UNIVERSIDAD DE ALMERÍA

Doble grado en Derecho y Administración y Dirección de Empresas
Facultad de Derecho
Facultad de Ciencias Económicas y Empresariales

La Ciberseguridad en el Marco Europeo. El caso de España.

Cibersecurity in the European framework. The case of Spain.

Autora: Marina Jurado del Águila
Directora: Eva María Díez Peralta

Resumen: Debido al desarrollo de la Tecnologías de la Información y la Comunicación (TICs), la ciberseguridad se ha posicionado en un lugar preferente dentro de las estrategias de seguridad de los Estados y de las organizaciones internacionales. Como consecuencia, se ha desarrollado un nuevo entramado legal que da respuesta a la vertiente digital de la seguridad.

Abstract: Due to the development of Information and Communication Technologies (ICT), cybersecurity has been positioned in a preferential place within security strategies of nations and international organizations. As a consequence, a new legal framework has been developed to make a response to the digital aspect of the security.

jueves, 4 de junio de 2020

ÍNDICE

ABREVIATURAS

Abreviatura	Significado
AED	Agencia Europea de Defensa
BOE	Boletín Oficial del Estado
CEP	Cooperación Estructurada Permanente
CERT-EU	Equipo de Respuesta para Emergencias Informáticas de la Unión Europea
EMUE	Estado Mayor de la Unión Europea
ENISA	Agencia Europea de Seguridad de las Redes y de la Información. El acrónimo proviene de su nombre en inglés: *European Union Agency for Network and Information Security*. El 17 de abril de 2019, como se verá en este trabajo, el Parlamento Europeo y el Consejo adoptan el Reglamento sobre la Ciberseguridad convirtiéndose, así, en la *European Union Agency for Cybersecurity*, traducida al castellano: Agencia de la Unión Europea para la Ciberseguridad. No confundir con la Empresa Nacional de Innovación Sociedad Anónima, cuyo acrónimo en español es el mismo.
I+T	Investigación y Tecnología
Ibid	Igual que la referencia anterior
INCIBE	Instituto Nacional de Ciberseguridad
NSA	*National Security Agency* (Agencia de Seguridad Nacional de los Estados Unidos de América)
ONU	Naciones Unidas
OSCE	Organización para la Salud y la Cooperación en Europa
OTAN	Organización del Tratado del Atlántico Norte
p	En la página
PCSD	Política Común de Seguridad y Defensa de la Unión Europea
pp	Entre las páginas

pymes	Pequeñas y medianas empresas
SEAE	Servicio Europeo de Acción Exterior
SIT	Sistemas de Información y Telecomunicaciones
TFUE	Tratado de Funcionamiento de la Unión Europea
TIC	Tecnologías de la Información y la Comunicación
TUE	Tratado de la Unión Europea
UE	Unión Europea

INTRODUCCIÓN

Debido al constante crecimiento y desarrollo las tecnologías que se sirven de Internet para desempeñar sus funciones, el aseguramiento de un correcto funcionamiento político, económico, social, técnico y legal se hace imprescindible en estas materias. Es aquí donde entra en juego la ciberseguridad, entendida como aquella disciplina que vela por la protección, defensa y licitación de todo el entramado físico y digital, de personas y objetos, que circunvalan el mundo de Internet.

En este Trabajo de Fin de Grado vamos a exponer la problemática más reciente que presentan los sistemas de seguridad nacionales que, teniendo en cuenta el fenómeno de la globalización y el desarrollo de las Tecnologías la Información y la Comunicación (en adelante, TICs), podemos establecer que es la seguridad en el ámbito ciberespacial, el último de los espacios denominado como comunes. En primer lugar, vamos a definir qué ha de entenderse por ciberseguridad -entre otros conceptos relevantes-, así como esclarecer el porqué de su relevancia.

Seguidamente, aclararemos la función que ocupan los Estados en relación con la seguridad cibernética. Destacaremos la importancia que tienen las acciones u omisiones que estos lleven a cabo, así como deber que recae sobre los mismos de tutelar, juzgar y ejecutar -en su caso- los actos que queden dentro de su jurisdicción y que estén sometidos a su soberanía. También haremos referencia a la relevancia que ocupan en este punto algunos entes no estatales.

En el tercer punto hablaremos (desde una óptica internacionalista) acerca de uno de los sistemas de cooperación estatal en el que, entre otras cuestiones, se encuentra la ciberseguridad y en el que encontramos un mayor compromiso por parte de los países. Se trata del sistema implementado en la Unión Europea (en adelante, UE). Para explicarlo, comenzaremos con el esclarecimiento del marco político común implementado. En relación con este, hablaremos de forma concreta sobre del Reglamento especialmente creado en la UE para la ciberseguridad. Continuaremos analizando el régimen de sanciones que la UE ha diseñado para imponer a los ciberataques y terminaremos comentando cuáles son las últimas preocupaciones de la UE en este ámbito.

En el apartado número cuatro, desde una perspectiva nacional, estudiaremos cómo han ido evolucionando las estrategias seguidas por el Estado español en materia de seguridad cibernética, desde 2011 hasta la actualidad.

Por último, con la intención de completar la sección anterior y confeccionar un estudio menos individualista, analizaremos brevemente los sistemas de seguridad nacional y ciberseguridad de otros dos Estados europeos: Francia y Alemania.

1. PRESENTACIÓN DEL TEMA

1.1. Definición de ciberseguridad y otras aclaraciones terminológicas de interés

Antes de comenzar con el desarrollo de este Trabajo de Fin de Grado, resulta esencial aportar una definición del término "ciberseguridad". Atendiendo a la definición del diccionario del centro estadounidense *National Initiative for Cybersecurity Careers and Studies* (NICCS) -página web oficial de la Agencia de Ciberseguridad e Infraestructura de Seguridad de los Estados Unidos, cuyo homólogo europeo sería la Agencia de la Unión Europea para la Ciberseguridad (en adelante, ENISA)- la ciberseguridad es "la actividad o proceso, capacidad o estado por el cual los sistemas de información y comunicaciones y la información contenida en ellos están protegidos y/o defendidos contra daños, uso no autorizado, modificación o explotación" (Signaturit, 2017).

Así, podríamos decir que el concepto de ciberseguridad engloba a aquellas medidas que se toman con el objeto de proteger a los usuarios (personas tanto físicas, como jurídicas) que operan en Internet de ataques o actuaciones ilícitas de terceros en la red. De hecho, la ciberseguridad pertenece a la familia de la seguridad de la información, cuyo propósito es proteger la información digital contenida en sistemas interconectados (Signaturit, 2017).

Por otra parte, cabría reseñar otros conceptos relacionados con la ciberseguridad, cuya definición también va a resultar muy provechosa de cara a comprender mejor este trabajo:

- Hacker (o hacktivista): individuo al que, lejos de la imagen negativa que se le ha atribuido, le gusta tener una comprensión profunda del funcionamiento interno de un sistema informático para mejorarlo. No es un delincuente, sino que investiga y expande los límites de la red (Alonso, 2016). No existe en ellos intención de hacer daño, sino de aprender.
- Cracker, pirata informático o ciberdelincuente: son programadores informáticos con amplios conocimientos, capaces de obtener datos confidenciales y acceder a otros ordenadores para destruir o almacenar información ajena. Buscan producir daño u obtener información de forma ilegal con la que comercializar posteriormente. Al contrario de los hackers, cometen violaciones en la seguridad de los sistemas informáticos para obtener un beneficio propio. Sus acciones son siempre maliciosas (Aucal Business School, 2015).
- Cibercrimen: Consiste en todas aquellas conductas delictivas que se practican mediante el aprovechamiento de la red (Signaturit, 2017).

- Ciberamenazas: Son las posibilidades de comisión de daños a personas u organismos mediante el uso de Internet (Signaturit, 2017).
- Ciberresiliencia: es la capacidad para resistir, proteger y defender el uso del ciberespacio de los atacantes (INCIBE, 2014).
- Ciberespacio: espacio cuya naturaleza y caracteres son diferentes a los conocidos. Atendiendo a Robles Carrillo, su definición es la que sigue: "es artificial, por ser el único creado por el hombre. Es virtual pero, también, físico porque depende del entramado material de sistemas y de redes que le sirven de sustento y porque interacciona y se proyecta en el mundo no virtual". Es ilimitado, en el sentido de no ser susceptible de "delimitación espacial, material, funcional o temporal. Es universal, global, abierto, descentralizado y transnacional, transversal y esencialmente mutable". Como caracteres distintivos posee la neutralidad, la popularidad y el anonimato. Evoluciona a un ritmo asombroso por su capacidad de expansión, que se nutre del desarrollo tecnológico, y por su enraizada relación con el espacio físico. A diferencia del resto de *Global Commons*, puede alterar las realidades de otros dominios (Robles Carrillo, 2016, p. 7). Su concepto es más vasto que el del propio Internet, herramienta esencial de la que se sirve.

1.2. La relevancia de la ciberseguridad

El mundo, tal y como lo conocemos hoy en día, es globalizado. La globalización hace referencia a la "variedad de cambios económicos, culturales, sociales y políticos que han dado forma al mundo en los últimos 50 años, desde la muy celebrada revolución de la tecnología de la información a la disminución de las fronteras nacionales y geo-políticas en la cada vez mayor circulación transnacional de bienes, servicios y capitales. La creciente homogeneización de los gustos de los consumidores, la consolidación y expansión del poder corporativo, el fuerte aumento de la riqueza y la pobreza, la "McDonaldisation" de los alimentos y la cultura, y la creciente ubicuidad de las ideas democráticas liberales, de una u otra manera, se atribuyen a la globalización" (Guttal, 2007)[1].

Por su parte, la Asamblea Parlamentaria del Consejo de Europa define la globalización como "la cada vez mayor integración económica de todos los países del mundo como consecuencia

[1] Referencia obtenida mediante la página web del Consejo de Europa, en el *COMPASS: Manual de Educación en los Derechos Humanos con jóvenes*, p. 1, 2020, en https://www.coe.int/es/web/compass/globalisation (consultada a 08 de mayo de 2020).

de la liberalización y el consiguiente aumento en el volumen y la variedad de comercio internacional de bienes y servicios, la reducción de los costos de transporte, la creciente intensidad de la penetración internacional de capital, el inmenso crecimiento de la fuerza de trabajo mundial y la acelerada difusión mundial de la tecnología, en particular las comunicaciones"[2].

En este punto, lo que importa no es qué definición nos parezca más acertada, sino darnos cuenta de que ambas tienen en común una cosa: que el proceso de interconexión entre los diferentes puntos del globo terráqueo no habría sido posible sin las redes cibernéticas. Cuando Bill Gates -empresario de renombre, informático y cofundador de Microsoft- afirmó aquello de "si tu negocio no está en Internet, tu negocio no existe" pocos se imaginarían que, con el paso de los años, Internet mutaría hasta hacer válida esta afirmación para las personas.

En enero de 2019, de los 7.676 billones de personas que poblaban la Tierra, 5.112 billones eran usuarios exclusivos de móvil (un 2% más que el año pasado), 4.388 billones eran usuarios de Internet (un 9,1% más que el año pasado), 3.484 billones eran usuarios activos de redes sociales, lo que supone un 9% más en relación al año anterior (Kemp, 2019)[3]. Esta información resulta sumamente útil para comprender que existe un incremento constante del número de usuarios y del uso de Internet, hecho que está propiciando la convergencia digital de nuestro entorno: el dinero y otros medios de pago; los documentos (certificados, resguardos, etc.) que tradicionalmente se extendían en papel; el trabajo (tal y como hemos podido comprobar durante el estado de alarma declarado por la alerta sanitaria a causa de la COVID-19); incluso las relaciones personales.

