, Jefa de la Oficina de Seguridad del Departamento de Seguridad Nacional, aborda las líneas principales del Plan Nacional de Ciberseguridad[549]. López lo enmarca en una hoja de ruta que incluye los siguientes hitos:

[547] MÉNDEZ DE VIGO, Beatriz: *Entrevista en revista SIC*. Revista SIC, Ciberseguridad, Seguridad de la Información y Privacidad nº 115, junio de 2015, p. 71.

[548] ARTEAGA, Félix y FOJÓN CHAMORRO, Enrique: *En favor de una política nacional de ciberseguridad en España, Opus citada.*

[549] LÓPEZ, María del Mar: *Plan Nacional de Ciberseguridad*, Ponencia en la II Jornada de Ciberseguridad en Andalucía, Sevilla, 8 de junio de 2015. http://www.slideshare.net/Ingenia_es/mara-del-mar-lpezcibersegand15 consulta: 19 de octubre de 2015.

Figura 61: Hoja de ruta de la ciberseguridad en España.

Fuente: López, María del Mar: Plan Nacional de Ciberseguridad[550].

Señala López que la misión del Plan Nacional de Ciberseguridad es lograr que España haga un uso seguro de los sistemas de información y telecomunicaciones, fortaleciendo las capacidades de prevención, defensa, detección, recuperación y

[550] *Ibídem.*

respuesta a los ciberataques, mediante el cumplimiento de los objetivos recogidos en la Estrategia de Ciberseguridad Nacional. Este plan Nacional asigna los cometidos y nivel de implicación a los órganos y organismos representados en el Consejo Nacional de Ciberseguridad; identifica los planes de acción derivados; plantea mecanismos para determinar los recursos necesarios; y establece las estructuras de coordinación y control[551].

López identifica además los nueve Planes Derivados del Plan Nacional de Ciberseguridad, que incorporan ejes de acción, que a su vez se dividen en acciones y tareas.

Figura 62: Planes Derivados del Plan Nacional de Ciberseguridad

Plan de fortalecimiento y potenciación de Capacidades y aseguramiento de la Cooperación para la Ciberseguridad y la Ciberdefensa
Plan de seguridad de los sistemas de información y telecomunicaciones que soportan las Administraciones Públicas
Plan de protección y resiliencia de los sistemas de información y telecomunicaciones que soportan las infraestructuras críticas
Plan contra la ciberdelincuencia y el ciberterrorismo
Plan de protección y resiliencia de las TIC en el sector privado
Plan de impulso al desarrollo industrial, capacitación de los profesionales y refuerzo de la I+D+i en materia de ciberseguridad
Plan de cultura de ciberseguridad
Plan de cooperación internacional y Unión Europea
Plan para el Intercambio de información sobre ciberamenazas

Fuente: Fuente: López, María del Mar: Plan Nacional de Ciberseguridad[552].

[551] *Ibídem.*

[552] *Ibídem.*

Señala López que el Departamento de Seguridad Nacional lidera el Plan de Cultura de Ciberseguridad, que contempla los siguientes objetivos[553]:

- Desarrollar contenidos dirigidos a la educación primaria, universitaria y de profesionales
- Incrementar la cultura de ciberseguridad a distintos niveles: altos cargos, profesionales y ciudadanos.
- Creación de foros dirigidos a grandes empresas, pymes, profesionales, Administración Pública y ciudadanos.
- Apoyar la creación y desarrollo de foros internacionales.
- Desarrollar buenas prácticas sobre el uso seguro de la tecnología.

El Ministerio de Asuntos Exteriores y de Cooperación, señala en su página web[554] que el Consejo Nacional de Ciberseguridad aprobó en 2014 el Plan Nacional de Ciberseguridad, donde se encuentran las líneas de acción para desarrollar la Estrategia de Ciberseguridad Nacional durante los dos próximos años. En concreto, el MAEC tiene una responsabilidad especial en la aplicación de la línea de acción número 8: "Compromiso Internacional. Promover un ciberespacio internacional seguro y confiable, en apoyo a los intereses nacionales".

Los objetivos específicos de dicha línea de acción, que reproduce los contenidos en Estrategia de Ciberseguridad Nacional, son los siguientes:

- Potenciar la presencia de España en organizaciones y foros internacionales y regionales sobre ciberseguridad, apoyando y participando activamente en las diversas iniciativas y coordinando la posición de los agentes nacionales implicados.

[553] *Ibídem.*

[554] Ministerio de Asuntos Exteriores y de Cooperación: *El MAEC y la Ciberseguridad*. http://www.exteriores.gob.es/Portal/es/PoliticaExteriorCooperacion/Ciberseguridad/Paginas/El-MAEC-y-la-Ciberseguridad.aspx consulta: 25 de octubre de 2015.

- Promover la armonización legislativa y la cooperación judicial y policial internacionales en la lucha contra la ciberdelincuencia y el ciberterrorismo, apoyando la negociación y la adopción de convenios internacionales en la materia.

- Propiciar la conclusión de acuerdos internacionales para fortalecer la cooperación y desarrollar un enfoque coordinado en la lucha contra las ciberamenazas.

- Establecer canales internacionales de información, detección y respuesta.

- Promover la participación coordinada de instituciones públicas y del sector privado en simulacros y ejercicios internacionales.

- En la UE, armonizar las legislaciones nacionales, implantar la "Estrategia de Ciberseguridad de la UE" e impulsar una política internacional en el ciberespacio.

- Cooperar con la OTAN en ciberdefensa: respuesta ante incidentes cibernéticos e intercambio de información técnica sobre amenazas y vulnerabilidades.

6.6. LA CIBERSEGURIDAD EN EL INFORME ANUAL DE SEGURIDAD NACIONAL.

6.6.1. El Informe Anual de Seguridad Nacional.

El Informe Anual de Seguridad Nacional es aprobado cada año por el Consejo de Seguridad Nacional, para su posterior presentación y debate en las Cortes. Esta práctica se inauguró en España en 2013. En la primera edición del Informe Anual de Seguridad Nacional se explican los objetivos y su proceso de su confección[555].

De este modo, se señala que "El Consejo de Seguridad Nacional, como Comisión Delegada del Gobierno para la Seguridad Nacional, tiene entre sus cometidos la aprobación del Informe Anual de Seguridad Nacional (IASN), antes de su presentación

[555] Consejo de Seguridad Nacional: *Informe Anual de Seguridad Nacional 2013.* abril 2014, p.9. http://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/Documents/_Informe_Seguridad_Nacional%20Accesible%20y%20Definivo.pdf consultado 27 de julio de 2015.

ante las Cortes Generales". "El IASN forma parte de la nueva política española de Seguridad Nacional, cuyos principios, organización y desarrollo son expuestos con detalle en el primer capítulo del Informe. En el marco de esta política, el Informe cumple tres propósitos fundamentales:

a. Realizar una presentación estructurada de los desarrollos más destacados de la Seguridad Nacional durante el año de referencia.

b. Ayudar a evaluar el grado de cumplimiento de la Estrategia de Seguridad Nacional de 2013.

c. Permitir, en futuros procesos de revisión de la Estrategia, identificar el surgimiento de nuevos retos a la Seguridad Nacional, la evolución de los ya identificados y la posible actualización de las Líneas de Acción Estratégicas.

El Informe Anual de Seguridad Nacional 2014, recoge en su introducción que "en España, la política de Seguridad Nacional se configura como una política pública de Estado, que implica a todas las Administraciones Públicas de acuerdo con sus respectivas competencias y a la sociedad en general. La ciudadanía debe estar debidamente informada sobre los desafíos que se afrontan en este espacio de actuación de los poderes públicos y ser partícipe de la toma de decisiones que tienen siempre por objetivo incrementar nuestros umbrales de seguridad sin renunciar a nuestras garantías y derechos".[556]

Continúa señalando el citado Informe, que la Seguridad Nacional es un proyecto compartido por las diferentes Administraciones, los órganos constitucionales, en especial las Cortes Generales, y la sociedad. Este compromiso con la necesaria transparencia es la razón de ser del Informe Anual de Seguridad Nacional que cada año es aprobado por el Consejo de Seguridad Nacional, en su condición de Comisión

[556] Consejo de Seguridad Nacional: *Informe Anual de Seguridad Nacional 2014*. abril 2015. p. 29.http://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Nacional/2015/Informe_Anual_de_Seguridad_Nacional_2014.pdf consultado 27 de julio de 2015.

Delegada del Gobierno, para su posterior presentación y debate en las Cortes, práctica que se inauguraba en julio de 2013.

Siguiendo el esquema de la Estrategia de Seguridad Nacional 2013, el Informe Anual de Seguridad Nacional realiza un diagnóstico completo de la evolución de los retos de la Seguridad Nacional, los valora según su manifestación al término del año y traza su posible desarrollo futuro. Igualmente, expone las realizaciones más sobresalientes que se han llevado a cabo en los distintos ámbitos de la Seguridad Nacional y detalla las medidas de anticipación, prevención y respuesta que anualmente se implementan para salvaguardar la Seguridad Nacional.

De esta forma, el Informe apunta como su seña de identidad la aproximación integral a la Seguridad Nacional toda vez que los distintos riesgos y amenazas se interrelacionan debido a su elevada transversalidad, afectan las competencias de varios actores y solo desde una perspectiva amplia es posible analizarlos y dimensionarlos correctamente.

6.6.2. La ciberseguridad en el Informe Anual de Seguridad Nacional 2013

En el ámbito de la ciberseguridad, este Informe señala que en el último Consejo de Seguridad Nacional del año 2013, celebrado el 5 de diciembre, se aprobó la Estrategia de Ciberseguridad Nacional, en su condición de estrategia sectorial derivada de la Estrategia de Seguridad Nacional. Asimismo se creó el Comité Especializado de Ciberseguridad, con la denominación de Consejo Nacional de Ciberseguridad, y cuya naturaleza jurídica es la de órgano colegiado de apoyo al Consejo de Seguridad Nacional.[557]

Señala el Informe Anual de Seguridad Nacional que “en la Estrategia de Ciberseguridad Nacional (ECSN) se desarrollan las previsiones de la Estrategia de Seguridad Nacional en materia de protección del ciberespacio, con el fin de implantar

[557] *Ibídem*. p. 14. También se aprobó en este Consejo la Estrategia de Seguridad Marítima, creándose el Comité Especializado de Seguridad Marítima, con la denominación de Consejo Nacional de Seguridad Marítima y equivalente naturaleza jurídica al Consejo Nacional de Ciberseguridad.

de forma coherente y estructurada las acciones de prevención, defensa, detección y respuesta frente a las ciberamenazas. La Estrategia de Ciberseguridad Nacional es el marco de referencia de un modelo integrado basado en la implicación, coordinación y armonización de todos los actores y recursos del Estado, así como en la colaboración público-privada y la implicación de los españoles en la ciberseguridad. Dado el carácter transnacional de la ciberseguridad, la cooperación con la Unión Europea y con otros organismos de ámbito internacional o regional con competencias en la materia forma parte esencial de este modelo".[558]

El citado Informe señala que la Estrategia crea una estructura orgánica que se integra en el marco del Sistema de Seguridad Nacional, siendo el elemento central de dicha estructura el Consejo Nacional de Ciberseguridad (CNCS), que tiene la función de apoyar al Consejo de Seguridad Nacional en el cumplimiento de sus funciones y, en particular, en la asistencia al Presidente del Gobierno en la dirección de la Política de Seguridad Nacional en el ámbito de la ciberseguridad.[559]

[558] *Ibídem*. p. 15.

[559] *ibídem*. p. 15.Se indica que la presidencia será anual y rotatoria entre autoridades de los Ministerios de la Presidencia, del Interior, de Industria, Energía y Turismo, de Defensa y de Asuntos Exteriores y de Cooperación, así como que su puesta en funcionamiento tuvo lugar en febrero de 2014.

Figura 63: Consejo Nacional de Ciberseguridad.

Fuente: López, María del Mar: Plan Nacional de Ciberseguridad[560].

En este Informe se enumeran las estructuras que se han creado en materia de ciberseguridad durante 2013, que se reflejan en el siguiente cuadro:

Figura 64: Estructuras creadas en materia de ciberseguridad en 2013 en España

Estructuras de ciberseguridad	Cometidos
Mando Conjunto de Ciberdefensa de las Fuerzas Armadas (MCCD).	Llevar a cabo el planeamiento y la ejecución de las acciones de ciberdefensa militar en las redes de sistemas de telecomunicaciones e información (CIS) de las Fuerzas Armadas u otras que pudiera tener encomendadas, así como contribuir a la respuesta adecuada en el

[560] LÓPEZ, María del Mar*: Plan Nacional de Ciberseguridad. Opus citada.*

	ciberespacio ante amenazas o agresiones que puedan afectar a la Defensa nacional.
Centro de Respuesta a Incidentes (CERT) de Seguridad e Industria.	Centro de Respuesta a Incidentes de Seguridad Cibernética dentro del marco de actuación de la protección de las infraestructuras críticas y del sector privado en general.
Dirección General de Tecnologías de la Información y de las Comunicaciones (TIC) de la Administración General del Estado.	Coordinación del proceso de racionalización de las Tecnologías de la Información y de las Comunicaciones (TIC) en la Administración General del Estado.
Oficina de Coordinación Cibernética (OCC) en el seno del Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC).	Centralizar todas las actividades relacionadas con la ciberdelincuencia, el ciberterrorismo y la ciberseguridad en la protección de las infraestructuras críticas.
División de Servicios y Supervisión de Red (SYSRED) de Aeropuertos y Navegación.	Con su propio centro de coordinación centralizado de la red de Navegación Aérea encargado de supervisar y monitorizar toda la red de AENA Navegación Aérea, con el fin de poder prevenir y actuar ante cualquier Incidencia o contingencia que pudiera ocurrir, minimizando así las posibles afecciones que pudieran tener a la gestión segura y eficaz del tráfico aéreo en España.

Fuente: Informe Anual de Seguridad Nacional 2013[561].

Otras acciones que recoge el mencionado Informe realizadas en 2013, relacionadas con el desarrollo de iniciativas en el campo de la ciberseguridad, son[562]:

- La aprobación de la Agenda Digital para España del Ministerio de Industria, Energía y Turismo como estrategia del Gobierno para desarrollar la economía y la sociedad digital en España durante el periodo 2013-2015 y el lanzamiento del Plan de Confianza Digital 2013-2015 de la Agenda Digital para España.
- El despliegue del Sistema de Alerta Temprana de Internet en 48 organismos, entre ellos, 8 Comunidades Autónomas y 7 empresas estratégicas, que permite al CERT de las Administraciones Públicas del Centro Criptológico Nacional

[561] Consejo de Seguridad Nacional: *Informe Anual de Seguridad Nacional 2013*, o*pus citada.* pp. 38-39.
[562] *Ibídem*, p. 39.

(CCN-CERT) la detección en tiempo real de ataques que sufren estos organismos.

- El refuerzo de las capacidades tecnológicas y operativas del Instituto Nacional de Tecnologías de la Comunicación (INTECO), que ha facilitado a la entidad gestionar los incidentes de ciberseguridad de los ciudadanos, la red de telecomunicaciones académicas (RedIRIS), los dominios ".es" y las empresas.
- Firmas de convenios y acuerdos para el intercambio de información y optimización de capacidades.

El Informe Anual de Seguridad 2013, indica también acciones llevadas a cabo para garantizar la seguridad de los sistemas de información y de las telecomunicaciones que soportan las Administraciones Públicas, que se recogen en la siguiente tabla:

Figura 65: Acciones en el ámbito de la ciberseguridad en las Administraciones Públicas en 2013.

Seguimiento trimestral del progreso de adecuación al Esquema Nacional de Seguridad (ENS), que se inició en la Administración General del Estado en febrero de 2013 y, posteriormente, se realizó de forma trimestral en mayo, septiembre y diciembre del mismo año, acordándose realizar una oleada adicional de seguimiento en marzo de 2014. Dicho seguimiento se ha extendido a las demás Administraciones Públicas, Comunidades Autónomas, entes locales y Universidades, de forma que en diciembre de 2013 se recibieron 131 cuestionarios de seguimiento de entidades de todas las Administraciones Públicas, correspondiendo 78 de ellos a la Administración General del Estado.
Elaboración y publicación de guías de seguridad, según lo previsto en el Real Decreto 3/2010 y en virtud de las recomendaciones del CCN-CERT, de manera que la serie 800 de apoyo al ENS cuenta ya con un total de 25 guías.
Despliegue del Servicio de Alerta Temprana (SAT) en la Red SARA (Sistema de Aplicaciones y Redes para las Administraciones), para facilitar la detección de ataques dirigidos contra las Administraciones Públicas en el contexto de la colaboración entre el CCN y el Ministerio de Hacienda y Administraciones Públicas, así como el despliegue de sondas en los accesos a Internet. Asimismo, se ha desplegado la herramienta CARMEN (Centro de Análisis de Registros y Minería de Eventos Nacionales), para el análisis de *logs* y búsqueda de anomalías de tráfico.

Preparación de las bases para la realización del informe anual del estado de la seguridad previsto en el Real Decreto 3/2010, para dar continuidad al seguimiento del progreso de adecuación al ENS.
Elaboración del proyecto de Real Decreto de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el ENS en el ámbito de la Administración Electrónica. Con esta modificación se persigue avanzar en la armonización del modo de actuar en ciertas cuestiones, perfeccionar los mecanismos para conocer periódicamente el estado de la seguridad en las Administraciones Públicas, reforzar la capacidad de respuesta del CCN-CERT frente a incidentes y mejorar las medidas de seguridad.
Formación presencial y en línea de personal especialista de las Administraciones Públicas en colaboración con el Instituto Nacional de Administración Pública (INAP), extendida en 2013 a unos 500 profesionales de las diferentes Administraciones Públicas.
Desarrollo de buenas prácticas, con la publicación y actualización de guías CCN-STIC, que incluyen normas, procedimientos, instrucciones técnicas y guías de securización de las diferentes tecnologías.
En el ámbito de la ciberdefensa se desarrollaron importantes ejercicios organizados por OTAN y por el MCCD como, por ejemplo, el ECD-2013, en el que participaron los Ministerios de Defensa, del Interior y de Industria, Energía y Turismo.
Desarrollos practicados en el Sistema de Comunicaciones Especiales de la Presidencia del Gobierno, habiéndose iniciado en 2013 el proceso de optimización del modelo de estructura CIS nacional de gestión de crisis, que incluye la asignación a todos los miembros del Consejo de Seguridad Nacional de terminales de comunicaciones y, también, la futura acreditación de seguridad del sistema.

Fuente: Informe Anual de Seguridad Nacional 2013[563].

Otro de los aspectos que señala el Informe Anual 2013 es la colaboración público-privada, con el fin de mejorar de la seguridad y resiliencia de las TIC en el sector privado. A tal fin, se ha participado en la negociación de la propuesta de Directiva de

[563] Ibídem, pp. 39-40.

Redes y Sistemas de Información en el grupo del Consejo de Telecomunicaciones, Transporte y Energía de la UE. Otras actuaciones en este ámbito incluyen el inicio de prestación de servicios de respuesta a incidentes en el ámbito de la Red académica y de investigación IRIS operados por INTECO; el diseño y la definición del Foro Nacional para la Confianza Digital (FNCD); con el objetivo de establecer un mecanismo de cooperación público-privado como respuesta a la necesidad de definición de actuaciones coordinadas.[564]

En la siguiente tabla se detallan los desarrollos más significativos, ligados a las Líneas de Acción Estratégicas definidas en la Estrategia de Seguridad Nacional de 2013.

Figura 66: Desarrollos más significativos en materia de ciberseguridad en 2013 en España, relacionados con las Líneas de Acción de la Estrategia de Seguridad Nacional 2013.

Desarrollo de la ESN 2013	
Ciberseguridad	
Objetivo para este ámbito de actuación establecido en la ESN de 2013 "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"	
Líneas de Acción Estratégicas	**Desarrollos más importantes durante 2013**
LAE 1 Incremento de la capacidad de prevención, detección, investigación y respuesta	Aprobación de la Estrategia de Ciberseguridad Nacional y creación del Consejo Nacional de Ciberseguridad, y aprobación de la Agenda Digital para España y del Plan de confianza Digital 2013-2015. Creación del Mando Conjunto de Ciberdefensa, del CERT de Seguridad e Industria, de la Oficina de Coordinación Cibernética (OCC) del Ministerio del Interior, la Dirección General de TIC de la AGE y de la División de Servicios y Supervisión de Red de Aeropuertos y Navegación (SYSRED). Fortalecimiento de las capacidades de detección y respuesta a los

[564] *Ibídem*, pp. 40-41.

	ciberataques contra las infraestructuras críticas y el sector privado. Refuerzo de las capacidades de investigación y persecución del ciberterrorismo y la ciberdelincuencia (CNPIC, Cuerpo Nacional de Policía, Guardia Civil). Mejora de las estructuras y capacidades de inteligencia (CNI/CCN) para mejor alerta de la amenaza.
LAE 2 Garantizar la seguridad de los sistemas de información y de las redes de comunicaciones	Seguimiento trimestral del progreso de adecuación al ENS en las Administraciones Públicas durante el ejercicio 2013. Elaboración del proyecto de Real Decreto de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad. Realización de los trabajos preparatorios relativos al informe del estado de la seguridad de las Administraciones Públicas. Publicación de una serie de guías de seguridad de carácter técnico de apoyo al ENS. Despliegue del Sistema de Alerta Temprana en la Red SARA, de sondas en los accesos a Internet de las AA. PP., del sistema CARMEN para el análisis de logs y búsqueda de anomalías de tráfico. Formación presencial y en línea de personal especialista de las AA. PP. en colaboración con el INAP. Desarrollo de diversos productos de cifra y para la seguridad de las tecnologías de la información con capacidad verificada. Fortalecimiento de las capacidades de respuesta del CERT de las Administraciones Públicas (CCN-CERT). Realización por el MCCD de ciberejercicio ECD-2013. Optimización del Sistema de Comunicaciones Especiales de la Presidencia del Gobierno
LAE 3 Mejora de la seguridad y resiliencia de las TIC en el sector privado	Negociación sobre la Propuesta de Directiva de Redes y Sistemas de Información. Propuesta de modificación de la Ley de Servicios de la Sociedad de la Información (proyecto de Ley General de Telecomunicaciones). Creación del Servicio de Respuesta a Incidentes de Seguridad de ICs (CNPIC e INTECO). Prestación de servicios de respuesta a incidentes en el ámbito de la Red IRIS. Definición del Foro Nacional para la Confianza Digital. Puesta en marcha del GT Operadores de Telecomunicaciones SETSI e INTECO y de Punto de Gestión de Incidentes. Participación en ciberejercicios que involucran al sector privado en los ámbitos de la energía, el transporte, el agua y el sector financiero. Actividades del Organismo de Certificación del CCN-CNI.
LAE 4	Diseño de un programa integral que cubra el ciclo de vida del emprendimiento y de la I+D+i para el bienio 2014-2015.

Promoción de la capacitación de profesionales en ciberseguridad e impulso a la industria española (I+D+i)	Incorporación de INTECO en la estructuras nacionales de evaluación de proyectos de I+D+i. Puesta en marcha del Programa de Excelencia en Ciberseguridad. Inauguración del Centro Nacional de Excelencia en Ciberseguridad promovido por el Ministerio de Interior y la Universidad de Madrid, con participación de las FCSE, el CNPIC y el sector privado. Participación en foros internacionales de normalización técnica. Puesta en marcha del programa de certificación de profesionales de ciberseguridad.
LAE 5 Implantación de una cultura de ciberseguridad sólida	Plan de Sensibilización de INTECO. Desarrollo por las FCSE de varias iniciativas de concienciación. Nuevas Guías CCN-STIC. 14 cursos CCN-STIC para personal de las Administraciones Públicas. Puesta en marcha del Centro Nacional de Excelencia en Ciberseguridad.
LAE 6 Intensificación de la colaboración internacional	Potenciación de la presencia de España en los principales foros internacionales. Contribución a la elaboración de la Estrategia de Ciberseguridad de la UE y de la Directiva NIS. Colaboración con el CERT-UE, presencia en grupos de trabajo de EUROPOL e INTERPOL y participación en ciberejercicios. Apoyo de España a Resoluciones de NN. UU. relativas al “Derecho a la Privacidad en la Era Digital” y a los “Desarrollos en el campo de la Información y las Telecomunicaciones en el contexto de la Seguridad Internacional”. Participación en reuniones OSCE de expertos sobre medidas de fomento de la confianza en ciberseguridad. Cumplimiento de las tareas de la Política de Ciberdefensa de la OTAN de 2011, apoyo a que la Ciberdefensa esté en la agenda de la Cumbre de 2014 y defensa de la actualización de dicha Política. Apoyo a distintos convenios desarrollados en ámbito del Consejo de Europa. Participación en la Conferencia Internacional sobre el Ciberespacio. Acuerdo de colaboración entre CCN-CERT y CERT de OTAN (NCIRC).

Fuente: Informe Anual de Seguridad Nacional 2013[565].

[565] *Ibídem*, pp. 45-46.

6.6.3. La ciberseguridad en el Informe Anual de Seguridad Nacional 2014

El Gobierno de España publicó la segunda edición del Informe Anual de Seguridad Nacional, con la revisión de los avances desarrollados durante 2014.[566]

En este documento, se señala que "el Informe realiza un diagnóstico completo de la evolución de los retos de la Seguridad Nacional, los valora según su manifestación y traza su posible desarrollo futuro, siempre con un enfoque integral, toda vez que los desafíos a la Seguridad Nacional se interrelacionan debido a su elevada transversalidad, afectan a las competencias de varios actores y solo desde una perspectiva amplia es posible analizarlos y dimensionarlos correctamente". De esta forma, el Informe es considerado "un instrumento que permite evaluar el grado de cumplimiento de la Estrategia de Seguridad Nacional y, en futuros procesos de revisión de la Estrategia, identificar el surgimiento de nuevos desafíos a la Seguridad Nacional, la evolución de los ya incluidos y la posible actualización de las Líneas de Acción Estratégica con la finalidad de proteger la libertad y el bienestar de los españoles, garantizar la defensa de España y sus principios y valores constitucionales, así como contribuir junto a nuestros socios y aliados a la seguridad internacional en el cumplimiento de los compromisos asumidos".[567]

En el campo de la Ciberseguridad, el Consejo Nacional de Ciberseguridad, órgano colegiado de apoyo al Consejo de Seguridad Nacional y en concreto de asistencia al Presidente del Gobierno en la dirección de la Política de Seguridad Nacional en el ámbito de la ciberseguridad, adoptó el Plan Nacional, al que el 31 de octubre el Consejo de Seguridad Nacional dio su conformidad.

---

[566] Consejo de Seguridad Nacional. Informe Anual de Seguridad Nacional 2014. Abril 2015. http://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Nacional/2015/Informe_Anual_de_Seguridad_Nacional_2014.pdf consultado 27 de julio de 2015.

[567] *Ibídem*. p. 1.

Se trata del primer nivel en la planificación resultante de la Estrategia de Ciberseguridad Nacional y desarrollará, a través de planes de acción derivados, las líneas de acción previstas en la Estrategia. Estos planes derivados abordan distintos aspectos de la ciberseguridad como incrementar las capacidades de prevención, defensa, detección, análisis, respuesta, recuperación y coordinación ante las ciberamenazas, haciendo énfasis en la Administraciones Públicas, las infraestructuras críticas, las capacidades militares y de Defensa y otros sistemas de interés nacional, la investigación y persecución del ciberterrorismo, el ciberespionaje y la ciberdelicuencia, así como la ciberseguridad en el sector privado o la cultura de ciberseguridad.

En el ámbito de la Ciberseguridad, tendencias como el uso masivo de servicios en la nube, las tecnologías móviles y redes sociales, han motivado un aumento del riesgo, que hace necesario la adopción de modelos basados en el refuerzo de las capacidades de prevención y detección, el desarrollo efectivo de una cultura de ciberseguridad, así como medidas dirigidas a aumentar la cooperación, colaboración y coordinación, que fomenten el intercambio de información.

Destacan en este ámbito la creación del Consejo Nacional de Ciberseguridad antes referido, el Centro de Respuesta ante Incidentes de Ciberseguridad del Ministerio de Defensa y el Centro de Respuesta ante Incidentes de Ciberseguridad conjunto de los Ministerios de Interior e Industria. Además, con la finalidad de mejorar la capacidad de prevención, detección, investigación y respuesta ante ciberamenazas con apoyo en un marco legal operativo y eficaz, se han llevado a cabo reformas en el ordenamiento jurídico.

Del mismo modo, en 2014 el Centro Criptológico Nacional ha seguido realizando el seguimiento del progreso de adecuación al Esquema Nacional de Seguridad, al objeto de garantizar la seguridad de las Tecnologías de la Información y las Comunicaciones que apoyan a las Administraciones Públicas y los sistemas de Defensa y de Seguridad Nacional para lo cual se ha impulsado la coordinación entre el Centro Criptológico Nacional y un órgano de nueva creación, la Dirección de Tecnologías de la Información

y las Comunicaciones, al que se le han atribuido competencias para prestar servicios comunes orientados a la mejora de la seguridad en la Administración General del Estado.

Otro de los aspectos prioritarios ha sido la seguridad de las Tecnologías de la Información y la Comunicación mediante el refuerzo del concepto de seguridad integral en los Planes Estratégicos Sectoriales.

Asimismo, se ha dedicado una atención preferente en 2014 a la mejora de la seguridad y resiliencia de las Tecnologías de la Información y las Comunicaciones en el sector privado, para lo que se ha fomentado la colaboración público-privada a través de iniciativas de intercambio de información.

También se ha trabajado en actuaciones relativas a la promoción de la capacitación de profesionales en ciberseguridad y al impulso a la industria española, como aquellas dirigidas a la gestión del talento, el desarrollo de instrumentos de financiación del emprendimiento y de la I+D+i en ciberseguridad y confianza digital, y el desarrollo de diversas actividades de formación y concienciación encaminada a profesionales de las diferentes Administraciones Públicas, así como múltiples actuaciones dirigidas a la concienciación y sensibilización de empresas y particulares, con la finalidad de implantar una sólida cultura de ciberseguridad.

Otras realizaciones relevantes se refieren a la participación activa de España en las iniciativas estratégicas promovidas en la Unión Europea, las Naciones Unidas, la Organización para la Seguridad y la Cooperación en Europa, la OTAN o el Consejo de Europa. Se destaca también la firma, con el Organismo de Certificación por el Ministerio de Hacienda y Administraciones Públicas y del Centro Criptológico Nacional, de la nueva versión del Arreglo sobre el Reconocimiento de los Certificados de Criterios Comunes en el campo de la Seguridad de la Tecnología de la Información.

El Informe Anual de Seguridad Nacional 2014 también apunta la importancia de las ciberamenazas en ámbitos específicos, como el marco de la lucha contra el crimen organizado, en el que señala que “Las principales amenazas en este ámbito son el

narcotráfico, el cibercrimen, el blanqueo de capitales, la trata de seres humanos con fines de explotación sexual o laboral, u otras formas de criminalidad asociadas o emergentes, así como la creciente relación entre grupos criminales y terroristas".[568]

El Informe Anual de Seguridad Nacional 2014 dedica su parte tercera íntegramente a la ciberseguriad, señalando los progresos realizados, de los que a continuación se recogen los más significativos.

Figura 67: Desarrollos más significativos en materia de ciberseguridad en 2014 en España, relacionados con las Líneas de Acción de la Estrategia de Seguridad Nacional 2013.

Desarrollo de la ESN 2013	
Ciberseguridad	
Objetivo para este ámbito de actuación establecido en la ESN de 2013 "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"	
Líneas de Acción Estratégicas	**Desarrollos más importantes durante 2014**
LAE 1 Incremento de la capacidad de prevención, detección, investigación y respuesta	Creación del Centro de Respuesta ante incidentes de Ciberseguridad del Ministerio de Defensa (ESPCERTDEF) en las dependencias del Mando Conjunto de Ciberdefensa, para facilitar las labores de defensa, explotación y respuesta, a través de laboratorios de análisis forense y de I+D+i. Transformación de la estructura del Centro Criptológico Nacional mediante la integración de las capacidades de la Inteligencia,defensa de redes y SIGINT (Inteligencia de Señales). Desarrollo de la herramienta INES (Informe Nacional del Estado de Seguridad) por el Centro Criptológico Nacional, cuyo CERT es

[568] *Ibídem*. p. 5.

	el encargado de articular la respuesta a los incidentes de seguridad en el Esquema Nacional de Seguridad. El Centro Criptológico Nacional ha publicado informes mensuales de actividad y de amenazas e informes técnicos relacionados con incidentes y auditorías de seguridad. Por otra parte ha realizado la publicación de información técnica acerca de distintas vulnerabilidades y códigos dañinos con el fin de permitir su detección y limpieza. El CCN-CERT ha desarrollado la herramienta LUCIA (Listado Unificado de Coordinación de Incidentes y Amenazas) para la gestión de incidentes y el despliegue de la implantación de la herramienta CARMEN (Centro de Análisis de Registros y Minería de Eventos) que permite, mediante el análisis de anomalías de tráfico, la detección de ataques no conocidos.
LAE 2 Garantizar la seguridad de los sistemas de información y de las redes de comunicaciones	Creación de la Oficina de Coordinación Cibernética,en el seno del Centro Nacional para la Protección de las Infraestructuras Críticas del Ministerio del Interior. Designación del Mando Conjunto de Ciberdefensa como responsable del desarrollo, dirección de la ejecución y control de cumplimiento de las políticas de Seguridad de la Información TIC en el ámbito del Ministerio de Defensa. Proyecto de Real Decreto de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. El Equipo de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional (CCN-CERT) se ha dotado de diversas herramientas dirigidas a mejorar el Sistema de Alerta Temprana de la Intranet Administrativa en la Red SARA (Sistema de Aplicaciones y Redes para las Administraciones).[569] El CCN-CERT ha desarrollado la herramienta LUCIA (Listado Unificado de Coordinación de Incidentes y Amenazas) para la gestión de incidentes y el despliegue de la implantación de la herramienta CARMEN (Centro de Análisis de Registros y Minería de Eventos) que permite, mediante el análisis de anomalías de tráfico, la detección de ataques no conocidos.
LAE 3	Centro de Respuesta ante Incidentes de Ciberseguridad del Instituto Nacional de Ciberseguridad de España (INCIBE) para la gestión de la ciberseguridad de ciudadanos y empresas.

[569] Este sistema conecta a los diferentes Ministerios y Agencias de la Administración General del Estado, a las Comunidades Autónomas y, a través de estas, a más de cuatro mil ayuntamientos, optimizando las capacidades de correlación, gestión de incidentes e incorporado nuevas fuentes de análisis para facilitar la detección de ataques dirigidos. A estos efectos se ha desplegado el Sistema de Alerta Temprana de la Red SARA en cuarenta y nueve organismos y el Sistema de Alerta Temprana de acceso a Internet en sesenta y cuatro organismos.