Dado que las personas cada vez son más dependientes de Internet y arrojan -muchas veces sin darse cuenta- cantidades ingentes de información sensible a éste[4], resulta fundamental establecer sistemas de seguridad que garanticen el uso apropiado de las redes cibernéticas porque, de caer en malas manos todos esos datos, se estarían vulnerando -de hecho o en potencia- los derechos humanos de los individuos.

---

[2] *Ibid*. p.1.

[3] Traducción propia de la fuente.

[4] Por información sensible puede entenderse, por ejemplo, los datos de las constantes vitales que registran las pulseras inteligentes, la geolocalización constante que pueden registrar los dispositivos móviles, las conversaciones privadas de los usuarios de Internet que mantienen por chats o redes sociales, fotografías y vídeos, informes médicos en los que aparezcan patologías, el acceso a los micrófonos de los dispositivos con conexión a Internet, etc.

Por último, cabe destacar que la ciberseguridad no sólo debe de concebirse como un concepto reactivo en el que los sistemas de seguridad responden frente ataques cibernéticos, sino que debe dársele suma importancia a su vertiente proactiva. La vertiente proactiva debe entenderse como aquella que previene o emplea fórmulas de minimización de impactos frente a los ataques cibernéticos: cortafuegos, copias de seguridad, sistemas de alarma, etc.

2. EL PAPEL QUE OCUPAN LOS ESTADOS EN RELACIÓN CON LA CIBERSEGURIDAD

Los Estados son entes con un peso relativo en el escenario del mundo mucho más importante que las personas de forma individual. Debido a este mayor poder de negociación y gestión, son ellos quienes han de velar por su propia ciberseguridad, así como por la de los ciudadanos que están bajo su soberanía o sobre su territorio. Han de establecer reglas y protocolos de actuación, así como negociar con otros países pactos de cooperación y/o integración para luchar de forma conjunta contra el cibercrimen, en aras de realizar una actuación más eficaz.

Por otra parte, los Estados también tienen un "deber de vigilar" -a modo de analogía con el "*deber in vigilando"* civil[5] que tienen los padres y tutores sobre los menores o incapacitados a su cargo-. Es decir, se puede llegar a responsabilizar[6] y sancionar a los Estados -al menos, por parte de la Unión Europea- por los ciberataques cometidos y/u originados desde su territorio, o los que se han servido de infraestructuras o personas cuya actividad se ejerce en su territorio, tal y como veremos en el apartado *3.3* de este trabajo, relativo al *análisis del régimen de sanciones impuestas a los ciberataques*.

No es nada desdeñable el hecho de que, si bien es cierto que los individuos no pueden hacer mucho por sí solos -como regla general-, en ocasiones ocurre que se organizan con el objetivo de adquirir la suficiente relevancia en el ámbito del ciberespacio como para poder actuar de manera destacada, bien sea para realizar acciones adecuadas o conformes a la ley, bien sea para realizar acciones contrarias a la misma.

---

[5] BOE, *Código Civil, Capítulo II. De las obligaciones que nacen de culpa o negligencia*, 1889, artículo 1.903, en https://www.boe.es/buscar/act.php?id=BOE-A-1889-4763 (consultada a 25 de mayo de 2020).

[6] La atribución de responsabilidad a un Estado por la comisión de un ciberataque sólo corresponde a otro Estado, no a la UE, como veremos en el apartado *3.3. Análisis del régimen de sanciones impuestas a los ciberataques.*

Tal y como estableció el informe del Grupo de Expertos Gubernamentales de la Asamblea General de las Naciones Unidas sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional de 2015[7], "Los Estados no deben recurrir a terceros para cometer hechos internacionalmente ilícitos mediante las TIC y deberían tratar de garantizar que su territorio no sea utilizado por agentes no estatales para cometer tales hechos".

De esta forma, encontramos que, de manera oficial, se reconoce institucionalmente la existencia de entes no estatales con capacidad de cometer delitos cibernéticos.

La naturaleza de estos entes tiene una variedad amplísima y no es el objetivo de este Trabajo de Fin de Grado analizar todos y cada uno de los tipos. Mas, podemos mencionar, a modo de ejemplo, a los más característicos:

a) Red Team, Blue Team y Purple Team

Estos equipos de seguridad están formados por empresas y usuarios que, lejos de cometer hechos ilícitos a través de la red, lo que hacen es una labor de *hacking* ético. Es decir, pueden llegar a realizar actividades que entran dentro de la tipicidad de los delitos cibernéticos pero, siempre con permiso de la parte que va a sufrir la vulneración y con una intención de mejora de la seguridad o educativa. De esta forma, muchas de las empresas que forman parte de estos equipos lo que realmente realizan es una labor de auditoría técnica, en gran parte legalizada mediante su monetización y consentimiento contractual por la parte de la que va a experimentar dichos ataques.

- El *Red Team* -equipo rojo- se ocupa de la "seguridad ofensiva". Desarrolla el rol de atacante, utilizando herramientas iguales o similares y explotando las vulnerabilidades de seguridad que encuentre. Recrea los escenarios de amenazas a los que se puede enfrentar una organización, analizando la seguridad desde el punto de vista de los atacantes, para dar al equipo de seguridad (*Blue Team*) la posibilidad de defenderse. De esta forma, el *Red Team* es un entrenamiento para el *Blue Team* donde se evalúa la aptitud de una organización para proteger sus activos críticos, así como la capacidad de detección y respuesta que tiene (Revista UNIR, 2020). Como ejemplo, podemos mencionar a la compañía *ZEROLYNX S.L.*, perteneciente al *Red Teaming* del INCIBE.

[7] Asamblea General de las Naciones Unidas, *Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional*, p. 16, en https://undocs.org/sp/A/70/174, (consultada a 22 de mayo de 2020).

Se define como una empresa que cuenta con "especialistas en seguridad ofensiva capaces de evaluar, mediante técnicas automáticas o manuales, dispositivos, sistemas o redes desde la perspectiva de cualquier potencial adversario: desde un *hacktivista* o un empleado descontento, hasta amenazas avanzadas como un APT" (INCIBE, Red Teaming, 2020).

- Por su parte, el ***Blue Team*** -equipo azul- se encarga de la seguridad defensiva, defendiendo a las organizaciones de ataques de una manera proactiva. Su principal objetivo es evaluar las distintas amenazas que puedan afectar a las empresas y recomendar planes de actuación para mitigar los riesgos. Además, cuando hay incidentes, realizan tareas de respuesta (análisis forense de las máquinas afectadas, trazabilidad de los vectores de ataque, propuesta de soluciones y establecimiento de medidas de detección para futuros casos) (Revista UNIR, 2020).
- Por último, el ***Purple Team*** -equipo morado- asegura y maximiza la efectividad de los dos equipos anteriores, integrando las tácticas y controles defensivos del *Blue Team* con las amenazas y vulnerabilidades encontradas por el *Red Team*. (Revista UNIR, 2020)

b) Anonymous

Es una organización no gubernamental internacional formada por un número indeterminado de *ciberhacktivistas* anónimos (de ahí su nombre). En teoría, en esta organización no hay líderes y todos son iguales. Sus miembros se encuentran distribuidos por todo el mundo, de manera que no tienen una sede. Tampoco pertenecen a ningún partido político. Todos se representan bajo un mismo símbolo, la máscara que utiliza V en la novela gráfica V de Vendetta (Sierra, 2012).

Supuestamente, *Anonymous* realiza sus acciones para defender la libertad de expresión, el acceso a la información y la independencia de Internet. También está en contra de diversas organizaciones como Dáesh, la Cienciología, los servicios públicos, los consorcios con presencia global, las sociedades de derechos de autor y todos los sistemas de censura gubernamentales. En sus inicios, los participantes actuaban solamente en Internet, pero con el tiempo fueron desarrollando también sus actividades fuera de la red (Wikipedia, 2020).

c) Chaos Computer Club

El *Chaos Computer Club* (*CCC*) es el grupo de hackers más grande de Europa. Sus objetivos son conseguir la transparencia del gobierno, el acceso para todas las personas a un ordenador e información. El *CCC* no es un grupo que busque crear problemas. Por el contrario, están centrados en buscar vulnerabilidades de seguridad que exponen, con el ánimo de educar a las personas. Creen firmemente que todos los humanos deberían tener acceso gratuito a los ordenadores (Townsend, 2020).

d) Shadow brokers

A diferencia de los grupos anteriores, este está compuesto exclusivamente por *crackers*. En 2015, por ejemplo, el grupo se atribuyó la autoría del crackeo a la NSA. Posteriormente, en 2016 publicaron parte la información sustraída en una cuenta de *Tumblr* (que retiraron) y sacaron a subasta dichos archivos (Martí, 2017).

3. LA CIBERSEGURIDAD EN EL ÁMBITO DE LA COOPERACIÓN EN LA UNIÓN EUROPEA

La ciberseguridad es muy importante para la UE. Reflejo de ello es que aparece como una prioridad en la Estrategia Global sobre Política Exterior y de Seguridad de la Unión Europea[8]. En consecuencia, no es de extrañar que se hayan orquestado toda una serie de sistemas diversos que fomentan la cooperación entre los Estados miembros, así como políticas comunes para el territorio de la UE que pretenden mejorar e incrementar los sistemas de ciberseguridad que hallamos en el ámbito europeo.

3.1. El marco político común

Para el desarrollo de este apartado del trabajo he tomado como referencia el *Marco político de ciberdefensa de la UE (actualización de 2018)*[9].

En aras de realizar un mejor análisis del marco político común que da soporte a la ciberseguridad en el ámbito europeo, voy a dividir este apartado en los cuatro siguientes subapartados:

---

[8] Consejo de la Unión Europea, *Council conclusions on implementing the EU Global Strategy in the area of Security and Defence*, 14 de noviembre de 2016, en: https://www.consilium.europa.eu/media/22459/eugs-conclusions-st14149en16.pdf, (consultada a 22 de mayo de 2020).

[9] Consejo de la Unión Europea, *Marco político de ciberdefensa de la UE (actualización de 2018)*, 19 de noviembre de 2018, en: http://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/es/pdf, (consultada a 22 de mayo de 2020).

- Ámbito de aplicación y objetivos del marco político de ciberdefensa de la UE de 2018.
- Contexto y breve evolución histórica del marco político de ciberdefensa de la UE de 2018.
- Prioridades del marco político de ciberdefensa de la UE de 2018.
- Actuación consecutiva.

3.1.1. Ámbito de aplicación y objetivos del marco político de ciberdefensa de la UE de 2018.

Si nos fijamos en el ámbito de aplicación y en los objetivos del marco político de ciberdefensa de la UE de 2018[10], podemos establecer que éste actualiza al marco político de 2014 para responder a los retos cambiantes en el ámbito de la seguridad.

Además de la tierra, el mar, el aire y el espacio, el ciberespacio constituye el quinto ámbito de actuación en que operan la UE, sus Estados miembros y el resto de Estados. Sin perjuicio de la legislación nacional de cada Estado miembro y de la UE, este marco político pretende seguir desarrollando políticas de ciberdefensa de la UE en aras de incrementar las capacidades en seguridad cibernética y defensa -individualmente para los Estados miembros y, en conjunto, para la UE- y de mejorar, como consecuencia, la ciberresiliencia de los entes internacionales mencionados.

3.1.2. Contexto y breve evolución histórica del marco político de ciberdefensa de la UE de 2018

En cuanto al contexto[11] en el que se desarrolla el marco político, cabe destacar que en 2013, tanto en las Conclusiones del Consejo Europeo sobre la Política Común de Seguridad y Defensa de la Unión Europea (en adelante, PCSD), como en las del Consejo, 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 (en adelante, a AED). El Consejo adoptó el marco político de ciberdefensa de la UE el 14 de noviembre de 2014[12].