Mejora de la seguridad y resiliencia de las TIC en el sector privado	Foro Nacional para la Confianza Digital. Proyecto de Ley Orgánica por el que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal y el Anteproyecto de Ley Orgánica de Modificación de la Ley de Enjuiciamiento Criminal para la agilización de la Justicia penal, el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológicas. Impulso de la colaboración de las Fuerzas y Cuerpos de Seguridad del Estado con entidades privadas en materia de ciberdelincuencia. Destaca el *Programa COOPERA* y la *Red Azul* del Ministerio del Interior. Ejercicios de Ciberseguridad Nacional de Operadores Estratégicos, organizados por el Instituto Nacional de Ciberseguridad y asociaciones empresariales, así como por el Centro Nacional para la Protección de Infraestructuras Críticas. Polo Tecnológico de Ciberseguridad y definición de la Agenda Estratégica de Investigación Nacional.
LAE 4 Promoción de la capacitación de profesionales en ciberseguridad e impulso a la industria española (I+D+i)	El Centro Criptológico Nacional ha continuado desarrollado actuaciones de buenas prácticas a través de la publicación y actualización de diferentes normas, procedimientos, instrucciones técnicas y guías de configuración de seguridad. La Dirección de Tecnologías de la Información y las Comunicacione ha definido normas de seguridad y calidad tecnológicas y de la información a los que deberán ajustarse todas las unidades de la Administración General del Estado y sus Organismos Públicos. Plan de formación en materia de ciberdefensa para el conjunto del personal del Ministerio de Defensa. Programa de formación y concienciación del Centro Criptológico Nacional, incluyendo un total de dieciséis cursos presenciales con modalidades de apoyo en línea, con los que se ha instruido a 525 profesionales de las diferentes Administraciones Públicas.
LAE 5 Implantación de una cultura de ciberseguridad sólida	Los diversos organismos con competencias en materia de ciberseguridad han participado en multitud de jornadas y foros civiles y militares, de ámbito nacional e internacional, donde se ha hecho difusión, análisis y debates sobre cuestiones relacionadas con la ciberseguridad. El Instituto Nacional de Ciberseguridad desarrolló actuaciones específicas de concienciación, información y formación, tanto para ciudadanos a través de su canal específico de la Oficina de Seguridad del Internauta (OSI),así como para empresas,a través de la sección *Protege tu empresa* alojada en su página web. El Ministerio del Interior, a través del *Plan Director para la Mejora de la Convivencia y Seguridad Escolar*, colaboró con la comunidad

	educativa para la erradicación, en el entorno escolar, de cualquier conducta violenta relacionada con el uso del ciberespacio.
LAE 6 Intensificación de la colaboración internacional	Reglamento del Parlamento Europeo y del Consejo relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (Reglamento eIDAS) y en la negociación de la propuesta de Directiva de Redes y Sistemas de Información (Directiva NIS). En la Organización para la Seguridad y la Cooperación en Europa (OSCE), España ha aportado información relativa al cumplimiento de las once Medidas de Fomento de la Confianza. En el ámbito de la Unión Europea destaca la participación en el seguimiento de la aplicación de la Estrategia de Ciberseguridad de la Unión Europea. En el marco de la ONU se ha participado en las reuniones del Grupo de Expertos Gubernamentales de Naciones Unidas relativas a los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional. En la OTAN, la agenda de la ciberdefensa ha estado marcada por la participación activa en el cumplimiento de las acciones dirigidas a revisar la Política de Ciberdefensa 2011, y el apoyo a la Política Reforzada de Ciberdefensa 2014, adoptada en la Cumbre de Gales. En el ámbito del Consejo de Europa, como Estado parte del Convenio sobre la Ciberdelincuencia de 2001 (Convenio de Budapest), se ha participado en la promoción de la ratificación del Convenio por parte de otros países, a la vez que se ha continuado la adaptación de la normativa interna, para cumplir con los mecanismos de cooperación policial y judicial previstos.

Fuente: Elaboración propia sobre datos recogidos del Informe Anual de Seguridad Nacional 2014[570].

Por último, el Informe Anual de Seguridad Nacional 2014 recoge las Tendencias y objetivos en materia de ciberseguridad:[571]

> El aumento de la superficie de exposición, propiciado por tendencias como el uso masivo de servicios en la nube de Internet, tecnologías

[570] *Informe Anual de Seguridad Nacional 2014*, *opus citada*, pp. 66-73.
[571] *Ibídem,* p. 73.

móviles y redes sociales, junto con el aumento de las amenazas, han motivado un aumento del riesgo, tendencia que parece consolidarse.

En cuanto a las amenazas se refiere, el ciberespionaje y la ciberdelincuencia se prevén que sigan aumentando a corto y medio plazo. Por su criticidad, también hay que mencionar la tendencia a la explotación de las vulnerabilidades presentes en los equipos y dispositivos que componen los sistemas de control industrial de las infraestructuras críticas.

Se deben perseguir modelos basados en reforzar las capacidades de prevención y detección, con un desarrollo efectivo de una cultura de ciberseguridad (concienciación, sensibilización y formación) en todos los ámbitos (Fuerzas y Cuerpos de Seguridad del Estado, ciudadanos, empresas, Administraciones Públicas, infraestructuras críticas, etc.), así como medidas dirigidas a aumentar la cooperación, colaboración y coordinación que fomenten el intercambio de información y el refuerzo de las capacidades de detección junto con la realización de ciberejercicios sectoriales (sector financiero, energético, etc.).

Finalmente se debe avanzar en el desarrollo y ejecución de los planes derivados del *Plan Nacional de Ciberseguridad*, que implementa lo establecido en la Estrategia de Ciberseguridad Nacional.

6.7. EL ESQUEMA NACIONAL DE SEGURIDAD (ENS) EN EL ÁMBITO DE LA ADMINISTRACIÓN ELECTRÓNICA

6.7.1. Desarrollo del ENS en el ámbito de la Administración Electrónica

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica[572], señala en su preámbulo

[572] Gobierno de España: *Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica*.

que la necesaria generalización de la sociedad de la información es subsidiaria, en gran medida, de la confianza que genere en los ciudadanos la relación a través de medios electrónicos. En el ámbito de las Administraciones públicas, la consagración del derecho a comunicarse con ellas a través de medios electrónicos comporta una obligación correlativa de las mismas, que tiene, como premisas, la promoción de las condiciones para que la libertad y la igualdad sean reales y efectivas, y la remoción de los obstáculos que impidan o dificulten su plenitud, lo que demanda incorporar las peculiaridades que exigen una aplicación segura de estas tecnologías.

A ello vino a dar respuesta la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos[573], que en su artículo 42.2 crea el Esquema Nacional de Seguridad, cuyo objeto es el establecimiento de los principios y requisitos de una política de seguridad en la utilización de medios electrónicos que permita la adecuada protección de la información.

Este artículo 42 también crea el Esquema Nacional de Interoperabilidad, que comprende el conjunto de criterios y recomendaciones en materia de seguridad, conservación y normalización de la información, de los formatos y de las aplicaciones que deberán ser tenidos en cuenta por las Administraciones Públicas para la toma de decisiones tecnológicas que garanticen la interoperabilidad. Se añade en el artículo 42 que en la elaboración de ambos Esquemas se tendrán en cuenta las recomendaciones de la Unión Europea, la situación tecnológica de las diferentes Administraciones Públicas, así como los servicios electrónicos ya existentes. A estos efectos se considerará la utilización de estándares abiertos, así como los estándares que sean de uso generalizado por los ciudadanos.

El preámbulo del Real Decreto 3/2010, continúa señalando que la finalidad del Esquema Nacional de Seguridad es la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar

https://www.boe.es/buscar/pdf/2010/BOE-A-2010-1330-consolidado.pdf consulta: 17 de octubre de 2015.

[573] Gobierno de España: *Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos*, http://www.boe.es/diario_boe/txt.php?id=BOE-A-2007-12352 consulta: 17 de octubre de 2015.

la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos, que permita a los ciudadanos y a las Administraciones públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

De esta forma, el Esquema Nacional de Seguridad persigue fundamentar la confianza en que los sistemas de información prestarán sus servicios y custodiarán la información de acuerdo con sus especificaciones funcionales, sin interrupciones o modificaciones fuera de control, y sin que la información pueda llegar al conocimiento de personas no autorizadas. Se tiene en cuenta, además, que actualmente los sistemas de información de las administraciones públicas están fuertemente imbricados entre sí y con los sistemas de información del sector privado: empresas y de los administrados. De esta manera, la seguridad tiene un nuevo reto que va más allá del aseguramiento individual de cada sistema.

Tal como se señalaba en el artículo 42 de la Ley 11/2007, el Esquema Nacional de Seguridad tiene presentes las recomendaciones de la Unión Europea (Decisión 2001/844/CE CECA, Euratom de la Comisión, de 29 de noviembre de 2001, por la que se modifica su Reglamento interno y Decisión 2001/264/CE del Consejo, de 19 de marzo de 2001, por la que se adoptan las normas de seguridad del Consejo[574]), la situación tecnológica de las diferentes Administraciones públicas, así como los servicios electrónicos existentes en las mismas, la utilización de estándares abiertos y, de forma complementaria, estándares de uso generalizado por los ciudadanos. Además, su articulación se ha realizado atendiendo a la normativa nacional sobre Administración electrónica, protección de datos de carácter personal, firma electrónica y documento nacional de identidad electrónico, Centro Criptológico Nacional, sociedad de la información, reutilización de la información en el sector público y órganos colegiados responsables de la Administración Electrónica; así como la regulación de diferentes instrumentos y servicios de la Administración, las directrices y guías de la OCDE y disposiciones nacionales e internacionales sobre normalización.

[574] Comisión Europea: *Decisión de la Comisión, de 3 de febrero de 2005, por la que se modifica la Decisión 2001/844/CE, CECA, Euratom*. https://www.boe.es/buscar/doc.php?id=DOUE-L-2005-80234 consulta: 17 de octubre de 2015.

También se tiene en cuenta la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal[575] y sus normas de desarrollo, que determinan las medidas para la protección de los datos de carácter personal; y que aportan criterios para establecer la proporcionalidad entre las medidas de seguridad y la información a proteger.

La Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común[576], referente legal imprescindible de cualquier regulación administrativa, determina la configuración de numerosos ámbitos de confidencialidad administrativos, diferentes a la información clasificada y a los datos de carácter personal, que necesitan ser materialmente protegidos. Asimismo determina el sustrato legal de las comunicaciones administrativas y sus requisitos jurídicos de validez y eficacia, sobre los que soportar los requerimientos tecnológicos y de seguridad necesarios para proyectar sus efectos en las comunicaciones realizadas por vía electrónica.

La Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público[577], que determina la regulación básica del régimen jurídico aplicable a la reutilización de documentos elaborados en el sector público, configura un ámbito excepcionado de su aplicación en el que se encuentra la información a la que se refiere el Esquema Nacional de Seguridad.

Junto a las disposiciones indicadas, el preámbulo del Real Decreto 3/2010 señala que han inspirado el contenido de la norma del Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, documentos de la Administración en materia de seguridad electrónica, tales como los Criterios de Seguridad, Normalización y Conservación, las Guías CCN-STIC de Seguridad de los Sistemas de Información y

---

575 Gobierno de España: *Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.* https://www.boe.es/buscar/doc.php?id=BOE-A-1999-23750 consulta: 17 de octubre de 2015.

576 Gobierno de España: *Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común*. http://www.boe.es/buscar/act.php?id=BOE-A-1992-26318 consulta: 17 de octubre de 2015.

577 Gobierno de España: *Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público.* http://www.boe.es/diario_boe/txt.php?id=BOE-A-2007-19814 consulta: 17 de octubre de 2015.

Comunicaciones, la Metodología y herramientas de análisis y gestión de riesgos o el Esquema Nacional de Interoperabilidad, también desarrollado al amparo de lo dispuesto en la Ley 11/2007, de 22 de junio.

Este real decreto se limita a establecer los principios básicos y requisitos mínimos que, de acuerdo con el interés general, naturaleza y complejidad de la materia regulada, permiten una protección adecuada de la información y los servicios, lo que exige incluir el alcance y procedimiento para gestionar la seguridad electrónica de los sistemas que tratan información de las Administraciones públicas en el ámbito de la Ley 11/2007, de 22 de junio. Con ello, se logra un común denominador normativo, cuya regulación no agota todas las posibilidades, y permite ser completada, mediante la regulación de los objetivos, materialmente no básicos, que podrán ser decididos por políticas legislativas territoriales.

Para dar cumplimiento a lo anterior se determinan las dimensiones de seguridad y sus niveles, la categoría de los sistemas, las medidas de seguridad adecuadas y la auditoría periódica de la seguridad; se implanta la elaboración de un informe para conocer regularmente el estado de seguridad de los sistemas de información a los que se refiere el presente real decreto, y se establece el papel de la capacidad de respuesta ante incidentes de seguridad de la información del Centro Criptológico Nacional.

La norma se estructura en diez capítulos, cuatro disposiciones adicionales, una disposición transitoria, una disposición derogatoria y tres disposiciones finales. A los cuatro primeros anexos dedicados a la categoría de los sistemas, las medidas de seguridad, la auditoría de la seguridad, y el glosario de términos, se les une un quinto que establece un modelo de cláusula administrativa particular a incluir en las prescripciones administrativas de los contratos correspondientes.

En este real decreto se concibe la seguridad como una actividad integral, en la que no caben actuaciones puntuales o tratamientos coyunturales, debido a que la debilidad de un sistema la determina su punto más frágil y, a menudo, este punto es la coordinación entre medidas individualmente adecuadas pero deficientemente ensambladas. La información tratada en los sistemas electrónicos a los que se refiere

este real decreto estará protegida teniendo en cuenta los criterios establecidos en la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal..

El Esquema Nacional de Seguridad está constituido por los principios básicos y requisitos mínimos requeridos para una protección adecuada de la información. Será aplicado por las Administraciones públicas para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que gestionen en el ejercicio de sus competencias[578].

Las líneas de defensa que se perfilan en el Esquema Nacional de Seguridad estarán constituidas por medidas de naturaleza organizativa, física y lógica. Estas líneas de defensa se basan en que el sistema ha de disponer de una estrategia de protección constituida por múltiples capas de seguridad, dispuesta de forma que, cuando una de las capas falle, permita: a) Ganar tiempo para una reacción adecuada frente a los incidentes que no han podido evitarse. b) Reducir la probabilidad de que el sistema sea comprometido en su conjunto. c) Minimizar el impacto final sobre el mismo[579].

En relación con la capacidad de respuesta a incidentes de seguridad de la información. El Centro Criptológico Nacional (CCN) articulará la respuesta a los incidentes de seguridad en torno a la estructura denominada CCN-CERT (Centro Criptológico Nacional Computer Emergency Reaction Team), que actuará sin perjuicio de las capacidades de respuesta a incidentes de seguridad que pueda tener cada administración pública y de la función de coordinación a nivel nacional e internacional del CCN[580].

El CCN-CERT prestará a las Administraciones públicas los siguientes servicios[581]:

a) Soporte y coordinación para el tratamiento de vulnerabilidades y la resolución de incidentes de seguridad que tengan la Administración General del Estado, las

[578] Gobierno de España: *Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica*. *Opus citada*, art. 1.
[579] *Ibídem,* art. 8.
[580] *Ibídem,* art. 36.
[581] *Ibídem,* art. 37.

Administraciones de las comunidades autónomas, las entidades que integran la Administración Local y las Entidades de Derecho público con personalidad jurídica propia vinculadas o dependientes de cualquiera de las administraciones indicadas. El CCN-CERT, a través de su servicio de apoyo técnico y de coordinación, actuará con la máxima celeridad ante cualquier agresión recibida en los sistemas de información de las Administraciones públicas. Para el cumplimiento de los fines indicados en los párrafos anteriores se podrán recabar los informes de auditoría de los sistemas afectados.

b) Investigación y divulgación de las mejores prácticas sobre seguridad de la información entre todos los miembros de las Administraciones públicas. Con esta finalidad, las series de documentos CCN-STIC (Centro Criptológico Nacional-Seguridad de las Tecnologías de Información y Comunicaciones), elaboradas por el Centro Criptológico Nacional, ofrecerán normas, instrucciones, guías y recomendaciones para aplicar el Esquema Nacional de Seguridad y para garantizar la seguridad de los sistemas de tecnologías de la información en la Administración.

c) Formación destinada al personal de la Administración especialista en el campo de la seguridad de las tecnologías de la información, al objeto de facilitar la actualización de conocimientos del personal de la Administración y de lograr la sensibilización y mejora de sus capacidades para la detección y gestión de incidentes.

d) Información sobre vulnerabilidades, alertas y avisos de nuevas amenazas a los sistemas de información, recopiladas de diversas fuentes de reconocido prestigio, incluidas las propias.

Además, el CCN desarrollará un programa que ofrezca la información, formación, recomendaciones y herramientas necesarias para que las Administraciones públicas puedan desarrollar sus propias capacidades de respuesta a incidentes de seguridad y en el que el CCN, será coordinador a nivel público estatal.

Aplicación del Esquema Nacional de Seguridad a las entidades vinculadas o dependientes de las Administraciones Públicas

Ante la cuestión de si el ENS es de aplicación a las entidades vinculadas o dependientes de las Administraciones Públicas, el CCN considera que a la luz de la Ley 11/2007, la Ley 30/1992 y la Ley 6/1997, cabe interpretar lo siguiente[582]:

• El ENS es aplicable a las entidades de derecho público vinculadas o dependientes de las Administraciones Públicas (Administración General del Estado, Comunidades Autónomas y Entidades Locales), aunque puede ser necesario un análisis caso por caso.

• Ciertos "organismos públicos", según la disposición adicional décima de la Ley 6/1997 están vinculados a la AGE y, por tanto, entran dentro del ámbito de aplicación del ENS.

• Lo mismo ocurre con otras entidades empresariales vinculadas o dependientes de la Administración General del Estado.

• Las Universidades Públicas son Administración Pública vinculada (que no dependiente) a las administraciones de las Comunidades Autónomas y, por tanto, les aplica el ENS.

• En el caso de los órganos constitucionales (Casa Real, Congreso, Senado, Consejo General del Poder Judicial, Tribunal Constitucional, Defensor del Pueblo, Tribunal de Cuentas, Consejo Económico y Social) la aplicación del ENS, o no, sería una decisión propia.

• No obstante, hay que analizar caso por caso para determinar si se trata de una entidad de derecho público vinculada o dependiente de alguna de las Administraciones Públicas. No parece necesario que ejerzan potestades administrativas, ni que su actividad esté sujeta a la Ley 30/1992 por imperativo de ésta.

Plan de adecuación al Esquema Nacional de Seguridad

[582] Centro Criptológico Nacional: *Esquema Nacional de Seguridad: Preguntas Frecuentes*, Madrid, noviembre 2012, p. 8. file:///Users/Anibal/Downloads/Esquema_Nacional_de_Seguridad_-_Preguntas_frecuentes.pdf consulta: 17 de octubre de 2015.

En la disposición transitoria del Real Decreto 3/2010 se articula un mecanismo escalonado para la adecuación a lo previsto en el Esquema Nacional de Seguridad de manera que los sistemas de las administraciones deberán estar adecuados a este Esquema en unos plazos en ningún caso superiores a 48 meses desde la entrada en vigor del mismo.

Una adecuación ordenada al Esquema Nacional de Seguridad requiere el tratamiento de las siguientes cuestiones:

• Preparar y aprobar la política de seguridad, incluyendo la definición de roles y la asignación de responsabilidades[583].

• Categorizar los sistemas atendiendo a la valoración de la información manejada y de los servicios prestados[584].

• Realizar el análisis de riesgos, incluyendo la valoración de las medidas de seguridad existentes.

• Preparar y aprobar la Declaración de aplicabilidad de las medidas del Anexo II del ENS[585].

[583] Véase Centro Criptológico Nacional: *Guía de Seguridad CCN-STIC-805. Esquema Nacional de Seguridad: Política de Seguridad de la Información*, Madrid, septiembre de 2011. https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/805-Politica_de_seguridad_del_ENS/805-ENS_politica-sep11.pdf consulta: 17 de octubre de 2011.

[584] Véase Centro Criptológico Nacional: *Guía de Seguridad CCN-STIC-803. Esquema Nacional de Seguridad: Valoración de los Sistemas. Política de Seguridad de la Información*, Madrid, enero de 2011. https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/803-Valoracion_en_el_ENS/803_ENS-valoracion_ene-11.pdf consulta: 17 de octubre de 2011.

[585] Véase Centro Criptológico Nacional: *Guía de Seguridad CCN-STIC-804. Esquema Nacional de Seguridad: Guía de Implantación*, Madrid, 26 de octubre de 2011. https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/804-Medidas_de_implantacion_del_ENS/804-Medidas_de_implantacion_del_ENS-20111026.pdf consulta: 17 de octubre de 2015.

• Elaborar un plan de adecuación para la mejora de la seguridad, sobre la base de las insuficiencias detectadas, incluyendo plazos estimados de ejecución[586].

• Implantar operar y monitorizar las medidas de seguridad a través de la gestión continuada de la seguridad correspondiente[587].

• Auditar la seguridad[588].

• Informar sobre el estado de la seguridad[589].

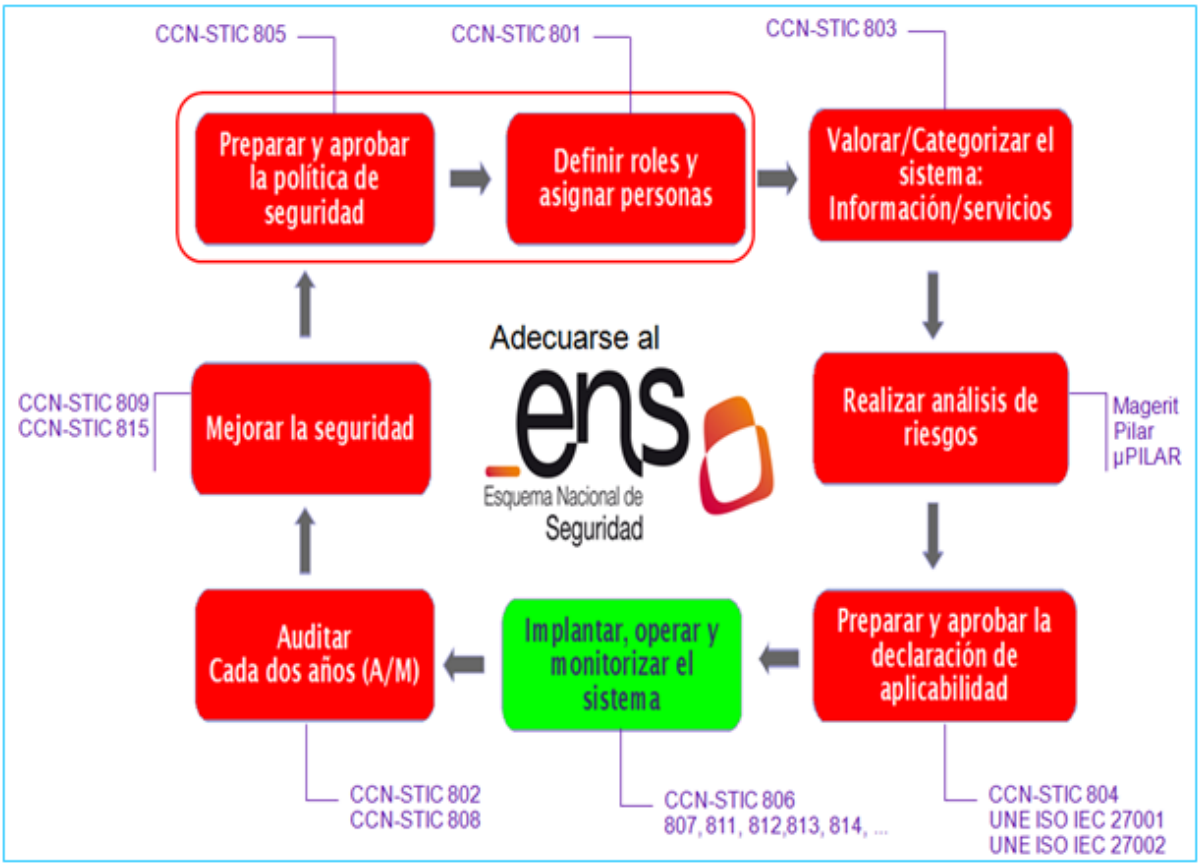
[586] Véase Centro Criptológico Nacional: *Guía de Seguridad CCN-STIC-806. Esquema Nacional de Seguridad: Plan de Adecuación*, Madrid, enero de 2011. https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/806-Plan_adecuacion_ENS/806_ENS-adecuacion_ene-11.pdf consulta: 17 de octubre de 2015.

[587] Véase Centro Criptológico Nacional: *Serie 800 de Guías Esquema Nacional de Seguridad* https://www.ccn-cert.cni.es/guias/guias-series-ccn-stic/800-guia-esquema-nacional-de-seguridad.html consulta: 17 de octubre de 2015.

[588] Véase Centro Criptológico Nacional: *Guía de Seguridad CCN-STIC-802. Esquema Nacional de Seguridad: Guía de Auditoría*, Madrid, junio de 2010 https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/802-Auditoria_ENS/802-Auditoria_ENS-jun10.pdf ; y Centro Criptológico Nacional: *Guía de Seguridad CCN-STIC-808. Esquema Nacional de Seguridad: Verificación del cumplimiento de las medidas en el ENS*, Madrid, septiembre de 2011. https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/808/808-Verificacion_del_cumplimiento_medidas_ENS-sep11.pdf consulta: 17 de octubre de 2015.

[589] Véase Centro Criptológico Nacional: *Guía de Seguridad CCN-STIC-815. Esquema Nacional de Seguridad: Métricas e Indicadores*, Madrid, julio de 2013 https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/815-Metricas_e_Indicadores_en_el_ENS/815_metricas_e_indicadores_ENS.pdf y Centro Criptológico Nacional: Guía de Seguridad CCN-STIC-815. Esquema Nacional de Seguridad: Métricas e Indicadores, Madrid, julio de 2013. consulta: 17 de octubre de 2015.

Figura 68: Adecuación al Esquema Nacional de Seguridad en el ámbito de la administración electrónica



Fuente: Centro Criptológico Nacional[590].

En relación con las herramientas que aparecen en la figura anterior, hay que señalar que el CCN ha ido creando a lo largo de los años de actividad un ecosistema de herramientas tecnológicas para poder disponer de servicios sin depender excesivamente de empresas y de otros estados; en concreto Pilar (análisis de riesgos), Clara (análisis de cumplimiento del ENS), Carmen (detección de APTs), Lucía (Listado Unificado de Coordinación de Incidentes y Amenazas), Marta (análisis de Caballos de Troya avanzados), María (multiantivirus) y Reyes (Repositorio Común y Estructurado de Amenazas y Código Dañino). La Secretaria General del CNI señala que la filosofía que hay detrás del desarrollo de todas estas herramientas puede resumirse en tres

[590] Centro Criptológico Nacional: *Esquema Nacional de Seguridad: Preguntas Frecuentes*, *Opus citada*, p. 21.

premisas. En primer lugar, evitar la dependencia tecnológica en cuestiones de seguridad. Las herramientas son de la Administración española. En segundo término, intentar que el conocimiento se quede en la organización. Las herramientas propias permiten que el "Know-How" resida en los propios organismos de la Administración. Por último, se trata de promover la universidad española y la colaboración público-privada. Todas las herramientas se han desarrollado con la universidad y con la participación de empresas privadas[591].

Joseba Enjuto señala en sus conclusiones sobre el RD. 3/2010, que la aparición del Esquema Nacional de Seguridad supuso un gran reto para todo el sector público nacional, que tenía la obligación legal de mejorar el nivel de seguridad ofrecido por su infraestructura de administración electrónica en un contexto de crisis económica y creciente conflictividad social que hacia todavía más compleja la ya de por sí difícil labor de adecuarse a las exigencias recogidas por dicho Real Decreto. No obstante, Enjuto señalaba que a pocos meses de cumplirse el periodo máximo establecido por dicho Real Decreto para que todas las Administraciones Públicas adecuen sus sistemas de información a lo establecido por el ENS, una gran parte de las mismas todavía no había llevado a cabo los cambios organizativos, normativos, operativos ni tecnológicos necesarios para cumplir con las exigencias del ENS. En ese escenario es donde Enjuto planteaba un análisis para permitir que cualquier Administración Pública pudiera utilizarlo como aclaración práctica para su propia adecuación a las exigencias del Esquema Nacional de Seguridad[592].

6.7.2. La adecuación del ENS en el ámbito de la Administración Electrónica

[591] MÉNDEZ DE VIGO, Beatriz: *Entrevista en revista SIC*. Revista SIC, Ciberseguridad, Seguridad de la Información y Privacidad nº 115, junio de 2015, p. 71.

[592] ENJUTO, Joseba: *Estudio del Esquema Nacional de Seguridad*: *Modelo de Aplicación Práctica del Real Decreto 3/2010*. Máster en Derecho de Internet y Nuevas Tecnologías del Instituto Europeo Campus Stellae, 2013, p. 34.
http://www.criptored.upm.es/descarga/EstudioEsquemaNacionalSeguridadJosebaEnjuto.pdf consulta: 18 de octubre de 2015.

El portal de administración electrónica, en el sitio dedicado al Esquema Nacional de Seguridad, presenta el proyecto de RD. de modificación del RD. 3/2010 de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica[593].

Se señala en este proyecto de Real Decreto que la Ley 11/2007, en su artículo 42.3, establece que el Esquema Nacional de Seguridad debe mantenerse actualizado de manera permanente y, en desarrollo de este precepto, el Real Decreto 3/2010, establece que el Esquema Nacional de Seguridad se desarrollará y perfeccionará a lo largo del tiempo en paralelo al progreso de los servicios de Administración electrónica, la evolución de la tecnología, los nuevos estándares internacionales sobre seguridad y auditoría, y la consolidación de las infraestructuras que le sirven de apoyo, manteniéndose actualizado de manera permanente. De esta forma, los ciudadanos confían en que los servicios públicos disponibles por el medio electrónico se presten en unas condiciones de seguridad equivalentes a las que encuentran cuando se acercan personalmente a las oficinas de la Administración.

Por otra parte, continúa señalando el proyecto de Real Decreto que las ciberamenazas, que constituyen riesgos que afectan singularmente a la Seguridad Nacional, se han convertido en un potente instrumento de agresión contra particulares y entidades públicas y privadas, de manera que la ciberseguridad figura entre los doce ámbitos prioritarios de actuación de la Estrategia de Seguridad Nacional como instrumento actualizado para encarar el constante y profundo cambio mundial en el que nos hayamos inmersos y como garantía de la adecuada actuación de España en el ámbito internacional.

En particular, dicho ámbito de actuación de ciberseguridad se refiere a la garantía de la seguridad de los sistemas de información y las redes de comunicaciones e infraestructuras comunes a todas las Administraciones Públicas y a que se finalizará

[593] Véase: Portal de administración electrónica. http://administracionelectronica.gob.es/ctt/altaSuscripcion.htm?idIniciativa=146#.VIlsRRO8PGc consulta: 17 de octubre de 2015.

la implantación del Esquema Nacional de Seguridad, previsto en la Ley 11/2007, de 22 de junio. Profundizando en la cuestión, la Estrategia de Ciberseguridad Nacional en su Objetivo I se refiere a "Garantizar que los Sistemas de Información y Telecomunicaciones que utilizan las Administraciones Públicas poseen el adecuado nivel de ciberseguridad y resiliencia" y en su línea de acción 2, titulada "Seguridad de los Sistemas de Información y Telecomunicaciones que soportan las Administraciones Públicas", se incluye la medida relativa a "Asegurar la plena implantación del Esquema Nacional de Seguridad y articular los procedimientos necesarios para conocer regularmente el estado de las principales variables de seguridad de los sistemas afectados".

Por todo ello, y en particular dada la rápida evolución de las tecnologías de aplicación y la experiencia derivada de la implantación del Esquema Nacional de Seguridad aconsejan la actualización de esta norma. Y en ese sentido, se modifican una serie de artículos (11, 15, 18, 19, 24, 29, 35 a 37 inclusive) y los Anexos II a V con dicha finalidad y con el fin de adecuarse a lo previsto en el Reglamento nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014[594], relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE.

Es significativa la modificación del artículo 24 del Real Decreto por el que se regula el ENS, que se refiere a los incidentes de seguridad, que recogía en su apartado 2 que "Se registrarán los incidentes de seguridad que se produzcan y las acciones de tratamiento que se sigan", lo que queda modificado señalando que "Se dispondrá de procedimientos de gestión de incidentes de seguridad y de debilidades detectadas en los elementos del sistema de información. Estos procedimientos cubrirán los mecanismos de detección, los criterios de clasificación, los procedimientos de análisis y resolución, así como los cauces de comunicación a las partes interesadas y el

[594] Unión Europea: *Reglamento (UE) No 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE*. https://www.boe.es/doue/2014/257/L00073-00114.pdf consulta: 17 de octubre de 2015.

registro de las actuaciones". Se estima que estas acciones mejoran la calidad del proceso y contribuirán a reforzar el proceso de gestión de incidentes.

También, fruto de la experiencia, se modifica el artículo 29 del citado Real Decreto, El título del artículo 29, "Guías de seguridad", queda modificado como "Instrucciones y guías de seguridad", modificando el texto que señalaba que el el Centro Criptológico Nacional, en el ejercicio de sus competencias, elaborará y difundirá las correspondientes guías de seguridad de las tecnologías de la información y las comunicaciones, que queda ampliado añadiendo dos apartados, 2 y 3, con la siguiente redacción: "2. El Ministerio de Hacienda y Administraciones Públicas, a propuesta del Comité Sectorial de Administración Electrónica previsto en el artículo 40 de la Ley 11/2007, de 22 de junio, y a iniciativa del Centro Criptológico Nacional, aprobará las instrucciones técnicas de seguridad de obligado cumplimiento y se publicarán mediante Resolución de la Secretaria de Estado de Administraciones Públicas. Para la redacción y mantenimiento de las instrucciones técnicas de seguridad se constituirán los correspondientes grupos de trabajo en los órganos colegiados con competencias en materia de administración electrónica. 3. Las instrucciones técnicas de seguridad tendrán en cuenta las normas armonizadas a nivel europeo que resulten de aplicación". De esta forma, se refuerza el sistema obteniendo estas instrucciones y guías de seguridad un carácter obligatorio.

La modificación del artículo 29 del Real Decreto se considera especialmente significativa, como se recoge en la memoria de acompañamiento de la propuesta de Real Decreto[595], que señala que las Guías CCN-STIC de la serie 800, han venido proporcionando orientación extensa, de naturaleza tanto organizativa como técnica, relativa a la implantación del ENS en los organismos públicos españoles. Sin embargo, dado que los contenidos de tales guías tienen la naturaleza jurídica de recomendaciones, su efecto es limitado en aquellos aspectos que puedan requerir una

[595] Ministerio de Hacienda y Administraciones Públicas: *Memoria del análisis de impacto normativo sobre el proyecto de Real Decreto de modificación del Real Decreto 3/2010 de 8 de enero por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica*. 29 de abril de 2015.

armonización más allá de la mera recomendación en el modo de actuar. Para superar esta limitación se introduce la figura de las “instrucciones técnicas de seguridad”, para las que se aplicarían los procedimientos de elaboración, publicación y adopción ya consolidados en el ámbito de la Interoperabilidad. Esta medida persigue disponer de regulaciones de obligado cumplimiento sobre aquellas cuestiones que, de forma especialmente significativa, afectan a la seguridad de la información de los organismos públicos y los servicios que prestan, y que hicieran necesaria una mayor concreción y detalle, señalando el modo común de actuar.

La modificación del artículo 35 del RD, sobre “Informe del estado de la seguridad” es también de calado, incorporando que **“**El Centro Criptológico Nacional articulará los procedimientos necesarios para la recogida y consolidación de la información, así como los aspectos metodológicos para su tratamiento y explotación, a través de los correspondientes grupos de trabajo que se constituyan al efecto en el Comité Sectorial de Administración Electrónica y en la Comisión de Estrategia TIC para la Administración General del Estado”. En la citada memoria justificativa de la modificación del Real Decreto se señala que es necesario el despliegue de mecanismos periódicos de recogida de información, en las adecuadas condiciones de eficacia y eficiencia, para lo que deben añadirse referencias expresas a la articulación de los procedimientos necesarios para la recogida y consolidación de la información y organismos responsables de su realización.

La memoria justificativa mencionada, dedica un apartado a la modificación del artículo 36, “Capacidad de respuesta a incidentes de seguridad de la información”, señalando que la figura de la notificación de incidentes de seguridad que tengan un impacto significativo se está introduciendo en el ámbito normativo comunitario, configurando una tendencia de actuación en la materia, de esta forma. se introduce la obligación de notificar ciertos incidentes, reservando para la correspondiente instrucción técnica de seguridad la determinación de las características de los incidentes sujetos a notificación y el procedimiento para realizarlo. En este sentido, este artículo 36 expresa que “Las Administraciones Públicas notificarán al Centro Criptológico Nacional

aquellos incidentes que tengan un impacto significativo en la seguridad de la información manejada y de los servicios prestados".

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, incluye la disposición adicional segunda titulada "Instituto Nacional de Tecnologías de la Comunicación (INTECO) y organismos análogos", que señalaba que "El Instituto Nacional de Tecnologías de la Comunicación (INTECO), como centro de excelencia promovido por el Ministerio de Industria, Turismo y Comercio para el desarrollo de la sociedad del conocimiento, podrá desarrollar proyectos de innovación y programas de investigación dirigidos a la mejor implantación de las medidas de seguridad contempladas en el presente real decreto. Asimismo, las Administraciones públicas podrán disponer de entidades análogas para llevar a cabo dichas actividades u otras adicionales en el ámbito de sus competencias". El proyecto de RD. de modificación del RD. 3/2010 elimina esta disposición.

El Consejo de Estado, en su dictamen número 710/2015, emitido por unanimidad, tras examinar el expediente relativo al proyecto de Real Decreto de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, dictaminó que este proyecto de Real decreto podía someterse a la aprobación del Consejo de Ministros.

Este Real Decreto viene a facilitar la mejora del ENS, aunque deberá realizarse un esfuerzo para mejorar la gestión técnica de la seguridad de la información tratada en sistemas tecnológicos y su adecuación al ENS y otras legislaciones y normas sectoriales. Como apunta la Secretaria General del CNI, la impresión no era positiva en cuanto a la apreciación de la necesidad de que los CIO (Directores de Tecnologías de la Información, o *Chief Information Officers* en idioma inglés) de empresas estratégicas y los CIO del sector público inviertan una cantidad adecuada de su presupuesto de TIC en este ámbito. Actualmente el objetivo del CIO es invertir en tener ajustado su cumplimiento normativo respecto a lo que se les pide en protección de datos, Esquema Nacional de Seguridad y en su caso infraestructuras críticas. La

impresión de la Secretaria General del CNI es que solo conseguir este objetivo de cumplir lo que demanda el Gobierno no es suficiente para hacer frente a ataques complejos y necesitamos la potenciación de las capacidades de vigilancia y respuesta[596].

6.7 3. Análisis y gestión de riesgos de la ciberseguridad en España en el ENS

El análisis y la gestión de los riesgos constituyen aspectos clave del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, que tiene la finalidad de poder dar satisfacción al principio de proporcionalidad en el cumplimiento de los principios básicos y requisitos mínimos para la protección adecuada de la información[597].

Las herramientas de análisis de riesgos - EAR - soportan el análisis y la gestión de riesgos de un sistema de información siguiendo la metodología metodología de análisis y gestión de riesgos - Magerit - elaborada por el Consejo Superior de Administración Electrónica. La razón de ser de esta metodología está directamente relacionada con la generalización del uso de las tecnologías de la información[598].

Los activos están expuestos a amenazas que, cuando se materializan, degradan el activo, produciendo un impacto. Si estimamos la frecuencia con que se materializan las amenazas, podemos deducir el riesgo al que está expuesto el sistema. Degradación y frecuencia califican la vulnerabilidad del sistema. El gestor del sistema de información dispone de salvaguardas, que o bien reducen la frecuencia de ocurrencia, o bien reducen o limitan el impacto. Dependiendo del grado de

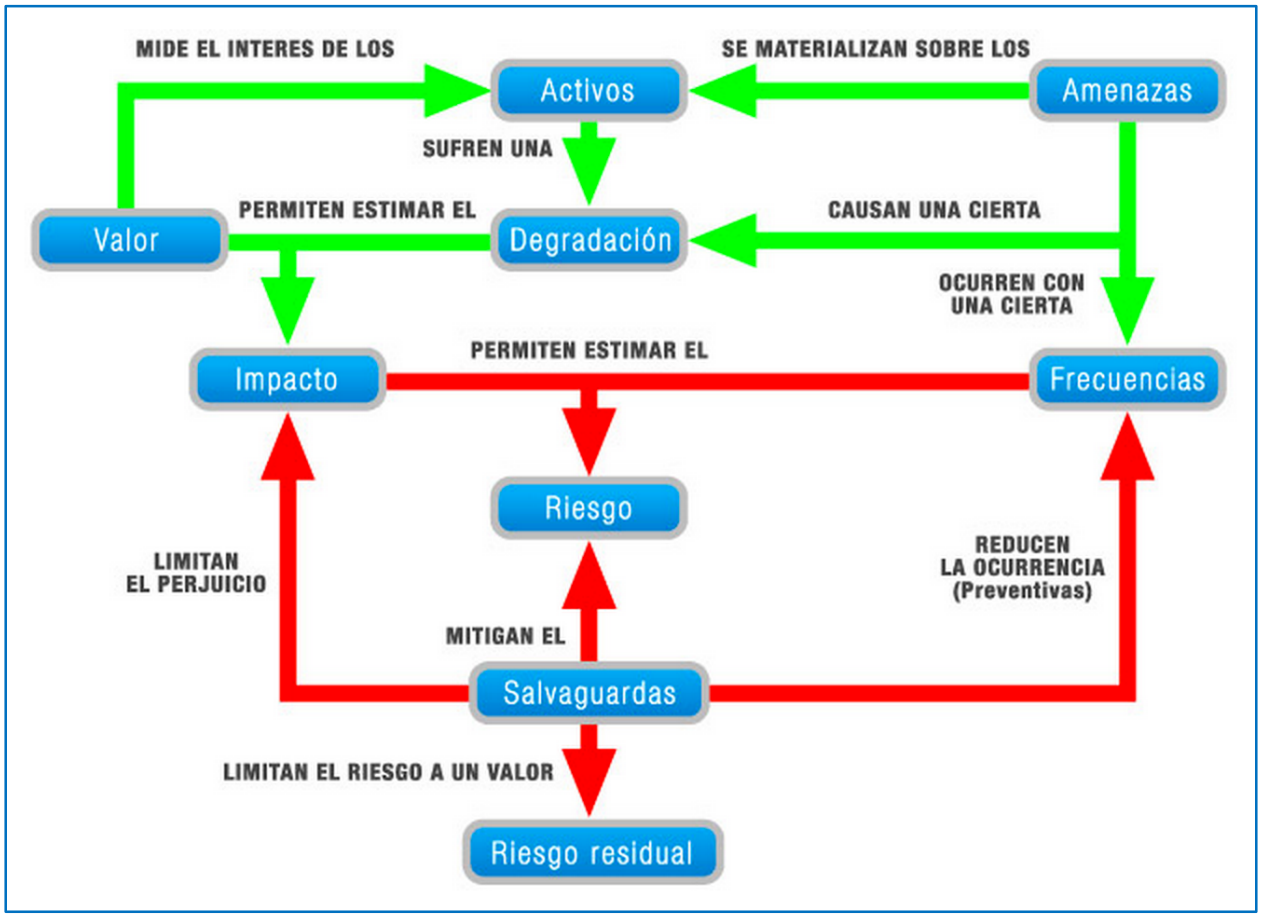
[596] MÉNDEZ DE VIGO, Beatriz: *opus citada*, p. 71.

[597] Gobierno de España: Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. https://www.boe.es/buscar/doc.php?id=BOE-A-2010-1330 consulta: 14 de septiembre de 2015.

[598] Gobierno de España, Portal de Administración Electrónica. Magerit: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.VfdTmNPtmko consulta 14 de septiembre de 2015.

implantación de estas salvaguardas, el sistema pasa a una nueva estimación de riesgo que se denomina riesgo residual[599].

Figura 69: Diagrama de gestión de riesgos de la ciberseguridad en España



Fuente: CCN-CERT[600].

El Centro Criptológico Nacional ha patrocinado el desarrollo de la herramienta comercial PILAR, que está siendo ampliamente utilizada en la administración pública española. PILAR, acrónimo de "Procedimiento Informático-Lógico para el Análisis de Riesgos" es una herramienta desarrollada bajo especificación del Centro Nacional de

[599] CCN-CERT: *Análisis de riesgos*. https://www.ccn.cni.es/index.php?option=com_content&view=article&id=7&Itemid=10&lang=es consulta: 14 de septiembre de 2015.

[600] *Ibídem.*

Inteligencia para soportar el análisis de riesgos de sistemas de información siguiendo la metodología Magerit, soportando la herramienta todas las fases del método: caracterización de los activos, identificación, clasificación, dependencias y valoración; caracterización de las amenazas; y evaluación de las salvaguardas. La herramienta incorpora catálogos generales que permiten una homogeneidad en los resultados del análisis: tipos de activos; dimensiones de valoración; criterios de valoración; catálogo de amenazas. Para incorporar estos catálogos, PILAR diferencia entre el motor de cálculo de riesgos y la biblioteca de elementos, que puede ser reemplazada para seguir el paso de la evolución en el tiempo de los catálogos de elementos. La herramienta evalúa el impacto y el riesgo, acumulado y repercutido, potencial y residual, presentándolo de forma que permita el análisis de por qué se da cierto impacto o cierto riesgo. Las salvaguardas se califican por fases, permitiendo la incorporación a un mismo modelo de diferentes situaciones temporales. Típicamente se puede incorporar el resultado de los diferentes proyectos de seguridad a lo largo de la ejecución del plan de seguridad, monitorizando la mejora del sistema[601].

[601] Ministerio de Hacienda y Administraciones Públicas: *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método*. Madrid, octubre de 2012. http://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Documentacion/Metodologias-y-guias/Mageritv3/2012_Magerit_v3_libro1_metodo_ES_NIPO_630-12-171-8/2012_Magerit_v3_libro1_m%C3%A9todo_es_NIPO_630-12-171-8.pdf consulta: 14 de septiembre de 2015.

CAPÍTULO 7. PROPUESTA DE UN MODELO DE ORGANIZACIÓN DE LA CIBERSEGURIDAD EN ESPAÑA.

7.1. ORGANIZACIÓN ACTUAL DE LA GOBERNANZA DE LA CIBERSEGURIDAD EN ESPAÑA.

Al analizar el proceso de planeamiento de la ciberseguridad en España, se han ido presentando diferentes organismos relacionados con esta planificación. Este **proceso de planeamiento comprende tres niveles**: **político estratégico**, **operacional** y **táctico / técnico**.

Existen también unos **niveles de ejecución y desarrollo** de estos procesos de planeamiento que se encuentran asociados a diferentes organismos con responsabilidad de ejecutar y llevar a cabo las decisiones adoptadas en los diferentes niveles de planeamiento. Estos niveles orgánicos de responsabilidad se encuentran asociados a diferentes autoridades y quedan establecidos en **nivel estratégico**, **nivel operacional** y **nivel táctico / técnico**.

Algunos organismos tienen solamente responsabilidad en el planeamiento o en la ejecución, mientras que otros poseen competencias tanto en planeamiento como en ejecución.

A continuación se van a presentar los diferentes organismos que conforman el **modelo actual de la gobernanza de ciberseguridad en España**, especificando en qué niveles de responsabilidad se encuentran.

7.1.1. NIVEL POLÍTICO ESTRATÉGICO

La Ley 36/2015, de 28 de septiembre, de Seguridad Nacional especifica los órganos competentes en materia de Seguridad Nacional, que se incorporan en el **nivel político estratégico**[602].

[602] *Ley 36/2015, de 28 de septiembre, de Seguridad Nacional*, opus citada, artículos 12-17.

Las Cortes Generales: Debaten las líneas generales de la política de Seguridad Nacional. En el seno de la Comisión Mixta Congreso-Senado de Seguridad Nacional comparecerá anualmente el Gobierno, para informar sobre la evolución de la Seguridad Nacional. En esta Comisión Mixta será presentada la Estrategia de Seguridad Nacional y sus revisiones.

El Gobierno tiene la responsabilidad de establecer y dirigir la política de Seguridad Nacional y asegurar su ejecución; aprobar la Estrategia de Seguridad Nacional y sus revisiones; y efectuar la Declaración de Recursos de Interés para la Seguridad Nacional en coordinación con las Comunidades Autónomas.

Al **Presidente del Gobierno** le corresponde: dirigir la política de Seguridad Nacional y el Sistema de Seguridad Nacional; proponer la Estrategia de Seguridad Nacional y sus revisiones; declarar la Situación de Interés para la Seguridad Nacional; y ejercer el resto de competencias en el marco del Sistema de Seguridad Nacional.

A los Ministros, como responsables de desarrollar la acción del Gobierno en las materias que les son propias, les corresponde desarrollar y ejecutar la política de Seguridad Nacional en los ámbitos de sus respectivos departamentos ministeriales.

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.

En el ámbito específico de la ciberseguridad, en el **nivel político estratégico** se encuentra el **Consejo Nacional de Ciberseguridad (CNCS)**. El CNCS es el órgano colegiado de apoyo del Consejo de Seguridad Nacional para el cumplimiento de sus funciones y, en particular, en la asistencia al Presidente del Gobierno en la dirección y coordinación de la Política de Seguridad Nacional en el ámbito de la ciberseguridad.

Este Consejo se encuentra presidido desde su conformación, el 24 de febrero de 2015, por el Secretario de Estado Director del Centro Nacional de Inteligencia, que también

es Director del Centro Criptológico Nacional, organismo adscrito al CNI. En este Consejo se encuentran representados todos los Ministerios con competencias en materia de ciberseguridad. Es significativo señalar que aunque cuando se estableció este Consejo Nacional de Ciberseguridad se especificó que la presidencia sería anual y rotatoria, entre autoridades de los Ministerios de la Presidencia, del Interior, de Industria, Energía y Turismo, de Defensa y de Asuntos Exteriores y de Cooperación, el Consejo de Seguridad Nacional decidió que el secretario de Estado Director del CNI continuara presidiendo el Consejo Nacional de Ciberseguridad.

El Consejo Nacional de Ciberseguridad ha confeccionado el Plan Nacional de Ciberseguridad, que fue aprobado por el Consejo de Seguridad Nacional. El CNCS aprobó posteriormente nueve Planes Derivados de este Plan Nacional de Ciberseguridad, para desarrollar las líneas de acción de la Estrategia de Ciberseguridad Nacional.

El CNCS se encuentra en el nivel político estratégico del planeamiento de la ciberseguridad nacional, aunque no tiene competencias para establecer la conducción de la ciberseguridad en España. Por consiguiente, se encuentra fuera de la estructura orgánica de la conducción de la ciberseguridad.

En el **nivel político estratégico de la conducción** de la ciberseguridad nacional para la implementación del resultado del planeamiento nacional de la ciberseguridad se encuentran los **Ministros y Secretarios de Estado**, que deben ejecutar las decisiones del CNCS y las suyas propias que desarrollen las del Consejo Nacional de Ciberseguridad, u otras acciones en el marco de sus competencias.

7.1.2. NIVEL OPERACIONAL

En este nivel se encuentran los organismos encargados de traducir la estrategia decidida por el nivel superior en acciones concretas a cumplir por el nivel táctico y técnico.

En el caso de la ciberseguridad **el nivel operacional se focaliza en las Secretarías de Estado y el Mando de Operaciones en el caso del Ministerio de Defensa**.

El Centro Nacional de Inteligencia, según lo establecido en la Ley 11/2002, de 6 de mayo, tiene como misión facilitar al Presidente del Gobierno y al Gobierno de la Nación las informaciones, análisis, estudios o propuestas que permitan prevenir y evitar cualquier peligro, amenaza o agresión contra la independencia o integridad territorial de España, los intereses nacionales y la estabilidad del Estado de derecho y sus instituciones. Entre sus funciones se encuentran obtener, evaluar e interpretar información y difundir la inteligencia necesaria para proteger y promover los intereses políticos, económicos, industriales, comerciales y estratégicos de España; obtener, evaluar e interpretar el tráfico de señales de carácter estratégico, para el cumplimiento de los objetivos de inteligencia señalados al Centro; coordinar la acción de los diferentes organismos de la Administración que utilicen medios o procedimientos de cifra, garantizar la seguridad de las tecnologías de la información en ese ámbito y velar por el cumplimiento de la normativa relativa a la protección de la información clasificada.

La Secretaría de Estado de Seguridad del Ministerio del Interior, está regulada por el Real Decreto 1823/2011 por el que se reestructuran los departamentos ministeriales, y por Real Decreto 400/2012, por el que se desarrolla la estructura orgánica básica del Ministerio del Interior, que le asigna funciones como el ejercicio del mando de las Fuerzas y Cuerpos de Seguridad del Estado (funciones recogidas en la Ley Orgánica 2/1986) y la dirección, impulso y coordinación de las actuaciones del Departamento en materia de crimen organizado, tráfico de drogas, blanqueo de capitales relacionado con dicho tráfico y delitos conexos, el control de las empresas y personal de seguridad privada, terrorismo, y la dirección y coordinación de la cooperación policial internacional.

La Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, regulada por el Real Decreto 1823/2011 por el que se reestructuran los departamentos ministeriales y por Real Decreto 344/2012 de 10 de febrero, por el que

se desarrolla la estructura orgánica básica del Ministerio de Industria, Energía y Turismo, tiene encomendadas las funciones de: elaboración y propuesta de la normativa referente a la ordenación y regulación de las telecomunicaciones y la Sociedad de la Información; colaboración con los órganos responsables del Ministerio de Asuntos Exteriores y de Cooperación en el estudio, propuesta y coordinación de la política que se debe seguir en la Unión Europea y en los demás organismos internacionales en materia de telecomunicaciones; el fomento e integración de las tecnologías de la información en todos los ámbitos de la actividad económica y social; fomento del uso y acceso a la Sociedad de la Información y a las comunicaciones electrónicas a empresas, organismos y ciudadanos garantizando los derechos de consumidores y usuarios; el mantenimiento de las relaciones de la Administración General del Estado con los prestadores de servicios y redes de telecomunicaciones; y cualesquiera otras funciones relativas al sector de las telecomunicaciones y las tecnologías de la información que el ordenamiento jurídico atribuya al Departamento y que no estén específicamente asignadas a otros órganos.

Adscrita al Ministerio de Industria, Energía y Turismo a través de la Secretaria de Estado de Telecomunicaciones y para la Sociedad de la Información, se encuentra la entidad pública empresarial Red.es, que es accionista única de INCIBE S.A.

Según el Real Decreto 872/2014, de 10 de octubre, por el que se establece la organización básica de las Fuerzas Armadas, el **Estado Mayor de la Defensa** es el órgano que posibilita el cumplimiento de sus funciones al Jefe de Estado Mayor de la Defensa. Se organizará de forma que permita la definición y el desarrollo de la estrategia militar, el planeamiento militar, el planeamiento, seguimiento y conducción de las operaciones militares y el ejercicio del resto de sus competencias. Entre otras funciones, al Estado Mayor de la Defensa le corresponderán:

a) El desarrollo y detalle de las políticas de Seguridad de la Información en los Sistemas de Información y Telecomunicaciones, así como la dirección de la ejecución y el control del cumplimiento de estas políticas.

b) La planificación, dirección y, en su caso, ejecución, en su ámbito, de las actuaciones en materia de cartografía.

c) La dirección y coordinación de la sanidad operativa.

El mismo RD atribuye al **Comandante del Mando de Operaciones** el control operacional de las organizaciones operativas que se creen, tanto con carácter temporal como permanente.

En el **nivel operacional**, **no existe un organismo con competencias a nivel nacional** para realizar el **planeamiento** de ciberseguridad nacional en este nivel, desarrollando de modo integral los planes que emanan del Consejo Nacional de Ciberseguridad. **Tampoco existe este nivel en el aspecto orgánico de la conducción** de la ciberseguridad nacional. **Solamente el Centro Criptológico Nacional** tiene por ley competencias que desarrollan **aspectos concretos a nivel operacional** en los ámbitos de la formación, certificación, respuesta a incidentes que afecten a las Administraciones Públicas y empresas de carácter estratégico; además de los especificados en el Esquema de Seguridad Nacional en el ámbito de la Administración Electrónica.

Las Secretarías de Estado de los Ministerios y el Mando de Operaciones de las Fuerzas Armadas, desarrollan, en algunos casos, funciones que pueden considerarse encuadradas en el nivel operacional de la ciberseguridad, aunque circunscritas al ámbito específico de sus áreas de responsabilidad y no de modo integral en el ámbito nacional.

7.1.3. NIVEL TÁCTICO Y TÉCNICO

En el **nivel táctico y técnico** de la ciberseguridad en España se encuentran varios organismos con diferentes grados de responsabilidad en distintos ámbitos.

En el nivel táctico se integran los objetivos diseñados en proceso de planeamiento del nivel operacional.

Además, en el caso de la ciberseguridad, se introduce un **nivel técnico**, relacionado con las capacidades en las fases de prevención, detección y respuesta a incidentes de ciberseguridad, generalmente a través de los Equipos de Respuesta ante Incidentes Informáticos, CERT. En la actualidad, los CERT no solamente gestionan ciberincidentes, sino que han ido evolucionando hacia un modelo integral de gestión de la ciberseguridad en donde se tienen en cuenta todos los elementos técnicos, humanos, materiales y organizativos de un sistema, y en donde predominan los servicios proactivos y de alerta temprana.

A continuación se van a presentar las principales organizaciones con responsabilidades en este nivel, en diferentes ámbitos de actuación y con diferentes responsabilidades.

CCN-CERT

El Centro Criptológico Nacional se ha tratado en esta tesis doctoral de modo extenso, dado que sus competencias en materia de ciberseguridad nacional son amplias, y se han incorporado elementos relacionados con el CCN en diferentes fases de la investigación.

El CCN desarrolla actividades en el nivel operacional, señalándose en el Real Decreto 421/2004 que el Secretario de Estado Director del Centro Nacional de Inteligencia, como Director del Centro Criptológico Nacional (CCN), es la autoridad responsable de coordinar la acción de los diferentes organismos de la Administración que utilicen medios o procedimientos de cifra, garantizar la seguridad de las tecnologías de la información en ese ámbito, informar sobre la adquisición coordinada del material criptológico y formar al personal de la Administración especialista en este campo. En este sentido, el Director del CCN es la autoridad de certificación de la seguridad de las tecnologías de la información y la autoridad de certificación criptológica. Asimismo es responsable de velar por el cumplimiento de la normativa relativa a la protección de la información clasificada en los aspectos de los sistemas de información y

telecomunicaciones, de acuerdo a lo señalado en el artículo 4.e) y f) de la Ley 11/2002, de 6 de mayo[603].

En el nivel táctico y técnico, el Centro Criptológico Nacional desarrolla la mayor parte de sus actividades en relación con el formato de CERT gubernamental. El CCN-CERT es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional. Este servicio se creó a finales del año 2006 como CERT gubernamental español, y sus funciones quedan recogidas en el capítulo VII del RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad. Este texto legal, en su artículo 37 señala los servicios que el CCN-CERT ya prestaba desde su constitución (en parte recogidos en el RD 421/2004 de regulación del CCN).

Su principal objetivo es contribuir a la mejora del nivel de seguridad de los sistemas de información de las tres administraciones públicas existentes en España (general, autonómica y local). Su misión es convertirse en el centro de alerta nacional que coopere y ayude a todas las administraciones públicas a responder de forma rápida y eficiente a los incidentes de seguridad que pudieran surgir, y afrontar de forma activa las nuevas amenazas a las que hoy en día están expuestas.

Para contribuir a esta mejora del nivel de seguridad, el CCN-CERT ofrece sus servicios a todos los responsables de Tecnologías de la Información de las diferentes administraciones públicas a través de cinco grandes líneas de actuación:

- Soporte y coordinación para el tratamiento de vulnerabilidades y la resolución de incidentes de seguridad que tengan la Administración General del Estado, las administraciones de las comunidades autónomas, las entidades que integran la Administración Local y las Entidades de Derecho público con personalidad jurídica propia vinculadas o dependientes de cualquiera de las administraciones indicadas. El CCN-CERT, a través de su servicio de apoyo técnico y de coordinación, actuará con la máxima celeridad ante cualquier

[603] *Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional*. Publicado en: «BOE» núm. 68, de 19 de marzo de 2004, artículo 1. http://www.boe.es/diario_boe/txt.php?id=BOE-A-2004-5051 consulta: 31 de octubre de 2015.

agresión recibida en los sistemas de información de las administraciones públicas. Para el cumplimiento de los fines indicados en los párrafos anteriores se podrán recabar los informes de auditoría de los sistemas afectados.

- Investigación y divulgación de las mejores prácticas sobre seguridad de la información entre todos los miembros de las administraciones públicas. Con esta finalidad, las series de documentos CCN-STIC ofrecerán normas, instrucciones, guías y recomendaciones para aplicar el ENS y para garantizar la seguridad de los sistemas de Tecnologías de la Información en la Administración.
- Formación destinada al personal de la Administración especialista en el campo de la seguridad TIC, al objeto de facilitar la actualización de conocimientos y de lograr la sensibilización y mejora de sus capacidades para la detección y gestión de incidentes.
- Información sobre vulnerabilidades, alertas y avisos de nuevas amenazas a los sistemas de información, recopiladas de diversas fuentes de reconocido prestigio, incluidas las propias.
- Impulso de nuevas capacidades de respuesta a incidentes en las AAPP. El CCN desarrollará un programa que ofrezca la información, formación, recomendaciones y herramientas necesarias para que las administraciones públicas puedan desarrollar sus propias capacidades de respuesta a incidentes de seguridad.

EL CCN-CERT viene desarrollando, desde el año 2008, un Sistema de Alerta Temprana (SAT) que busca actuar antes de que se produzca un incidente o, por lo menos, detectarlo en un primer momento para reducir su impacto y alcance. Este sistema para la detección rápida de incidentes y anomalías dentro de la Administración y de las empresas de interés estratégico, se enmarca dentro de las acciones preventivas, correctivas y de contención realizadas por el CERT Gubernamental Nacional. El SAT cuenta con dos vertientes con un denominador común: la detección temprana de intrusiones. En ambos casos existe un portal de informes al que los

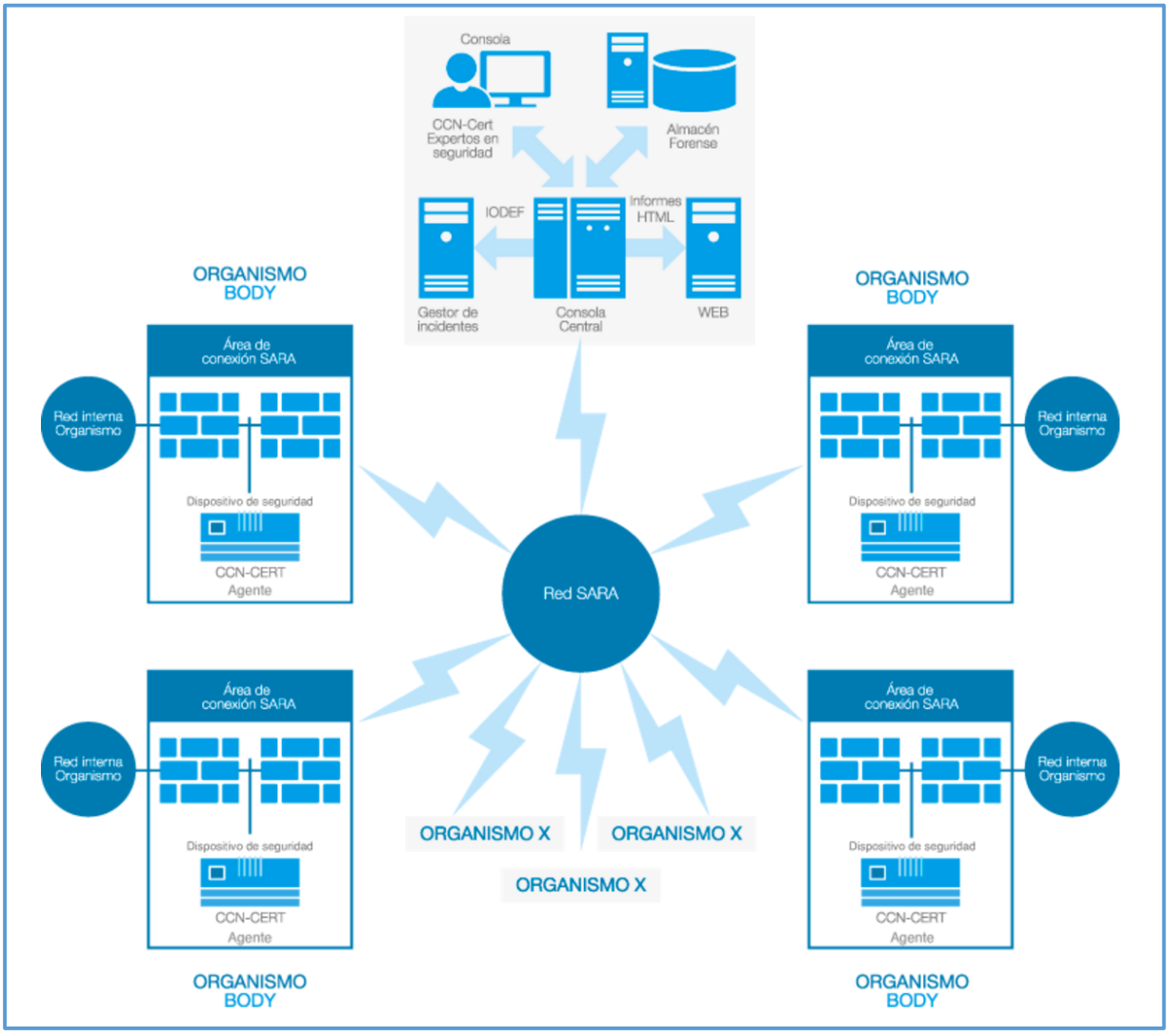
responsables de seguridad autorizados pueden acceder para la consulta en tiempo real de eventos de seguridad y para la generación de informes a medida[604].

El CCN-CERT da servicio también a la red SARA (Sistema de Aplicaciones y Redes para las Administraciones), que es un conjunto de infraestructuras de comunicaciones y servicios básicos que conecta las redes de las Administraciones Públicas Españolas e instituciones europeas facilitando el intercambio de información y el acceso a los servicios. Su implantación se establece como una obligación en el artículo 43 de la Ley 11/2007 de Acceso Electrónico de los Ciudadanos a los Servicios Públicos y en el artículo 13 del Real Decreto 4/2010 que regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica. La Resolución de 19 de julio de 2011, aprueba la Norma Técnica de Interoperabilidad de requisitos de conexión a la red de comunicaciones de las Administraciones Públicas españolas, estableciendo las condiciones en las que cualquier órgano de una administración, o entidad de derecho público vinculada o dependiente de aquella, accederá a la Red SARA.

El Sistema de Alerta Temprana (SAT) de la red SARA (SAT-SARA) es un servicio desarrollado por el CCN-CERT en colaboración con el Ministerio de Hacienda y Administraciones Públicas (Organismo responsable de la red SARA). Su objetivo es la detección en tiempo real de ataques y amenazas, llevado a cabo a través del análisis del tráfico de red que circula entre las redes de los Organismos de las Administraciones Públicas conectados a la red SARA. El sistema se complementa con el análisis de otras fuentes de detección (registros de log) que son recogidas por un Sistema Central para su análisis y correlación. En ningún momento el sistema se centra en el análisis del contenido del tráfico, si no es relevante en la detección de una amenaza[605].

[604] Véase la información facilitada por el CCN-CERT en https://www.ccn-cert.cni.es/gestion-de-incidentes/sistema-de-alerta-temprana-sat.html consulta: 31 de octubre de 2015.
[605] Véase la información facilitada por el CCN-CERT en https://www.ccn-cert.cni.es/gestion-de-incidentes/sistema-de-alerta-temprana-sat/sat-sara.html consulta: 31 de octubre de 2015.

Figura 69: Arquitectura de la red SAT-SARA



Fuente: CCN-CERT[606].

El CCN-CERT también ha desarrollado la herramienta LUCIA (Listado Unificado de Coordinación de Incidentes y Amenazas) para la gestión de ciberincidentes en las entidades del ámbito de aplicación del Esquema Nacional de Seguridad. Con ella se pretende mejorar la coordinación entre el CERT Gubernamental Nacional y los distintos organismos y organizaciones con las que colabora. LUCIA ofrece un lenguaje común de peligrosidad y clasificación del incidente y mantiene la trazabilidad y el

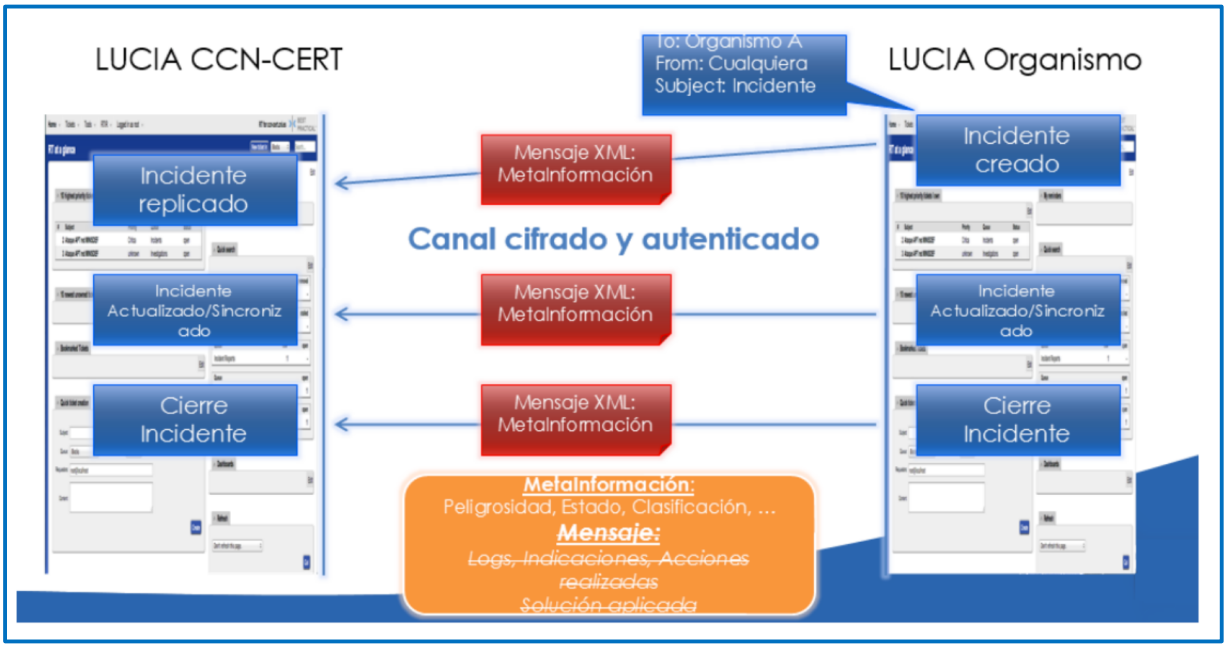
[606] *Ibídem.*

seguimiento del mismo. El sistema permite, además, automatizar las tareas e integrarse con otros sistemas ya implantados.

Con la herramienta LUCIA, el organismo podrá gestionar tres tipos de ciberincidentes:

- Los incidentes propios del Organismo
- Los provenientes del Sistema de Alerta Temprana de Red SARA (SAT-SARA).
- Los provenientes del Sistema de Alerta Temprana de Internet (SAT-INET).

Figura 70: Comunicación de ciberincidentes



Fuente: CCN-CERT[607].

Es significativo resaltar que aunque el CCN-CERT, como CERT Gubernamental Nacional, sirve a las Administraciones Públicas, a los sistemas clasificados y a las empresas de interés estratégico para el país, buena parte de sus servicios (formación,

[607] CCN-CERT*: Presentación de LUCIA (Listado Unificado de Coordinación de Incidentes y Amenazas)*. https://www.ccn-cert.cni.es/documentos-publicos/877-lucia-presentacion/file.html consulta: 31 de octubre de 2015.

informes, guías, herramientas, etc.) están publicados en su portal web y son de libre disposición para cualquier persona.