De este modo, queda patente que el marco común político de 2018 no se crea de la nada, sino que se basa en el marco político de 2014 sobre el que practica ciertas actualizaciones.

[10] *Ibid.*, p. 2.

[11] *Ibid.*, pp. 3-8.

[12] Documento del Consejo n.º 15585/14 de 18 de noviembre de 2014 (consultada a 22 de mayo de 2020).

A partir de la aplicación del marco político inicial de ciberdefensa de la UE, se han mejorado significativamente las capacidades en ciberdefensa de los Estados miembros. Cabe destacar que, en vista de la necesidad de reforzar la ciberresiliencia de la UE, se ha creado una "plataforma específica de formación y educación para apoyar la oferta de los Estados miembros en materia de formación en ciberdefensa". Además, los Estados miembros -en el marco de la Cooperación Estructurada Permanente (en adelante, CEP)- están desarrollando proyectos relacionados con la ciberdefensa y la UE está cooperando con la Organización del Tratado del Atlántico Norte (en adelante, OTAN) en causas relacionadas con la ciberseguridad y la ciberdefensa[13].

Como parte del Informe anual sobre ciberdefensa[14], en diciembre de 2017, los Estados miembros pidieron que se actualizara el marco político de ciberdefensa de la UE. Cuando la UE decide actualizar el marco político primitivo, en 2018, lo hace con la intención de intensificar la cooperación de los Estados en el ámbito de la ciberseguridad, para que refuercen su capacidad de respuesta frente a los ciberataques, así como su habilidad para disuadir los mismos. No resulta nada desdeñable el hecho de que la actualización permitió que la UE tuviera en cuenta la evolución de los desafíos en materia de seguridad que sucedieron desde 2014 hasta junio de 2018[15].

En relación con lo anterior, según la Secretaría General del Consejo de la UE (2018)[16], algunos de los acontecimientos más destacables que han tenido lugar desde la entrada en vigor del marco político de ciberdefensa de 2014 hasta la actualización de 2018 son:

a) En febrero de 2016 se amplió el ámbito de cooperación entre la UE y la OTAN. El Equipo de Respuesta para Emergencias Informáticas de las instituciones, órganos y organismos de la Unión Europea (CERT-EU) y la Capacidad de Respuesta ante Incidentes Informáticos de la OTAN, firmaron un acuerdo para facilitar el intercambio de información entre ambas organizaciones en aras de incrementar la prevención, la detección y la respuesta ante sucesos cibernéticos relevantes.

---

[13] Consejo de la Unión Europea, *Marco político de ciberdefensa de la UE (actualización de 2018)*, *op. cit*., pp. 3-8 (consultada a 19 de mayo de 2020).

[14] Parlamento Europeo, *Informe sobre Ciberdefensa (2018/2004(INI))*, 25 de mayo de 2018, p. 20, en: https://www.europarl.europa.eu/doceo/document/A-8-2018-0189_ES.pdf (consultada a 22 de mayo de 2020).

[15] Consejo de la Unión Europea, *Marco político de ciberdefensa de la UE (actualización de 2018)*, *op. cit.*, pp. 8-25 (consultada a 19 de mayo de 2020).

[16] *Ibid.*, pp. 4-8.

b) En julio de 2016, el Parlamento Europeo y el Consejo adoptaron la Directiva sobre Seguridad de las Redes y Sistemas de Información[17] (en adelante, Directiva SRI), que mejoraría la formación y capacidades de los Estados miembros de la UE frente a las ciberamenazas y fomentaría la cooperación dentro de la UE. La Directiva se estableció con el objetivo de conseguir un elevado nivel común de seguridad de las redes y sistemas de información dentro de la UE para que, a su vez, progresara el mercado interior.

c) En septiembre de 2017, la propuesta de un nuevo Reglamento de Ciberseguridad de la UE incluyó las nuevas instrucciones para la renovada ENISA, así como el establecimiento de un marco de certificación común para toda la UE. Además, la Comisión fue más allá: pretendió preparar a la UE para el supuesto de que se produjeran incidentes de ciberseguridad transfronterizos de gran envergadura. Actualmente está trabajando con los Estados miembros y otras instituciones, agencias y organismos en el desarrollo de la cooperación europea en caso de crisis de ciberseguridad mediante el Dispositivo Integrado de Respuesta Política a las Crisis. Por otra parte, cabe destacar que el marco apoyaba la inclusión de la ciberdefensa entre los mecanismos de gestión de crisis de la Unión cuando, para hacer frente a las consecuencias de una cibercrisis, pudieran aplicarse los artículos 222 del Tratado de Funcionamiento de la Unión Europea (en adelante, TFUE) y 42.7 del Tratado de la Unión Europea (en adelante, TUE), teniendo en cuenta el artículo 17 del TUE.

d) En el último mes del año 2017, se puso en marcha la CEP, estableciendo un marco de cooperación ambicioso, vinculante e inclusivo entre 25 Estados miembros, incorporando un compromiso para aumentar la cooperación en materia de ciberdefensa entre estos.

e) En junio de 2018, el Consejo Europeo destacó la necesidad de reforzar el sistema de ciberresiliencia de Europa y las capacidades de lucha contra las amenazas en materia de ciberseguridad procedentes de fuera de la UE y señaló como objetivo común el contribuir a la autonomía estratégica de Europa. Actualmente, en 2020, la necesidad

[17] *Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión*, de 19 de julio de 2016, p. 1 (consultada a 22 de mayo de 2020).

de refuerzo de la ciberresiliencia de los Estados sigue siendo una prioridad para la UE, tal y como podremos comprobar a lo largo del trabajo.

3.1.3. Prioridades del marco político de ciberdefensa de la UE de 2018

En cuanto a las prioridades[18] del marco político se han determinado seis objetivos centrales, que pasamos a comentar a continuación:

a) Apoyar el desarrollo de las capacidades de ciberdefensa de los Estados miembros

Dentro de la ciberdefensa, la mejora de las capacidades[19] y tecnologías implica que los Estados miembros han de multiplicar sus los esfuerzos para garantizar la eficacia de las capacidades en ciberdefensa. El Servicio Europeo de Acción Exterior (en adelante, SEAE), la Comisión y la AED deberán trabajar conjuntamente y apoyar dichos esfuerzos.

Resulta imprescindible una evaluación permanente acerca de la vulnerabilidad de las infraestructuras de información de las que se sirve la PCSD para sus misiones y operaciones, además de disponer, en tiempo prácticamente real, de información acerca de la eficacia de la protección. Operativamente, uno de los principales ámbitos de atención de las actividades de ciberdefensa será mantener la disponibilidad, la integridad y la confidencialidad de la red de comunicación e información de la PCSD.

Aquellos que llevan a cabo actividades cibernéticas malintencionadas deberán responder de sus actos, tal y como veremos en el apartado *3.3. Análisis del régimen de sanciones impuestas a los ciberataques*. Para posibilitar la punibilidad de estos actores, es importante que los Estados miembros de la UE, apoyados por el SEAE, promuevan un espacio de cooperación recíproca. Gracias a la elaboración de un conjunto de instrumentos de ciberdiplomacia, el SEAE y la AED pueden organizar de forma regular ejercicios con el fin de contribuir a lograr una respuesta mutua frente a las actividades cibernéticas malintencionadas.

Por otro lado, el marco hace hincapié en una cuestión que a simple vista puede parecer muy intranscendente pero que, realmente, es esencial: el desarrollo un concepto común y general

[18] Consejo de la Unión Europea, *Marco político de ciberdefensa de la UE (actualización de 2018), op. cit.*, pp. 8-24 (consultada a 19 de mayo de 2020).

[19] Por capacidades ha de entenderse doctrina, liderazgo, organización, personal, formación, industria, tecnología, infraestructuras, logística e interoperabilidad.

sobre el ámbito de la ciberdefensa, ya que este difiere según acudamos a una legislación nacional u otra, bien sea de cualquiera de los Estados miembros, bien sea de la UE.

En cuanto a las operaciones militares PCSD, cuando se planifiquen los requisitos de las infraestructuras de información en materia de ciberdefensa, se requerirá cierta convergencia estratégica entre los Estados puesto que estas infraestructuras necesitan, a su vez, de otras infraestructuras de mando, control, comunicaciones y ordenadores facilitadas, usualmente, por los Estados miembros.

b) Mejorar la protección de las redes de comunicación y los sistemas de información de la PCSD utilizados por entidades de la UE

Respetando las funciones del CERT-EU, el SEAE impulsará la comprensión de los asuntos relativos a la seguridad de las redes. La razón por la que se crea es el ánimo de mejorar la resiliencia de las redes PCSD del SEAE, centrándose en la prevención, detección, respuesta ante incidentes, conocimiento de la situación, intercambio de información y mecanismos de alerta temprana.

En cuanto a la responsabilidad económica, la protección de los sistemas de comunicación e información del SEAE y el desarrollo de capacidades de seguridad tecnologías de la información son competencia de la Dirección de Presupuesto y Administración de SEAE, aunque el Estado Mayor de la Unión Europea (en adelante, EMUE[20]), la Dirección de Gestión de Crisis y Planificación, y la Capacidad Civil de Planificación y Ejecución proporcionarán recursos y apoyo adicionales.

Para una mejor comprensión por parte de todos los destinatarios, resulta necesario simplificar las normas de seguridad de los sistemas de información que proporcionan los agentes institucionales de la UE, durante el desempeño de las misiones y operaciones PCSD.

Con la intención de mejorar la coordinación y reforzar la protección y resiliencia de las redes y los sistemas de comunicación e información de la PCSD, en el año 2017 se creó una junta de cibergobernanza del SEAE.

c) Fomentar la cooperación cívico-militar

Como hemos mencionado en numerosas ocasiones a lo largo de este trabajo, el ciberespacio es un ámbito en constante y rápida evolución. Estas características obligan a que todos los

[20] El EMUE es un departamento de la UE responsable de supervisar las operaciones en el ámbito de la Seguridad Común y Política de Defensa.

avances tecnológicos (sean civiles o militares) tengan que estar reforzados con sistemas de seguridad. Por razones de economía y ecología de los recursos, en los casos en que unos avances tecnológicos similares aporten soluciones tanto para el ámbito civil, como para el militar, debe preverse una coordinación entre ambos. Por el contrario, cuando las capacidades militares y los sistemas armamentísticos sean muy específicos, no habrá posibilidad de compartirlos con tecnologías civiles.

La cooperación cívico-militar en el ámbito cibernético puede resultar interesante para, por ejemplo, el intercambio de prácticas apropiadas, de información, de mecanismos de alerta temprana y de formación, siempre que no se menoscabe la organización interna y la legislación de los Estados miembros.

Por su parte, cabe destacar aquí que la Directiva SRI[21] aumenta el grado de preparación individual de los Estados miembros y refuerza la cooperación estratégica y operativa entre estos[22].

d) Investigación y tecnología

Los operadores de infraestructuras y servicios de TIC -ya sean con fines civiles o con fines militares- se enfrentan a retos parecidos cuando hablamos de ciberseguridad.

En materia de Investigación y Tecnología (en adelante, I+T), si existen necesidades y requisitos comunes en los sistemas militares y civiles, resultará mucho más fácil que se compartan datos y se intercambie información y conocimiento entre ambos, sobre todo a largo plazo. Dado que el desarrollo de la capacidad ciberdefensiva tiene una importante dimensión de I+T, en la medida en que se reduzcan los costes del desarrollo de soluciones y se facilite el alcance de economías de escala, las posibilidades de desarrollar una industria en ciberdefensa competitiva en Europa serán mayores. Cuanto más se fomenten y desarrollen las capacidades tecnológicas en Europa, más asequible resultará mitigar las amenazas y paliar los puntos débiles.