MANDO CONJUNTO DE CIBERDEFENSA DE LAS FUERZAS ARMADAS

El Mando Conjunto de Ciberdefensa de las Fuerzas Armadas (MCCD) es el órgano de la estructura operativa, subordinado al Jefe de Estado Mayor de la Defensa (JEMAD), responsable de realizar el planeamiento y la ejecución de las acciones relativas a la ciberdefensa militar en las redes y sistemas de información y telecomunicaciones de las Fuerzas Armadas u otros que pudiera tener encomendados, así como contribuir a la respuesta adecuada en el ciberespacio ante amenazas o agresiones que puedan afectar a la Defensa Nacional[608].

La creación del Mando Conjunto de Ciberdefensa de las Fuerzas Armadas es el resultado de un proceso gradual en el que se destacan cuatro hitos[609]:

- 28 de enero de 2001, aprobación por el JEMAD de la "Visión de la Ciberdefensa Militar". Esta visión orienta la definición, desarrollo y empleo de las capacidades militares nacionales necesarias que permitan garantizar la eficacia en el uso del ciberespacio en las operaciones militares.
- 28 de julio de 2011, aprobación por el JEMAD del "Concepto de Ciberdefensa Militar". Este concepto establece los principios, objetivos y retos de la ciberdefensa en el ámbito militar.
- 12 de julio de 2012, aprobación por el JEMAD del "Plan de Acción para la Obtención de la Capacidad de Ciberdefensa Militar". Este plan se configura como un documento vivo para adaptarse a la naturaleza dinámica del ciberespacio y a la evolución de las tecnologías de la información, y busca la sinergia mediante la coordinación de los esfuerzos entre el ámbito conjunto

[608] Véase definición proporcionada por el Estado Mayor de la Defensa en http://www.emad.mde.es/CIBERDEFENSA/ consulta: 31 de octubre de 2015.
[609] Véase información proporcionada por el Estado Mayor de la Defensa en http://www.emad.mde.es/CIBERDEFENSA/historia/ consulta: 31 de octubre de 2015.

(EMAD), el ámbito corporativo (DIGENIN) y los ámbitos específicos (Ejércitos), así como mediante el aprovechamiento de las estructuras existentes.

- 19 de febrero de 2013, el Ministro de Defensa promulga la "Orden Ministerial 10/2013, por la que se crea el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas".

Esta Orden Ministerial 10/2013 presenta los motivos de la creación del MCCD, al señalar que el ciberespacio plantea un nuevo escenario de posibilidades, pero también de vulnerabilidades y amenazas que lo hacen muy atractivo para determinados actores que quieran infligir un daño a la sociedad mediante la realización de ciberataques. La Estrategia Española de Seguridad de 2011 considera los ciberataques como una amenaza actual, real y en crecimiento para los intereses nacionales, haciendo hincapié en la necesidad de garantizar el uso seguro del ciberespacio[610].

La Directiva de Defensa Nacional de 2012 establece que la disuasión es el resultado de disponer de unas capacidades y de la determinación de utilizarlas si fuera necesario. Para ello, entre otras directrices, establece que el Ministerio de Defensa participe en el impulso de una gestión integral de la ciberseguridad, en el marco de los principios que se establezcan al efecto en la Estrategia de Ciberseguridad Nacional[611].

Esta gestión integral requiere que el Ministerio de Defensa contribuya a la ciberseguridad nacional, no limitándose a la protección de los sistemas de utilización puramente militar. Por lo expresado anteriormente, y debido al carácter crítico de la información que procesan los sistemas de información y telecomunicaciones, su múltiple dependencia, complejidad técnica, cantidad y dispersión geográfica de sus

[610] Ministro de Defensa: *Orden Ministerial 10/2013, de 19 de febrero, por la que se crea el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas*. Boletín Oficial del Ministerio de Defensa núm. 40, 26 de febrero de 2013, Sec. I., pp. 4154-4156.
http://www.ieee.es/Galerias/fichero/Varios/BOD_26.02.2013_MandoConjuntoCiberdefensa.pdf consulta: 31 de octubre de 2015.

[611] Presidencia del Gobierno: *Directiva de Defensa Nacional de 2012: Por una Defensa Necesaria. Por una Defensa Responsable*.
http://www.lamoncloa.gob.es/documents/directivadedefensanacional2012.pdf consulta: 31 de octubre de 2015.

infraestructuras, se requiere la creación de un Mando Conjunto de Ciberdefensa que dirija y coordine las acciones de las Fuerzas Armadas en este ámbito.

El ámbito de actuación del MCCD son las redes y los sistemas de información y telecomunicaciones de las Fuerzas Armadas, así como aquellas otras redes y sistemas que específicamente se le encomienden y que afecten a la Defensa Nacional[612].

La misión del MCCD es el planeamiento y la ejecución de las acciones relativas a la ciberdefensa militar en las redes y sistemas de información y telecomunicaciones de las Fuerzas Armadas u otros que pudiera tener encomendados, así como contribuir a la respuesta adecuada en el ciberespacio ante amenazas o agresiones que puedan afectar a la Defensa Nacional[613].

Figura 71: Cometidos del Mando Conjunto de Ciberdefensa de las Fuerzas Armadas

1. Garantizar el libre acceso al ciberespacio, con el fin de cumplir las misiones y cometidos asignados a las Fuerzas Armadas, mediante el desarrollo y empleo de los medios y procedimientos necesarios.
2. Garantizar la disponibilidad, integridad y confidencialidad de la información, así como la integridad y disponibilidad de las redes y sistemas que la manejan y tenga encomendados.
3. Garantizar el funcionamiento de los servicios críticos de los sistemas de información y telecomunicaciones de las Fuerzas Armadas en un ambiente degradado debido a incidentes, accidentes o ataques.
4. Obtener, analizar y explotar la información sobre ciberataques e incidentes en las redes y sistemas de su responsabilidad.
5. Ejercer la respuesta oportuna, legítima y proporcionada en el ciberespacio ante amenazas o agresiones que puedan afectar a la Defensa Nacional.
6. Dirigir y coordinar, en materia de ciberdefensa, la actividad de los centros de respuesta a incidentes de seguridad de la información de los Ejércitos y el de operaciones de seguridad de la información del Ministerio de Defensa.

[612] Ministro de Defensa: *Orden Ministerial 10/2013, de 19 de febrero, por la que se crea el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas, opus citada,* artículo 3.
[613] *Ibídem*, artículo 4.

7. Ejercer la representación del Ministerio de Defensa en materia de ciberdefensa militar en el ámbito nacional e internacional.
8. Cooperar, en materia de ciberdefensa, con los centros nacionales de respuesta a incidentes de seguridad de la información, de acuerdo con lo que determinen las estrategias y políticas nacionales de ciberseguridad en vigor, así como con otros centros militares de respuesta a incidentes de seguridad de la información en el ámbito internacional.
9. Definir, dirigir y coordinar la concienciación, la formación y el adiestramiento especializado en materia de ciberdefensa.

Fuente: Orden Ministerial 10/2013[614].

En cuanto al mando y dependencias, el Comandante Jefe del MCCD debe ser un Oficial General dependiente orgánicamente del Jefe de Estado Mayor de la Defensa; y el MCCD constituye un órgano perteneciente al Estado Mayor de la Defensa, integrado en la estructura operativa de las Fuerzas Armadas[615].

En el Informe Informe Anual de Seguridad Nacional 2014 se recoge que para facilitar las labores de defensa, explotación y respuesta, a través de laboratorios de análisis forense y de I+D+i, se ha establecido el Centro de Respuesta ante incidentes de Ciberseguridad del Ministerio de Defensa (ESPCERTDEF) en las dependencias del Mando Conjunto de Ciberdefensa[616].

CNPIC

La Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, señala que cada vez es mayor la dependencia que las sociedades tienen del complejo sistema de infraestructuras que dan soporte y posibilitan el normal desenvolvimiento de los sectores productivos, de gestión y de la vida ciudadana en general. Además, estas infraestructuras suelen ser sumamente interdependientes entre sí, razón por la cual los problemas de seguridad que pueden desencadenarse en cascada a través del propio sistema tienen la posibilidad de

[614] *Ibídem,* artículo 5.
[615] *Ibídem,* artículo 6.
[616] Consejo de Seguridad Nacional: *Informe Anual de Seguridad Nacional 2014*, *opus citada*, p. 66.

ocasionar fallos inesperados y cada vez más graves en los servicios básicos para la población. Dentro de las prioridades estratégicas de la seguridad nacional se encuentran las infraestructuras, que están expuestas a una serie de amenazas. Para su protección se hace imprescindible diseñar un planeamiento que contenga medidas de prevención y protección eficaces contra las posibles amenazas hacia tales infraestructuras, tanto en el plano de la seguridad física como en el de la seguridad de las tecnologías de la información y las comunicaciones[617].

Figura 72: Sistema de Protección de Infraestructuras Críticas

a) La Secretaría de Estado de Seguridad del Ministerio del Interior.
b) El Centro Nacional para la Protección de las Infraestructuras Críticas.
c) Los Ministerios y organismos integrados en el Sistema, que serán los incluidos en el anexo de esta Ley.
d) Las Comunidades Autónomas y las Ciudades con Estatuto de Autonomía.
e) Las Delegaciones del Gobierno en las Comunidades Autónomas y en las Ciudades con Estatuto de Autonomía.
f) Las Corporaciones Locales, a través de la asociación de Entidades Locales de mayor implantación a nivel nacional.
g) La Comisión Nacional para la Protección de las Infraestructuras Críticas.
h) El Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas.
i) Los operadores críticos del sector público y privado

Fuente: Ley 8/2011, de 28 de abril[618].

La Secretaría de Estado de Seguridad es el órgano superior del Ministerio del Interior responsable del Sistema de Protección de las infraestructuras críticas nacionales. La Ley crea el Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC), como órgano de asistencia al Secretario de Estado de Seguridad en la

[617] *Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas*. Publicado en: «BOE» núm. 102, de 29 de abril de 2011, preámbulo. http://www.cnpic.es/Biblioteca/Legislacion/Generico/Ley_8-2011_PIC.pdf consulta: 31 de octubre de 2015.
[618] *Ibídem,* artículo 5.

ejecución de las funciones que se le encomiendan a éste como órgano responsable del sistema[619].

El Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas, especifica las funciones del CNPIC[620]:

a) Asistir al Secretario de Estado de Seguridad, actuando como órgano de contacto y coordinación con los agentes del Sistema.

b) Ejecutar y mantener actualizado el Plan Nacional de Protección de las Infraestructuras Críticas.

d) Mantener operativo y actualizado el Catálogo Nacional de infraestructuras estratégicas.

e) Llevar a cabo funciones respecto a los instrumentos de planificación.

f) Elevar al Secretario de Estado de Seguridad las propuestas para la declaración de una zona como crítica.

g) Implantar, bajo el principio general de confidencialidad, mecanismos permanentes de información, alerta y comunicación con todos los agentes del Sistema.

h) Recopilar, analizar, integrar y valorar la información sobre infraestructuras estratégicas procedente de instituciones públicas, servicios policiales, operadores y de los diversos instrumentos de cooperación internacional.

i) Participar en la realización de ejercicios y simulacros en el ámbito de la protección de las infraestructuras críticas.

---

[619] *Ibídem,* artículo 6 y preámbulo.

[620] *Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas*. Publicado en: «BOE» núm. 121, de 21 de mayo de 2011. http://www.cnpic.es/Biblioteca/Legislacion/Generico/REAL_DECRETO_704-2011_BOE-A-2011-8849.pdf consulta: 31 de octubre de 2015.

j) Coordinar los trabajos y la participación de expertos en los diferentes grupos de trabajo y reuniones sobre protección de infraestructuras críticas, en los ámbitos nacional e internacional.

k) Ser, en el ámbito de la Protección de las Infraestructuras Críticas, el Punto Nacional de Contacto con organismos internacionales y con la Comisión Europea.

l) Ejecutar las acciones derivadas del cumplimiento de la Directiva 2008/114/CE[621] en representación de la Secretaría de Estado de Seguridad.

En el ámbito de la ciberseguridad, el CNPIC informa en su sitio web que la Secretaría de Estado de Seguridad y la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información han suscrito un acuerdo en el que se sientan las bases para la colaboración del CNPIC e Instituto Nacional de Ciberseguridad (INCIBE) en materia de respuesta a incidentes para las tecnologías de la información de las infraestructuras críticas ubicadas en España. De esta forma, señala esta información, INCIBE se convierte en una herramienta de apoyo al CNPIC en la gestión de incidentes de ciberseguridad. Ambas entidades han puesto en marcha un Equipo de Respuesta a Incidentes de Seguridad especializado en el análisis y gestión de problemas e incidencias de seguridad tecnológica. De este modo, este Equipo de Respuesta se convierte en el CERT especializado en la gestión de incidentes relacionados con las infraestructuras críticas a nivel nacional[622].

De otra parte, el Informe Anual de Seguridad Nacional 2014 recoge que la nueva Oficina de Coordinación Cibernética, creada en el seno del Centro Nacional para la Protección de las Infraestructuras Críticas del Ministerio del Interior, tiene como fin establecer el vínculo necesario para transmitir las alertas del Centro de Respuesta

[621] *Directiva 2008/114/CE del Consejo de 8 de diciembre de 2008 sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección*. https://www.ccn-cert.cni.es/publico/InfraestructurasCriticaspublico/DirectivaEuropea2008-114-CE.pdf consulta: 31 de octubre de 2015.

[622] Véase *CNPIC - Respuesta a Incidentes en Infraestructuras Críticas* en http://www.cnpic.es/Ciberseguridad/1_Respuesta_a_incidentes/index.html consulta: 31 de octubre de 2015.

ante Incidentes de Ciberseguridad de Seguridad e Industria a los operadores críticos por medio de un canal de comunicación seguro, así como mejorar la coordinación en materia de ciberdelincuencia y ciberterrorismo, fundamentalmente con las Fuerzas y Cuerpos de Seguridad del Estado[623].

INCIBE

Recoge el "Instituto Nacional de Ciberseguridad de España, S.A." (INCIBE) en sus estatutos que se rige por esos mismos estatutos, por el Real Decreto Legislativo 1/2010 de 2 de julio, por el que se aprueba el texto refundido de la Ley de Sociedades de Capital, y por las demás disposiciones vigentes que le sean de aplicación. La Sociedad tendrá como objeto social la gestión, asesoramiento, promoción y difusión de proyectos tecnológicos en el marco de la Sociedad de la Información[624].

La anterior denominación de esta S.A. era "Instituto de las Tecnologías de la Comunicación, S.A." (INTECO). INCIBE informa en su sitio web que el 27 de enero de 2006, el Consejo de Ministros estudió la creación de una sociedad mercantil estatal de las previstas en el artículo 166.2 de la Ley 33/2003, de 3 de noviembre, del Patrimonio de las Administraciones Públicas y en el apartado 2.b) del artículo 3 de la Ley 47/2003, de 26 de noviembre, General Presupuestaria, que revistiendo la forma de sociedad anónima, se denominara Instituto de las Tecnologías de la Comunicación, S.A. (INTECO), teniendo como objeto social la gestión, asesoramiento, promoción y difusión de proyectos tecnológicos en el marco de la Sociedad de la Información[625].

El Consejo de Ministros de 29 de abril de 2005 fue informado sobre la creación, con sede en León, del Instituto de las Tecnologías de la Comunicación (INTECO). La creación de INTECO responde a un doble objetivo: por un lado, contribuir a la

[623] Consejo de Seguridad Nacional: *Informe Anual de Seguridad Nacional 2014*, *opus citada*, p. 66.
[624] INCIBE S.A.: Estatutos Sociales. León, 27 de octubre de 2014. https://www.incibe.es/extfrontinteco/img/File/estatutos_sociales_incibe_2014_10_27.pdf consulta: 31 de octubre de 2015.
[625] Véase la información en https://www.incibe.es/pressRoom/Prensa/Actualidad_INCIBE/El_Consejo_de_Ministros_autoriza_la_creacion_del_I consulta: 31 de octubre de 2015.

convergencia de España con Europa en el ámbito de la sociedad de la información desarrollando proyectos innovadores en el sector de la tecnología de la comunicación (TIC) y, por otro, promover el desarrollo regional, enraizando en León un proyecto con vocación global[626].

Señala INCIBE S.A. que INTECO se constituye con un capital social inicial de 1.400.000 euros, siendo la titularidad del 100% de las acciones en las que se divide el capital social de la Entidad Pública Empresarial Red.es, dependiente del Ministerio de Industria, Turismo y Comercio que ejercerá la tutela de acuerdo con el artículo 176 de la Ley 33/2003, de 3 de noviembre, de Patrimonio de las Administraciones Públicas. La sociedad creada se regirá, en todo lo no expresamente regulado por sus Estatutos, por la Ley del Patrimonio de las Administraciones Públicas, la Ley General Presupuestaria, la Ley de Sociedades Anónimas vigente y demás normas de carácter general que sean de aplicación[627].

El centro desarrollará actuaciones en las siguientes líneas[628]:

- Accesibilidad. Inclusión social, basada en políticas de accesibilidad y equidad de todos los ciudadanos ante las opciones de la Sociedad de la Información.
- Seguridad tecnológica. Establecimiento de las bases de coordinación de distintas iniciativas públicas en torno a la seguridad informática.
- Centro de innovación en soluciones TIC para las PYMEs.
- Ciudadanía e Internet. Impulso de proyectos que, desde la innovación tecnológica, contribuyan a la mejora de la calidad democrática.
- e-Salud. Serán objeto de especial atención las áreas de investigación avanzada desarrolladas en los ámbitos de telemedicina y seguridad alimentaria.

El Presidente del Consejo de Administración de INCIBE S.A. es el Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información del Ministerio de

[626] *Ibídem.*
[627] *Ibídem.*
[628] *Ibídem.*

Industria, Energía y Turismo. La composición del Consejo se detalla en el sitio web de INCIBE[629].

El Instituto Nacional de Tecnologías de la Comunicación, como sociedad mercantil estatal con forma de sociedad anónima, se rige íntegramente por el ordenamiento jurídico privado, salvo en las materias en que le sea de aplicación la normativa presupuestaria, contable, de control financiero y de contratación, según prevé el apartado 1 de la DA 12ª de la Ley 6/1997, de 14 de abril, de Organización y Funcionamiento de la Administración General del Estado (LOFAGE)[630].

La contratación de la Sociedad se rige por las disposiciones de la legislación de contratos del sector público (Real Decreto Legislativo 3/2011, de 14 de noviembre) previstas para los poderes adjudicadores. La Sociedad no forma parte de la Administración General del Estado y está sometida a derecho privado en sus relaciones jurídicas.

Como ya se mencionó al tratar el CNPIC, INCIBE también recoge entre la información que proporciona en su sitio web que La Secretaría de Estado de Seguridad y la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información han suscrito un acuerdo en el que, entre otros aspectos, se sientan las bases para la colaboración de CNPIC e Instituto Nacional de Ciberseguridad (INCIBE) en materia de Respuesta a Incidentes para las Tecnologías de la Información de las Infraestructuras Críticas ubicadas en España. De esta forma, INCIBE se convierte en una herramienta de apoyo al CNPIC en la gestión de incidentes de ciberseguridad a través del denominado CERT de Seguridad e Industria (CERTSI)[631].

OTRAS ORGANIZACIONES CON CAPACIDAD CERT

[629] INCIBE S.A. Consejo de Administración. https://www.incibe.es/que_es_incibe/quienes_somos/organigrama/ consulta: 31 de octubre de 2015.
[630] *Ley 6/1997, de 14 de abril, de Organización y Funcionamiento de la Administración General del Estado*. Publicado en: «BOE» núm. 90, de 15 de abril de 1997. https://www.boe.es/buscar/act.php?id=BOE-A-1997-7878 consulta: 31 de octubre de 2015.
[631] Véase información del CERTSI en https://www.incibe.es/CERT/Infraestructuras_Criticas/ consulta: 31 de octubre de 2015.

Existen otras organizaciones con capacidad de respuesta a incidentes de ciberseguridad en España, entre las que se encuentran las recogidas en la asociación internacional FIRST, organización de primer nivel y reconocido líder mundial en respuesta a incidentes. La pertenencia a FIRST permite a los equipos de respuesta a incidentes responder con mayor eficacia a los incidentes de seguridad, proporcionando acceso a las mejores prácticas, herramientas y comunicación de confianza con los equipos miembros. En la lista de FIRST, además del CCN-CERT Gubernamental Nacional y el CERTSI, aparecen: BBVA CERT; Telefónica-CSIRT; ESCERT-UPC; e-LaCaixa CSIRT; S2 Grupo CERT; S21sec CERT; y MAPFRE-CCG-CERT[632].

7.3. PROPUESTA DE UN MODELO DE ORGANIZACIÓN DE LA CIBERSEGURIDAD EN ESPAÑA.

Del análisis realizado hasta el momento se desprenden una serie de conclusiones:

1. El uso del ciberespacio oportunidades extraordinarias para el progreso de las sociedades.
2. La dependencia de la conexión a Internet es cada vez más amplia y abarca sectores claves de la sociedad.
3. Existen riesgos asociados a la utilización del ciberespacio, tanto naturales como provocados.
4. Las infraestructuras críticas no son ajenas a esta dependencia de la conexión a las redes.
5. Las infraestructuras críticas han cambiado el paradigma y ya no son estancas; además ya utilizan herramientas comerciales y, no como anteriormente, herramientas especialmente diseñadas para ellas, lo que elevaba el nivel de protección.
6. La capacidad de recuperación de los sistemas es clave.

632

7. En el escenario de catástrofes naturales, es importante la adopción de medidas preventivas y el establecimiento de opciones alternativas durante la transición a la recuperación de los sistemas.

8. Las agresiones en las redes han adquirido un volumen creciente.

9. Las tendencias detectadas apuntan a que los ciberataques elevarán su número, peligrosidad y persistencia.

10. Las agresiones que utilizan el ciberespacio se producen por diversos actores, Estados, criminales, hacktivistas, profesionales de la ciberdelincuencia, cibervándalos y script kiddies, grupos terroristas, actores internos, ciberinvestigadores y actores privados.

11. Los objetivos de las agresiones cibernéticas son variados, destacando el espionaje digital, la interrupción del funcionamiento de los sistemas, la sustracción de información, las desfiguraciones en páginas web, y la toma de control de sistemas.

12. La atribución de los ciberataques es, en muchos casos, extremadamente complicada.

13. En la atribución de los ciberataques es fundamental la colaboración con la comunidad internacional de Inteligencia.

14. Los ciberataques tienen niveles de peligrosidad diferentes.

15. La aproximación de la UE y de otros actores políticos es que la legislación vigente es aplicable en el ámbito del ciberespacio.

16. El paradigma de la sociedad TIC ha cambiado. Se ha pasado de prevenir los ataques a detectarlos; de “depender de la tecnología” a “depender de las personas”; de invertir en proyectos tecnológicos a invertir en personas cualificadas.

17. Los países avanzados disponen de un corpus legislativo que al menos contiene una estrategia de seguridad nacional, una estrategia nacional de ciberseguridad, y un plan nacional de implementación de la estrategia de ciberseguridad.

18. El planeamiento de la ciberseguridad se incardina en las estrategias de seguridad nacionales, que a la vez incorporan elementos del pensamiento estratégico adaptado a las sociedades, con un elevado componente geopolítico.

19. La ciberseguridad no deja de ser de ser un aspecto incardinado en la seguridad en general, que utiliza un dominio nuevo, el ciberespacio y otras herramientas novedosas basadas en las tecnologías y las comunicaciones.

20. La concepción de la ciberseguridad y la ciberdefensa no escapa a los modos en que las naciones ven su propia seguridad, incorporando las corrientes de pensamiento tradicionales (según la teoría de trayectorias dependientes: “la historia importa”), que tienen un impacto sobre las políticas, estrategias y modelos organizativos.

21. Estados Unidos, Rusia y China se encuentran en un estadio superior de complejidad en el planeamiento y en las soluciones organizativas en el ámbito de la ciberseguridad, que inspiran a otros países.

22. Los retos y amenazas a que se enfrentan las sociedades en el ámbito del ciberespacio son, en gran parte, compartidos.

23. Los países avanzados tienen un consejo de seguridad nacional y un consejo nacional de ciberseguridad.

24. En el ámbito de la ciberseguridad, los países más avanzados tienen definidos los niveles político estratégico, operacional y táctico / técnico.

25. Los países más avanzados tienen un consejo nacional de ciberseguridad, que además de la labor que realiza de asesoramiento al consejo de seguridad nacional, tiene capacidad ejecutiva.

26. Los Servicios de Inteligencia tienen el liderazgo en diversos países en la prevención, protección y respuesta a ciberataques, así como en la recuperación de los sistemas.

27. En un mundo complejo y con ciberamenazas cada vez más sofisticadas, la colaboración entre Servicios de Inteligencia aliados cobra un valor especial.

28. La ciberseguridad de encuentra muy presente en las agendas de seguridad de las organizaciones internacionales, UE, ONU, OTAN y OSCE.

29. La Unión Europea se encuentra especialmente activa en el ámbito de la ciberseguridad, enfocando sus necesidades de protección y recuperación de los sistemas para facilitar el libre comercio y los flujos económicos.

30. Los países de la Unión Europea se encuentran en un nivel de desarrollo elevado en cuanto al planeamiento de la ciberseguridad a nivel estratégico, contando un número elevado de ellos con estrategias nacionales de ciberseguridad.

31. El planeamiento subordinado al nacional en los países de la UE se encuentra en fase de desarrollo dispar, y solamente los países más avanzados han desarrollado sus estrategias de ciberseguridad mediante planes de implementación de la misma.

32. El Reino Unido, Alemania y Francia se encuentran desarrollando proyectos en ciberseguridad, tanto de planeamiento como organizativos, que se encuentran muy cercanos a la situación en España.

33. España ha realizado un significativo esfuerzo legislativo y de planeamiento de la seguridad nacional, destacando la Ley de seguridad nacional y la estrategia nacional de seguridad.

34. En el ámbito de la ciberseguridad, España se encuentra muy avanzada en el diseño del sistema de prevención, análisis y recuperación de sistemas debido a ciberataques, destacando el papel del Centro Criptológico Nacional en su modalidad CERT de respuesta a incidentes de ciberseguridad.

35. El Esquema Nacional de Seguridad (ENS) en el ámbito de la Administración Electrónica en España proporciona una excelente estructura para facilitar la protección y recuperación de los sistemas asociados a las tecnologías de información y comunicaciones.

36. La reciente revisión del ENS en el ámbito de la Administración Electrónica, que databa de 2010, va a suponer un impulso de las capacidades mediante la racionalización de las competencias.

37. La actualización de este Esquema Nacional de Seguridad refuerza la posición del CERT Gubernamental Nacional CCN-CERT, en beneficio de la eficiencia del ENS.

38. La organización de la ciberseguridad en España en el nivel político estratégico, con la decisión de creación del Consejo Nacional de Ciberseguridad (CNCS) se ha mostrado muy acertada.

39. Desde su constitución el 25 de febrero de 2014, el CNCS ha desarrollado un Plan Nacional de Ciberseguridad y nueve planes derivados de este plan general, que

desarrollan las líneas de acción y los cometidos diseñados en la Estrategia de Ciberseguridad Nacional.

40. Se considera muy positiva la decisión del Consejo de Seguridad Nacional, presidido por el Presidente del Gobierno, que en enero de 2015 decidió eliminar la rotación anual prevista de la presidencia del Consejo Nacional de Ciberseguridad, manteniendo en este puesto al Secretario de Estado Director del CNI y del CCN.

41. No obstante, si bien el CNCS ha demostrado una elevada capacidad de planeamiento en el ámbito de la ciberseguridad, el diseño de este CNCS no permite que realice un adecuado seguimiento y conducción de sus decisiones, ya que adolece de capacidad ejecutiva para implementar sus decisiones.

42. El nivel operacional es prácticamente inexistente en el diseño del modelo organizativo de la ciberseguridad en España a nivel nacional, tanto a nivel de planeamiento como de conducción, excepto en lo que se refiere al Centro Criptológico Nacional y las competencias que se le dan en el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

43. El nivel táctico y técnico se encuentra cubierto con las actividades del CCN-CERT en su calidad de CERT Gubernamental Nacional, a semejanza de otros países de nuestro entorno.

44. El CCN-CERT, que tiene por ley la responsabilidad de la protección y recuperación de los sistemas e información de las administraciones públicas (estatal, autonómica y local) de aquellos que utilicen información clasificada, así como de empresas de carácter estratégico, se ha convertido en la piedra angular del sistema, a semejanza también de otros países aliados.

45. Otras iniciativas en la gestión de ciberincidentes de otros organismos y entidades, en otros ámbitos de competencia, probablemente necesiten un organismo coordinador a nivel nacional que facilite una aproximación integral a la ciberseguridad y facilite una coordinación de calidad, que redundaría en una más adecuada capacidad de protección y recuperación.

46. Los ciberataques están adquiriendo elevados niveles de complejidad y persistencia.

47. Tras los ataques más complejos se encuentran los Estados.

48. Ante los ataques mediante APTs (herramientas persistentes avanzadas) es necesario un enfoque integral y la incorporación de patrones y algoritmos complejos, que necesitan de laboratorios e investigación propia nacional, pero que deben incorporar los procesos de otros países aliados.

49. Prácticamente todos los dispositivos electrónicos son susceptibles de ser intervenidos.

50. Las organizaciones que realizan ciberataques utilizan los dispositivos de particulares (ordenadores de sobremesa, ordenadores portátiles, tabletas y móviles, principalmente) para facilitar su estructura de proceso y de almacenamiento de datos, convirtiendo a estos dispositivos en robots, creando redes (botnets) que utilizan desde sus servidores de mando y control para aumentar sus capacidades.

51. El aumento del "internet de las cosas" (IoT) va a llevar aparejado que la conexión a la red de cualquier dispositivo sea lo habitual, lo que incrementará el grado de vulnerabilidad para poder incorporar nuevos vectores de ataque en el ciberespacio.

52. El CCN-CERT se encuentra realizando una labor de prevención y respuesta a los ciberataques de alta calidad en los entornos en que tiene competencia: administraciones públicas y empresas de carácter estratégico.

53. El CCN-CERT se encuentra facilitando que la sociedad incremente sus niveles de protección en el ciberespacio, al poner a disposición del público en general las guías y otra documentación para mejorar las capacidades de protección y respuesta ante ciberataques.

54. La responsabilidad competencial del CCN-CERT en relación a las administraciones públicas (estatal, autonómica y local) y empresas de carácter estratégico debería ser respetada por los diferentes organismos.

55. Que la Secretaría de Estado de Seguridad del Ministerio de Interior acuerde con la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información del Ministerio de Industria, Energía y Turismo, que una sociedad anónima con carácter mercantil (el Instituto Nacional de Ciberseguridad en España, INCIBE S.A.) conforme el denominado CERT de Seguridad e Industria, con competencias exclusivas en la protección de infraestructuras críticas, introduce en el sistema nacional de protección de infraestructuras críticas una vulnerabilidad de alto nivel.

56. INCIBE S.A. no es un organismo público y realiza las contrataciones de acuerdo al derecho laboral.

57. INCIBE S.A. no tiene supervisión ni de seguridad ni técnica acerca de sus actividades y capacidades por algún organismo de la administración pública, siendo controlada por su junta general y consejo de administración, este último presidido por el Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información del Ministerio de Industria, Energía y Turismo, y donde se encuentran representantes de este mismo Ministerio y otros, como Presidencia del Gobierno.

58. Que el CCN-CERT no tenga capacidades ejecutivas de control o al menos de coordinación de las actividades que realiza INCIBE S.A. en el marco de la respuesta a incidentes de ciberseguridad en el ámbito de las infraestructuras críticas, introduce una gran vulnerabilidad en el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica y en la protección de activos nacionales con elevado impacto potencial en la seguridad nacional.

59. A nivel político estratégico, España se ha dotado de un reciente corpus legislativo que aborda con carácter integral la seguridad nacional, contando con una Estrategia de Seguridad Nacional de 2013 y la reciente Ley de Seguridad Nacional de octubre de 2015.

60. En el ámbito de la ciberseguridad, el corpus legislativo es también de muy alta calidad, destacando la Estrategia Nacional de Ciberseguridad de diciembre de 2013, derivada de la Estrategia de Seguridad Nacional; así como la reciente revisión de 23 de octubre de 2015 del Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

Es en este escenario que se propone el siguiente modelo de organización de la ciberseguridad nacional en España.

Se propone incrementar la capacidad, tanto de planeamiento como de ejecución en los tres niveles: político estratégico, operacional y táctico / técnico.

Nivel político estratégico

En el nivel político estratégico, se considera que en los aspectos relacionados con el planeamiento a su más alto nivel se ha alcanzado un nivel de gran calidad, tal como se manifiesta en los siguientes documentos que han sido analizados: La Ley de Seguridad Nacional, el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, la Estrategia de Seguridad Nacional y la Estrategia Nacional de Ciberseguridad.

En cuanto al modelo de organización, la creación del Consejo de Seguridad Nacional (CSN) –presidido por el Presidente del Gobierno– y el Consejo Nacional de Ciberseguridad (CNCS) –presidido por el Secretario de Estado Director del Centro Nacional de Inteligencia y Director del Centro Criptológico Nacional– ha demostrado su valor en lo que respecta al planeamiento de la ciberseguridad, habiéndose confeccionado por el CNCS y aprobado por el CSN el Plan Nacional de Ciberseguridad, que desarrolla las líneas de acción y objetivos diseñados en la Estrategia Nacional de Ciberseguridad. Posteriormente, el CNCS ha elaborado y aprobado nueve planes derivados del mencionado Plan Nacional de Ciberseguridad.

En cuanto a la conducción y seguimiento de la implementación del planeamiento político estratégico realizado en el seno del Consejo Nacional de Ciberseguridad, este CNCS no ha dispuesto de la capacidad para realizar estas tareas, al haber sido diseñado sin estas capacidades ejecutivas, lo que ha derivado en una implementación a la carta de este planeamiento por parte de los diferentes organismos con responsabilidades de ciberseguridad en España.

La atribución de capacidades ejecutivas en materia de ciberseguridad nacional se considera prioritaria en el modelo nacional de ciberseguridad que se propone.

En cuanto a la presidencia del Consejo Nacional de Ciberseguridad, se valora de modo extraordinariamente positivo la decisión del Consejo de Seguridad Nacional, de enero de 2015, de establecer una presidencia permanente del CNCS en el cargo del actual Presidente –Secretario de Estado Director del Centro Nacional de Inteligencia y

Director del Centro Criptológico Nacional–, lo que deja sin efecto el diseño inicial de rotación anual entre autoridades de diversos ministerios.

Se estima de gran importancia la permanencia de la presidencia por más de un año para aportar continuidad a un proceso que estaría de otra forma en permanente inestabilidad.

Además, la elección del presidente en la figura del Secretario de Estado Director del Centro Nacional de Inteligencia y Director del Centro Criptológico Nacional se estima extremadamente acertada. De una parte, en calidad de Director del Servicio de Inteligencia incorpora la visión de un organismo cuya responsabilidad es velar por la seguridad del Estado de modo integral, y cuyo acceso a elementos informativos procedentes de otros Servicios de Inteligencia aliados, con los que se comparten riesgos y amenazas, es de alto valor. De otro lado, en calidad de Director del Centro Criptológico Nacional, el Secretario de Estado es la autoridad responsable de aspectos de ciberseguridad específicos para coordinar la acción de los diferentes organismos de la Administración en la protección de sistemas que utilicen información clasificada, certificación, y formación de personal especialista en este campo. En la modalidad de CERT Gubernamental Nacional el Director del Centro Criptológico Nacional tiene la responsabilidad de prevenir y gestionar los ciberataques, favoreciendo la recuperación de los sistemas, en el ámbito de las administraciones públicas en los tres niveles (estatal, autonómico y local), así como en el ámbito de las empresas de carácter estratégico. Para favorecer esta sinergia, el Centro Criptológico Nacional está adscrito al Centro Nacional de Inteligencia, y comparte con éste medios, procedimientos, normativa y recursos. De esta forma, el Centro Criptológico Nacional tiene la capacidad de incorporar elementos informativos de otros Servicios de Inteligencia aliados en beneficio de la ciberseguridad nacional.