[21] Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, *op. cit.* (consultada a 22 de mayo de 2020).

[22] La supervisión de las políticas de ciberseguridad corresponde, en este caso, a las autoridades nacionales, a los CERT nacionales y al CERT-EU.

Por otro lado, hay que fomentar el desarrollo de la industria (dado que, en el ámbito de la ciberdefensa, es y seguirá siendo el motor principal de la tecnología y la innovación[23]) y de una cadena de suministro industrial europea en materia de ciberseguridad competitiva, apoyando la participación, sobre todo, de las pequeñas y medianas empresas (pymes) con motivo de que son el tamaño de empresa más numeroso en la mayoría de países[24].

Asegurar que Europa sea capaz de seguir el ritmo a la competencia internacional en capacidad tecnológica cibernética depende de la capacidad que tengamos para impulsar la innovación de vanguardia mediante instrumentos que sean nacionales, así como de la Unión (por ejemplo, el Consejo Europeo de la Innovación).

e) Mejorar las posibilidades de educación, formación y ejercicios

La mejora y aumento de las posibilidades de formación en ciberdefensa se hacen necesarias para, a su vez, mejorar la preparación ante las ciberamenazas y desarrollar una cultura común de ciberdefensa en la UE.

Resulta esencial que los presupuestos de educación y formación se utilicen de forma eficaz y eficiente. Para ello, resultará esencial la puesta en común europea de la educación y formación en materia de ciberdefensa.

También es necesario que los agentes militares y civiles encargados de la PCSD realicen ejercicios -individuales y conjuntos- en materia de ciberdefensa para que las fuerzas nacionales mejoren su preparación con vistas a actuar en un entorno multinacional.

f) Incrementar la cooperación con los socios internacionales pertinentes

Dentro de la cooperación internacional, resulta necesario garantizar el diálogo con los socios internacionales (en concreto la OTAN y otras organizaciones internacionales) en aras de transformar en eficaces las capacidades de ciberdefensa.

Se deberá otorgar mayor participación a las actividades realizadas en el marco de la Organización para la Salud y la Cooperación en Europa (en adelante, OSCE) y de las Naciones Unidas (en adelante, ONU), en favor de presentar un marco estratégico para

[23] Algunos de los ámbitos susceptibles de mejora son la criptografía, los sistemas empotrados seguros, la detección de programas malintencionados, las técnicas de simulación y visualización, la protección de las redes y sistemas de comunicación y la tecnología de identificación y la autenticación.

[24] Ministerio de Industria, Comercio y Turismo. *Cifras PyME*. Enero de 2019. En http://www.ipyme.org/es-ES/ApWeb/EstadisticasPYME/Documents/CifrasPYME-enero2019.pdf (consultada a 23 de mayo de 2020).

prevenir conflictos, reforzar la cooperación entre los Estados y dotar de estabilidad al ciberespacio.

Por parte de la UE, existe voluntad política de reforzar la cooperación con la OTAN en materia de ciberdefensa, a partir del desarrollo de capacidades en ciberdefensa sólidas y resilientes[25].

3.1.4. Actuación consecutiva

En aplicación del marco político de ciberdefensa, el SEAE, la AED y la Comisión deberán presentar al Grupo Político-Militar, con la participación de los miembros del Grupo Horizontal "Cuestiones Cibernéticas", y al Comité Político y de Seguridad, un informe anual sobre el desarrollo de los trabajos, para examinar los seis puntos expuestos anteriormente, con el fin de evaluar la aplicación del marco.

Por otra parte, también resulta de vital importancia que, de acuerdo con el desarrollo y la evolución de las diferentes amenazas cibernéticas, se establezcan nuevos requisitos en materia de ciberdefensa. Así las cosas, la próxima revisión del marco político de ciberdefensa debía presentarse por estas fechas (a mediados de 2020), como muy tarde, previa consulta a los Estados miembros[26].

3.2. El Reglamento europeo sobre la ciberseguridad

El 17 de abril de 2019, se adopta el denominado Reglamento sobre la Ciberseguridad[27]. Su objeto es mejorar la resistencia a los ciberataques y proporcionar un marco de certificación de la ciberseguridad para productos y servicios, aumentando así la confianza en el ámbito digital[28].

---

[25] Las características de las capacidades son fruto de la exigencia De la declaración conjunta firmada por el presidente del Consejo Europeo, el presidente de la Comisión Europea y el secretario general de la OTAN.

[26] Consejo de la Unión Europea, *Marco político de ciberdefensa de la UE (actualización de 2018), op. cit.* p. 25 (consultada a 19 de mayo de 2020).

[27] Parlamento Europeo y Consejo de la Unión Europea, *Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo de 17 de abril de 2019 relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) n.o 526/2013 («Reglamento sobre la Ciberseguridad»)*, p. 1, 2019, en https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32019R0881&from=ES (consultada a 27 de mayo de 2020).

[28] Consejo de la Unión Europea, *Marco político de ciberdefensa de la UE (actualización de 2018), op. cit.* p. 15 (consultada a 19 de mayo de 2020).

La nueva normativa[29] consta de 69 artículos, que se encuentran clasificados en cuatro títulos, a saber:

I. Disposiciones generales.
II. ENISA (Agencia de la Unión Europea para la Ciberseguridad).
III. Marco de Certificación de la Ciberseguridad.
IV. Disposiciones finales.

De esta forma, a modo de resumen, podemos establecer que el Reglamento introduce de un lado, un sistema de certificación común aplicable dentro del ámbito de la UE; de otro lado, una Agencia de la UE para la Ciberseguridad que reemplazará y mejorará a la anterior Agencia de Seguridad de las Redes y de la Información de la Unión Europea (ENISA).

3.2.1. Certificación común de la ciberseguridad

El Reglamento establece fórmulas de implementación de los sistemas europeos de certificación de la ciberseguridad de procesos, productos y servicios de TIC. Dichos certificados se distribuyen insertándose en los dispositivos conectados a Internet, entre los que pueden incluirse: juguetes conectados, pulseras, relojes y toda clase de accesorios inteligentes, teléfonos inteligentes, tabletas electrónicas, ordenadores, etc. Así, una vez que el certificado se expida correctamente, será legítimo en todos los Estados miembros de la UE, facilitando que los usuarios confíen en este tipo de tecnologías, y facilitando el avance de las actividades de las empresas a través de las fronteras.

Los esquemas de certificación se elaborarán sobre lo que ya existe en los ámbitos internacional, europeo y nacional y serán adoptados por la Comisión, mientras que de su aplicación y supervisión se encargarán las autoridades nacionales de certificación de la ciberseguridad. De esta forma, se intentará evitar la "multiplicación de los esquemas de certificaciones nacionales de la ciberseguridad contradictorias o redundantes" reduciendo, consecuentemente, "los costes para las empresas que operan en el mercado único digital".

Por último, cabe destacar que la certificación será voluntaria, salvo que se disponga otra cosa en el Derecho de la UE o en el de los Estados miembros. Por su parte, la Comisión observará

[29] Parlamento Europeo y Consejo de la Unión Europea, *Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo de 17 de abril de 2019 relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) n.o 526/2013 («Reglamento sobre la Ciberseguridad»), op. cit.,* pp. 32-67 (consultada a 27 de mayo de 2020).

con asiduidad el impacto que tienen los certificados y determinará en qué medida los proveedores de servicios y fabricantes hacen uso de estos. En cuanto a los niveles de seguridad, se clasifican en tres dependiendo del riesgo asociado a la previsión de uso de los productos.

3.2.2. Agencia de Ciberseguridad de la UE

La ENISA lleva contribuyendo a la seguridad de las redes y de la información de la UE desde 2004. Su mandato caducaba en junio de 2020 de manera que, de forma puntual, el nuevo Reglamento europeo de ciberseguridad convertirá a la ENISA en una Agencia de Ciberseguridad de la UE de forma permanente.

La Directiva SRI[30] -el primer precepto legal emanado de la UE para el ámbito de la seguridad cibernética- asignaba a la ENISA competencias suficientemente relevantes. Por ejemplo, la ENISA actuaba como oficina de administración del conjunto de equipos de respuesta a incidentes de seguridad informática (CSIRT) y apoyaba, de forma activa, la cooperación entre estos.

Ahora, entre las nuevas funciones que se asignan a la ENISA encontramos:

- Tareas de apoyo a los Estados miembros, a las instituciones de la UE y a otras partes interesadas en cuestiones cibernéticas.
- Funciones de soporte a la política de la UE sobre certificación de la ciberseguridad. Por ejemplo, preparando los esquemas de certificación.
- Cometidos relacionados con la aceptación del nuevo sistema de certificación. Por ejemplo, con la creación de un sitio web que facilite información sobre los certificados.
- Organización de ejercicios periódicos de ciberseguridad a nivel de la UE (entre ellos, un ejercicio general a gran escala cada dos años).
- Creación de una red de funcionarios de enlace nacionales en aras de facilitar el intercambio de información entre los Estados miembros.

[30] Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, *op. cit.* (consultada a 22 de mayo de 2020).

3.3. Análisis del régimen de sanciones impuestas a los ciberataques

En opinión de Robles Carrillo, las amenazas cibernéticas suponen un cambio en los arquetipos conocidos hasta el momento en cuanto que se encuentran totalmente deslocalizadas, están infravaloradas y poseen una naturaleza estructural. Éstas se manifiestan de forma singular mediante sus propias figuras ilícitas: la cibercriminalidad, el ciberespionaje, el ciberterrorismo y la ciberguerra; diferenciándose, así "de sus homólogas no virtuales y difuminándose los límites entre esas diversas categorías" (Robles Carillo, 2016, p. 1).

Tal y como establecen la Decisión del Consejo de 16 de mayo de 2019[31], el Consejo permite que la UE pueda imponer sanciones consistentes en medidas restrictivas concretas que permitan impedir y contrarrestar los ciberataques que constituyen una amenaza externa para la UE[32] o sus Estados miembros (así como para terceros Estados u organizaciones internacionales, en su caso[33]) y responder a ellos.

3.3.1. Ámbito de aplicación y definición de ciberataque constituyente de amenaza

El ámbito de aplicación de las medidas aparece en el artículo 1 apartado primero de la Decisión[34], y señala como objeto "los ciberataques con un efecto significativo, incluidas las tentativas con un efecto significativo potencial".

Por su parte, los apartados 2, 3 y 4 del mismo artículo establecen diferentes opciones acerca de qué ha de entenderse por ciberataque constituyente de amenaza externa. Un rasgo característico de éstos es el elemento de externalidad. Es decir, se originan y/o cometen desde el exterior de la Unión, o se sirven de infraestructuras o personas cuya actividad se ejerce fuera de la Unión.

---

[31] Consejo de la Unión Europea, *Decisión del Consejo relativa a medidas restrictivas contra los ciberataques que amenacen a la Unión o a sus Estados miembros*, 16 de mayo de 2019, en http://data.consilium.europa.eu/doc/document/ST-7299-2019-INIT/es/pdf (consultada a 24 de mayo de 2020).

[32] En el artículo 1.5 del marco se establece qué es un ciberataque constituyente de amenaza para la Unión: *Los cometidos contra sus instituciones, órganos y organismos, delegaciones en terceros países o ante organizaciones internacionales, sus operaciones y misiones de la PCSD y sus representantes especiales*.

[33] En El artículo 1.6 del marco se establece la cláusula de extensión a los terceros Estados u organizaciones internacionales: *cuando se estimen necesarias para el cumplimiento de los objetivos de la PESC […] podrán aplicarse medidas restrictivas […] a ciberataques que tengan un efecto significativo contra terceros Estados u organizaciones internacionales.*

[34] Consejo de la Unión Europea, *Decisión del Consejo relativa a medidas restrictivas contra los ciberataques que amenacen a la Unión o a sus Estados miembros*, *op, cit.* p.6.(consultada a 24 de mayo de 2020).