Se propone, por tanto, **mantener el Consejo Nacional de Ciberseguridad con la actual presidencia y composición de todos los ministerios con responsabilidades en ciberseguridad**.

Se propone dotar a este CNCS de capacidad ejecutiva para realizar el seguimiento y la conducción de sus decisiones, para lo cual deberá adoptarse esta decisión en el seno del Consejo de Seguridad Nacional.

Nivel operacional

En la actualidad no se ha establecido en España, de modo formal, el nivel de planeamiento operacional. Tampoco existe de modo reglado el nivel operacional como nivel orgánico para la conducción y el seguimiento de la implementación de las decisiones del nivel político estratégico en el modelo de la ciberseguridad en España.

La implementación del planeamiento realizado en el Consejo Nacional de Ciberseguridad debe realizarse directamente por los diferentes organismos afectados, sea cual sea su nivel orgánico, y de acuerdo a sus competencias en materia de ciberseguridad.

Esta situación lleva a que no se produzca una adecuada transición de las decisiones del CNCS mediante un proceso de planeamiento operacional que articule adecuadamente las decisiones político estratégicas y las integre de modo que puedan ser incorporadas de modo adecuado por el nivel táctico y técnico, y que en muchas ocasiones encuentren extremadamente complejo trasladar esas acciones de tipo macro a un universo micro en el ámbito de la ejecución de la implementación de las políticas de ciberseguridad.

Además de carecer de este nivel de planeamiento operacional, no existe una plataforma de nivel operacional que con carácter ejecutivo tenga responsabilidad de realizar la conducción y el seguimiento de modo integral de los planes y decisiones político estratégicas emanadas del Consejo Nacional de Ciberseguridad.

Solamente las Secretarías de Estado de los ministerios, y en el caso del Ministerio de Defensa también del Mando de Operaciones en el ámbito de las operaciones militares, tienen ese nivel de responsabilidad operacional, pero que en el ámbito de la ciberseguridad provoca una dispersión en la implementación de las decisiones político

estratégicas dependiendo del enfoque y nivel de capacidades y prioridades de los diferentes organismos.

En el ámbito de la ciberseguridad, el Director TIC de la Administración General del Estado realiza algunas funciones que podrían considerarse en este nivel operacional. No obstante, la mayor parte de sus responsabilidades son de tipo técnico, escapando el diseño de esta Dirección de la realización de un planeamiento integral de la ciberseguridad nacional en el nivel operacional, así como de las responsabilidades de implementación de las decisiones político estratégicas, que abarcan un campo mucho más amplio en otros sectores que el de diseño de los sistemas nacionales relacionados con las tecnologías de información y comunicaciones.

También el Centro Criptológico Nacional realiza acciones que podrían considerarse en el nivel operacional, pero ni se encuentra diseñado para realizar un planeamiento integral operacional de la ciberseguridad en España ni para realizar el seguimiento de las decisiones político estratégicas de modo integral en los organismos tácticos y técnicos que deben incorporarlas. Sí es cierto, que en el Esquema Nacional de Seguridad en el ámbito de la Administración electrónica, el Centro Criptológico Nacional realiza funciones que encajan en este nivel operacional, aunque limitadas a aspectos concretos de la ciberseguridad.

En este escenario, **se propone la creación de un Centro de Ciberseguridad Nacional que asuma las responsabilidades de planeamiento y conducción en el nivel operacional de la ciberseguridad en España**.

En este Centro de Ciberseguridad Nacional, a semejanza de otros países de nuestro entorno, se realizaría la traslación del planeamiento político estratégico a niveles que puedan ser integrados e incorporados a los organismos con responsabilidades tácticas y técnicas. Además, desde este Centro de Ciberseguridad Nacional se realizaría el seguimiento y el impulso de los diferentes planes y decisiones en el ámbito de la ciberseguridad de modo integral en el ámbito nacional.

Este Centro de Ciberseguridad Nacional no interferiría en las competencias que las autoridades nacionales tienen en la actualidad en relación con la ciberseguridad, pero sí aportaría una capa necesaria de integración y coordinación de las decisiones de carácter político estratégico y el impulso de las decisiones que se produzcan a través del planeamiento adecuado en este nivel.

Este Centro de Ciberseguridad Nacional, además de contar con sede propia y recursos humanos y materiales propios, debería incorporar a personal de los diferentes ministerios y organismos con competencias en ciberseguridad, que deben estar representados en este Centro con carácter permanente.

Este Centro de Ciberseguridad Nacional debería establecer los mecanismos adecuados para la incorporación del sector privado en este nivel operacional para favorecer los intereses de seguridad nacional al agregar la visión de clientes de ciberseguridad en otros ámbitos que pudieran tener impacto en el diseño e implementación de aspectos relacionados con la ciberseguridad nacional.

Este Centro de Ciberseguridad Nacional se encontraría bajo la dependencia directa del consejo Nacional de Ciberseguridad, tanto a efectos de planeamiento como orgánicamente.

Al encontrarnos en un ámbito de seguridad nacional del máximo nivel, el Centro de Ciberseguridad Nacional estaría dirigido por un alto funcionario de la Administración General del Estado, con rango de Subsecretario y dependencia del Secretario de Estado que presida el Consejo Nacional de Ciberseguridad.

Nivel táctico y técnico

En el nivel táctico y técnico se estima que el diseño del actual modelo de ciberseguridad en España es el adecuado.

El Director TIC, con responsabilidades definidas en el ámbito del diseño y coordinación de los diferentes aspectos que conforman los sistemas de información y comunicaciones, debería continuar realizando esa importante labor.

En el ámbito de prevención, respuesta y recuperación de los sistemas que utilizan los tres niveles de las administraciones públicas (Administración General del Estado, nivel autonómico y autoridades locales), las empresas de carácter estratégico, y los sistemas que utilizan información clasificada, se estima conveniente mantener el modelo, que tan buenos resultados está obteniendo, por el cual se sustenta la capacidad de respuesta a incidentes de ciberseguridad que tiene por ley el Centro Criptológico Nacional en su condición de CERT Nacional Gubernamental.

En el escenario de riesgos y amenazas a la ciberseguridad, otros actores en el ámbito público y en el privado han desarrollado mecanismos de prevención y respuesta a incidentes de ciberseguridad de acuerdo a sus necesidades:

- Se ha presentado el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas (MCCD) en el ámbito de la defensa nacional, así como la reciente generación de capacidades del Ministerio de Defensa a través del Centro de Respuesta ante incidentes de Ciberseguridad del Ministerio de Defensa (ESPCERTDEF).
- Se han analizado el Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC) y los riesgos que ataques físicos o cibernéticos a estas infraestructuras pueden ocasionar en el ámbito de la seguridad nacional, y también se han presentado las soluciones ofrecidas desde la Secretaría de Estado de Seguridad y la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, con la firma de un acuerdo de cooperación por el que la sociedad anónima INCIBE creaba un CERT denominado CERT de Seguridad e Industria (CERTSI) como CERT especializado en la gestión de incidentes relacionados con las infraestructuras críticas a nivel nacional; para lo que a su vez el CNPIC creaba la Oficina de Coordinación Cibernética.
- En el ámbito privado, además de INCIBE S.A., se están incorporando otros centros de respuesta a incidentes de ciberseguridad, bien en repuesta a

necesidades de las organizaciones que quieren contar con sus propias herramientas de gestión de ciberincidentes, bien en el ámbito empresarial para ofrecer estas herramientas a otros clientes. Se han mencionado en este sentido las que aparecen listadas en la asociación internacional FIRST: BBVA CERT; Telefónica-CSIRT; ESCERT-UPC; e-LaCaixa CSIRT; S2 Grupo CERT; S21sec CERT; y MAPFRE-CCG-CERT.

Conviene resaltar la disfunción que se ha detectado relativa a que la respuesta a incidentes de ciberseguridad en el ámbito de las infraestructuras críticas se desarrolle a través de una institución privada, sociedad anónima de carácter mercantil, en un ámbito con tan altas repercusiones para la seguridad nacional y existiendo un organismo –CCN-CERT– que tiene las responsabilidades por ley de realizar esa función.

En este escenario, **se propone que el CCN-CERT, como CERT Gubernamental Nacional** que es en la actualidad, según la legislación vigente, **tenga funciones de organismo coordinador nacional en materia de ciberseguridad, para las administraciones públicas, actuando como organismo de referencia en lo que se refiere a las capacidades CERT**, como sucede en el Reino Unido o en Alemania.

Estas labores de coordinación, definidas en el ámbito de las administraciones públicas, se desarrollarían **también para las empresas de carácter estratégico**, como se viene realizando en la actualidad.

En relación **con el sector privado**, el **CCN-CERT** no realizaría labores de coordinación, y sí actuando como **centro de referencia para la ciberseguridad en el ámbito nacional, en lo relativo a la gestión de ciberincidentes**, para de esta forma facilitar las labores de control de calidad e incorporación de buenas prácticas en materia de ciberseguridad.

El Director del CCN-CERT debería tener, al menos, rango de Director General, para poder incardinarse en el sistema nacional de ciberseguridad de modo adecuado.

CONCLUSIONES

Esta tesis doctoral nació inspirada en las corrientes del *neo institucionalismo*, al estimar que el estudio de las instituciones constituye un campo de actividad en el que la ciencia política puede aportar valor, utilizando el método científico, incorporando una mirada diferente a la de otras disciplinas.

El estudio de los modelos de organización de las instituciones también puede abordarse desde otras perspectivas científicas distintas a la ciencia política, en ocasiones fundamentadas en teorías de organizaciones y de análisis de modelos organizativos, pudiendo tener un enfoque más utilitarista, y desde donde se aborda el análisis mediante diversos criterios en la búsqueda de la eficiencia de estos modelos.

En el caso de la presente tesis doctoral, la decisión de emprender esta investigación se encuentra alimentada por la oportunidad de haber participado en el diseño de la primera estrategia de seguridad nacional en España y de realizar en la actualidad labores de asesoramiento al Presidente del Consejo Nacional de Ciberseguridad, desde la constitución de este Consejo a finales de febrero de 2014.

Durante el proceso de elaboración del Plan Nacional de Ciberseguridad y de los nueve Planes derivados de este Plan Nacional, se ha producido un debate recurrente acerca de la necesidad de disponer de un modelo apropiado de organización de la ciberseguridad en España.

Este debate, que tuvo lugar entre los representantes de los diversos organismos que participaron en el proceso de planeamiento, se mantuvo una vez aprobados el Plan Nacional de Ciberseguridad y los Planes Derivados del mismo al intentarse la implementación de estos planes, ya que existían diferentes visiones sobre el modo de desarrollo de estos planes en otros subordinados y sobre las autoridades que debían ejecutarlos.

Esta situación condujo a diferentes reflexiones que derivaron en la confección de la pregunta de investigación: ¿Cuál puede ser un modelo apropiado de organización de la ciberseguridad en España? Esta pregunta de investigación se estima cumple las condiciones enumeradas en la presentación de la metodología de esta tesis doctoral: *que el problema de investigación se formule del modo más explícito y comprensible posible, delimitando con precisión el objeto de estudio y los propósitos de la investigación; la necesidad de que el problema y las preguntas tengan una respuesta adecuada al tipo de investigación que se emprenda; y que la pregunta tenga valor o relevancia teórica, contribuyendo al desarrollo y a la ampliación del conocimiento existente*.

De esta forma, la pregunta encajaba en un tipo de investigación prescriptiva, pues era su intención proponer soluciones para mejorar la organización de modelos políticos de gobernanza en el ámbito de la ciberseguridad en España.

En el proceso de análisis para el diseño de este trabajo de investigación, aprecié la importancia de incardinar este posible modelo de organización en los estadios superiores de la seguridad nacional, tomando en consideración que la ciberseguridad, independientemente de lo novedoso del ámbito de su aplicación, el ciberespacio, formaba parte de un conjunto superior de la seguridad, y que su singularidad se encontraba limitada a esta nueva dimensión de la red y a unas nuevas tecnologías que desarrollaban nuevos espacios para incorporar los riesgos y amenazas clásicos, ligados a la voluntad del ser humano.

En este estadio, cobraba valor la corriente de análisis político denominada *trayectorias dependientes*, y su conocido lema “la historia importa”, que liga las posibilidades de cambio a esas trayectorias históricas que conforman corrientes de pensamiento y que influyen en la manera de desarrollarse de las sociedades, teniendo también impacto, en última instancia, en la gobernanza y los modelos organizativos.

La elección del modelo de investigación teórica en lugar del modelo empírico vino dada por el valor de estas *trayectorias dependientes*, que aconsejaban incorporar técnicas

que se encuadran en la investigación histórica, ya que se consideró necesario estudiar la evolución del pensamiento estratégico y del recorrido histórico de las soluciones que se han ido conformando en el campo de la seguridad, las cuales han dado lugar a diferentes modelos organizativos en el dominio de la ciberseguridad.

No obstante, se han utilizado recursos que incorporan elementos de la investigación explicativa, necesarios para comprender los comportamientos de los actores políticos en el ámbito de la ciberseguridad; asimismo, se emplean recursos del análisis conceptual, presente en cualquier tipo de investigación teórica, teniendo en cuenta que los conceptos relacionados con el ciberespacio son novedosos y no se encuentran en algunos casos suficientemente consolidados; así como también se han empleado técnicas de investigación evaluativa.

Este trabajo de investigación se ha construido como un estudio de caso sobre la ciberseguridad en España, estimando su relevancia y su naturaleza en relación con la propuesta de un modelo de organización de la ciberseguridad en España, el cual pueda ser realizable y tenga un impacto positivo en el incremento de los niveles de la seguridad nacional.

Este caso, atendiendo al objeto de estudio, se basa en procesos; en cuanto al alcance, se trata de un caso genérico o ejemplar, ya que no constituye una excepcionalidad: Según su naturaleza, este caso es también ejemplar, ilustrativo de un fenómeno; y además es típico, en la medida en que se le considera uno más de un grupo, el de los países afectados por los riesgos y amenazas derivados del uso del ciberespacio. Atendiendo al tipo de acontecimiento, objeto o fenómeno, este caso es de tipo mixto o híbrido, ya que por una parte es contemporáneo y de otro lado hace referencia a fenómenos históricos. En cuanto al uso del caso, encaja en el tipo de naturaleza analítica, ya que persigue estudiar el funcionamiento de un fenómeno y de su relación con otros, aunque en algunas fases de la investigación podría considerarse un caso mixto, ya que se recurre a elementos descriptivos en relación con acontecimientos pasados para explicar el proceso presente que configura el caso. Por último, según el número de casos, este trabajo de investigación encaja en el caso múltiple o colectivo,

al analizar los riesgos asociados al uso del ciberespacio y las soluciones que ofrecen otros modelos de organización de la ciberseguridad nacional.

En este trabajo de investigación se ha utilizado el método de comparación analítica por similitud, basando su aportación en la comparación de un número reducido de casos seleccionados por sus características.

Aunque en las investigaciones teóricas predomina el pensamiento deductivo, se ha recurrido también al método inductivo para alcanzar conclusiones a partir de los casos particulares observados.

Dependiendo del estadio de la investigación, en esta tesis doctoral se han realizado varias selecciones de casos. En primer lugar se eligió a Estados Unidos, China y Rusia al ser pioneros en el diseño de estrategias y estructuras nacionales de seguridad, en las que se inspiran la mayor parte del resto de las estrategias nacionales de seguridad y sus modelos organizativos. Posteriormente, se seleccionaron para su análisis diversas organizaciones internacionales que poseen una componente de ciberseguridad: Unión Europea, Naciones Unidas, OTAN y OSCE, dando preeminencia a la UE, ya que España se encuentra obligada por el corpus normativo de la Unión Europea. Con posterioridad, se han seleccionado diversos países de la Unión Europea debido a que comparten con España características comunes en mayor medida que otros de regiones geopolíticas diferentes. Entre los Estados miembros de la Unión Europa se seleccionó al Reino Unido, Alemania y Francia, ya que se estimó que presentaban entornos que podrían inspirar de modo más adecuado la mejora del modelo nacional de ciberseguridad en España.

La investigación presentó en primer lugar la evolución de los incidentes de ciberseguridad en España entre 2011 y 2015, encuadrándolos en un contexto general, ya que gran parte de las ciberamenazas son compartidas por otros Estados. Se destaca que, en 2014, el CERT Gubernamental Nacional (CCN-CERT) abordó 12.916 incidentes, de los cuales, 132 fueron catalogados como críticos, apreciándose la

tendencia de incremento en número, virulencia y persistencia de los ciberataques en el futuro.

A continuación se incorporó a la investigación un espacio dedicado a la evolución del pensamiento estratégico, ya que las diferentes aproximaciones a la ciberseguridad, como derivada de un concepto de seguridad más amplio, se alimentan también de esa corriente de pensamiento estratégico que impregna a los actores políticos que deben conformar los modelos de organización de la ciberseguridad.

Del estudio de las estrategias y modelos nacionales de seguridad en Estados Unidos, Rusia y China se extrajeron diversas conclusiones, entre las que pueden destacarse que las estrategias nacionales de seguridad se han convertido en un modelo del que se desprende la planificación de la seguridad nacional; que la integración de los intereses nacionales es total, destacando la capacidad económica como referente transversal de la seguridad; que se ha establecido un modelo organizativo similar basado en un consejo de seguridad nacional; y que las estrategias nacionales de seguridad se desarrollan mediante estrategias sectoriales, como es el caso de las estrategias nacionales de ciberseguridad.

Posteriormente, se analizaron las iniciativas internacionales en el ámbito de la ciberseguridad. De la Unión Europea cabe destacar la importancia capital que la UE da a la ciberseguridad para favorecer el espacio económico y de desarrollo, habiendo desarrollado su propia estrategia de ciberseguridad, que constituye la piedra angular en la que se sustenta numerosa reglamentación comunitaria. De la ONU cabe destacar el proceso de alto nivel en materia de ciberseguridad, basado en las recomendaciones de un Grupo de Expertos orientadas al marco de la legalidad y seguridad internacionales en el ciberespacio. En la OTAN la ciberdefensa forma parte del Concepto Estratégico de la Alianza desde la Cumbre de Lisboa en 2010 y cuenta con una Política de Ciberdefensa. En el ámbito de la OSCE se ha impulsado un paquete de medidas de confianza en el ámbito de la ciberseguridad. El resumen es que, en el ámbito internacional, la ciberseguridad forma parte de las agendas de las organizaciones (ya sean públicas o privadas) al máximo nivel.

Seguidamente se estudiaron en profundidad las estrategias de ciberseguridad de Estados Unidos, China y Rusia, países que ya se habían estudiado como referencias en el planeamiento estratégico de la seguridad nacional, así como los modelos institucionales y organizativos que han constituido en el ámbito de la ciberseguridad, modelos que han conformado una referencia casi obligada para el resto de países en el ámbito del desarrollo de sus estrategias de ciberseguridad y sus patrones organizativos.

Después se analizó el estado de la ciberseguridad en los países de la Unión Europea, utilizando cinco bloques de parámetros: fundamentos legales para la ciberseguridad; capacidades operativas; asociaciones público-privadas; planes de ciberseguridad en sectores específicos; y educación en ciberseguridad. De este modo se obtuvo una visión de la situación de la ciberseguridad en cada uno de los países de la UE en comparación con el resto.

A continuación se estudiaron con más detalle los casos de Reino Unido, Alemania y Francia, señalando que estos tres países de referencia en la UE disponen de una Estrategia de Ciberseguridad Nacional, una legislación específica en materia de ciberseguridad, se han dotado de un Consejo Nacional de Ciberseguridad y disponen de un CERT nacional competente que actúa como coordinador nacional en la comunidad CERT, tanto en el ámbito público como en el privado.

Este análisis comparado dio paso al planeamiento de la ciberseguridad en España, incardinado en el sistema de seguridad nacional. En este apartado se ha analizado la reciente Ley de Seguridad Nacional, el Sistema de Seguridad Nacional, las Estrategias de Seguridad Nacional, El esquema Nacional de Seguridad en el ámbito de la Administración electrónica, y la Estrategia de Ciberseguridad Nacional y su desarrollo: el Consejo Nacional de Ciberseguridad, que ha organizado la gobernanza de la ciberseguridad en España, mediante la confección del Plan Nacional de Ciberseguridad y los nueve Planes Derivados del mismo.

Por último, después de revisarse el modelo de gobernanza actual en España, se ha realizado una propuesta de modelo de organización nacional de la ciberseguridad. En el nivel político estratégico se propone mantener el Consejo Nacional de Ciberseguridad con su composición y misión de planeamiento político estratégico, pero incorporando a este CNCS una capacidad ejecutiva para realizar el seguimiento de la implementación del Plan Nacional de Ciberseguridad y de sus Planes Derivados. Tras detectar la inexistencia de un nivel operacional de carácter nacional que pueda continuar el proceso de planeamiento a ese nivel de modo integral, así como realizar la implementación de estos planes y su control en los organismos subordinados, se propone la creación de un Centro de Ciberseguridad Nacional, directamente dependiente del Consejo Nacional de Ciberseguridad. Por último, tras valorarse positivamente el diseño del nivel táctico y técnico de la ciberseguridad en España, se propone que el CERT Gubernamental Nacional actual (CCN-CERT) realice funciones de coordinación nacional en el ámbito de la prevención y respuesta a ciberataques, para los tres niveles de las administraciones públicas y para empresas de carácter estratégico, y que se constituya además en centro de referencia para el sector privado.

Se estima que con esta propuesta se han alcanzado los objetivos de la investigación y se da respuesta a la pregunta de investigación: ¿Cuál puede ser un modelo apropiado de organización de la ciberseguridad en España?

Querría apuntar en este estadio que, a nivel metodológico, se ha realizado una investigación basada en un modelo teórico para definir un modelo de organización de un sistema de ciberseguridad nacional, teniendo en cuenta que las investigaciones sobre modelos organizativos suelen estar basadas en modelos empíricos de investigación. En este sentido, se estima que se verifica lo apuntado en el apartado de metodología, señalándose que el modelo teórico se inspira en lo apuntado por Chuliá y Agulló al citar a Marsh y Stoker, para señalar que la teoría política incluye entre sus objetivos los de ofrecer una alternativa deseable a lo existente que se encuentre normativamente fundada, evaluar esa realidad conforme a los ideales y valores políticos que se tienen por preferibles y prescribir los medios adecuados –instituciones, procesos y normas– para que las alternativas deseables puedan hacerse realidad.

También se ha mostrado válido para esta investigación lo señalado en el apartado de metodología relativo a la “fecundación cruzada”, sobre las ventajas de afrontar las investigaciones en ciencia política desde una perspectiva abierta a otras ciencias sociales, incorporando factores históricos, sociales, culturales, económicos, jurídicos o específicos del ámbito de la seguridad. En este sentido cabe destacar también el componente técnico de esta investigación sobre la ciberseguridad y su ajuste a los objetivos de la investigación.

En el campo de la ciencia política, resaltaría de esta investigación su carácter prescriptivo, de tal forma que, utilizando el método científico mediante un modelo teórico de investigación, se han facilitado soluciones a problemas complejos de organización de modelos de seguridad en el ámbito de la utilización del ciberespacio. Estas propuestas se han incardinado en el modelo de gobernanza nacional de la seguridad, estimándose que son factibles y que, de ser implementadas, aumentarían los índices de protección de la sociedad en el ámbito de la ciberseguridad.

Para finalizar, solamente quería expresar que confío en que, al menos, uno de los efectos que se puedan derivar de la lectura de esta tesis doctoral sea el de inspirar otras líneas de investigación relacionadas con la ciencia política y con otras disciplinas sociales en el ámbito de la ciberseguridad.

BIBLIOGRAFÍA

Publicaciones

ALONSO TRONCOSO, Víctor: *Neutralidad y neutralismo en la guerra del Peloponeso, 431-404 a.C.* Universidad Autónoma. Madrid, 1987.

ANDUIZA, Perea; CRESPO, Ismael; y MÉNDEZ LAGO, Mónica: *Metodología de la Ciencia Política*. Centro de Investigaciones Sociológicas, Cuadernos Metodológicos, núm. 28, diciembre de 1999.

ARÓSTEGUI, Julio: *La Investigación Histórica: Teoría y Método*. Editoria Crítica S.L., Barcelona, 2001, ISBN 84-8432-137-1.

ARTETA, Aurelio; GARCÍA GUITIÁN, Elena, y MAÍZ, Ramón (Eds.): *Teoría política: poder, moral, democracia*. Alianza Editorial, Madrid, 2003.

BALLESTEROS, Miguel Ángel: "Para lograr la paz". Revista de Política Exterior, p. 175, volumen XVI, número 88. Madrid, 2002.

BARADO, Francisco. *Literatura militar española*. Ministerio de Defensa. Madrid, 1996.

BENTÉGEAT, Henri. "*Nous avons développé un sentiment de confiance dans l'efficacité de la PESD"*. ESDP newsletter. European Security and Defence Policy 1999-2009. Octubre 2009.

BEYERCHEN, Alan D.: "Clausewitz Nonlinearity, and the Importance of Imagery", en *Complexity, Global Politics and National Security*, pp. 155-156. Editado por David S. Alberts y Thomas J. Czerwinski. National Defense University, Washington D. C., 1997.

BOCHENSKI, I. M.: Los métodos actuales de pensamiento. Rialp, Madrid, 1981.

BOND, Brian y ALEXANDER, Martin: "Liddell Hart y De Gaulle: las doctrinas de los recursos limitados y de la defensa móvil", en PARET, Peter: *Creadores de la Estrategia moderna: desde Maquiavelo a la era nuclear*, p. 627. Ministerio de Defensa. Madrid, 1992.

BOUDET, Jaques, director. Historia Universal de los Ejércitos, 1300-1700, de Soliman a Vauban. Robert Laffont. París, 1965. Edición española Hispano Europea. Barcelona, 1966.

BRODIE, Bernard: "La permanente importancia de De la guerra", en CLAUSEWITZ, Carl von: *De la guerra*, p. 73. Ministerio de Defensa. Madrid, 1999.

BROOKE, Christopher: *Europa en el centro de la Edad Media 962-1154*. Traducción de Matilde Vilarroig. Aguilar. Madrid, 1973.

BRUCE, Anthony. *A Bibliography of British Military History from the Roman Invasions to the restoration 1660*. Saur. Londres, 1981.

CABALLERO MÍGUEZ, Gonzalo. *Nuevo institucionalismo en ciencia política, institucionalismo de elección racional y análisis político de costes de transacción: una primera aproximación*. RIPS. Revista de Investigaciones Políticas y Sociológicas, 6, 2007.

CCN-CERT: *Ciberamenazas 2014. Tendencias 2015*, *Resumen Ejecutivo*, IA-09/15, Madrid, marzo de 2015.

Centro Nacional de Ciberseguridad de los Países Bajos: *Cyber Security Assessment Netherlands 4*, La Haya, octubre de 2014.

CHALIAND, Gérard: *Anthologie mondiale de la stratégie: des origines au nucléaire.* Robert Laffon. París, 1990.

CHULIÁ, Elisa y AGULLÓ, Marco V. *Cómo se hace un trabajo de investigación en Ciencia Política*, Madrid: Los Libros de la Catarata, 2012.

COLLER, Xavier: *Estudio de casos*. Centro de Investigaciones Sociológicas, Cuadernos Metodológicos, núm. 30, junio de 2000.

CONDE, Francisco Javier. *El saber político en Maquiavelo*. Instituto Nacional de Estudios Jurídicos. Madrid, 1948.

CORTÉS, Hernán: "Cartas de Relación", *Historia 16*. Madrid, 1985.

COUTAU-BÉGARIE, Hervé: Traité de Stratégie, Economica. París, 1999.

CREVELD, Martin van: The Art of War, War and Military Tought, pp. 24-25. Londres, Cassell, 2002.

DEBS HENIL, Robert jr.: *Dictionary of Military and Naval Quotations*. United States Naval Institute. Annapolis, 1966.

DESPORTES, Vincent: "Vies et morts de Clausewitz aux Etats-Unis", en *Défense Nationale*, pp. 39 y 47. París, febrero 2002.

ENCEL, Frédéric. *El arte de la guerra. Estrategas y batallas*. Alianza Editorial. Madrid, 2002.

GADY, Franz-Stefan y AUSTIN, Greg. “Russia, The United States, And Cyber Diplomacy. Opening the Doors”. pág. i; 2010 EastWest Institute. Nueva York.

GIL PICACHE, Baltasar. *Elementos de Historia Militar*. Imprenta del Colegio de Santiago para Huérfanos del Arma de Caballería. Valladolid, 1908.

GILBERT, Félix: "Maquiavelo: el renacimiento del arte de la guerra", en PARET, Peter: *Makers of Modern Strategy: from Machiavelli to the nuclear age.* Princeton University Press, Princeton, 1986. Traducción en español Creadores de la Estrategia moderna: desde Maquiavelo a la era nuclear. Ministerio de Defensa. Madrid, 1992.

GOODIN, Robert E. y KLINGEMANN, Hans-Dieter (Eds.). *A New Hadbook of Political Science*. Oxford University Press, Oxford, 1996.

GUERLAC, Henry: "Vauban: El impacto de la ciencia en la guerra", en PARET, Peter: *Creadores de la Estrategia moderna: desde Maquiavelo a la era nuclear,* pp. 77-100. Ministerio de Defensa. Madrid, 1992.

HITTLE, J. D. *Jomini and his Summary of the Art of War*. Military Service Publishing Company. Harrisburg, 1974.

HOWARD, Michael: "La influencia de Clausewitz", en CLAUSEWITZ, Carl von: *De la guerra*, pp. 51-52. Ministerio de Defensa. Madrid, 1999.

Jenofonte. *Anábasis*. Edición y traducción de Carlos Varias. Cátedra. Madrid, 1999.

JOMINI, Henri Antoine de. *Compendio del arte de la guerra.* Ministerio de Defensa. Madrid, 1991.

JULIO CÉSAR: *Comentarios de la Guerra de las Galias.* Espasa Calpe. Madrid, 1980.

JULIO CÉSAR: *Guerra de las Galias, Libros I, II y III.* Gredos, Madrid, 1945.

KAPLAN, Robert D.: El retorno de la Antigüedad: La política de los guerreros. Ediciones B. Barcelona, 2002.

LÓPEZ-BARAJAS ZAYAS, Emilio: *Fundamentos de metodología científica*. Universidad Nacional de Educación a Distancia, Madrid, 1988.

MACISAAC, David: "Voces desde el azul del cielo: los teóricos del poder aéreo", en PETER, Paret: *Creadores de la Estrategia moderna: desde Maquiavelo a la era nuclear*, p. 643. Ministerio de Defensa. Madrid, 1992.

MARCU, Valeriu. *Maquiavelo, la escuela del poder*. Espasa Calpe. Madrid, 1967.

MARSH, David y STOKER, Gerry (Eds.): *Teoría y métodos de la ciencia política*. Alianza Editorial, Madrid, 2013.

MARTÍNEZ TEIXIDÓ, Antonio, drector. *Enciclopedia del arte de la guerra*. Planeta. Barcelona, 2001.

MAURER, Tim y MORGUS, Robert. *Compilation of Existing Cybersecurity and Information Security Related Definitions*, New America, octubre de 2014.

MEAD EARLE, Edward. *Makers of Modern Strategy: Military Thought from Machiavelli to Hitler*, Princeton University Press, Princeton, 1944.

MÉNDEZ DE VIGO, Beatriz: "Entrevista en revista SIC". *Revista SIC, Ciberseguridad, Seguridad de la Información y Privacidad* nº 115, junio de 2015.

Microsoft Corporation: *Microsoft Security Intelligence Report, Volume 18, julio a diciembre de 2014, España*, Redmond, WA, 2015.

MITRE FERNÁNDEZ, Emilio y ALVIRA CABRER, Martín: "Ideología y guerra en los reinos de la España medieval", en *Revista de Historia Militar*, pp. 308-309. Ministerio de Defensa. Mayo, 2001.

NASSIMBENI, Mary. "The information society in South Africa: from global origins to local vision". *South African Journal of Libraries and Information Science*. Vol 66 No 4, 1998.

PALMER, R. R.: "Federico el Grande, Guibert, Bülow: De las guerras dinásticas a las nacionales", en PARET, Peter: *Creadores de la Estrategia moderna: desde Maquiavelo a la era nuclear*, pp. 107-108. Ministerio de Defensa. Madrid, 1992.

PARET, Peter: "La génesis de la guerra", en CLAUSEWITZ, Carl von: *De la guerra*, p. 25. Ministerio de Defensa. Madrid, 1999.

PARET, Peter: *Makers of Modern Strategy: from Machiavelli to the nuclear age*, Princeton University Press, Princeton, 1986. Traducción en español titulada *Creadores de la Estrategia moderna: desde Maquiavelo a la era nuclear.* Ministerio de Defensa. Madrid, 1992.

PETERS, B. Guy; PIERRE, Jon; y KING, Desmond S. *The Politics of Path Dependency: Political Conflict in Historical Institutionalism*. Southern Political Science Association, The Journal of Politics, vol. 67, núm. 04, noviembre de 2005.

QUESADA GÓMEZ, Agustín, director. *Pensamiento y pensadores militares Iberoamericanos del siglo XX y su influencia en la Comunidad Iberoamericana*, Monografía del CESEDEN número 63. Ministerio de Defensa. Madrid, 2003.

RAMOS-OLIVEIRA, Antonio. *Historia crítica de España y de la civilización española, la Edad Media*. Oasis, México, D.F., segunda edición, 1974.

Revista SIC, Ciberseguridad, Seguridad de la Información y Privacidad: *Alemania endurece el castigo a las negligencias en infraestructuras críticas*. nº 116, septiembre de 2015.

ROMANO, Ruggiero y TENENTI, Alberto. "Los fundamentos del mundo moderno"; "Edad Media tardía"; "Renacimiento" y "Reforma", en Historia Universal del siglo XXI, Madrid, 1978.

ROTHENBERG, Gunther E.: "Moltke, Schlieffen y la Doctrina del Envolvimiento Estratégico", en PARET, Peter: *Creadores de la Estrategia moderna: desde Maquiavelo a la era nuclear*, p. 313. Ministerio de Defensa. Madrid, 1992.

SALUSTIO: *Conjuración de Catilina*. Versión literaria Manuel C. Díaz y Díaz. Gredos. Madrid, 1979.

SÁNCHEZ PRIETO y BELÉN, Ana. *Guerra y guerreros en España según las fuentes canónicas de la Edad Media*. Servicio de Publicaciones del Estado Mayor del Ejército. Colección Adalid. Madrid, 1990.

SAWYER, Ralph D.: *The Tao of War. The Martial Tao Te Ching*. Westview Press. Cambridge, 2003.

SHY, John: "Jomini", en PARET, Peter: *Creadores de la Estrategia moderna: desde Maquiavelo a la era nuclear*, p. 157. Ministerio de Defensa. Madrid, 1992.

SUN TZU: Los trece artículos sobre el arte de la guerra. Ministerio de Defensa. Madrid, 1998.

VEGECIO RENATO, Flavio. *Instituciones Militares.* Ministerio de Defensa. Madrid, 1988.

VILLALBA FERNÁNDEZ, Aníbal: “La evolución del pensamiento estratégico”, en *Fundamentos de la estrategia desde el siglo XXI*, pp. 67-140. Monografías del CESEDEN número 67. Ministerio de Defensa. Madrid, marzo 2004.

VILLALBA FERNÁNDEZ, ANÍBAL: “El Tratado de Lisboa y la Política Común de Seguridad y Defensa”, en Panorama Estratégico 2009/2010, pp. 151-184. Ministerio de Defensa; Instituto Español de Estudios Estratégicos y Real Instituto Elcano. Madrid, marzo 2010.

WESTIN, Stu; ROY Matthew; y KIM Chai K. *Cross-Fertilization of Knowledge: The Case of MIS and its Reference Disciplines.* Information Resources Management Journal, University of Rhode Island, primavera de 1994.

WHEELER EVERETT, L.: "The Origins of Military Theory in Ancient Greece and China". Actes des colloques de la Commission Internationale d'Histoire Militaire, número 5, Bucarest, 1980.

Páginas web

A / 54/213. Los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional. 54 sesión plenaria de la Asamblea General de Naciones Unidas. Informe del Secretario General, 10 de agosto de 1999. https://disarmament-library.un.org/UNODA/Library.nsf/f4c497d5f90e302d85257631005152d2/fae7e8060174f22c8525764e0051ce60/$FILE/A-54-213.pdf

A/RES/51/210. Medidas para eliminar el terrorismo internacional. 55 sesión plenaria de la Asamblea General de Naciones Unidas. 16 de enero de 1997. http://www.un.org/documents/ga/res/51/ares51-210.htm

A/RES/53/70. Los avances en la informatización y las telecomunicaciones en el contexto de la seguridad internacional. 79a sesión plenaria de la Asamblea General de Naciones Unidas. 4 de diciembre de 1998. http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/53/70&referer=http://www.un.org/disarmament/topics/informationsecurity/&Lang=S

A/RES/54/49. Los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional. 69a sesión plenaria de la Asamblea General de Naciones Unidas. 1 de diciembre de 1999. https://gafc-vote.un.org/UNODA/vote.nsf/91a5e1195dc97a630525656f005b8adf/0e4088ff35d5505d0525681200673c74?OpenDocument&ExpandSection=4

A/RES/58/32. Los avances en la informatización y las telecomunicaciones en el contexto de la seguridad internacional. 58 sesión plenaria de la Asamblea General de Naciones Unidas. 8 de diciembre de 2003. https://ccdcoe.org/sites/default/files/documents/UN-031208-ITIS_0.pdf

A/RES/61/54. Los avances en la informatización y las telecomunicaciones en el contexto de la seguridad internacional. 61 sesión plenaria de la Asamblea General de Naciones Unidas. 6 de diciembre de 2006. https://ccdcoe.org/sites/default/files/documents/UN-061206-ITIS.pdf

Acta Goldwater-Nichols de reorganización del Departamento de Defensa. Public Law. pp. 99-433. 1 de octubre de 1986. http://history.defense.gov/Portals/70/Documents/dod_reforms/Goldwater-NicholsDoDReordAct1986.pdf consulta: 3 de agosto de 2015.

AL-RODHAN, Nayef. *Strategic Culture and Pragmatic National Interest. Global Policy*, 22 de julio de 2015. http://www.globalpolicyjournal.com/blog/22/07/2015/strategic-culture-and-pragmatic-national-interest consulta: 4 de agosto de 2015.

ARTEAGA, Félix y FOJÓN CHAMORRO, Enrique: *En favor de una política nacional de ciberseguridad en España*. Real Instituto Elcano, 23 de marzo de 2015. http://www.realinstitutoelcano.org/wps/portal/web/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/comentario-arteaga-fojon-en-favor-de-una-politica-nacional-de-ciberseguridad-en-espana consulta: 20 de octubre de 2015.

ASAMBLEA DE LA UNIÓN EUROPEA OCCIDENTAL. "*The EU-NATO Berlin Plus agreements*". Factsheet Nº 14. Noviembre 2009. http://www.assembly-weu.org/en/documents/Fact%20sheets/14E_Fact_Sheet_Berlin_Plus.pdf?PHPSESSID=ad7ba3060e75d20eca30f2c9c9daaedd

ASHTON, CATHERINE. "La ambición de actuar". *El Mundo*. 22 de diciembre de 2009. http://www.elmundo.es/elmundo/2009/12/22/union_europea/1261454578.html

Basic Principles for State Policy of the Russian Federation in the field of International Information Security in 2020. http://en.ambruslu.com/wp-content/uploads/2013/09/state-policy.doc consulta: 20 de agosto de 2015

BISCOP, SVEN. *"Permanent Structured Cooperation and the future of ESDP"*. Egmont Paper 20. Royal Institute for International relations. http://www.egmontinstitute.be/paperegm/ep20.pdf

BSA - The Software Alliance: *Country Report, Germany*. http://cybersecurity.bsa.org/assets/PDFs/country_reports/cs_germany.pdf consulta: 21 de octubre de 2015.

BSA - The Software Alliance: *EU Cybersecurity Dashboard. A Path to a Secure European Cyberspace*. Washington D.C., 2015. http://cybersecurity.bsa.org/assets/PDFs/study_eucybersecurity_en.pdf consulta: 21 de octubre de 2015.

CABALLERO MÍGUEZ, Gonzalo: http://www.redalyc.org/articulo.oa?id=38060201 consulta: 25 de octubre de 2015.

CARR, Jeffrey: *Inside Cyber Warfare, Russian cyber security structure*, p. 220. O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472, segunda edición, diciembre 2011.

CASEY, Tim: *Research on Topics in Information Security. The National Strategy to Secure Cyberspace: an In-depth Review,* Global Information Assurance Certification (GSEC), SANS Institute, 2003. http://www.giac.org/paper/gsec/2875/national-

strategy-secure-cyberspace-in-depth-review/104847 consulta: 12 de octubre de 2015.

CCN-CERT: *Análisis de riesgos*. https://www.ccn.cni.es/index.php?option=com_content&view=article&id=7&Itemid=10&lang=es consulta: 14 de septiembre de 2015.

CCN-CERT: *Ciberamenazas 2014. Tendencias 2015*, *Resumen Ejecutivo*, IA-09/15, Madrid, marzo de 2015. https://www.ccn-cert.cni.es/publico/dmpublidocuments/IE-Ciberamenazas2014-Tendencias-2015.pdf consulta: 5 de septiembre de 2015.

CCN-CERT: *Ciberamenazas 2014. Tendencias 2015*, *Resumen Ejecutivo*, IA-09/15: https://www.ccn-cert.cni.es/publico/dmpublidocuments/IE-Ciberamenazas2014-Tendencias-2015.pdf consulta: 5 de septiembre de 2015.

CCN-CERT: *Guía de Seguridad CCN-STIC-401. Glosario y Abreviaturas,* agosto 2015. https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/401-glosario_abreviaturas/index.html consulta: 13 de septiembre de 2015.

CCN-CERT: *Guía de seguridad de las TIC, CCN-STIC-817, Esquema Nacional de Seguridad, Gestión de Ciberincidentes,* mayo 2015. https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/988-ccn-stic-817-gestion-de-ciberincidentes/file.html consulta: 13 de septiembre de 2015.

CCN-CERT: https://www.ccn-cert.cni.es/informes/informes-de-amenazas-ia/813-ccn-cert-ia-09-15-ciberamenazas-2014-tendencias-2015/file.html consulta: 5 de septiembre de 2015.

Centro Criptológico Nacional: *Esquema Nacional de Seguridad: Preguntas Frecuentes*, Madrid, noviembre 2012, p. 8. file:///Users/Anibal/Downloads/Esquema_Nacional_de_Seguridad_-_Preguntas_frecuentes.pdf consulta: 17 de octubre de 2015.

Centro Criptológico Nacional: *Guía de Seguridad CCN-STIC-802. Esquema Nacional de Seguridad: Guía de Auditoría*, Madrid, junio de 2010 https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/802-Auditoria_ENS/802-Auditoria_ENS-jun10.pdf consulta: 17 de octubre de 2015.

Centro Criptológico Nacional: *Guía de Seguridad CCN-STIC-803. Esquema Nacional de Seguridad: Valoración de los Sistemas. Política de Seguridad de la Información*, Madrid, enero de 2011. https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/803-Valoracion_en_el_ENS/803_ENS-valoracion_ene-11.pdf consulta: 17 de octubre de 2011.

Centro Criptológico Nacional: *Guía de Seguridad CCN-STIC-804. Esquema Nacional de Seguridad: Guía de Implantación*, Madrid, 26 de octubre de 2011. https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/804-Medidas_de_implantacion_del_ENS/804-Medidas_de_implantacion_del_ENS-20111026.pdf consulta: 17 de octubre de 2015.

Centro Criptológico Nacional: *Guía de Seguridad CCN-STIC-805. Esquema Nacional de Seguridad: Política de Seguridad de la Información*, Madrid, septiembre de 2011. https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/805-Politica_de_seguridad_del_ENS/805-ENS_politica-sep11.pdf consulta: 17 de octubre de 2011.

Centro Criptológico Nacional: *Guía de Seguridad CCN-STIC-806. Esquema Nacional de Seguridad: Plan de Adecuación*, Madrid, enero de 2011. https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/806-Plan_adecuacion_ENS/806_ENS-adecuacion_ene-11.pdf consulta: 17 de octubre de 2015.

Centro Criptológico Nacional: *Guía de Seguridad CCN-STIC-808. Esquema Nacional de Seguridad: Verificación del cumplimiento de las medidas en el ENS*, Madrid, septiembre de 2011. https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/808/808-Verificacion_del_cumplimiento_medidas_ENS-sep11.pdf consulta: 17 de octubre de 2015.

Centro Criptológico Nacional: *Guía de Seguridad CCN-STIC-815. Esquema Nacional de Seguridad: Métricas e Indicadores*, Madrid, julio de 2013 https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/815-Metricas_e_Indicadores_en_el_ENS/815_metricas_e_indicadores_ENS.pdf consulta: 17 de octubre de 2015.

Centro Criptológico Nacional: Guía de Seguridad CCN-STIC-815. Esquema Nacional de Seguridad: Métricas e Indicadores, Madrid, julio de 2013. consulta: 17 de octubre de 2015.

Centro Criptológico Nacional: *Serie 800 de Guías Esquema Nacional de Seguridad* https://www.ccn-cert.cni.es/guias/guias-series-ccn-stic/800-guia-esquema-nacional-de-seguridad.html consulta: 17 de octubre de 2015.

Centro Nacional de Ciberseguridad de los Países Bajos: Cyber Security Assessment Netherlands: https://www.ncsc.nl/english/current-topics/news/cyber-securty-assessment-netherlands-4-cybercrime-and-digital-espionage-remain-the-biggest-threat.html consulta: 4 de septiembre de 2015.

CERT: https://www.ccn.cni.es/ consulta: 5 de septiembre de 2015.

CHINA LAW TRANSLATE: *Cybersecurity Law (Draft),* 6 de julio de 2015. http://chinalawtranslate.com/cybersecuritydraft/?lang=en consulta: 11 de agosto de 2015.

CLINTON, Hillary: *Remarks by Hillary Rodham Clinton at Conference on Internet Freedom*, The Hague, Netherlands, 8 de diciembre de 2011. Disponible en: http://iipdigital.usembassy.gov/st/english/texttrans/2011/12/20111209083136su0.3596874.html#axzz3jNXkemIm consulta: 20 de agosto de 2015.

Código de Estados Unidos. 31 § 1105 - *Budget contents and submission to Congress.* Cornell University Law School. https://www.law.cornell.edu/uscode/text/31/1105 consulta: 3 de agosto de 2015.

Código de Estados Unidos. 50 USC § 404A – *Annual National Security Strategy Report.* National Security Strategy Archive. http://nssarchive.us/50-usc-%C2%A7-404a-annual-national-security-strategy-report/ consulta 3: de agosto de 2015.

COLE, Ronald H.: *Grenada, Panama and Haiti: join operational reform*. Joint Force Quaterly. Otoño-invierno 1988-1989. http://www.dtic.mil/dtic/tr/fulltext/u2/a422959.pdf consulta: 3 de agosto de 2015.

Comisión Ejecutiva sobre China del Congreso de Estados Unidos. http://www.cecc.gov/chinas-state-organizational-structure consulta: 9 de agosto de 2015.

Comisión Europea y la Alta Representante de la UE para Asuntos Exteriores y Política de Seguridad: *Estrategia de Ciberseguridad de la Unión Europea: Un ciberespacio abierto*, *protegido y seguro*, Bruselas, 7 de febrero de 2013. http://register.consilium.europa.eu/doc/srv?f=ST+6225+2013+INIT&l=es consulta: 6 de octubre de 2015.

Comisión Europea: *Decisión de la Comisión, de 3 de febrero de 2005, por la que se modifica la Decisión 2001/844/CE, CECA, Euratom*. https://www.boe.es/buscar/doc.php?id=DOUE-L-2005-80234 consulta: 17 de octubre de 2015.

Consejo de Estado de la República Popular China, *China's Military Strategy*. http://www.chinadaily.com.cn/china/2015-05/26/content_20820628.htm consulta: 7 de agosto de 2015.

Consejo de Europa: *Convenio sobre la Ciberdelincuencia*, Budapest, 23 de noviembre de 2001 https://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/consejo_europa/convenios/common/pdfs/Convenio_Ciberdelincuencia.pdf consulta: 6 de octubre de 2015.

Consejo de Europa: *Convenio sobre la Ciberdelincuencia;* Budapest, 23 de noviembre de 200*1*. http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/ETS_185_spanish.PDF

CONSEJO DE LA UNIÓN EUROPEA. "*Diez años de PESD: Retos y Oportunidades*". Declaración Ministerial del 2974 Consejo de Relaciones Exteriores. 17 de noviembre de 2009. http://www.consilium.europa.eu/uedocs/cms_Data/docs/pressdata/en/gena/111253.pdf

Consejo de la Unión Europea: *Conclusiones del Consejo sobre la comunicación conjunta de la Comisión y de la Alta Representante de la Unión para Asuntos Exteriores y Política de Seguridad, titulada "Estrategia de ciberseguridad de la Unión Europea: un ciberespacio abierto, protegido y seguro"*, Bruselas, 22 de julio de 2013. http://register.consilium.europa.eu/doc/srv?f=ST+12109+2013+INIT&l=es consulta: 6 de octubre de 2015.

Consejo de la Unión Europea: *Marco Político de Ciberdefensa de la UE*, Bruselas, 18 de noviembre de 2014. http://data.consilium.europa.eu/doc/document/ST-15585-2014-INIT/es/pdf consulta: 10 de octubre de 2015.

Consejo de la Unión Europea: *Una estrategia para una sociedad de la información segura en Europa*, Bruselas, 12 de diciembre de 2006. http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/es/trans/92382.pdf consulta: 6 de octubre de 2015.

Consejo de Seguridad de la Federación de Rusia. http://en.kremlin.ru/structure/security-council/members consulta: 15 de agosto de 2015.

Consejo de Seguridad Nacional. Informe Anual de Seguridad Nacional 2014. Abril 2015. http://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Nacional/2015/Informe_Anual_de_Seguridad_Nacional_2014.pdf consultado 27 de julio de 2015. OJO REPETIDO

Consejo de Seguridad Nacional: *Informe Anual de Seguridad Nacional 2013.* abril 2014. http://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/Documents/_Informe_Seguridad_Nacional%20Accesible%20y%20Definivo.pdf consultado 27 de julio de 2015

Consejo de Seguridad Nacional: *Informe Anual de Seguridad Nacional 2014*. abril 2015. http://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Nacional/2015/Informe_Anual_de_Seguridad_Nacional_2014.pdf consulta: 27 de julio de 2015.

Consejo Europeo: *Estrategia Europea de Seguridad: Una Europa segura en un mundo mejor*, Bruselas, 12 de diciembre de 2013. http://www.consilium.europa.eu/uedocs/cmsUpload/031208ESSIIES.pdf consulta: 6 de octubre de 2015.

Consejo Europeo: *Informe sobre la aplicación de la Estrategia Europea de Seguridad: Ofrecer seguridad en un mundo en evolución*, Bruselas, 11 de diciembre de 2008, p. 5. http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressdata/ES/reports/104637.pdf consulta: 6 de octubre de 2015.

Constitución de Rusia, capítulo 4, artículo 83, g. http://www.constitution.ru/en/10003000-05.htm consulta: 15 de agosto de 2015.

CONSULTANCY.UK: *IT firms lead mega project at UK Ministry of Defence*, 20 de agosto de 2015. http://www.consultancy.uk/news/2464/it-firms-lead-mega-project-at-uk-ministry-of-defence consulta: 21 de octubre de 2015.

Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales. Boletín Oficial del Estado. https://www.boe.es/buscar/doc.php?id=BOE-A-1979-24010 consulta: 20 de agosto de 2015.

Council on Foreign Relations: *Cybersecurity Law of the People's Republic of China*, 6 de julio de 2015. http://www.cfr.org/internet-policy/cybersecurity-law-peoples-republic-china/p36788 consulta: 11 de agosto de 2015.

DAGAND, SOPHIE. "*The impact of the Lisbon Treaty on CFSP and ESDP*". European Security Review, Nº 37, marzo 2008. http://www.isis-europe.org/pdf/2008_artrel_150_esr37tol-mar08.pdf

Diario Oficial de la Unión Europea. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:285:0047:0071:ES:PDF

DIMITRAKOPOULOU, Sophia y LIAROPOULOS, Andrew: "Russia's National Security Strategy to 2020: A Great Power in the Making?" *Caucasian Review of International Affairs*, Vol. 4 (1) – Winter 2010. http://www.cria-online.org/Journal/10/Done_Russias_National_Security_Strategy_To_2020_A_Great_Power_In_The_Making_Dimitrakopoulou_Liaropoulos.pdf consulta: 18 de agosto de 2015.

Documentos de la III Sesión Plenaria del XVIII Comité Central del Partido Comunista de China, p. 7. 9-12 de noviembre de 2013. http://www.politica-china.org/imxd/noticias/doc/1389789646Documentos_de_la_III_Sesion_Plenaria_del_XVIII_Comite_Central_del_Partido_Comunista_de_China.pdf consulta: 9 de agosto de 2015.

DUTTA Soumitra, GEIGER Thierry y LANVIN Bruno, Eds.: *The Global Information Technology Report 2015,* World Economic Forum & INSEAD, Ginebra, 2015. http://www3.weforum.org/docs/WEF_Global_IT_Report_2015.pdf consulta: 12 de septiembre de 2015.

Eneken Tikk-Ringas, "*Developments in the Field of Information and Telecommunication in the Context of International Security: Work of the UN First Committee 1998-2012*", ICT4Peace http://www.ict4peace.org/wp-content/uploads/2012/08/Eneken-GGE-2012-Brief.pdf

ENJUTO, Joseba: *Estudio del Esquema Nacional de Seguridad*: *Modelo de Aplicación Práctica del Real Decreto 3/2010*. Máster en Derecho de Internet y Nuevas Tecnologías del Instituto Europeo Campus Stellae, 2013. http://www.criptored.upm.es/descarga/EstudioEsquemaNacionalSeguridadJosebaEnjuto.pdf consulta: 18 de octubre de 2015.

Estatuto del Consejo de Seguridad de la Federación de Rusia. Puede consultarse una version en idioma ingles en http://fas.org/irp/world/russia/docs/edict_1024.htm consulta: 15 de agosto de 2015.

FIDLER, David P.: *International Law and the Future of Cyberspace: The Obama Administration's International Strategy for Cyberspace*, American Society of International Law, Insights, volumen 15, 8 de junio de 2011. http://www.asil.org/insights/volume/15/issue/15/international-law-and-future-cyberspace-obama-administration%E2%80%99s consulta: 13 de octubre de 2015.

FIRST (Forum for Incident Response and Security Teams). http://www.first.org/ y sobre APCERT en http://www.apcert.org/ consulta: 11 de octubre de 2015.

FOJÓN CHAMORRO, Enrique: *La ciberdefensa en la Unión Europea*, Real Instituto Elcano, Madrid, 25 de junio de 2015. http://www.blog.rielcano.org/reto-la-ciberdefensa-la-union-europea/ consulta: 11 de octubre de 2015.

GILES, Keir: *Russia's National Security Strategy to 2020*. NATO Defense College, Research Division, junio 2009. http://www.conflictstudies.org.uk/files/rusnatsecstrategyto2020.pdf consulta: 18 de agosto de 2015.

GILES, Keir: *Russia's Public Stance on Cyberspace Issues*, p. 63, Conflict Studies Research Centre Oxford, UK; 4th International Conference on Cyber Conflict; C. Czosseck, R. Ottis, K. Ziolkowski (Eds.), Publicado a través de NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), Tallinn, junio 2012. Disponible en: http://www.ccdcoe.org/publications/2012proceedings/2_1_Giles_RussiasPublicStanceOnCyberInformationWarfare.pdf consulta: 20 de agosto de 2015.

Gobierno de España, Portal de Administración Electrónica. Magerit: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.VfdTmNPtmko consulta 14 de septiembre de 2015.

Gobierno de España: *Estrategia de Ciberseguridad Nacional*. Madrid, 5 de diciembre de 2015. http://www.lamoncloa.gob.es/documents/20131332estrategiadeciberseguridadx.pdf consulta: 20 de octubre de 2015.

Gobierno de España: *Estrategia de Seguridad Nacional, un proyecto compartido*. Madrid, 31 de mayo de 2013. http://www.lamoncloa.gob.es/documents/seguridad_1406connavegacionfinalaccesiblebpdf.pdf consulta: 20 de coctubre de 2015.

Gobierno de España: *Estrategia Española de Seguridad, una responsabilidad de todos*. Madrid, 24 de junio de 2011. http://www2.urjc.es/ceib/investigacion/publicaciones/REIB_05_01_Document03.pdf consulta: 19 de octubre de 2015.

Gobierno de España: *Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos*, http://www.boe.es/diario_boe/txt.php?id=BOE-A-2007-12352 consulta: 17 de octubre de 2015.

Gobierno de España: *Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común*. http://www.boe.es/buscar/act.php?id=BOE-A-1992-26318 consulta: 17 de octubre de 2015.

Gobierno de España: *Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público.* http://www.boe.es/diario_boe/txt.php?id=BOE-A-2007-19814 consulta: 17 de octubre de 2015.

Gobierno de España: *Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.* https://www.boe.es/buscar/doc.php?id=BOE-A-1999-23750 consulta: 17 de octubre de 2015.

Gobierno de España: Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. https://www.boe.es/buscar/doc.php?id=BOE-A-2010-1330 consulta: 14 de septiembre de 2015.

Gobierno de España: *Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica*. https://www.boe.es/buscar/pdf/2010/BOE-A-2010-1330-consolidado.pdf consulta: 17 de octubre de 2015.

Gobierno de España: *Real Decreto 385/2013, de 31 de mayo, de modificación del Real Decreto 1886/2011, de 30 de diciembre, por el que se establecen las Comisiones Delegadas del Gobierno*. http://www.boe.es/diario_boe/txt.php?id=BOE-A-2013-5771 consulta: 20 de octubre de 2015.

Gobierno de España: *Reunión del Consejo de Seguridad Nacional*. Madrid, 5 de diciembre de 2013. http://www.lamoncloa.gob.es/presidente/actividades/Paginas/2013/051213CSN.aspx consulta: 20 de octubre de 2015.

Gobierno de España; *Proyecto de Ley de Seguridad Nacional*, Boletín Oficial de las Cortes Generales, Senado, 31 de julio de 2015, art. 3. http://www.senado.es/legis10/publicaciones/pdf/senado/bocg/BOCG_T_10_574.PDF consulta: 23 de septiembre de 2015.

Gobierno del Reino Unido, Cabinet Office: *The UK Cyber Security Strategy. Protecting and promoting the UK in a digital world*. Londres, noviembre de 2011, p. 7. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf consulta: 22 de octubre de 2015.

HAGUE, William: London Conference on Cyberspace: Chair's statement, 2 de noviembre de 2011. Disponible en: https://www.gov.uk/government/news/london-conference-on-cyberspace-chairs-statement

Horizonte 2020. http://ec.europa.eu/research/innovation-union/index_en.cfm consulta: 9 de octubre de 2015.

HOWARD. Alex: *A Manhattan Project for online identity*: *A look at the White House's National Strategy for Trusted Identities in Cyberspace*. O'Reilly Radar, 4 de mayo de 2011. http://radar.oreilly.com/2011/05/nstic-analysis-identity-privacy.html consulta: 13 de octubre de 2015.

Ibíd. Parte I, Capítulo I, Sección III. pp.1-2. http://www.mod.go.jp/e/publ/w_paper/pdf/2015/DOJ2015_1-1-3_1st_0730.pdf consulta: 8 de agosto de 2015.

Informe a la Asamblea General de las Naciones Unidas del Grupo de Expertos Gubernamentales en el Campo de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional. A/65/20 de 30 de julio de 2010. http://www.unidir.org/files/medias/pdfs/final-report-eng-0-189.pdf consulta: 21 de agosto de 2015.

Informe a la Asamblea General de las Naciones Unidas del Grupo de Expertos Gubernamentales en el Campo de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional. A/68/98 de 24 de junio de 2013. Disponible

en http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98 consulta: 21 de agosto de 2015.

Institute for Defence Studies and Analyses. *Russian Foreign Policy Documents and Military Doctrines*. http://www.idsa.in/eurasia/resources.html consulta: 15 de agosto de 2015.

Institute for Information Security Issues, Moscow State University & Conflict Studies Research Centre, Oxford: *Russia's "Draft Convention on International Information Security" A Commentary*, abril de 2012. http://www.conflictstudies.org.uk/files/20120426_CSRC_IISI_Commentary.pdf consulta: 20 de agosto de 2015.

KAROCK, Ulrich: La Política Común de Seguridad y Defensa, Parlamento Europeo, fichas técnicas, febrero 2015. http://www.europarl.europa.eu/ftu/pdf/es/FTU_6.1.2.pdf consulta: 6 octubre 2015.

KEJIN, Zhao. *China's National Security Commission*. Carnegie-Tsinghua Center for Global Policy, 14 de julio de 2015. http://carnegietsinghua.org/2015/07/09/china-s-national-security-commission/id7i consulta: 9 de agosto de 2015.

KUMAR, Amit: Russian Military Reforms: An Evaluation. Institute for Defence Studies and Analyses, 23 de mayo de 2013. http://www.idsa.in/~idsa/issuebrief/RussianMilitaryReforms_amitk_230513.html consulta: 17 de agosto de 2015.

La Casa Blanca: "*Defending America's Cyberspace, National Plan for Information Systems Protection, Version 1.0, An Invitation to a Dialogue*", Washington D.C., 2000. https://fas.org/irp/offdocs/pdd/CIP-plan.pdf consulta: 12 de octubre de 2015.

La Casa Blanca: "*The National Strategy to Secure Cyberspace*", Washington D.C., febrero de 2003. https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf consulta: 12 de octubre de 2015.

La Casa Blanca: *Cyber Space Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, Washington D.C., mayo de 2009. https://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf consulta: 12 de octubre de 2015.

La Casa Blanca: *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, Washington D.C., mayo de 2011. https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf consulta: 13 de octubre de 2015.

La Casa Blanca: *National Strategy for Trusted Identities in Cyberspace: Enhancing Online Choice, Efficiency, Security, and Privacy*, Washington D.C., abril de 2011. https://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf consulta: 12 de octubre de 2015.

La Casa Blanca: *The Comprehensive National Cybersecurity Initiative*, 2009 https://www.whitehouse.gov/sites/default/files/cybersecurity.pdf

LELLOUCHE, PIERRE. "*8 propositions pour donner à l'Union une défense commune*". Le Figaro. 31 de enero de 2008. http://www.lefigaro.fr/debats/2008/01/31/01005-20080131ARTFIG00515--propositions-pour-donner-a-l-union-une-defense-commune.php

Ley Federal Nº 40-FZ, del Servicio Federal de Seguridad de la Federación de Rusia, realizada por el Consejo de Europa de 24 de febrero de 2102 CDL-REF(2012)011 http://www.legislationline.org/download/action/download/id/3708/file/RF_law_fed_security_service_1999_am2011_en.pdf consulta: 18 de agosto de 2015.

LÓPEZ, María del Mar: *Plan Nacional de Ciberseguridad*, Ponencia en la II Jornada de Ciberseguridad en Andalucía, Sevilla, 8 de junio de 2015. http://www.slideshare.net/Ingenia_es/mara-del-mar-lpezcibersegand15 consulta: 19 de octubre de 2015.

Lu Wei (perfil) en NETmundial Initiative https://www.netmundial.org/lu-wei consulta: 13 de agosto de 2015.

MANUTSCHARJAN, Aschot: *Russia's National Security Strategy until 2020*. Konrad-Adenauer-Stiftung, Dr. Gerhard Wahlers, ed. Berlín, 31 de Agosto de 2009. http://www.kas.de/wf/en/33.17407/ consulta: 18 de agosto de 2015.

MARTÍN CUBEL, Fernando: "ESN-2013: Propuesta de Sistema de Seguridad Nacional". Instituto Español de Estudios Estratégicos.Documento Opinión 118/2013. 02 diciembre de 2013. http://www.ieee.es/Galerias/fichero/docs_opinion/2013/DIEEEO118-2013_Prop.SisteSegNacional_FdoMartinCubel.pdf consulta: 28 de julio de 2015.

MAURER, Tim y MORGUS, Robert: http://www.giplatform.org/sites/default/files/Compilation%20of%20Existing%20Cybersecurity%20and%20Information%20Security%20Related%20Definition.pdf consulta: 12 de septiembre de 2015.

Microsoft Corporation: *Microsoft Security Intelligence Report, Volume 18, julio a diciembre de 2014:* http://www.microsoft.com/security/sir/threat/ consulta: 12 de septiembre de 2015.

Ministerio de Asuntos Exteriores y de Cooperación: *El MAEC y la Ciberseguridad*. http://www.exteriores.gob.es/Portal/es/PoliticaExteriorCooperacion/Ciberseguridad/Paginas/El-MAEC-y-la-Ciberseguridad.aspx consulta: 25 de octubre de 2015.

Ministerio de Defensa de Japón: *Defensa 2015*. http://www.mod.go.jp/e/publ/w_paper/2015.html consulta: 8 de agosto de 2015.

Ministerio de Hacienda y Administraciones Públicas: *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método*. Madrid, octubre de 2012. http://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Documentacion/Metodologias-y-guias/Mageritv3/2012_Magerit_v3_libro1_metodo_ES_NIPO_630-12-171-8/2012_Magerit_v3_libro1_m%C3%A9todo_es_NIPO_630-12-171-8.pdf consulta: 14 de septiembre de 2015.

Ministerio de Relaciones Exteriores de la Federación de Rusia: *Convention on International Information Security (Concept).* Disponible en: http://www.mid.ru/bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/7b17ead7244e2064c3257925003bcbcc!OpenDocument consulta: 20 de Agosto de 2015.

Ministerio Federal de Interior de Alemania*: CIP Implementation Plan of the National Plan for Information Infrastructure Protection*. Berlín, 2005. http://www.bmi.bund.de/SharedDocs/Downloads/EN/Broschueren/2009/kritis.pdf;jsessionid=B0B3D978E9BA15DA303E89BF20F7CDA7.2_cid373?__blob=publicationFile consulta: 21 de octubre de 2015.

Ministerio Federal de Interior de Alemania: *Cyber Security Strategy for Germany*. Berlín, febrero de 2011. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CyberSecurity/Cyber_Security_Strategy_for_Germany.pdf?__blob=publicationFile consulta: 21 de octubre de 2011.

MÖLLING, CHRISTIAN. "*ESDP After Lisbon: More Coherent and Capable?*". Center for Security Studies (CSS), Zurich, Suiza. Vol. 3, Nº 28, febrero 2008. http://www.isn.ethz.ch/isn/Digital-Library/Publications/Detail/?ots591=0C54E3B3-1E9C-BE1E-2C24-A6A8C7060233&lng=en&id=46839

MORALES, Javier: *Russia's New National Security Strategy: Towards a 'Medvedev Doctrine'?* Real Instituto Elcano, ARI 135/2009, 25 de septiembre de 2009. http://www.realinstitutoelcano.org/wps/wcm/connect/0558db804fb4cfd6a6f7ff8bf7fc5c91/ARI135-2009_Morales_Russia_New_National_Security_Strategy_Medvedev.pdf?MOD=AJPERES&CACHEID=0558db804fb4cfd6a6f7ff8bf7fc5c91 consulta: 18 de agosto de 2015.

MORISSET, Nicolas: *Le Livre Blanc de la défense 2015 de la Chine*. Conflictualités et médiations, Université catholique de l'Ouest, 2 de junio de 2015. https://conflictualitemediation.wordpress.com/2015/06/02/le-livre-blanc-de-la-defense-2015-de-la-chine/ consulta: 8 de agosto de 2015.

NIMARK, Agnieszka y PAWLAK, Patryk: *Upgrading the Union's response to disasters*. http://www.iss.europa.eu/uploads/media/Brief_45_Crisis_response.pdf consulta: 10 de octubre de 2015.

OBAMA, Barack: *Declaración del Presidente sobre la organización de la Casa Blanca para la Seguridad Nacional y Contraterrorismo*. La Casa Blanca. 26 de mayo de 2009. http://fas.org/irp/news/2009/05/wh052609.html consulta: 6 de agosto de 2015.

OBAMA, Barack: *Estrategia de Seguridad Nacional 2015*. http://nssarchive.us/NSSR/1997.pdf consulta: 4 de agosto de 2015.

OBAMA, Barack: *Presidential Study Directive*, febrero de 2009. http://fas.org/irp/offdocs/psd/psd-1.pdf consulta: 6 de agosto de 2015.

Oficina Ejecutiva del Presidente y Consejo Nacional de Ciencia y Tecnología: *Strategic Plan for Cybersecurity Research and, Development*, Washington D.C., diciembre de 2011. https://www.whitehouse.gov/sites/default/files/microsites/ostp/fed_cybersecurity_rd_strategic_plan_2011.pdf consulta: 13 de octubre de 2015.

ORJI, Uchenna Jerome: *Russia and the Council of Europe Convention on Cybercrime. Computer and Telecommunications,* Law Review, Vol.18 Issue 1, 2012.

OTAN: *Ciberseguridad*. 1 de septiembre de 2015. http://www.nato.int/cps/en/natohq/topics_78170.htm consulta: 26 de octubre de 2015. En este informe la OTAN presenta un recorrido por las diferentes iniciativas de ciberseguridad de la Alianza.

OTAN: Declaración de la Cumbre de Praga. 21 de noviembre de 2002. http://www.nato.int/docu/pr/2002/p02-127e.htm consulta: 26 de octubre de 2015.

OTAN: Declaración de la Cumbre de Riga. 29 de noviembre de 2006. http://www.nato.int/docu/pr/2006/p06-150e.htm consulta: 26 de octubre de 2015.

Pacto Internacional de Derechos Civiles y Políticos. Boletín Oficial del Estado en https://www.boe.es/diario_boe/txt.php?id=BOE-A-1977-10733 consulta: 20 de Agosto de 2015.

Parlamento Europeo: *Resolución sobre Ciberseguridad y Defensa*, 22 de noviembre de 2012. http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2012-0457&language=EN&ring=A7-2012-0335 consulta: 11 de octubre de 2015.

Parlamento Europeo: *Resolución sobre el Informe anual de la Alta Representante de la Unión Europea para Asuntos Exteriores y Política de Seguridad al Parlamento Europeo*, Estrasburgo, 12 de marzo de 2015. http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P8-TA-2015-0075&language=EN&ring=A8-2015-0039 consulta: 11 de octubre de 2015.

Parlamento Europeo: *Resolución sobre las Cláusulas de Defensa Mutua y Solidaridad de la UE: Dimensiones políticas y operacionales*, 22 de noviembre de 2012. http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2012-0456&language=EN&ring=A7-2012-0356 consulta: 11 de octubre de 2015.

PAWLAK, Patryk: *Cybersecurity and cyberdefence EU Solidarity and Mutual Defence Clauses*. Servicio de Investigación Parlamentario Europeo, PE 559.488, Bruselas, junio de 2015. http://www.europarl.europa.eu/RegData/etudes/BRIE/2015/559488/EPRS_BRI(2015)559488_EN.pdf consulta: 8 de octubre de 2015.