3.3.2. Sujetos pasivos del marco

De esta forma, los sujetos pasivos a los que se aplica el marco son, básicamente, personas (físicas o jurídicas) y Estados no pertenecientes a la UE, y organizaciones internacionales que hayan orquestado ciberataques cuando se considere que la aplicación de las medidas restrictivas es necesaria para lograr los objetivos PESC. En concreto, en los artículos 4 y 5, podemos observar que, por vez primera, la decisión permite que la UE sancione a personas o entidades, siempre que cumplan los siguientes requisitos para convertirse en sujetos pasivos:

a) Sean responsables de ciberataques o intentos de ciberataques.
b) Ofrezcan apoyo financiero, técnico o material para esos ataques, o estén implicadas de otras formas (por ejemplo, mediante la planificación, preparación, dirección o fomento).
c) Sean personas físicas o entidades asociadas a las anteriores.

3.3.3. Medidas restrictivas aplicables

La aplicación del principio de prohibición del uso de la fuerza en el ciberespacio tiene sentido en tanto que constituye "una norma básica para la coexistencia social en cualquier sistema jurídico", así como una norma imperativa vinculante para todos los Estados, de forma independiente a que el medio de actuación sea el espacio virtual o el físico. El traslado de este principio al ámbito del ciberespacio no se encuentra exento de problemas: de un lado, encontramos los denominados técnicos-jurídicos, que son aquellos "derivados de la dificultad de calificar una acción cibernética como uso o amenaza del uso de la fuerza armada"; de otro lado tenemos a los bautizados como político jurídicos, que son resultado de las diversas interpretaciones a que se ve sometido este principio, con el propósito eventual, de "eludir su prohibición o de subvertir las condiciones legítimas que permiten excepciones a dicho principio" (Robles Carillo, 2016, p.2).

Respecto a las medidas restrictivas que encontramos en la decisión del Consejo, podemos dividirlas en dos grupos:

a) Medidas restrictivas de la libre circulación. El régimen de estas medidas lo encontramos en el artículo 4: "Los Estados miembros adoptarán las medidas necesarias para impedir la entrada o tránsito por sus territorios de las personas físicas" definidas anteriormente como sujetos pasivos.

b) Medidas de inmovilización de fondos y recursos económicos relacionados con ciberataques y que se encuentren bajo la soberanía de algún Estado miembro. El régimen de estas medidas lo encontramos el artículo 5. En concreto, el artículo establece que "serán inmovilizados todos los fondos y recursos económicos cuya propiedad, titularidad, tenencia o control correspondan a las personas físicas o jurídicas, entidades u organismos" definidas anteriormente como sujetos pasivos.

3.3.4. Otras consideraciones a tener en cuenta

Cabe destacar que no han de confundirse las medidas restrictivas específicas del marco con la imputación de responsabilidad por los ciberataques a un tercer Estado. La aplicación de las medidas restrictivas no implica tal imputación. Es decir, la imputación de ciberataques a un tercer Estado constituye una decisión política soberana casuística, en la que cada Estado miembro es libre de adoptar su propia determinación.

3.4. Últimas preocupaciones de la UE

Las Conclusiones del Consejo europeo de 3 de diciembre de 2019[35] pusieron de manifiesto una de las principales preocupaciones de la UE en este ámbito. Así las cosas, en estas Conclusiones se hace referencia a la importancia de la tecnología 5G para la economía europea y a la necesidad de mitigar los riesgos de seguridad que van unidos a ella.

El Consejo reconoce que la tecnología 5G va a incrementar el potencial de los proveedores de servicios de redes móviles y va a brindar oportunidades de innovación en los modelos de negocio de múltiples sectores, así como para los ciudadanos europeos, los operadores de telecomunicaciones, las compañías (incluyendo a las pymes), el sector público y otras partes interesadas.

Cabe destacar que la Unión ha desarrollado un marco legal para abordar y mitigar los riesgos de ciberseguridad vinculados a la tecnología 5G como, por ejemplo, la Directiva (EU) 2018/1972 del Parlamento Europeo y del Consejo de 11 de diciembre de 2018 que establece el Código Europeo de Comunicaciones Electrónicas (Código EECC), y la Directiva (EU)

[35] Consejo de la Unión Europea, *Council Conclusions on the significance of 5G to the European Economy and the need to mitigate security risks linked to 5G*, 3 de diciembre de 2019, en https://www.consilium.europa.eu/media/41595/st14517-en19.pdf (consultada a 26 de mayo de 2020). Traducción propia de la fuente.

2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016, que establece medidas para un nivel común elevado de seguridad de las redes y los sistemas de información en toda la Unión (Directiva NIS).

A pesar de la buena intención por parte de la UE, hay autores que han criticado ciertos aspectos de las Directivas. Así las cosas, en opinión de Robles Carrillo, a la Directiva NIS le falta transparencia, complejidad y razonabilidad, además de carecer de un enforque integral. La directiva ofrece un enfoque sectorializado que "conduce a que la normativa aplicable" dependa del tipo de servicio ofertado, en lugar de la titularidad de este, "de manera que un mismo sujeto, incluidas las administraciones, habrá de adaptarse respecto de la misma materia […] a regímenes normativos diferentes determinados en función del tipo de servicio prestado en cada caso" (Robles Carrillo, 2018, p. 598).

Las Conclusiones destacan que las redes 5G formarán parte de una infraestructura crucial para el mantenimiento de funciones sociales y económicas fundamentales, incluyendo su transformación digital, del mismo modo que subraya la importancia de la soberanía tecnológica europea. Por otra parte, establecen que el rápido despliegue de las redes 5G constituye un activo clave para la competitividad europea, la sostenibilidad y el desarrollo de servicios digitales futuros.

En relación a las zonas limítrofes entre los Estados miembros, las Conclusiones destacan cuán importante resulta la cooperación entre estos para una implementación efectiva de las redes 5G.

Asimismo, el Consejo respalda los resultados de la evaluación de riesgos de la tecnología 5G a escala europea, publicada en octubre por el grupo de coordinación de los Estados miembros sobre la seguridad de las redes y de la información.

Respecto al planteamiento europeo sobre la seguridad de la red 5G, las Conclusiones establecen que este debe hacerse desde una perspectiva global y estar basado en el riesgo. La seguridad de la tecnología 5G se considera un proceso continuo, que comienza con la selección de los proveedores y se mantiene a lo largo de toda la producción de los elementos de la red y de la vida útil de esta.

Debido a los cambios tecnológicos introducidos por el 5G, el perfil de riesgo de los proveedores de tecnología va a ser los suficientemente relevante como para tenerlo en consideración a la hora de seleccionarlos individualmente. Las Conclusiones destacan la importancia de no limitar el número de los proveedores a uno porque, en caso de que exista

algún fallo técnico, los riesgos y consecuencias van a ser mayores que si, por el contrario, se cuenta con varios proveedores de tecnología 5G diversificando, de este modo, los riesgos inherentes a dichos suministradores. En adición, los factores no técnicos también deben tenerse en cuenta a la hora de elaborar el perfil de riesgo de un proveedor. Y, en opinión del Consejo, los componentes fundamentales para la Seguridad Nacional -energía, sanidad, agricultura, finanzas y transportes- solo deben proceder de proveedores fiables.

4. EVOLUCIÓN DE LA CIBERSEGURIDAD EN ESPAÑA

Para España -al igual que le ocurre a la gran mayoría de países por la globalización- la ciberseguridad ocupa un papel fundamental dentro del conjunto de elementos que componen la seguridad a nivel nacional. De hecho, la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional[36], la considera como un ámbito de especial interés, atendiendo a los establecido en la Estrategia Nacional de Ciberseguridad de 2019, sobre la que hablaremos más adelante. En este apartado del trabajo vamos a analizar el conglomerado jurídico nacional que gravita alrededor de la ciberseguridad cibernética.

En primer lugar, de cara a determinar la normativa aplicable a todas las cuestiones jurídicas relacionadas con la seguridad cibernética, vamos a centrar nuestra atención en el Código de Derecho de la Ciberseguridad, publicado en el Boletín Oficial del Estado[37]. En el índice de este código encontramos toda una relación de normas aplicables perfectamente clasificadas[38]. Como puede observarse, el Código representa una mayúscula compilación de material legal aplicable a todas las cuestiones que circunvalan a la ciberseguridad nacional de España.

En segundo lugar, encontramos publicadas, igualmente en el Boletín Oficial del Estado, una serie de estrategias nacionales relacionadas con la ciberseguridad que se han venido desarrollando, perfeccionando y especificando a lo largo de los años y que nos resultan de interés. Vamos a ir analizándolas por orden cronológico, dado que así se puede entender mejor el propósito de cada una de ellas de forma individual, así como la evolución conjunta

---

[36] Boletín Oficial del Estado, *Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, 29 de septiembre de 2015*, en https://www.boe.es/buscar/pdf/2015/BOE-A-2015-10389-consolidado.pdf (consultada a 25/04/2020).

[37] Boletín Oficial del Estado, *Código de Derecho de la Ciberseguridad*, 2020, en https://www.boe.es/legislacion/codigos/codigo.php?id=173&nota=1&tab=2 (consultada a 27/04/2020).

[38] En el *Anexo 2. Sumario del Código de Derecho de la Ciberseguridad* podemos consultar todas las normas que el mismo contiene.

de las inquietudes nacionales en materia de seguridad cibernética y la forma de afrontarlas, estableciendo como límite inferior el año 2011.

4.1. La Estrategia Española de Seguridad de 2011

En primer lugar, la Estrategia Española de Seguridad de 2011 identifica a la ciberseguridad como uno de los apéndices de la Seguridad Nacional más importantes, en cuanto que constituye el "eje fundamental de nuestra sociedad y sistema económico"[39]. "Además, en ella se identifican por primera vez las ciberamenazas más comunes que tienen un origen ilícito, los ciberataques, incluido el espionaje" (Segura Serrano, 2017, p.522). En relación con lo dispuesto en el apartado 2 de este trabajo, recordemos que los ataques virtuales pueden emanar tanto de entes no gubernamentales organizados, como de los Estados[40].

Siguiendo a Segura Serrano, la Estrategia también hace referencia a los impedimentos legales para la gestión adecuada de las ciberamenazas, como pueden ser "la ausencia de una legislación común o de seguridad global" (Segura Serrano, 2017, p.523). En aras de suplir estas deficiencias, se fijan unas líneas de acción a desarrollar desde una perspectiva nacional, y otra internacional:

- La primera de ellas es la nacional, que se centra en reforzar la legislación y las capacidades[41].
- La segunda de ellas es la internacional, en la que se hace hincapié en la necesidad de cooperación entre los Estados para combatir las armas y la delincuencia cibernéticas. De forma más específica, para la UE, se establecen objetivos de mayor concreción y que requieren de un nivel superior de cooperación e integración por parte de los Estados, como son: el incremento de la armonización de normas penales en el ámbito europeo y el establecimiento de una acción coordinada en materia de ciberdefensa dentro del marco de la OTAN[42].

---

[39] Gobierno de España, *Estrategia Española de Seguridad: Una responsabilidad de todos*, Madrid, 2011, p.65, en https://www.cidob.org/es/publicaciones/serie_de_publicacion/monografias/monografias/la_estrategia_espanola_de_seguridad_ees_una_responsabilidad_de_todos (consultada el 27 de abril de 2020).