PEDROLETTI, Brice: *La marine, instrument de l'ambition planétaire de la Chine*. Le Monde, 28 de mayo de 2012. http://www.lemonde.fr/asie-pacifique/article/2015/05/28/la-marine-instrument-de-l-ambition-planetaire-de-la-chine_4642388_3216.html# consulta: 8 de agosto de 2015.

PÉREZ DE LAS HERAS, BEATRIZ Y CHURRUCA MUGURUZA, CRISTINA. *"Las capacidades civiles y militares de la UE: estado de la cuestión y propuestas de cara a la Presidencia Española 2010"*. Fundación Alternativas. Documento de Trabajo 41/2009. http://www.falternativas.org/opex/documentos-opex/documentos-de-trabajo/las-capacidades-civiles-y-militares-de-la-ue-estado-de-la-cuestion-y-propuestas-de-cara-a-la-presidencia-espanola-2010

PETERS, B. Guy; PIERRE, Jon; y KING, Desmond S.: http://web.iaincirebon.ac.id/ebook/moon/PoliticsMatters/j.1468-2508.2005.00360.x.pdf consulta: 25 de octubre de 2015.

Portal de administración electrónica. http://administracionelectronica.gob.es/ctt/altaSuscripcion.htm?idIniciativa=146#.VIlsRRO8PGc consulta: 17 de octubre de 2015.

Presidencia de Gobierno: *Aprobada la Estrategia de Seguridad Nacional de 2013*. Madrid, 31 de mayo de 2013. http://www.lamoncloa.gob.es/consejodeministros/Paginas/enlaces/310513Enlace%20%20seguridad.aspx consulta: 20 de octubre de 2015.

Public Law 107–296, 107th Congress, 25 de noviembre de 2002. http://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf consulta: 6 de agosto de 2015.

Puede consultarse este documento en su versión en idioma inglés, facilitado por el Ministerio de Asuntos Exteriores de la Federación Rusa, en el enlace: http://www.mid.ru/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/869c9d2b87ad8014c32575d9002b1c38?OpenDocument consulta: 20 de Agosto de 2015.

PUTIN, Vladimir: *Being strong: National security guarantees for Russia*. Rossiiskaya Gazeta, 20 de febrero de 2012. http://archive.premier.gov.ru/eng/events/news/18185/ consulta: 15 de Agosto de 2015.

QUILLE, GERRARD. "*The Lisbon Treaty and its implications for CFSP/ESDP*". Directorate-General for External Policies of the Union, European Parliament, febrero 2008. http://www.europarl.europa.eu/document/activities/cont/200805/20080513ATT28796/20080513ATT28796EN.pdf

REAGAN, *Ronald: Estrategia de Seguridad Nacional de los Estados Unidos 1987*. Uudley Knox Library Naval postgraduate School Monterey, California 93943.5002 Ejemplar firmado por el Presidente Reagan. http://history.defense.gov/Portals/70/Documents/nss/nss1987.pdf consulta 3 de agosto de 2015.

REAGAN, *Ronald: Estrategia de Seguridad Nacional de los Estados Unidos 1988*. http://nssarchive.us/NSSR/1988.pdf consulta: 4 de agosto de 2015.

REAGAN, Ronald: Intervención en la firma del Acta Goldwater-Nichols de reorganización del Departamento de Defensa. 1 de octubre de 1986. http://www.reagan.utexas.edu/archives/speeches/1986/100186e.htm consulta: 3 de agosto de 2015.

Real Decreto 421/2004, de 12 de marzo: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2004-5051 consulta 10 de septiembre de 2015.

Reglamento (CE) nº 460/2004. https://www.boe.es/doue/2004/077/L00001-00011.pdf consulta: 6 de octubre de 2015.

Revista SIC, Ciberseguridad, Seguridad de la Información y Privacidad: *El Ministerio de Defensa de Reino Unido confía el acceso seguro a sus redes al consorcio ATLAS*. nº 116, septiembre de 2015.

ROGIER, Creemers, ed. *China Copyright and Media; The law and policy of media in China*, *National Security Law of the People's Republic of China,* 2 de julio de 2015

https://chinacopyrightandmedia.wordpress.com/2015/07/01/national-security-law-of-the-peoples-republic-of-china/ consulta: 9 de agosto de 2015.

RÖHRIG, Wolfgang y SMEATON, Rob: *Cyber security and cyberdefence in the European Union: Opportunities, synergies and challenges*, Cyber Security Review, 2015. http://www.cybersecurity-review.com/articles/cyber-security-and-cyber-defence-in-the-european-union consulta: 11 de octubre de 2015.

ROLLINS, John y HENNING, Anna C.: *Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations*, Informe al Congreso, 10 de marzo de 2009. https://www.whitehouse.gov/files/documents/cyber/Congressional%20Research%20Service%20-%20CNCI%20-%20Legal%20Authorities%20and%20Policy%20Considerations%20(March%202009).pdf consulta: 12 de octubre de 2015.

ROY, Rajorshi: *Russia's New Military Doctrine: An Overview*. Institute for Defence Studies and Analyses, 16 de abril de 2015. http://www.idsa.in/idsacomments/RussiasNewMilitaryDoctrine_rroy_160415.html consulta: 15 de agosto de 2015.

SHAN Ding, *Conferencia del Encargado de Negocios de la Embajada de China en Uruguay*, Ding Shan, en la Universidad ORT de Uruguay, 4 de diciembre de 2013. http://uy.china-embassy.org/esp/whkjs/t1105987.htm consulta: 7 de agosto de 2015.

Sitio web de la Administración del Ciberespacio de China http://www.cac.gov.cn/english/ consulta: 13 de agosto de 2015.

Sitio web oficial del Departamento de Seguridad Nacional. http://www.dhs.gov/mission consulta: 6 de agosto de 2015.

Sitio web oficial del Departamento de Seguridad Nacional. http://www.dhs.gov/xlibrary/photos/orgchart-web.png consulta: 6 de agosto de 2015.

Sitio web oficial Kremlin: *Dmitry Medvedev signed an Executive Order on Russia's National Security Strategy through to 2020*. http://archive.kremlin.ru/eng/text/news/2009/05/216230.shtml consulta: 15 de agosto de 2015.

Sitio web oficial Kremlin: *Dmitry Medvedev signed Federal Law On Security*, 28 de octubre de 2010. http://en.kremlin.ru/events/president/news/9941 consulta: 15 de agosto de 2015.

Sitio web oficial Kremlin: *President of Russia, Security Council* http://archive.kremlin.ru/eng/articles/institut04.shtml consulta: 15 de agosto de 2015.

SNIDER, Don M.: *The National Security Strategy: Documenting Strategic Vision*. pp. 6-7. Strategic Studies Institute, U.S. Army War College, Carlisle Barracks, PA 17013-5050, 1995. http://nssarchive.us/wp-content/uploads/2012/05/Snider.pdf consulta 3: de agosto de 2015.

SOLANA, Javier. *"Ten years of European Security and Defence Policy"*. ESDP newsletter. European Security and Defence Policy 1999-2009. Octubre 2009. http://www.consilium.europa.eu/uedocs/cmsUpload/ESDP%20newsletter%20-%20Special%20issue%20ESDP@10.pdf

STRATFORD, Timothy P. y LUO, Yan: *China's New National Security Law*. The National Law Review, Covington & Burling LLP, 7 de julio de 2015. http://www.natlawreview.com/article/china-s-new-national-security-law consulta: 9 de agosto de 2015.

Texto de la Estrategia de Seguridad Nacional, publicado en el sitio web del Consejo de Seguridad de Rusia: http://www.scrf.gov.ru en http://www.scrf.gov.ru/documents/99.html (en ruso). Traducción al ingles en http://rustrans.wikidot.com/russia-s-national-security-strategy-to-2020 consulta: 15 de agosto de 2015.

The Military Doctrine of the Russian Federation, approved by Russian Federation Presidential Edict on 5 February 2010. The School of Russian and Asian Studies, 20 de febrero de 2010 http://www.sras.org/military_doctrine_russian_federation_2010

THEILER, Olaf: "*Nuevas amenazas: el ciberespacio.*" Revista de la OTAN, 11, 2011. http://www.nato.int/docu/review/2011/11-september/Cyber-Threads/ES/index.htm consulta: 26 de octubre de 2015.

THEOHARY, Catherine A. y HARRINGTON, Anne I: *Cyber Operations in DOD Policy and Plans: Issues for Congress,* Congressional Research Service, Washington D.C., 5 de enero de 2015. http://fas.org/sgp/crs/natsec/R43848.pdf consulta: 27 de septiembre de 2015.

THIBAULT, *Harold: Chine : bientôt des policiers chez les géants du Web*. Le Monde, 7 de agosto de 2015. http://www.lemonde.fr/economie/article/2015/08/07/chine-bientot-des-policiers-chez-les-geants-du-web_4715681_3234.html consulta: 13 de agosto de 2015.

TIEZZI, Shannon: *China's National Security Strategy*. The Diplomat, 24 de enero de 2015. http://thediplomat.com/2015/01/chinas-national-security-strategy/ consulta: 8 de agosto de 2015.

Translation and Analysis of the Doctrine of Information Security of the Russian Federation: Mass Media and the Politics of Identity; Carman, Douglas; Pacific Rim Law & Policy Journal 339 (2002). https://digital.law.washington.edu/dspace-

law/bitstream/handle/1773.1/757/16_11PacRimL%26PolyJ339%282002%29.pdf?sequence=1 consulta: 20 de Agosto de 2015.

Unión Europea: *Mapa educativo en ciberseguridad*. https://cybersecuritymonth.eu/references/universities consulta: 21 de octubre de 2015.

Unión Europea: *Mes Europeo de Ciberseguridad*. https://cybersecuritymonth.eu/ consulta: 21 de octubre de 2015.

Unión Europea: *Reglamento (UE) No 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014*. https://www.boe.es/doue/2014/257/L00073-00114.pdf consulta: 17 de octubre de 2015.

United States Government Accountability Office: *Informe a los Comités del Congreso, High-Risk Series: An Update, GAO-15-290*, Washington D.C.,11 de febrero de 2015. http://www.gao.gov/assets/670/668415.pdf consulta: 27 de septiembre de 2015.

United States Government Accountability Office: *Informe a los Congresistas,* Cybersecurity: National Strategy, roles, and responsibilities need to be better defined and more effectively, *GAO-13-187*, Washington D.C., febrero de 2013. http://www.gao.gov/assets/660/652170.pdf consulta: 12 de octubre de 2015.

VATANEN, ARI (Ponente): "Informe sobre la función de la OTAN en la arquitectura de seguridad de la UE", PE (2008/2197(INI)). Comisión de Asuntos Exteriores. Parlamento Europeo. 28 de enero de 2009. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A6-2009-0033+0+DOC+PDF+V0//ES

VILLALBA FERNÁNDEZ, Aníbal: "La evolución del pensamiento estratégico", en *Fundamentos de la estrategia desde el siglo XXI*, pp. 67-140. Monografías del CESEDEN número 67. http://www.portalcultura.mde.es/Galerias/publicaciones/fichero/00876.pdf

Vladimir Isachenkov: *New Russian military doctrine says NATO top threat.* Associated Press, The Washington Times, 26 de diciembre de 2014. http://www.washingtontimes.com/news/2014/dec/26/new-russian-military-doctrine-says-nato-top-threat/ consulta: 15 de agosto de 2015.

WESTIN, Stu; ROY Matthew; y KIM Chai K.: http://www.irma-international.org/viewtitle/50993/ consulta: 24 de octubre de 2015.

WILSON, Charles A.: *Goldwater-Nichols. The next evolution reorganizing the Joint Chiefs of Staff.*U.S. Army War College, Carlisle Barracks, PA 17013-5050. 2002. handle.dtic.mil/100.2/ADA404408 consulta: 3 de agosto de 2015.

WONG, Gillian: *China to Get Tough on Cybersecurity*. The Wall Street Journal, 9 de julio de 2015. http://www.wsj.com/articles/china-to-get-tough-on-cybersecurity-1436419416 consulta: 13 de agosto de 2015.

World Economic Forum: *Global Risks 2015*: http://reports.weforum.org/global-risks-2015/part-1-global-risks-2015/technological-risks-back-to-the-future/#frame/20ad6 consulta: 4 de septiembre de 2015.

World Economic Forum: *Global Risks 2015*: http://www3.weforum.org/docs/WEF_Global_Risks_2015_Report15.pdf consulta: 4 de septiembre de 2015.

World Economic Forum: *Riesgos Globales 2015*: http://reports.weforum.org/global-risks-2015/appendix-b-the-global-risks-perception-survey-2014-and-methodology/ consulta: 5 de septiembre de 2015.

World Economic Forum: *Technological Risks: Back to the Future*. http://reports.weforum.org/global-risks-2015/part-1-global-risks-2015/technological-risks-back-to-the-future/ consulta: 4 de septiembre de 2015.

XINHUA, *Canciller chino presenta 10 nuevas propuestas para cooperación China-Asean*. 6 de agosto de 2105. http://spanish.xinhuanet.com/2015-08/06/c_134485118.htm consulta 7 de agosto de 2015.

XINHUA, *China apoya el orden internacional de posguerra y contribuye a él*. 30 de julio de 2015. http://spanish.xinhuanet.com/2015-07/30/c_134460970.htm consulta: 7 de agosto de 2015.

XINHUA: *China adopta nueva ley de seguridad nacional*. 1 de julio de 2105. http://spanish.xinhuanet.com/china/2015-07/01/c_134372895.htm consulta: 9 de agosto de 2015.

XINHUA: *China eyes Internet power*, 8 de marzo de 2014. http://news.xinhuanet.com/english/special/2014-03/08/c_133171308.htm consulta: 13 de Agosto de 2015.

XINHUA: *Ley sobre seguridad cibernética de China busca proteger al público no minar su libertad*, 25 de julio de 2015. http://spanish.xinhuanet.com/2015-07/25/c_134445095.htm consulta: 11 de agosto de 2015.

XINHUA: *Liderazgo chino advierte de riesgos sin precedentes para seguridad nacional*. 23 de enero de 2015. http://spanish.xinhuanet.com/china/2015-01/23/c_133942602.htm consulta: 8 de agosto de 2015.

XINHUA: *Liderazgo chino advierte de riesgos sin precedentes para seguridad nacional*. *opus citada.*

XINHUA: *Voz de China: Seguridad cibernética es prioritaria para China*, 10 de julio de 2015. http://spanish.xinhuanet.com/china/2015-07/10/c_134400659.htm consulta: 11 de agosto de 2015.

YARGER, Harry R.: *Strategic theory for the 21st Century: The little book on big strategy*. Strategic Studies Institute, U.S. Army War College,Carlisle, PA 17013-5244, febrero 2006. http://www.comw.org/qdr/fulltext/0602yarger.pdf consulta: 4 de agosto de 2015.

Zhao Kejin (perfil). lhttp://carnegietsinghua.org/experts/?fa=622 consulta: 9 de agosto de 2015.

ANEXOS

Anexo 1: Legislación que el Consejo de la Unión Europea considera aplicable en el ámbito de la ciberseguridad, tras la aprobación de la Estrategia de ciberseguridad de la Unión Europea[633].

Parlamento Europeo, Consejo y Comisión

– Carta de los Derechos Fundamentales de la Unión Europea[634].

Parlamento Europeo y Consejo

– Reglamento (CE) no 460/2004 del Parlamento Europeo y del Consejo de 10 de marzo de 2004 por el que se crea la Agencia Europea de Seguridad de las Redes y de la Información[635].

– Directiva 2002/21/CE del Parlamento Europeo y del Consejo de 7 de marzo de 2002 relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas (Directiva marco), modificada por la Directiva 2009/140/CE[636].

Parlamento Europeo

– Resolución del Parlamento Europeo, de 11 de diciembre 2012, sobre una Estrategia de libertad digital en la política exterior de la UE.

– Informe del Parlamento Europeo sobre Informe sobre ciberseguridad y ciberdefensa de 2012.

Consejo

– Programa de Estocolmo – Una Europa abierta y segura que sirva y proteja al ciudadano[637].

– Una Europa segura en un mundo mejor – Estrategia Europea de Seguridad,12 de diciembre de 2003[638].

---

[633] Consejo de la Unión Europea: *Conclusiones del Consejo sobre la comunicación conjunta de la Comisión y de la Alta Representante de la Unión para Asuntos Exteriores y Política de Seguridad, titulada "Estrategia de ciberseguridad de la Unión Europea: un ciberespacio abierto, protegido y seguro"*, *opus citada*.

[634] DO C 364 de 18.12.2010, p. 1.

[635] DO L 077 de 13.03.2004.

[636] DO L 108 de 24.4.2002 y DO L 337/37 de 18.12.2009.

[637] Doc. 17024/09 CO EUR PREP 3 JAI 896 POLGEN 229.

[638] Doc. 15849/03 PESC 783.

– Estrategia de Seguridad Interior de la Unión Europea: "Hacia un modelo europeo de seguridad"[639].

– Directiva 2008/114/CE del Consejo de 8 de diciembre de 2008 sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección[640].

– Conclusiones del Consejo sobre la Comunicación de la Comisión titulada "La Estrategia de Seguridad Interior de la UE en acción"[641].

– Conclusiones del Consejo sobre la Comunicación de la Comisión sobre la protección de infraestructuras críticas de información: ("Logros y próximas etapas: hacia la ciberseguridad global")[642].

– Conclusiones del Consejo sobre la determinación de las prioridades de la UE para la lucha contra la delincuencia grave y organizada entre 2014 y 2017[643].

– Conclusiones del Consejo sobre la creación de un Centro Europeo de Ciberdelincuencia[644].

– Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a los ataques

contra los sistemas de información, por la que se sustituye la Decisión marco 2005/222/JAI 89 del Consejo. Aprobación del texto transaccional definitivo con vistas a un acuerdo con el Parlamento Europeo en primera lectura[645].

– Conclusiones del Consejo relativas a la Estrategia europea en favor de una Internet más adecuada para los niños[646].

---

[639] Doc. 5842/2/10 JAI 90.

[640] DO L 345 de 23.12.2008.

[641] Doc. 6699/11 JAI 124.

[642] Doc. 10299/11 TELECOM 71 DATAPROTECT 55 JAI 332 PROCIV 66 Esta comunicación es posterior a la Comunicación de la Comisión sobre Protección de Infraestructuras Críticas de Información "Proteger Europa de ciberataques e interrupciones a gran escala: aumentar la preparación, seguridad y resistencia" (doc. 8375/09).

[643] Doc. 9849/13 JAI 407 COSI 62 ENFOPOL 151 CRIMORG 77 ENFOCUSTOM 89 PESC 569 RELEX 434.

[644] Doc. 10603/12 ENFOPOL 154 TELECOM 116.

[645] Doc. 11399/12 DROIPEN 79 TELECOM 126 CODEC 1673.

[646] Doc. 15850/12 AUDIO 111 JEUN 95 EDUC 330 TELECOM 203 CONSOM 136 JAI 766 GENVAL 81.

– Conclusiones del Consejo sobre la lucha contra el abuso sexual y la explotación sexual de los niños y la pornografía infantil en internet - Mejora de la eficacia de la actuación policial en los Estados miembros y en terceros países[647].

– Conclusiones del Consejo sobre una Alianza Mundial contra el abuso sexual de menores en línea[648].

– Conclusiones del Consejo relativas a una estrategia de trabajo concertada y a medidas concretas contra la delincuencia informática[649] y conclusiones del Consejo sobre un plan de acción para aplicar la estrategia concertada contra la delincuencia informática[650].

– Orientación general parcial del Consejo sobre la propuesta de Reglamento de la Comisión por el que se establece Horizonte 2020, Programa Marco de Investigación e Innovación (2014-2020)[651].

– Acción Común del Consejo relativa a la creación de la Agencia Europea de Defensa[652].

– Propuesta conjunta de Decisión del Consejo relativa a las modalidades de aplicación por la Unión de la cláusula de solidaridad[653].

– Conclusiones del Consejo sobre la alfabetización mediática en el entorno digital[654].

– Derechos humanos y democracia: Marco estratégico y Plan de acción de la UE[655].

– Informe sobre la aplicación de la Estrategia Europea de Seguridad[656].

Comisión

[647] Doc. 15783/2/11 REV 2 GENVAL 108 ENFOPOL 368 DROPIEN 119 AUDIO 53.

[648] Doc. 10607/12 +COR 1 GENVAL 39 ENFOPOL 155 DROIPEN 69 AUDIO 62 JEUN 46.

[649] Doc. 15569/08 ENFOPOL 224 CRIMORG 190.

[650] Doc. 5957/2/10 REV 2 CRIMORG 22 ENFOPOL 32.

[651] Doc. 10663/12 RECH 207 COMPET 364 IND 102 MI 398 EDUC 152 TELECOM 118 ENER 233 ENV 446 REGIO 75 AGRI 362 TRANS 187 SAN 134 CODEC 1511.

[652] Doc 10556/04 COSDP 374 POLARM 17 IND 80 RECH 130 ECO 121.

[653] Doc. 18124/12 CAB 39 POLGEN 220 CCA 13 JAI 946 COSI 134 PROCIV 225 ENFOPOL 430 COPS 485 COSDP 1123 PESC 1584 COTER 125 COCON 45 COHAFA 165.

[654] Doc. 15441/09 AUDIO 47 EDUC 173 TELECOM 233 RECH 380.

[655] Doc. 11855/12 COHOM 163 PESC 822 COSDP 546 FREMP 100 INF 110 JAI 476 RELEX 603.

[656] Doc. 17104/08 CAB 66 PESC 1687 POLGEN 139.

– La Agenda digital para Europa[657] que es una de las siete iniciativas emblemáticas de Europa 2020, una estrategia para un crecimiento inteligente, sostenible e integrador[658] y la Agenda Digital para Europa – Motor del crecimiento europeo[659] que reorienta la Agenda Digital.

– Comunicación sobre la protección de la privacidad en un mundo interconectado – Un marco europeo de protección de datos para el siglo XXI[660].

– Comunicación "a represión del delito en la era digital: creación de un centro europeo de ciberdelincuencia"[661].

– Comunicación de la Comisión titulada "liberar el potencial de la computación en nube en Europa"[662].

– Comunicación de la Comisión sobre la protección de infraestructuras críticas de información "logros y próximas etapas: hacia la ciberseguridad global"[663].

– Comunicación de la Comisión sobre Protección de Infraestructuras Críticas de

Información "Proteger Europa de ciberataques e interrupciones a gran escala: aumentar la preparación, seguridad y resistencia"[664].

Naciones Unidas

– Resolución de la Asamblea General de las Naciones Unidas (A/RES 57/239) relativa a la creación de una cultura mundial de seguridad cibernética.

– Resolución del Consejo de Derechos Humanos de las Naciones Unidas (A/HR/20/L.13), de 29 de junio de 2012, sobre la Promoción, protección y disfrute de los derechos humanos en Internet.

---

[657] Doc. 9981/1/10 TELECOM 52 AUDIO 17 COMPET 165 RECH 193 MI 168 DATA PROTECT 141.

[658] Doc. 7110/10 CO EUR-PREP 7 POLGEN 28 AG 3 ECOFIN 136 UEM 55 SOC 174 COMPET 82 RECH 83 ENER 63 TRANS 55 MI 73 IND 33 EDUC 40 ENV 135 AGRI 74.

[659] Doc. 17963/12 TELECOM 262 MI 839 COMPET 786 CONSOM 161 DATAPROTECT149 RECH 472 AUDIO 137 POLGEN 216.

[660] Doc. 5852/12 DATAPROTECT 8 JAI 43 MI 57 DRS 10 DAPIX 11 FREMP 6.

[661] Doc. 8543/12 ENFOPOL 94 TELECOM 72 12109/13 jo/PGV/dru 5.

[662] Doc. 14411/12 TELECOM 170 MI 586 DATAPROTECT 112 COMPET 585.

[663] Doc. 8548/11 TELECOM 40 DATAPROTECT 27 JAI 213 PROCIV 38.

[664] Doc. 8375/09 TELECOM 69 DATAPROTECT 24 JAI 192 PROCIV 46.

– Resolución de la Asamblea General de las Naciones Unidas (A/RES 67/27) relativa a los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional.

– Creación de un grupo intergubernamental de expertos de composición abierta sobre el delito cibernético junto con la Oficina de las Naciones Unidas contra la Droga y el Delito, de conformidad con la Resolución de la Asamblea General 65/230.

Consejo de Europa

– Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal de 28 de enero de 1981.

– Convenio del Consejo de Europa sobre la ciberdelincuencia de 23 de noviembre de 2001.

Organización para la Seguridad y la Cooperación en Europa (OSCE)

– Decisión del Consejo Permanente n.° 1039, de 26 de abril de 2012, relativa al desarrollo de medidas de confianza para reducir los riesgos de conflictos provocados por el uso de las tecnologías de la comunicación y la información.

– Decisión Ministerial n.° 4/12, de 7 de diciembre de 2012, esfuerzos de la OSCE para responder a las amenazas transnacionales.

– Grupo informal y abierto de la OSCE cuya misión es elaborar un proyecto de conjunto de medidas de creación de confianza para reforzar la cooperación interestatal, la transparencia, la predictibilidad y la estabilidad, y reducir el riesgo de malas interpretaciones, escaladas de tensión y conflictos que pueden producir el uso de las TIC (Decisión del Consejo permanente de la OSCE n.° 1039 de 26 de abril de 2012).

Conferencias, iniciativas y actos

– Conferencia Internacional sobre el Ciberespacio, celebrada en Londres el 1 y 2 de noviembre de 2011 y seguida por la Conferencia Internacional sobre el Ciberespacio celebrada el 4 y 5 de octubre de 2012 en Budapest.

– Ejercicio de simulación conjunto UE-EEUU para hacer frente a un incidente cibernético "Cyber Atlantic 2011" y ejercicio paneuropeo con la participación de todos los Estados miembros ("ciber Europa 2010" y "Ciber Europa 2012")

– Un Grupo ad hoc sobre seguridad nuclear que debatió sobre la Seguridad informática/Ciberseguridad y elaboró su informe final sobre esta cuestión[665].

[665] Doc. 10616/12 AHGS 20 ATO 84.

Otros:

– Evaluación de la amenaza de la delincuencia grave y organizada (SOCTA)[666]

– Política de seguridad en materia de defensa de la red para proteger la información[667] y Directrices sobre Defensa de la Red[668].

[666] Doc. 7368/13 JAI 200 COSI 26 ENFOPOL 75 CRIMORG 41 CORDROGUE 27 ENFOCUSTOM 43 PESC 286 JAIEX 20 RELEX 211.

[667] Doc. 8408/12 CSCI 11 CSC 20.

[668] Doc. 10578/12 CSCI 20 CSC 34.

Anexo 2: Grado de cumplimiento de España de niveles de ciberseguridad

COUNTRY: **SPAIN**

Spain adopted the National Cyber Security Strategy in 2013. It is a comprehensive document, which sets objectives and targeted lines of actions. It is compatible with, and references, both the National Security Plan and existing security laws; and these plans and laws work together as a package.

Spain has established two computer emergency response teams (CERTs), INTECO-CERT and CCN-CERT, and the National Centre for Critical Infrastructure Protection (CNPIC). The latter appears to be the premier agency for information security and cybersecurity, while the role of the CERTs is limited to dealing with cybersecurity incidents. CNPIC is responsible for ensuring coordination and cooperation between the public and private sector. It also runs sectoral working groups and is working toward the development of sector-specific cybersecurity plans.

Additionally, cooperation with the private sector is formalised through the National Advisory Council on Cybersecurity, established in 2009, whose members are private sector representatives. The council is tasked with providing policy advice to the government, although its current status is somewhat unclear. Private sector associations are also active, with two prominent bodies dedicated specifically to cyber- and information security, as opposed to general IT matters.

	QUESTION	RESPONSE	EXPLANATORY TEXT
	LEGAL FOUNDATIONS		
1.	Is there a national cybersecurity strategy in place?	✔	The National Cyber Security Strategy <ieee.es/en/Galerias/fichero/docs_analisis/2013/DIEEEA65-2013_EstrategiaCiberseguridadNacional_MJCB.pdf> was adopted by the Spanish government in 2013. It is a comprehensive document with set objectives and targeted lines of actions. It is compatible with, and references, the National Security Plan and existing security law, and these laws and plans work together as a package.
2.	What year was the national cybersecurity strategy adopted?	2013	
3.	Is there a critical infrastructure protection (CIP) strategy or plan in place?	✔	Critical infrastructure protection is managed through a package of initiatives, including: • The National Plan for Critical Infrastructure Protection 2007; • The establishment of the National Centre for the Protection of Critical Infrastructure (CNPIC) <cnpic.es>; • The Regulation on Critical Infrastructure Protection 2011 <www.cnpic.es/Biblioteca/Legislacion/Generico/REAL_DECRETO_704-2011_BOE-A-2011-8849.pdf>; • Law 8/2011 on the Measures for the Protection of Critical Infrastructure 2011 <www.boe.es/boe/dias/2011/04/29/pdfs/BOE-A-2011-7630.pdf>; and, • The Royal Decree 704/2011 <www.cnpic.es/Biblioteca/Legislacion/Generico/REAL_DECRETO_704-2011_BOE-A-2011-8849.pdf>, which gives assent to, and expands on, the framework of Law 8/2011.
4.	Is there legislation/policy that requires the establishment of a written information security plan?	✖	There is no legislation or policy in place in Spain that requires the establishment of a written information security plan.
5.	Is there legislation/policy that requires an inventory of "systems" and the classification of data?	✔	The classification of information and the handling of such information is covered by: • Law 9/1968 <www.boe.es/boe/dias/1968/04/06/pdfs/A05197-05199.pdf>; • Law 11/2007 <www.boe.es/boe/dias/2007/06/23/pdfs/A27150-27166.pdf>; and, • Royal Decree 3/2010. <www.boe.es/boe/dias/2010/01/29/pdfs/BOE-A-2010-1330.pdf> Spain classifies information deemed a state secret according to a four-tier classification system. The classification levels are assigned according to the level of risk involved in disclosing the classified information.

	QUESTION	RESPONSE	EXPLANATORY TEXT
6.	Is there legislation/policy that requires security practices/ requirements to be mapped to risk levels?	✔	The classification of information and the handling of such information is covered by: • Law 9/1968 <www.boe.es/boe/dias/1968/04/06/pdfs/A05197-05199.pdf>; • Law 11/2007 <www.boe.es/boe/dias/2007/06/23/pdfs/A27150-27166.pdf>; and, • Royal Decree 3/2010. <www.boe.es/boe/dias/2010/01/29/pdfs/ BOE-A-2010-1330.pdf> Spain classifies information deemed a state secret according to a four-tier classification system. Some security practices are mapped to the level of risk involved in disclosing the classified information.
7.	Is there legislation/policy that requires (at least) an annual cybersecurity audit?	◑	Royal Decree 3/2010 <www.boe.es/boe/dias/2010/01/29/pdfs/BOE-A-2010-1330.pdf>, which regulates e-government within the National Security Framework, requires information security system to be audited at least once every two years, and contains the provision for additional auditing in times of emergency. The act details the necessary standards of such an audit.
8.	Is there legislation/policy that requires a public report on cybersecurity capacity for the government?	✖	There is no legislation or policy in place in Spain that requires a public report on cybersecurity capacity for the government. Royal Decree 3/2010 <www.boe.es/boe/dias/2010/01/29/pdfs/BOE-A-2010-1330.pdf>, which regulates e-government within the National Security Framework, requires an audit of information systems once every two years, however, this isn't a targeted cybersecurity capacity report and it is not required to be made public.
9.	Is there legislation/policy that requires each agency to have a chief information officer (CIO) or chief security officer (CSO)?	✖	There is no legislation in place in Spain that requires each agency to have a chief information officer or chief security officer.
10.	Is there legislation/policy that requires mandatory reporting of cybersecurity incidents?	✖	There is no legislation or policy in place in Spain that requires mandatory reporting of cybersecurity incidents. The National Cyber Security Strategy <ieee.es/en/Galerias/fichero/docs_ analisis/2013/DIEEEA65-2013_EstrategiaCiberseguridadNacional_MJCB.pdf>, adopted in 2013, states that enforced incident reporting is a line of action that the Spanish government will pursue.
11.	Does legislation/policy include an appropriate definition for "critical infrastructure protection" (CIP)?	✔	The National Centre for the Protection of Critical Infrastructure (CNPIC) <cnpic.es> provides an appropriate definition for critical infrastructure.
12.	Are requirements for public and private procurement of cybersecurity solutions based on international accreditation or certification schemes, without additional local requirements?	✔	The National security scheme for eGovernment (Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica) includes security certification requirement that can be met by reference to international certification or accreditation. <www.boe.es/buscar/doc.php?id=BOE-A-2010-1330> Their stated objective is to: "promote cyber security certification activities in accordance with the internationally recognised norms and standards, incorporating these criteria into processes for the development and acquisition of products or systems".
	OPERATIONAL ENTITIES		
1.	Is there a national computer emergency response team (CERT) or computer security incident response team (CSIRT)?	✔	INTECO-CERT <cert.inteco.es> was established in 2008. It is responsible for coordinating incident response measures across all Spanish networks. It also supports entities engaged with critical infrastructure through an agreement with the National Centre for Critical Infrastructure Protection (CNPIC) <cnpic.es>. CCN-CERT <www.ccn-cert.cni.es> has jurisdiction over government institutions.
2.	What year was the computer emergency response team (CERT) established?	2008	
3.	Is there a national competent authority for network and information security (NIS)?	✔	The National Centre for Critical Infrastructure Protection (CNPIC) <cnpic.es> acts as the national competent authority for network and information security in Spain.
4.	Is there an incident reporting platform for collecting cybersecurity incident data?	✔	INTECO-CERT <cert.inteco.es>, working in conjunction with the National Centre for Critical Infrastructure Protection (CNPIC) <cnpic.es>, is tasked with incident reporting and collecting information about cybersecurity incidents. There is an email-based reporting structure to log cybersecurity incidents.
5.	Are national cybersecurity exercises conducted?	◑	Spain has participated in multinational cybersecurity exercises organised by both the European Union and NATO.

	QUESTION	RESPONSE	EXPLANATORY TEXT
6.	Is there a national incident management structure (NIMS) for responding to cybersecurity incidents?	✔	The National Centre for Critical Infrastructure Protection (CNPIC) <cnpic.es> acts as the body responsible for coordinating responses to emergency incidents, including cybersecurity incidents. They are responsible for engaging with the relevant stakeholders and government departments in the event of an incident.
	PUBLIC-PRIVATE PARTNERSHIPS		
1.	Is there a defined public-private partnership for cybersecurity?	✔	The National Centre for Critical Infrastructure Protection (CNPIC) <cnpic.es> monitors the national critical infrastructure protection system, which includes owners, operators and users of Spanish critical infrastructure. As a result, CNPIC facilitates cooperation between the public and private sectors through initiatives like sectoral working groups. Furthermore, the National Advisory Council on Cybersecurity (CNCCS), whose membership comprised representatives from the information technology and critical infrastructure sectors, was convened by the Spanish government in 2009 to advise the government on future cybersecurity policy directions.
2.	Is industry organised (i.e. business or industry cybersecurity councils)?	✔	The Centre for Industrial Cybersecurity (CCI) <www.cci-es.org> is a non-profit organisation with objectives to provide and improve awareness of cybersecurity issues and to facilitate communication channels between industry and lawmakers — to improve cybersecurity outcomes. The Spanish Association for the Promotion of Information Security (ISMS Forum Spain) <www.ismsforum.es> is a non-profit organisation that organises multiple information security initiatives. The Cyber Security Spanish Institute, which publishes reports on cybersecurity in Spain, is one such initiative. In addition to the CCI and the ISMS Forum, AMETIC <www.ametic.es>, the representative body for Spanish electronic technology, information technology and telecommunications companies, engages with cybersecurity issues in the course of its duties.
3.	Are new public-private partnerships in planning or underway (if so, which focus area)?	–	Spain already has a public-private partnership dedicated to cybersecurity.
	SECTOR-SPECIFIC CYBERSECURITY PLANS		
1.	Is there a joint public-private sector plan that addresses cybersecurity?	✔	The National Centre for Critical Infrastructure Protection (CNPIC) <cnpic.es> facilitates cooperation between the public and private sectors through initiatives that include sectoral working groups.
2.	Have sector-specific security priorities been defined?	◑	The National Centre for Critical Infrastructure Protection (CNPIC) is working closely with 12 industry sectors to define sector-specific security priorities. These are expected to be made available following final consultations. Spain has also established the Centre for Industrial Cybersecurity (CCI) which promotes security best practices in the industrial sector. <https://www.cci-es.org>
3.	Have any sector-specific cybersecurity risk assessments been conducted?	✖	Sector-specific risk assessments have not been released.
	EDUCATION		
1.	Is there an education strategy to enhance cybersecurity knowledge and increase cybersecurity awareness of the public from a young age?	✔	The National Cyber Security Strategy 2013 <ieee.es/en/Galerias/fichero/docs_analisis/2013/DIEEEA65-2013_EstrategiaCiberseguridadNacional_MJCB.pdf> includes a commitment to raising general public awareness. Its focus is on "raising the awareness of citizens, professionals and companies about the importance of cyber security and the responsible use of new technologies and the services of the Information Society". The strategy includes a commitment to "develop education modules for sensitisation in cybersecurity, aimed at all levels of teaching".

Anexo 3: Grado de cumplimiento del Reino Unido de niveles de ciberseguridad

COUNTRY: **UNITED KINGDOM**

The United Kingdom has a comprehensive cybersecurity strategy, which was released in 2011. It is complemented by a strong cybersecurity legal framework and two computer emergency response teams (CERTs). CERT-UK mainly supports operators of critical infrastructure while GovCertUK supports government agencies. Other relevant bodies include the National Security Council and the Office of Cyber Security and Information Assurance.

The United Kingdom also has a well-developed system of public-private partnerships in which the private sector actively participates. This collaborative approach also is strongly supported by its cybersecurity strategy. The Centre for the Protection of National Infrastructure (CPNI), for example, organises sector-specific information exchanges, covering 14 sectors.

	QUESTION	RESPONSE	EXPLANATORY TEXT
	LEGAL FOUNDATIONS		
1.	Is there a national cybersecurity strategy in place?	✔	The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World <www.gov.uk/government/publications/cyber-security-strategy> was adopted in 2011. The strategy includes a strong statement of principles and an assessment of cybersecurity threats faced by the UK. The implementation plan contained within the strategy is based around key targeted objectives.
2.	What year was the national cybersecurity strategy adopted?	2011	
3.	Is there a critical infrastructure protection (CIP) strategy or plan in place?	✔	The Centre for the Protection of National Infrastructure (CPNI) <cpni.gov.uk> is tasked with the protection of the United Kingdom's critical infrastructure. The central document of the CPNI is the Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards <www.gov.uk/government/uploads/system/uploads/attachment_data/file/62504/strategic-framework.pdf>, which was adopted in 2010.
4.	Is there legislation/policy that requires the establishment of a written information security plan?	◑	There is no legislation or policy in place in the United Kingdom that requires the establishment of a written information security plan. The Communications Electronic Security Group (CESG) <cesg.gov.uk>, the information security arm of the UK's Government Communications Headquarters (GCHQ) intelligence agency, has published guidelines for public organisations related to information security.
5.	Is there legislation/policy that requires an inventory of "systems" and the classification of data?	✔	The Government Security Classifications Policy <www.gov.uk/government/publications/government-security-classifications>, which came into force in 2014, details a three-tiered system of classification for information that is required by domestic laws, including the Official Secrets Act 1989 <www.legislation.gov.uk/ukpga/1989/6>, to be classified. The three classification levels are assigned according to the sensitivity of the information and the risk level involved in disclosing the information.
6.	Is there legislation/policy that requires security practices/requirements to be mapped to risk levels?	✔	The Government Security Classifications Policy <https://www.gov.uk/government/publications/government-security-classifications> details a three-tiered classification system. The classification levels are assigned with consideration of the level risk involved in disclosing the information. The policy then maps specific security requirements according to classification level.
7.	Is there legislation/policy that requires (at least) an annual cybersecurity audit?	✖	There is no legislation or policy in place in the United Kingdom that requires an annual cybersecurity audit. The UK Cyber Security Strategy <www.gov.uk/government/publications/cyber-security-strategy> acknowledges the ease and benefits of continuous monitoring of data with relation to digitisation, however, a specific auditing process and the frequency with which it should be carried out is not detailed.
8.	Is there legislation/policy that requires a public report on cybersecurity capacity for the government?	◑	There is no legislation or policy in place in the United Kingdom that requires a public report on cybersecurity capacity for the government. The UK Cyber Security Strategy <www.gov.uk/government/publications/cyber-security-strategy> includes an assessment of the UK's cybersecurity capacity as of 2011.

	QUESTION	RESPONSE	EXPLANATORY TEXT
9.	Is there legislation/policy that requires each agency to have a chief information officer (CIO) or chief security officer (CSO)?	✖	There is no legislation or policy in place in the United Kingdom that requires each agency to have a chief information officer or chief security officer.
10.	Is there legislation/policy that requires mandatory reporting of cybersecurity incidents?	✖	There is no legislation or policy in place in the United Kingdom that requires mandatory reporting of cybersecurity incidents, however, voluntary guidelines issued by both CERT-UK <www.cert.gov.uk> and GovCertUK <www.govcertuk.gov.uk> recommend the reporting of all incidents.
11.	Does legislation/policy include an appropriate definition for "critical infrastructure protection" (CIP)?	✔	The Centre for the Protection of National Infrastructure (CPNI) <cpni.gov.uk> provides an appropriate definition for "critical infrastructure protection" in its policy documents — including the Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards. <www.gov.uk/government/uploads/system/uploads/attachment_data/file/62504/strategic-framework.pdf>
12.	Are requirements for public and private procurement of cybersecurity solutions based on international accreditation or certification schemes, without additional local requirements?	◑	The UK generally recognises international certification schemes, although some additional voluntary guidance on security standards is provided by the UK's National Technical Authority on Information Assurance. In June 2014 the government issued a new cybersecurity standard known as the Cyber Essentials Scheme. <www.gov.uk/government/publications/cyber-essentials-scheme-overview> From 1 October 2014, the UK government will require all suppliers bidding for certain sensitive and personal information handling contracts to be certified against the Cyber Essentials Scheme. The scheme includes some overlaps with, but also some differences to, international standards.
	OPERATIONAL ENTITIES		
1.	Is there a national computer emergency response team (CERT) or computer security incident response team (CSIRT)?	✔	CERT-UK <www.cert.gov.uk> was established in 2014. It is responsible for promoting cyber security situational awareness and for national cybersecurity incident management including providing support for entities engaged with national critical infrastructure. CERT-UK works closely with GovCertUK <www.govcertuk.gov.uk>, which is responsible for coordinating security and incident response measures for UK government institutions.
2.	What year was the computer emergency response team (CERT) established?	2014	
3.	Is there a national competent authority for network and information security (NIS)?	✔	The National Security Council <www.gov.uk/government/organisations/national-security/groups/national-security-council> and the Office of Cyber Security and Information Assurance <www.gov.uk/government/groups/office-of-cyber-security-and-information-assurance> act in conjunction to cover network and information security for the United Kingdom. The CESG <cesg.gov.uk> is the information security arm of the UK's GCHQ intelligence agency. It advises public organisations in helping them to maintain network integrity and strengthen cybersecurity.
4.	Is there an incident reporting platform for collecting cybersecurity incident data?	✔	CERT-UK <www.cert.gov.uk> is tasked with incident reporting and collecting information about cybersecurity incidents. It provides an online reporting structure to log cybersecurity incidents.
5.	Are national cybersecurity exercises conducted?	✔	The United Kingdom conducted the cybersecurity exercise White Noise in 2009. The UK has also participated in multi-national cyber exercises organised by NATO.
6.	Is there a national incident management structure (NIMS) for responding to cybersecurity incidents?	✔	CERT-UK <www.cert.gov.uk> acts according to the Cyber Security National Incident Management policy, which includes reporting and notification requirements.
	PUBLIC-PRIVATE PARTNERSHIPS		
1.	Is there a defined public-private partnership for cybersecurity?	✔	Cyber-Security Information Sharing Partnership (CISP) <cisp.org.uk> is a joint initiative of the United Kingdom government and industry to share information and collaborate on the issue of cyber threats. It follows the objectives and goals set out in the UK Cyber Security Strategy. <www.gov.uk/government/publications/cyber-security-strategy>

	QUESTION	RESPONSE	EXPLANATORY TEXT
2.	Is industry organised (i.e. business or industry cybersecurity councils)?	✔	There are multiple industry-organised and industry-engaged associations in the United Kingdom that provide a platform for cooperation and collaboration on cybersecurity, including: • The Information Technology Telecommunications and Electronics Association (techUK) <www.techuk.org>, a representative organisation of information technology and communication companies in the UK, hosts both a dedicated cybersecurity group as well as a general security and resilience group. • The Information Assurance Advisory Council (IAAC) <www.iaac.org.uk> is a not-for-profit research organisation comprised of representatives from the public, private, and academic sectors in order to promote a cross-sector approach to information assurance. • The UK Council for Electronic Business (UKCeB) <www.ukceb.oeg> is a representative organisation whose members come from the information technology and defence sectors. UKCeB sponsors a security and information assurance working group.
3.	Are new public-private partnerships in planning or underway (if so, which focus area)?	–	The United Kingdom already has a public-private partnership dedicated to cybersecurity in place.
	SECTOR-SPECIFIC CYBERSECURITY PLANS		
1.	Is there a joint public-private sector plan that addresses cybersecurity?	✔	The Centre for the Protection of National Infrastructure (CPNI) <www.cpni.gov.uk> organises public-private information exchanges around the fourteen different sectors involved with national infrastructure. The Network Security Information Exchange (NSIE) is the information exchange that engages directly with the cybersecurity sector.
2.	Have sector-specific security priorities been defined?	◑	The UK Cyber Security Strategy 2011 <www.gov.uk/government/publications/cyber-security-strategy> provides a sector based approach, particularly in addressing training and knowledge-sharing in sectors where small and medium-sized businesses operate. Security priorities have not been defined by sector.
3.	Have any sector-specific cybersecurity risk assessments been conducted?	✖	While the UK Cyber Security Strategy 2011 <www.gov.uk/government/publications/cyber-security-strategy> advocates both a sector-oriented and risk-based approach, sector-specific cybersecurity risk assessments have not yet been conducted.
	EDUCATION		
1.	Is there an education strategy to enhance cybersecurity knowledge and increase cybersecurity awareness of the public from a young age?	✔	The UK Cyber Security Strategy 2011 <www.gov.uk/government/publications/cyber-security-strategy> includes a plan to "look at the best ways to improve cybersecurity education at all levels so that people are better equipped to use cyberspace safely". There is also a commitment to "building a culture that understands the risks and enables people to use cyberspace and improving cybersecurity skills at all levels". In practice the UK has developed some of the most advanced cybersecurity education initiatives in the region, including the Get Safe Online program. <www.getsafeonline.org>

Anexo 4: Grado de cumplimiento de Alemania de niveles de ciberseguridad

COUNTRY: **GERMANY**

Germany has a comprehensive cybersecurity strategy, adopted in 2011 and complemented by a strong cybersecurity legal framework. The existence of the Federal Office for Information Security (BSI), in charge of managing computer and communication security for the German government, is a clear demonstration that cybersecurity is elevated to a high government level.

Germany also has a network of computer emergency response teams (CERTs), with the national CERT, CERT-BUND, working closely with both state-level and non-governmental CERTs.

Furthermore, the country has well-developed public-private partnerships, such as the Alliance for Cyber-Security and the UP KRITIS partnership, and its national policies and legal framework reflect this focus on cooperation.

	QUESTION	RESPONSE	EXPLANATORY TEXT
	LEGAL FOUNDATIONS		
1.	Is there a national cybersecurity strategy in place?	✔	The Cyber Security Strategy for Germany <www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CyberSecurity/Cyber_Security_Strategy_for_Germany.html> was adopted in 2011. It is a comprehensive strategy that includes guiding principles, clear goals, and an implementation plan.
2.	What year was the national cybersecurity strategy adopted?	2011	
3.	Is there a critical infrastructure protection (CIP) strategy or plan in place?	✔	The National Strategy for Critical Infrastructure Protection (CIP Strategy) <www.bmi.bund.de/cae/servlet/contentblob/598732/publicationFile/34423/kritis_englisch.pdf> was adopted by the German Government in 2009. Critical infrastructure protection, as it relates to cybersecurity, is also addressed in the Cyber Security Strategy for Germany. <www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CyberSecurity/Cyber_Security_Strategy_for_Germany.html>
4.	Is there legislation/policy that requires the establishment of a written information security plan?	✖	There is no legislation or policy in place in Germany that requires the establishment of a written information security plan. Recommendations issued by the Federal Office for Information Security (BSI) <www.bsi.bund.de>, such as those of cloud computing providers, partly cover information security.
5.	Is there legislation/policy that requires an inventory of "systems" and the classification of data?	✔	Section 93-95 of the German Criminal Code <www.gesetze-im-internet.de/englisch_stgb> is related to the definition of national security secrets. Additionally, the Safety Assessment Act 1994 <www.gesetze-im-internet.de/bundesrecht/s_g/gesamt.pdf> requires data deemed in need of secrecy to protect the public interest be classified. Paragraph 4 of the act outlines a four-tiered system of classification levels. The levels are assigned according to the level of risk involved in disclosing the classified information.
6.	Is there legislation/policy that requires security practices/requirements to be mapped to risk levels?	✔	The Regulation of the Ministry of the Interior for the Material and Organisational Protection of Classified Information (Allgemeine Verwaltungsvorschrift des Bundesministeriums des Innern zum materiellen und organisatorischen Schutz von Verschlusssachen) 2006, pursuant to the Safety Assessment Act 1994 <www.gesetze-im-internet.de/bundesrecht/s_g/gesamt.pdf>, maps various security practices to assigned classification levels. These levels are set out in Paragraph 4 of the act and are assigned according to the level of risk involved in disclosing the classified information.
7.	Is there legislation/policy that requires (at least) an annual cybersecurity audit?	Draft	The draft Act to Increase the Security of Information Technology <www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/Entwuerfe/Entwurf_IT-Sicherheitsgesetz.pdf?__blob=publicationFile> would require the Federal Office for Information Security (BSI) <www.bsi.bund.de> to conduct security audits of entities engaged with critical infrastructure once every two years.

	QUESTION	RESPONSE	EXPLANATORY TEXT
8.	Is there legislation/policy that requires a public report on cybersecurity capacity for the government?	Draft	The draft Act to Increase the Security of Information Technology <www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/Entwuerfe/Entwurf_IT-Sicherheitsgesetz.pdf?__blob=publicationFile> would require the Federal Office for Information Security (BSI) <www.bsi.bund.de> to, in cooperation with federal authorities, analyse the potential for cyber threats to entities engaged with critical infrastructure and to continually update the government with regard to the security situation of entities engaged with critical infrastructure.
9.	Is there legislation/policy that requires each agency to have a chief information officer (CIO) or chief security officer (CSO)?	✖	There is no legislation or policy in Germany that requires each agency to have a chief information officer or chief security officer.
10.	Is there legislation/policy that requires mandatory reporting of cybersecurity incidents?	✔	The Act on the Federal Office of Information Security 2009 <www.bmi.bund.de/SharedDocs/Downloads/EN/Gesetzestexte/bsi_act.html> requires federal authorities to report cybersecurity incidents to the Federal Office of Information Security upon detection. There is a draft amendment to the act <www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/Entwuerfe/Entwurf_it-sicherheitsgesetz.html>, which proposes the strengthening of mandatory reporting requirements covering telecommunication service providers and entities engaged with critical infrastructure.
11.	Does legislation/policy include an appropriate definition for "critical infrastructure protection" (CIP)?	✔	The National Strategy for Critical Infrastructure Protection (CIP Strategy) <www.bmi.bund.de/cae/servlet/contentblob/598732/publicationFile/34423/kritis_englisch.pdf> includes appropriate definitions for "critical infrastructure" and "critical infrastructure protection".
12.	Are requirements for public and private procurement of cybersecurity solutions based on international accreditation or certification schemes, without additional local requirements?	✔	Germany recognises international security certifications, and although some local security guidelines have been developed, they do not require additional local certification or accreditation. For example, refer to the Cloud-fahrplan für die öffentliche verwaltung — a guideline published by the Fraunhofer Institute (FOKUS) as a road map to help federal institutions migrate IT services to Cloud. <www.oeffentliche-it.de/documents/18/21941/Cloud-Fahrplan+oeffentliche+Verwaltung>
	OPERATIONAL ENTITIES		
1.	Is there a national computer emergency response team (CERT) or computer security incident response team (CSIRT)?	✔	CERT-Bund <www.cert-bund.de> was established in 2012 and is responsible for warning systems and coordinating incident response measures for German federal government authorities. It works closely with German CERT alliances and state-level CERTs to provide wider coverage.
2.	What year was the computer emergency response team (CERT) established?	2012	
3.	Is there a national competent authority for network and information security (NIS)?	✔	The Federal Office for Information Security (BSI) <www.bsi.bund.de> acts as Germany's national competent authority for network and information security. The National Cyberdefence Centre, which reports to BSI, is the agency primarily responsible for cybersecurity.
4.	Is there an incident reporting platform for collecting cybersecurity incident data?	✔	Operated by the Federal Office for Information Security (BSI) <www.bsi.bund.de>, CERT-Bund <www.cert-bund.de> is tasked with collecting information about cybersecurity incidents. They engage proactively by monitoring their constituency for cybersecurity incidents, as well as providing an online reporting structure to log cybersecurity incidents. The National Cyber Response Centre, which reports to BSI, provides a platform for cross-agency cooperation on cybersecurity. The Digital Agenda 2014-17 <www.bmi.bund.de/SharedDocs/Downloads/EN/Broschueren/2014/digital-agenda.html> states that the incident response capacities of the centre will be strengthened.
5.	Are national cybersecurity exercises conducted?	✔	Germany conducted three national cybersecurity exercises between 2010 and 2012. Germany also participated in multi-national exercises organised by the European Union and NATO.
6.	Is there a national incident management structure (NIMS) for responding to cybersecurity incidents?	✖	There is no national incident management structure in place in Germany for responding to cybersecurity incidents. The Act to Strengthen Federal Information Security 2009 <www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/BSI/bsiges2009_pdf.html> gives the Federal Office for Information Security the authority to act as the national authority for information security. The act does not outline a general incident management structure, nor specific practices related to cybersecurity.

	QUESTION	RESPONSE	EXPLANATORY TEXT
8.	Is there legislation/policy that requires a public report on cybersecurity capacity for the government?	Draft	The draft Act to Increase the Security of Information Technology <www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/Entwuerfe/Entwurf_IT-Sicherheitsgesetz.pdf?__blob=publicationFile> would require the Federal Office for Information Security (BSI) <www.bsi.bund.de> to, in cooperation with federal authorities, analyse the potential for cyber threats to entities engaged with critical infrastructure and to continually update the government with regard to the security situation of entities engaged with critical infrastructure.
9.	Is there legislation/policy that requires each agency to have a chief information officer (CIO) or chief security officer (CSO)?	✖	There is no legislation or policy in Germany that requires each agency to have a chief information officer or chief security officer.
10.	Is there legislation/policy that requires mandatory reporting of cybersecurity incidents?	✔	The Act on the Federal Office of Information Security 2009 <www.bmi.bund.de/SharedDocs/Downloads/EN/Gesetzestexte/bsi_act.html> requires federal authorities to report cybersecurity incidents to the Federal Office of Information Security upon detection. There is a draft amendment to the act <www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/Entwuerfe/Entwurf_it-sicherheitsgesetz.html>, which proposes the strengthening of mandatory reporting requirements covering telecommunication service providers and entities engaged with critical infrastructure.
11.	Does legislation/policy include an appropriate definition for "critical infrastructure protection" (CIP)?	✔	The National Strategy for Critical Infrastructure Protection (CIP Strategy) <www.bmi.bund.de/cae/servlet/contentblob/598732/publicationFile/34423/kritis_englisch.pdf> includes appropriate definitions for "critical infrastructure" and "critical infrastructure protection".
12.	Are requirements for public and private procurement of cybersecurity solutions based on international accreditation or certification schemes, without additional local requirements?	✔	Germany recognises international security certifications, and although some local security guidelines have been developed, they do not require additional local certification or accreditation. For example, refer to the Cloud-fahrplan für die öffentliche verwaltung — a guideline published by the Fraunhofer Institute (FOKUS) as a road map to help federal institutions migrate IT services to Cloud. <www.oeffentliche-it.de/documents/18/21941/Cloud-Fahrplan+oeffentliche+Verwaltung>
	OPERATIONAL ENTITIES		
1.	Is there a national computer emergency response team (CERT) or computer security incident response team (CSIRT)?	✔	CERT-Bund <www.cert-bund.de> was established in 2012 and is responsible for warning systems and coordinating incident response measures for German federal government authorities. It works closely with German CERT alliances and state-level CERTs to provide wider coverage.
2.	What year was the computer emergency response team (CERT) established?	2012	
3.	Is there a national competent authority for network and information security (NIS)?	✔	The Federal Office for Information Security (BSI) <www.bsi.bund.de> acts as Germany's national competent authority for network and information security. The National Cyberdefence Centre, which reports to BSI, is the agency primarily responsible for cybersecurity.
4.	Is there an incident reporting platform for collecting cybersecurity incident data?	✔	Operated by the Federal Office for Information Security (BSI) <www.bsi.bund.de>, CERT-Bund <www.cert-bund.de> is tasked with collecting information about cybersecurity incidents. They engage proactively by monitoring their constituency for cybersecurity incidents, as well as providing an online reporting structure to log cybersecurity incidents. The National Cyber Response Centre, which reports to BSI, provides a platform for cross-agency cooperation on cybersecurity. The Digital Agenda 2014-17 <www.bmi.bund.de/SharedDocs/Downloads/EN/Broschueren/2014/digital-agenda.html> states that the incident response capacities of the centre will be strengthened.
5.	Are national cybersecurity exercises conducted?	✔	Germany conducted three national cybersecurity exercises between 2010 and 2012. Germany also participated in multi-national exercises organised by the European Union and NATO.
6.	Is there a national incident management structure (NIMS) for responding to cybersecurity incidents?	✖	There is no national incident management structure in place in Germany for responding to cybersecurity incidents. The Act to Strengthen Federal Information Security 2009 <www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/BSI/bsiges2009_pdf.html> gives the Federal Office for Information Security the authority to act as the national authority for information security. The act does not outline a general incident management structure, nor specific practices related to cybersecurity.

Anexo 5: Grado de cumplimiento de Francia de niveles de ciberseguridad

COUNTRY: **FRANCE**

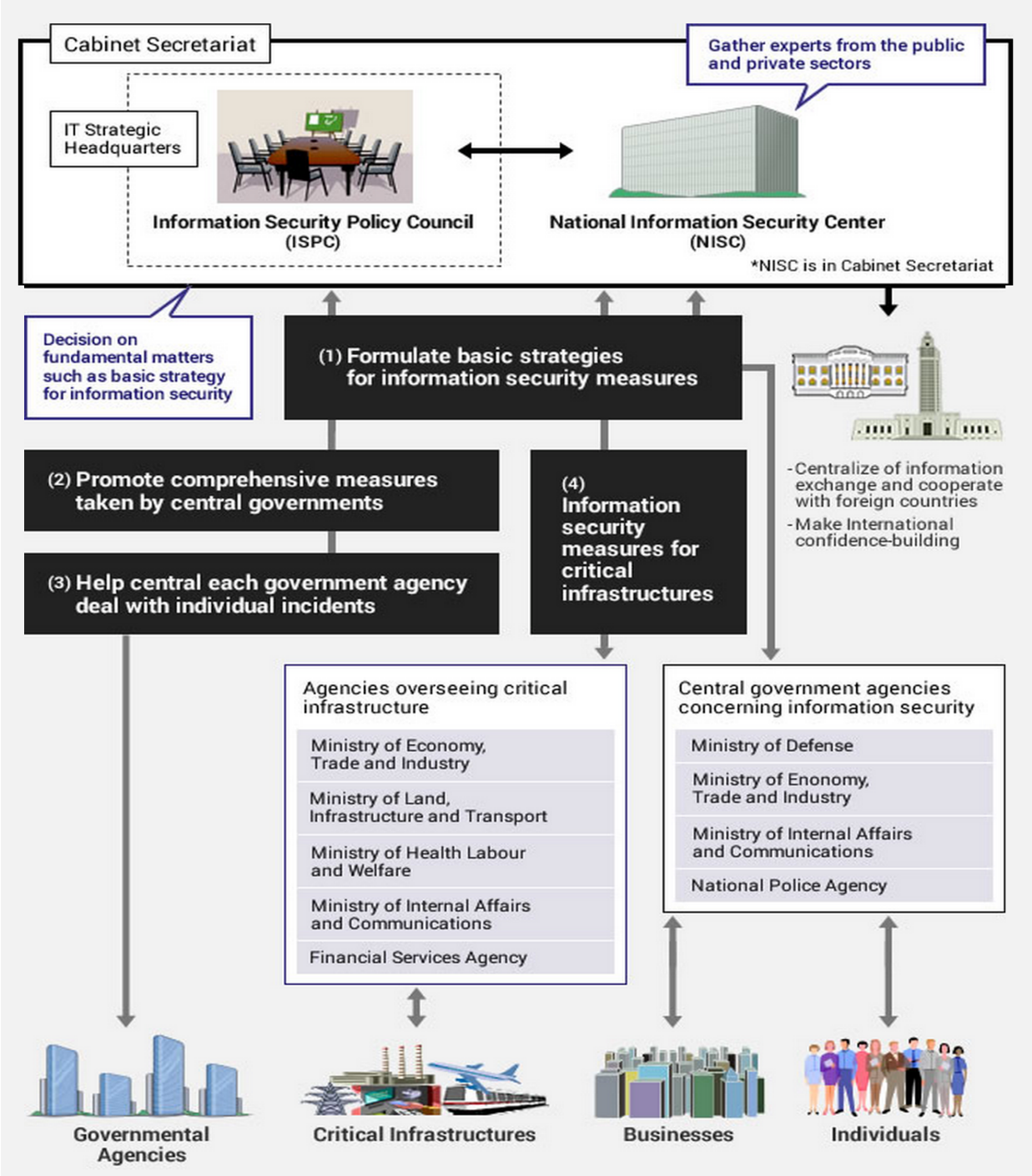
France has had a national cybersecurity strategy in place since 2011, although it has a strong focus on defence and national security issues. The National Agency for the Security of Information Systems (ANSSI) is a well-established authority dedicated to information security and is integrated with the country's computer emergency response team, CERT-FR. The cybersecurity strategy contains recommendations for closer cooperation with the private sector, but this has not been significantly developed. ANSSI has published sector-specific security measures, making France one of the few EU countries to adopt such a targeted approach to managing cybersecurity.

	QUESTION	RESPONSE	EXPLANATORY TEXT
	LEGAL FOUNDATIONS		
1.	Is there a national cybersecurity strategy in place?	✔	The Information Systems, Defence and Security Strategy was adopted in 2011. <www.ssi.gouv.fr/IMG/pdf/2011-02-15_Information_system_defence_and_security_-_France_s_strategy.pdf> The strategy has a condensed set of objectives and subsequent action items.
2.	What year was the national cybersecurity strategy adopted?	2011	
3.	Is there a critical infrastructure protection (CIP) strategy or plan in place?	✖	There is no discrete critical infrastructure plan in place in France. The responsibility for critical infrastructure protection is spread across government departments, but is coordinated by the General Secretariat for Defence and National Security (SGDSN). <www.sgdsn.gouv.fr>
4.	Is there legislation/policy that requires the establishment of a written information security plan?	✖	There is no legislation or policy in place in France that requires the establishment of a written information security plan.
5.	Is there legislation/policy that requires an inventory of "systems" and the classification of data?	✔	The French Penal Code <www.legifrance.gouv.fr/content/download/1957/13715/version/4/file/Code_33.pdf> requires data, of which disclosure may cause a threat to the national defence, to be classified. The French Defence Code outlines a primary three-tiered system of classification levels, with an additional seven special categories that can be applied. The specifics of the classifications levels are set out in the Decree of 30 November 2011 on the Protection of National Defence Secrets. <www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000024892134&fastPos=1&fastReqId=275001272&categorieLien=cid&oldAction=rechTexte> This decree mandates that classification levels are to be assigned according to the level of risk to national defence involved in disclosing classified information. The Recommendation for Information Systems Relating to Non-Defence Classified Sensitive Information <www.ssi.gouv.fr/IMG/pdf/1994_03_02_901_protection_systemes_d_information.pdf> deals with sensitive data, of which disclosure may not cause a threat to national security in particular, but may still be deemed sensitive to public or private interests. It does not require this data to be classified.

	QUESTION	RESPONSE	EXPLANATORY TEXT
6.	Is there legislation/policy that requires security practices/ requirements to be mapped to risk levels?	✔	The French Defence Code compels the French Prime Minister to determine the appropriate requirements for the protection of classified information, according to "government priorities". Ministers then carry out security practices in their department based on the requirements of the Prime Minister. The current requirements are set out in the Decree of 30 November 2011 on the Protection of National Defence Secrets <www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000024892134&fastPos=1&fastReqId=275001272&categorieLien=cid&oldAction=rechTexte> and these dictate security procedures that map to risk levels. The Recommendation for Information Systems Relating to Non-Defence Classified Sensitive Information <www.ssi.gouv.fr/IMG/pdf/1994_03_02_901_protection_systemes_d_information.pdf> and the Protection of Non-Defence Sensitive Information: Recommendations for Computer Work Stations 1993 <www.ssi.gouv.fr/IMG/pdf/1993_03_01_600_Protection_des_informations_sensibles_ne_relevant_pas_du_secret_de_defense_-_Recommandation_pour_les_postes_de_travail_informatiques.pdf> deal with sensitive data whose disclosure may not cause a particular threat to national security. It details recommended security procedures pertaining to such information.
7.	Is there legislation/policy that requires (at least) an annual cybersecurity audit?	✖	There is no legislation or policy in place in France that requires at least an annual cybersecurity audit. The Decree of 30 November 2011 on the Protection of National Defence Secrets <www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000024892134&fastPos=1&fastReqId=275001272&categorieLien=cid&oldAction=rechTexte> requires security audits to be part of the operation of the information security process in general, but does not dictate any requirements in terms of timing or scope.
8.	Is there legislation/policy that requires a public report on cybersecurity capacity for the government?	✖	There is no legislation or policy in place in France that requires a public report on cybersecurity capacity for the government. The Decree No. 2009-834 of 7 July establishing the National Agency for the Security of Information Systems <www.legifrance.gouv.fr/jopdf/common/jo_pdf.jsp?numJO=0&dateJO=20090708&numTexte=3&pageDebut=&pageFin=> makes it the agency responsible for conducting inspections of information security systems. This process is not elaborated upon however. The decree does not mention cybersecurity in particular.
9.	Is there legislation/policy that requires each agency to have a chief information officer (CIO) or chief security officer (CSO)?	✔	The Decree of 30 November 2011 on the Protection of National Defence Secrets <www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000024892134&fastPos=1&fastReqId=275001272&categorieLien=cid&oldAction=rechTexte> requires each department in possession of classified information, which pertains to national defence to appoint a central security officer, whose position is connected to the Department of Defence.
10.	Is there legislation/policy that requires mandatory reporting of cybersecurity incidents?	✖	There is no legislation or policy in place in France that requires mandatory reporting of cybersecurity incidents.
11.	Does legislation/policy include an appropriate definition for "critical infrastructure protection" (CIP)?	✖	French legislation or policy does not have an appropriate definition for "critical infrastructure protection".
12.	Are requirements for public and private procurement of cybersecurity solutions based on international accreditation or certification schemes, without additional local requirements?	◑	The National Agency of Information Systems' Security (ANSSI) <www.ssi.gouv.fr> promotes specific local requirements for the security of information systems (the PASSI standard). This standard is often applied to public authorities in terms of information systems' security, in addition to international standards such as the Common Criteria. However, application of the standard is not mandatory.
	OPERATIONAL ENTITIES		
1.	Is there a national computer emergency response team (CERT) or computer security incident response team (CSIRT)?	✔	CERT-FR <www.cert.ssi.gouv.fr>, formerly CERTA, was established in 2008. It is responsible for coordinating incident response measures for both government institutions and entities engaged with critical infrastructure.
2.	What year was the computer emergency response team (CERT) established?	2008	
3.	Is there a national competent authority for network and information security (NIS)?	✔	The National Agency for the Security of Information Systems (ANSSI) <www.ssi.gouv.fr> acts as France's national competent authority for network and information security.

	QUESTION	RESPONSE	EXPLANATORY TEXT
4.	Is there an incident reporting platform for collecting cybersecurity incident data?	✔	CERT-FR <www.cert.ssi.gouv.fr> is tasked with collecting information about cybersecurity incidents. They engage proactively by monitoring their constituency for cybersecurity incidents, as well as having in place an email-based reporting structure to log cybersecurity incidents.
5.	Are national cybersecurity exercises conducted?	✔	France conducted the national cybersecurity exercise Piranet in 2010 and 2012. France has also taken part in multi-national exercises organised by the European Union and NATO.
6.	Is there a national incident management structure (NIMS) for responding to cybersecurity incidents?	✖	A national incident management structure for responding to cybersecurity incidents, if it exists, is not publicly available.
	PUBLIC-PRIVATE PARTNERSHIPS		
1.	Is there a defined public-private partnership for cybersecurity?	✖	The French Cybersecurity Strategy (Information Systems, Defence and Security: France's Strategy <www.ssi.gouv.fr/IMG/pdf/2011-02-15_Information_system_defence_and_security_-_France_s_strategy.pdf>) calls for the establishment of a public-private partnership to assist in the detection of threats and ensure the protection of national critical infrastructure. The status of the public-private partnership is unclear.
2.	Is industry organised (i.e. business or industry cybersecurity councils)?	✖	There is no apparent significant industry-led association for cybersecurity in France.
3.	Are new public-private partnerships in planning or underway (if so, which focus area)?	◑	The French Cybersecurity Strategy (Information Systems, Defence and Security: France's Strategy <www.ssi.gouv.fr/IMG/pdf/2011-02-15_Information_system_defence_and_security_-_France_s_strategy.pdf>) calls for the establishment of a public-private partnership to assist in the detection of threats and ensure the protection of national critical infrastructure. The status of the public-private partnership is unclear.
	SECTOR-SPECIFIC CYBERSECURITY PLANS		
1.	Is there a joint public-private sector plan that addresses cybersecurity?	✔	The National Agency for the Security of Information Systems (ANSSI) <www.ssi.gouv.fr> has published proposed cybersecurity measures for sectors engaged with critical infrastructure, which cover identification of critical infrastructure and the application of security rules. These rules apply to both public and private entities within each sector.
2.	Have sector-specific security priorities been defined?	✖	Sector-specific security priorities have not been defined.
3.	Have any sector-specific cybersecurity risk assessments been conducted?	✖	Sector-specific risk assessments have not been released, as of August 2014.
	EDUCATION		
1.	Is there an education strategy to enhance cybersecurity knowledge and increase cybersecurity awareness of the public from a young age?	✔	The French Cybersecurity Strategy <www.ssi.gouv.fr/IMG/pdf/2011-02-15_Information_system_defence_and_security_-_France_s_strategy.pdf> includes a long-term objective to "raise citizens' awareness of cybersecurity issues during the education process". The Strategy includes a commitment to implement an active governmental communication policy and states that "appropriate communication campaigns will be conducted by National Agency for the Security of Information Systems (ANSSI) targeting the general public and companies".

Anexo 6: Organización de la ciberseguridad en Japón[669]



[669] http://www.space-cyber.jp/cyber/