[40] En el *Anexo 1: El Caso de Edward Snowden. Un civil que destapó el ciberespionaje masivo acometido por algunos Estados contra sus ciudadanos y contra otros Estados* podemos comprobar como algunos Estados han llevado a cabo acciones ilícitas en el marco del ciberespacio.

[41] Gobierno de España, *Estrategia Española de Seguridad: Una responsabilidad de todos, op. cit.*, pp. 66-68 (consultada el 28 de abril de 2020).

[42] *Ibid.*, pp. 69-70.

4.2. La Estrategia de Seguridad Nacional de 2013

La Estrategia de Seguridad Nacional de 2013[43] se presenta en un documento que contiene cinco capítulos. En concreto, el primero presenta de manera general el entorno que rodea a la Seguridad Nacional, así como los cuatro principios informadores de la Estrategia (unidad de acción, anticipación y prevención, eficiencia y sostenibilidad en el uso de los recursos, resiliencia o capacidad de resistencia y recuperación)[44].

El segundo capítulo aborda la seguridad de España desde una perspectiva universalista. Establece que España ha de hacer frente a un "mundo globalizado, altamente competitivo y en continuo cambio, que presenta importantes riesgos y amenazas, pero también ofrece grandes oportunidades a una sociedad abierta, avanzada y formada como la española". Asimismo, se detallan cuáles son los entornos estratégicos para nuestro país. Esto es: la UE, el Mediterráneo, América Latina, Estados Unidos y la relación transatlántica, África, Asia, Australia y Rusia[45].

El tercer capítulo – que, junto con el cuarto, es el más interesante a la luz de este trabajo- se titula "Los riesgos y amenazas para la Seguridad Nacional" y contiene una lista de doce elementos. El tercero de ellos se denomina "Ciberamenazas" y en él se trata de determinar qué acciones son constitutivas de las mismas[46].

En esta Estrategia, a diferencia de lo que ocurría con la de 2011, encontramos una mejor definición tanto del ciberespacio, como de Internet. Se aclara que Internet es un entorno con ventajas (como, por ejemplo, la accesibilidad) e inconvenientes (como, por ejemplo, la ausencia de legislación) [47].

En el capítulo cuarto, dentro del establecimiento genérico de las líneas de acción estratégicas encontramos, en tercera posición, unas destinadas exclusivamente a la mejora de la ciberseguridad[48]. Estas son:

---

[43] Gobierno de España, *Estrategia de Seguridad Nacional: Un proyecto compartido*, Madrid, 2013, en https://www.lamoncloa.gob.es/documents/seguridad_1406connavegacionfinalaccesiblebpdf.pdf (consultada el 28 de abril de 2020).

[44] *Ibid*., pp. 5-9.

[45] *Ibid.*, pp. 10-20.

[46] *Ibid.*, pp. 26-27.

[47] *Ibid.*, p. 26.

[48] *Ibid.*, p. 42.

- Mejorar las capacidades de prevención, de detección, de investigación y de respuesta ante las ciberamenazas mediante el apoyo en un marco jurídico operativo y eficaz.
- Garantizar la seguridad de los sistemas de información y de las redes de comunicación e infraestructura comunes a todas las Administraciones Públicas.
- Mejorar la seguridad y la resiliencia de las TIC en el sector privado mediante la colaboración con los poderes públicos.
- Capacitar a profesionales en ciberseguridad e impulsor a la industria española a través de un Plan de I+D+i.
- Implantar una cultura de ciberseguridad sólida.
- Promover la colaboración internacional.

Por último, el capítulo número cinco de la Estrategia de Seguridad Nacional detalla el nuevo Sistema de Seguridad Nacional, estableciendo su estructura, así como los principios y objetivos principales.

4.3. La Estrategia de Ciberseguridad Nacional de 2013

La Estrategia de Ciberseguridad Nacional de 2013[49] es el primer texto normativo aprobado por la Presidencia del Gobierno con voluntad de establecer una política de Estado en el entorno de la ciberseguridad.

Al igual que su homónimo en el ámbito de la Seguridad Nacional (la Estrategia de Seguridad Nacional de 2013) dispone de cinco capítulos en los que trata, en primer lugar, el ciberespacio y su seguridad, estableciendo las características de los ciberataques y los riesgos y amenazas a la Ciberseguridad nacional provenientes del ciberespacio[50].

Seguidamente, establece los propósitos y principios rectores que han de guiar a la ciberseguridad en España, que han de respetar, en su conjunto, los derechos fundamentales de la Constitución española y los instrumentos internacionales que resulten de aplicación, en su caso (Declaración Universal de los Derechos Humanos, Pacto Internacional de Derechos Civiles y Políticos y Convenio Europeo de los Derechos Humanos). Estos son: liderazgo nacional y coordinación de esfuerzos; responsabilidad compartida entre todos los agentes

[49] Gobierno de España, Presidencia del Gobierno, *Estrategia de Ciberseguridad Nacional*, Madrid, 2013, en https://www.dsn.gob.es/es/file/146/download?token=Kl839vHG (consultada el 28 de abril de 2020).

[50] *Ibid.*, pp. 8-11.

públicos, privados y los ciudadanos; proporcionalidad racionalidad y eficacia; y cooperación internacional[51].

En el tercer capítulo se establecen los objetivos de la Estrategia, los cuales son prácticamente iguales que las líneas de acción vistas en la Estrategia de Seguridad Nacional de 2013 en el apartado precedente. Vemos que los objetivos de la ciberseguridad se compilan en un objetivo global: que España use de forma segura los Sistemas de Información y Telecomunicaciones (en adelante, SIT), fortaleciendo la prevención, defensa, detección y respuesta a los ciberataques; y en seis objetivos específicos[52]:

a) Garantizar que las Administraciones Públicas sean ciberseguras y resilientes.
b) Mejorar la seguridad y resiliencia de los SIT usados por las empresas, en general, y por los operadores de infraestructuras críticas, en particular.
c) Potenciar la prevención, detección, reacción, análisis, recuperación, respuesta, investigación y coordinación frente al terrorismo y la delincuencia cibernéticos.
d) Sensibilizar a los ciudadanos, profesionales, empresas y Administraciones Públicas españolas de los riesgos derivados del ciberespacio.
e) Alcanzar y mantener los conocimientos, habilidades, experiencia y capacidades tecnológicas que necesita España para sustentar todos los objetivos de ciberseguridad.
f) Contribuir a la mejora de la ciberseguridad en el ámbito internacional. Este objetivo constituye un sistema de retroalimentación y sustento para el resto.

En el penúltimo capítulo se establecen las "Líneas de acción de la ciberseguridad nacional"[53], que suponen un conjunto de medidas concretas a desarrollar para alcanzar los objetivos precedentes. Tal y como establece Segura Serrano, "la Estrategia prevé el desarrollo de una serie de medidas" de corte internacionalista para los próximos años. En concreto: la intención de potenciar la presencia de España en organizaciones y foros internacionales; la promoción de la armonización legislativa y de la cooperación judicial y policial internacionales contra los delitos cibernéticos -incluido el terrorismo-, apoyando la adopción de convenios internacionales; la propiciación de la suscripción de acuerdos en el seno de organizaciones internacionales y con los principales socios y aliados, para reforzar

[51] *Ibid.,* pp. 15-17.

[52] *Ibid.,* pp. 21-28.

[53] *Ibid.,* pp. 31-40.

la cooperación; y la colaboración especial con la UE (para la Estrategia de Ciberseguridad de la UE) y la OTAN (para la ciberdefensa). (Segura Serrano, 2017, pp. 526-527). En apartados ulteriores comprobaremos que dichos pronósticos fueron acertados de forma mayoritaria.

Por último, el quinto capítulo establece el conglomerado legal mediante la que se inserta la ciberseguridad en el Sistema de Seguridad Nacional[54].

4.4. La Estrategia de Seguridad Nacional de 2017

Por su parte, la Estrategia de Seguridad Nacional de 2017[55] viene a sustituir la Estrategia de Seguridad Nacional de 2013, de manera que hereda gran parte del contenido de esta. Lo que hace es profundizar en algunos conceptos y líneas de acción definidos ya en 2013 y, adapta dicha Política a los nuevos y constantes cambios y desarrollos que se han producido en materia de seguridad. En concreto, de todo su texto normativo se desprende una gran innovación: la ciberseguridad es un terreno que tiene la suficiente transcendencia como para ocupar un espacio sustantivo y diferencial no solo en las estrategias españolas, sino en cualquier estrategia de seguridad nacional.

Los principios rectores que bautizan a la Estrategia de 2017 son la unidad de acción, la anticipación, la eficiencia y la resiliencia, así como una gran preocupación por la ciberseguridad. Esto es por lo que podemos establecer que, a pesar de actualizar el contenido de la Estrategia de 2013, su esencia no cambia. Como diferencia, el entorno de seguridad es aún más ambiguo, complejo, volátil e incierto que el de 2013 debido a que las dinámicas mundiales han seguido evolucionando a un ritmo frenético, intensificándose, en consecuencia, las incertidumbres en el ámbito de la geopolítica y de la tecnología.

Con la intención de actualizar la anterior Estrategia, encontramos las "Dinámicas de transformación de la seguridad global" en el segundo capítulo, que tienen por objeto analizar los cambios y tendencias que se han hecho más marcadas desde la publicación de la Estrategia de 2013[56].

---

[54] *Ibid.*, pp. 42-45.

[55] Boletín Oficial del Estado, *Real Decreto 1008/2017, de 1 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2017*, 2017, en https://www.boe.es/boe/dias/2017/12/21/pdfs/BOE-A-2017-15181.pdf (consultada a 28 de abril de 2020).

[56] *Ibid*. p. 125.969.

Por otro lado, en la Estrategia de 2017 se establecen algunos objetivos generales[57] para alcanzar la Seguridad Nacional como, por ejemplo: fomentar la prevención y anticipación con la ayuda de los sistemas de inteligencia e información -entre otros-; promover una cultura de seguridad nacional para los ciudadanos -entre otras-; favorecer el buen uso de los espacios comunes globales, entre los que se encuentran el ciberespacio; y fomentar que el desarrollo tecnológico y la innovación cumplan con estándares de seguridad.

Al igual que la Estrategia de 2013, en la nueva Estrategia también aparecen líneas de acción estratégicas[58], entre las que encontramos medidas específicamente destinadas a la mejora de la ciberseguridad. A pesar de que todas contienen, aunque sea indirectamente, medidas relacionadas con la ciberseguridad, a continuación solamente vamos a mencionar aquellas que, de forma directa, hacen referencia a preceptos del ámbito de la seguridad informática:

a) Defensa nacional: "dotar a las Fuerzas Armadas de las capacidades que demanda el actual escenario de seguridad".[59]
b) Lucha contra el terrorismo: "mejorar las capacidades de investigación e inteligencia, asegurar el desarrollo tecnológico de los servicios de inteligencia e información para hacer frente al uso intensivo de las nuevas tecnologías por parte de los grupos terroristas e impedir el acceso a las capacidades materiales necesarios para cometer atentados".
c) Lucha contra el crimen organizado: "mantener canales abiertos de formación continua en los métodos y herramientas utilizados por las organizaciones criminales"[60].
d) No proliferación de armas de destrucción masiva: "lucha contra el tráfico ilícito de materiales y tecnologías relacionadas con las armas de destrucción masiva y sus vectores de lanzamiento".
e) Contrainteligencia: "intensificar las actividades de contrainteligencia del ciberespacio".
f) Seguridad marítima: "mejorar la ciberseguridad en el ámbito marítimo".

[57] *Ibid*. pp. 125.990-125.991.
[58] *Ibid.,* pp. 125.992-126.003.

[59] El actual escenario de seguridad está fuertemente teñido por la tecnología de la información y la comunicación. Por ello, entre las dotaciones necesarias para las Fuerzas Armadas se encuentran los sistemas de seguridad cibernéticos.

[60] Actualmente, hay muchas organizaciones criminales especializadas la comisión de delitos cibernéticos.

g) Seguridad del espacio aéreo y ultraterrestre: "perseverar en el análisis de riesgos y evaluación de medidas contra ciberataques u otros conflictos que afecten a las instalaciones aeroportuarias, o al transporte aéreo dentro fuera del espacio aéreo español".
h) Protección de las infraestructuras críticas: "promover la coordinación en materia de protección de infraestructuras críticas, lucha contra el terrorismo y ciberseguridad entre todas las organizaciones responsables, mejorando las capacidades de todas ellas; favorecer la innovación en seguridad, equipando progresivamente las infraestructuras críticas de sistemas y componentes de seguridad".
i) Seguridad energética: "reforzar la seguridad integral de las infraestructuras del sector energético y, en particular, de aquellas consideradas críticas, frente a las amenazas físicas y cibernéticas que puedan poner las en grave riesgo".

De acuerdo con estas líneas de acción, la Estrategia contiene unos objetivos específicos[61] para la ciberseguridad, a saber:

- Reforzar las capacidades de prevención, detección, reacción, análisis, recuperación, respuesta investigación frente a las ciberamenazas, así como potenciar la coordinación en los niveles técnico y estratégico del Sistema de Seguridad Nacional en el ámbito de la ciberseguridad.
- Reforzar, impulsar y promover los mecanismos normativos, organizativos y técnicos, así como la aplicación de medidas, servicios, buenas prácticas y planes de continuidad para la protección, seguridad y resiliencia en el Sector Público, los sectores estratégicos (especialmente las infraestructuras críticas y servicios esenciales), el sector empresarial y la ciudadanía, de manera que se garantice un entorno digital seguro y fiable.
- Reforzar y mejorar las estructuras de cooperación público-público y público-privada nacionales en materia de ciberseguridad.
- Alcanzar las capacidades tecnológicas necesarias mediante el impulso de la industria española de ciberseguridad, promoviendo un entorno que favorezca la investigación, el desarrollo y la innovación, así como la participación del mundo académico.

[61] Boletín Oficial del Estado, *Real Decreto 1008/2017, de 1 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2017,* 2017, *op. cit.,* pp. 125.992-126.003.

- Promover el alcance y mantenimiento de los conocimientos, habilidades, experiencia, así como capacidades tecnológicas y profesionales que necesita España para sustentar los objetivos de la ciberseguridad.
- Contribuir a la seguridad del ciberespacio (en el ámbito de la UE e internacional) en defensa de los intereses nacionales, fomentando la cooperación y el cumplimiento del Derecho Internacional.

Por último, en cuanto a las nuevas iniciativas según los objetivos generales para la Seguridad Nacional, podemos destacar varias en relación con el ámbito de la seguridad cibernética: en primer lugar, se va a adaptar el marco estratégico sectorial de los espacios comunes a la nueva Estrategia de Seguridad Nacional, hecho que implica la revisión de las Estrategias de Seguridad Marítima Nacional y de Ciberseguridad Nacional, tal y como veremos en el siguiente apartado del trabajo, en el que vamos a estudiar la Estrategia Nacional de Ciberseguridad de 2019. En segundo lugar, con objeto de que el desarrollo tecnológico incorpore la dimensión de seguridad, el Consejo de Seguridad Nacional será el único punto de contacto en el ámbito de la seguridad de las redes y sistemas de información con las autoridades competentes de otros Estados miembros de la UE[62].

4.5. La Estrategia Nacional de Ciberseguridad de 2019 como actualización de la Estrategia de 2013

Como ya hemos comentado, en 2013 se aprobó por primera vez en España la Estrategia Nacional de Seguridad. Esta fijó las directrices para hacer frente al desafío que suponía -y supone- la vulnerabilidad del ciberespacio y diseñó el modelo de gobernanza para la ciberseguridad nacional. Durante estos años, España ha mantenido sus esfuerzos para lograr un ciberespacio seguro y fiable.

Por otra parte, cabe destacar que, en 2014, se crea el Consejo Nacional de Ciberseguridad, órgano de apoyo del Consejo de Seguridad Nacional, que ha asumido las tareas de coordinar a los organismos con competencia en la materia a nivel nacional y desarrollar del Plan Nacional de Ciberseguridad y sus planes derivados.

[62] *Ibid.,* p. 126.004.

Cinco años más tarde se aprueba la Estrategia Nacional de Ciberseguridad de 2019[63], cuyo objeto es desarrollar "las previsiones de la Estrategia de Seguridad Nacional de 2017 en el ámbito de la ciberseguridad, considerando los objetivos generales, el objetivo del ámbito y las líneas de acción establecidas para conseguirlo"[64].

La Estrategia se estructura en cinco capítulos[65]. Con la intención de realizar un estudio pormenorizado de esta Estrategia, vamos a ir analizándola capítulo a capítulo y deteniéndonos en los puntos que más interesen, a la luz de este trabajo.

a) El ciberespacio como espacio común global

De este modo, el primer capítulo, denominado *El ciberespacio como espacio común global*, ofrece una visión en conjunto del ámbito de la ciberseguridad, los avances que han tenido lugar desde la aprobación de la Estrategia 2013, y las razones principales que propulsan la elaboración de la Estrategia Nacional de Ciberseguridad de 2019.

Este capítulo comienza definiendo qué ha de entenderse por ciberespacio y estableciendo que este presenta tanto oportunidades, como desafíos. Continúa hablando de la infraestructura digital, en la que las redes y sistemas de información están expuestos a fallos intrínsecos y extrínsecos (como pueden ser las acciones deliberadas con fines malintencionados), que pueden poner en riesgo el funcionamiento de las infraestructuras críticas y de los servicios esenciales que dependen de los sistemas y redes digitales asociadas. Atendiendo a esto, y con el fin de garantizar la permanencia de la Seguridad Nacional y la creación de una sociedad digital basada en la confianza, cobra sentido que, en el plano internacional, la ciberseguridad se haya convertido en el principal objetivo de todas las agendas de los gobiernos.

En este contexto, España apuesta por un ciberespacio que sea abierto, plural y seguro. Permanece colaborando de forma activa en aquellas instituciones en la que la ciberseguridad ocupa un lugar destacado (como hemos visto, la UE, la Alianza Atlántica y de Naciones Unidas) y mantiene vínculos bilaterales con terceros Estados orientados a conseguir relaciones fluidas en el ámbito de la ciberseguridad.

---

[63] Boletín Oficial del Estado. *Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional*, 2019, en https://www.boe.es/buscar/pdf/2019/BOE-A-2019-6347-consolidado.pdf (consultada a 23 de abril de 2020).

[64] *Ibid*. p. 2.

[65] *Ibid.* pp. 4-18.

En la nueva concepción del ciberespacio que establece la Estrategia, se deben potenciar las capacidades de ciberdefensa; ha de emplearse la ciberinteligencia como herramienta ciberdefensiva; y la sociedad, en general, debe implicarse más mediante el fomento de una cultura de ciberseguridad.

b) Las amenazas y desafíos en el ciberespacio

Para paliar la ciberamenazas, la Estrategia propone incrementar la prevención, detección y respuesta, y aumentar la seguridad tanto en el desarrollo de productos y servicios tecnológicos, como en sus actualizaciones o formas de uso.

Dentro de las actividades ilegales que emplean el ciberespacio como medio, se incluyen el ciberespionaje y la cibercriminalidad. La Estrategia evidencia la existencia de diferentes actores -tanto estatales, como no estatales; bien de forma directa, o bien indirecta- que aprovechan las facilidades que ofrece Internet para realizar actividades de desinformación y propaganda. A este respecto, la Estrategia constata que el uso con malas intenciones de los datos personales y las campañas de desinformación tienen una elevada capacidad desestabilizadora en la sociedad y, por ello, las naciones deberán dedicar esfuerzos para paliar estas acciones.

Por otro lado, la Estrategia advierte de que las campañas de desinformación se sirven de elementos como las *fake news* para influir en la opinión pública. Así, se erige un arma intangible muy peligrosa que amplifica sus efectos y alcance mediante Internet y las redes sociales. Su posible mal uso puede dirigirse contra organizaciones internacionales, Estados, iniciativas políticas, personajes públicos o, incluso, procesos electorales democráticos. De ahí su elevada peligrosidad.

c) Propósito, principios y objetivos para la ciberseguridad

Tal y como hemos comentado en la introducción de este apartado, el objetivo general de la Estrategia Nacional de Ciberseguridad 2019 es fijar unas directrices generales en el ámbito de la ciberseguridad, de manera que se alcancen los objetivos establecidos en la Estrategia de Seguridad Nacional de 2017.

Para alcanzar este propósito, España ha de continuar reforzando las capacidades de que dispone para hacer frente a las ciberamenazas. Para contar con una sociedad más preparada frente a las amenazas y desafíos a los que se enfrenta España, es imprescindible fomentar la cultura de ciberseguridad. Asimismo, la ciberseguridad supone, para cualquier nación,

progresar y, por ello, la Estrategia decreta que se ha de impulsar la industria española de ciberseguridad, así como promocionarse la I+D+i nacionales.

Por otro lado, resulta imprescindible que España coopere y cumpla con el Derecho Internacional, respetando los principios recogidos en la Constitución y en la Carta de Naciones Unidas, sin perjuicio de la Estrategia de Seguridad Nacional.

En cuanto a los principios rectores de la Estrategia, son los mismos que orientan a la Seguridad Nacional: unidad de acción, anticipación, eficiencia y resiliencia. Para alcanzar el objetivo general anteriormente mencionado, la Estrategia señala una serie de objetivos específicos[66] cuyo fin es contribuir a alcanzarlo. Son los siguientes:

- Objetivo I. Seguridad y resiliencia de las redes y los sistemas de información y comunicaciones del sector público y de los servicios esenciales.
- Objetivo II. Uso seguro y fiable del ciberespacio frente a su uso ilícito malicioso.
- Objetivo III. Protección del ecosistema empresarial y social y de los ciudadanos.
- Objetivo IV. Cultura y compromiso con la ciberseguridad y potenciación de las capacidades humanas y tecnológicas.
- Objetivo V. Seguridad del ciberespacio en el ámbito internacional.

d) Líneas de acción y medidas

En el cuarto capítulo, como bien puede observarse en el título, se recogen unas líneas de acción para alcanzar los objetivos establecidos en el subapartado anterior, con las concretas y respectivas medidas para alcanzarlos[67]. Para evitar una excesiva extensión del trabajo, me voy a limitar a mencionar las líneas de acción y a señalar el objetivo específico con el que está vinculada:

1. Reforzar las capacidades ante las amenazas provenientes del ciberespacio. La línea se corresponde con el Objetivo I de la Estrategia.
2. Garantizar la seguridad y resiliencia de los activos estratégicos para España. La línea se corresponde con el Objetivo I de la Estrategia.
3. Reforzar las capacidades de investigación y persecución de la cibercriminalidad, para garantizar la seguridad ciudadana y la protección de los derechos y libertades en el ciberespacio. La línea se corresponde con el Objetivo II de la Estrategia.

[66] *Ibid*. pp. 9-12.

[67] *Ibid*. pp. 12-16.

4. Impulsar la ciberseguridad de ciudadanos y empresas. La línea se corresponde con el Objetivo III de la Estrategia.
5. Potenciar la industria española de ciberseguridad, y la generación y retención de talento, para el fortalecimiento de la autonomía digital. La línea se corresponde con el Objetivo IV de la Estrategia.
6. Contribuir a la seguridad del ciberespacio en el ámbito internacional, promoviendo un ciber espacio abierto, plural, seguro y confiable, en apoyo de los intereses nacionales. La línea se corresponde con el Objetivo V de la Estrategia.
7. Desarrollar una cultura de ciberseguridad. La línea se corresponde con el Objetivo IV de la Estrategia.

e) La ciberseguridad en el Sistema de Seguridad Nacional

Por último, el capítulo 5 establece la integración de la ciberseguridad en el actual Sistema de Seguridad Nacional. Los componentes de la estructura de ciberseguridad[68] en el marco del Sistema de Seguridad Nacional son:

1. El Consejo de Seguridad Nacional.
2. El Comité de Situación, único para el conjunto del sistema de seguridad nacional ante situaciones de crisis.
3. El Consejo Nacional de Ciberseguridad.
4. La Comisión Permanente de Ciberseguridad.
5. El Foro Nacional de Ciberseguridad.
6. Las autoridades públicas competentes y los CSIRT de referencias nacionales.

5. COMPARACIÓN DE LAS ESTRATEGIAS ESPAÑOLAS EN MATERIA DE SEGURIDAD CON LAS DE OTROS ESTADOS EUROPEOS: FRANCIA Y ALEMANIA

Dentro del entorno europeo, dos de los países más desarrollados y ejemplares son Alemania y Francia. De hecho, ocupan los puestos 4º y 26º dentro del ranking global del Índice de Desarrollo Humano (United Nations Development Programme, 2019), respectivamente. Además, en ambos sistemas jurídicos encontramos numerosas semejanzas con el sistema español. Por estas razones, he escogido a Francia y Alemania con la intención de comparar sus estrategias de seguridad con las recientemente analizadas.

[68] *Ibid*. p. 16.

5.1. Francia

El respaldo normativo de la ciberseguridad en Francia se encuentra en dos cuerpos legales: el *Libro Blanco sobre la Seguridad y la Defensa Nacional de 2013*[69] y la *Estrategia nacional para la seguridad digital de 2015*[70].

En primer lugar, el Libro Blanco de 2013 no es un texto normativo genuino, sino que nace como actualización[71] del Libro Blanco de 2008[72]. En el se establecen, en primer lugar, las novedades que presenta el panorama estratégico, estableciendo que Francia es una potencia europea con influencia global quizás, en parte, porque forma parte de un de un todo político: la Unión Europea. A diferencia de la mayoría de países del mundo, Francia se encuentra en usa situación excepcional de paz y estabilidad con todos los países que la rodean[73].

En el segundo de los capítulos del Libro Blanco encontramos los fundamentos de la Estrategia de defensa y seguridad nacional. Y llama mucho la atención que, a diferencia de lo que ocurre con las Estrategias española o alemana, la francesa establece la "preservación de la independencia y soberanía", así como "garantizar la legitimidad de sus acciones a nivel nacional e internacional"[74]. Francia hace hincapié, así, en la importancia que supone para ella el concepto de soberanía y de nación.

En los capítulos sucesivos, la Estrategia expone, en orden de aparición: el estado del mundo; las prioridades estratégicas; el compromiso de Francia con la OTAN y con la UE; la implementación de la Estrategia; y los medios de la Estrategia.

---

[69] République Française, Président de la République, *Livre blanc sur la défense et la sécurité nationale*, 2013, en: https://fr.calameo.com/read/000331627d6f04ea4fe0e (consultado a 1 de junio de 2020) (Traducción propia).

[70] République Française, Premier Ministre, *Estrategia nacional francesa para la seguridad del ámbito digital*, 2015, en: https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_es.pdf (consultado a 1 de junio de 2020).

[71] République Française, Président de la République, *Livre blanc sur la défense et la sécurité nationale*, 2013, *op. cit.*, p. 7.

[72] République Française, Président de la République, *Défense et Sécurité nationale: Le Livre Blanc*, 2008, en: https://www.vie-publique.fr/sites/default/files/rapport/pdf/084000341.pdf (consultado a 1 de junio de 2020).

[73] République Française, Président de la République, *Livre blanc sur la défense et la sécurité nationale*, 2013, *op. cit.*, p. 13.

[74] *Ibid*., pp. 19-27.

Posteriormente, en 2015, como ya hemos señalado anteriormente, Francia publica la *Estrategia nacional para la seguridad del ámbito digital*[75] actualizando, de esta manera, la Estrategia precedente: la de 2010. Su estructura consta de cinco objetivos, a saber:

a) "Intereses fundamentales, defensa y seguridad de los sistemas de información del Estado y de las infraestructuras críticas, crisis informática mayor".

Este objetivo pretende avalar la seguridad de las infraestructuras críticas y de los operadores esenciales de la economía francesa y garantizar los intereses fundamentales de la nación. Sobre todo, en caso de que tenga lugar un ataque informático grave[76].

b) "Confianza digital, vida privada, datos personales, ciberataques".

Mediante este objetivo, Francia va a desarrollar, de acuerdo con sus valores, un uso del ciberespacio en el que protegerá la vida virtual de sus ciudadanos. Dentro de la vida digital de los ciudadanos, cobran especial relevancia los datos personales de estos que viajan por Internet. Además, a través del objetivo Francia incrementará su lucha contra la ciberdelincuencia y la prestación de asistencia a las víctimas de ciberataques[77].

c) "Sensibilización, formaciones iniciales, formaciones continuas".

A través del tercer objetivo, Francia "promoverá desde la escuela la sensibilización sobre la seguridad digital y los comportamientos responsables en el ciberespacio. Las formaciones iniciales superiores y continuas incorporarán un componente dedicado a la seguridad digital adaptado al sector correspondiente"[78].

d) "Entorno de las empresas del sector digital, política industrial, exportación e internacionalización".

El cuarto objetivo establece la necesidad de desarrollar un "ecosistema favorable a la investigación y a la innovación" para convertir a la seguridad digital en un factor de competitividad. Así, se fomentará el desarrollo interno de la economía y la promoción internacional de los productos y servicios digitales franceses[79].

---

[75] République Française, Premier Ministre, *Estrategia nacional francesa para la seguridad del ámbito digital*, 2015, *op. cit.*

[76] *Ibid*., pp. 13-17.

[77] *Ibid*., pp. 21-23.

[78] *Ibid.,* p. 26.

[79] *Ibid.,* p. 31.

e) "Europa, soberanía digital, estabilidad del ciberespacio".

El último de los objetivos estratégicos persigue que Francia sea, junto con aquellos Estados miembros que potestativamente así lo decidan, "el motor de una soberanía digital europea". Para alcanzar esta meta, reforzará su presencia e influencia en las discusiones internacionales sobre ciberseguridad y "desempeñará un papel activo en la promoción de un ciberespacio seguro, estable y abierto". Asimismo, este objetivo es más ambicioso y busca instaurar y conservar un espacio cibernético estable y seguro, que respete los derechos fundamentales[80].

5.2. Alemania

Al igual que ocurre con Francia, la estrategia política alemana en materia de seguridad se encuentra, sin perjuicio de las disposiciones de la UE, en el *Libro Blanco de Seguridad*, que nació en 1970 con el nombre de *Libro Blanco de la Defensa Alemán*[81] y que ha sufrido constantes reajustes hasta nuestros días.

La última actualización que se le realizó fue en 2016 dando lugar, de esta manera, al *Libro Blanco de la Defensa de 2016*[82]. En concreto, el documento se divide en dos partes: la primera, que se dedica a explicar la política de seguridad, consta de cuatro bloques: 1. Los elementos clave de la política de seguridad alemana; 2. El entorno de la seguridad alemana; 3. Las prioridades estratégicas alemanas; 4. Las áreas clave en el compromiso de la política de seguridad alemana. La segunda parte, dedicada al futuro de las Fuerzas Armadas, de forma análoga, se distribuye en cuatro bloques también: 5. Las Fuerzas Armadas del futuro-Misiones y tareas en un entorno de seguridad cambiante; 6. Principios guía para las Fuerzas Armadas del futuro; 7. Líneas de orientación para las Fuerzas Armadas; 8. Preparando a las Fuerzas Armadas para el futuro.

---

[80] *Ibid.*, pp. 37-40.

[81] Ministerio de Defensa Español (Centro de Documentación), *Libro Blanco Alemán 1970, acerca de la seguridad de la República Federal de Alemania y de la situación de las fuerzas armadas federales*, 1970, en https://dialnet.unirioja.es/descarga/articulo/4771880.pdf (consultado a 31 de mayo de 2020).

[82] Federal Ministry of Defence, *White Paper 2016 on Germany Security Policy and the future of the Bundeswehr*, 2016, en: https://www.dsn.gob.es/sites/dsn/files/2016_German_WhitePaper_SecurityPolicy_13jul2016.pdf (consultado a 31 de mayo de 2020) (Traducción propia).

De forma accesoria al Libro Blanco, en 2011, el Gobierno alemán, a través del Ministerio de Defensa, publica unas *Directrices de Política de Defensa*[83] en un documento muy reducido: apenas alcanza a las 17 páginas. Estas establecen el marco estratégico[84] para llevar a cabo las misiones y las tareas de las Fuerzas Armadas.

También publica en 2011, en este caso a través del Ministerio del Interior, la *Estrategia de Ciberseguridad para Alemania*[85]. Entre los principios básicos de la Estrategia se insiste, nuevamente, en lo importante que resulta la cooperación y coordinación internacional entre los Estados[86]. En la Estrategia se establecen diez objetivos y medidas[87], que coinciden o son muy similares a los establecidos en la Estrategia española de Ciberseguridad de 2019[88]:

a) Protección de las infraestructuras críticas de información.
b) Seguridad de los sistemas de infraestructura tecnológica alemanes.
c) Fortalecimiento de la seguridad de las infraestructuras tecnológicas en la Administración Pública.
d) Centro Nacional de Ciber Respuesta.
e) Consejo Nacional de Ciberseguridad.
f) Control efectivo del crimen en el ciberespacio.
g) Acción coordinada efectiva para asegurar la ciberseguridad tanto en Europa, como en todo el mundo.
h) Uso de tecnologías de la información confiables y fidedignas.
i) Desarrollo del personal de las autoridades federales.
j) Herramientas de respuesta a ciberataques.

---

[83] German Ministry of Defence, *Defence Policy Guidelines: Safeguarding National Interests, Assuming International Responsibility, Shaping Security Together*, 2011, en: https://www.bmvg.de/resource/blob/16136/0c1b6d8d0c0e6ba0aed5f0feb0af81d8/g-03-110527-vpr-engl-data.pdf (consultado a 1 de junio de 2020) (Traducción propia).

[84] *Ibid.*, p. 1.

[85] Federal Ministry of the Interior, Cyber Security Strategy for Germany, 2011, en: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-for-germany/view (consultado a 1 de junio de 2020) (Traducción propia).

[86] *Ibid.*, p. 5.

[87] *Ibid.*, pp. 6-12.

[88] Boletín Oficial del Estado, *Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional*, *op. cit.* (consultada a 1 de junio de 2020).

CONCLUSIONES

A lo largo del todo el trabajo ha quedado patente la importancia que la ciberseguridad ocupa en la vida de los Estados y las organizaciones internacionales, las empresas y la sociedad, en general. A pesar de que no existe una normativa común aplicable a nivel global para las cuestiones derivadas del uso de Internet, los Estados disponen de una normativa nacional y, tal y como hemos visto, en numerosas ocasiones crean pactos, acuerdos bilaterales y multilaterales, en virtud de los cuales establecen sistemas de cooperación lo que, con vistas al futuro, vaticina una mayor evolución normativa.

Resulta indudable que tanto la Unión Europea, como los países que la integran, están realizando incesantes esfuerzos por mantenerse actualizados en todos los temas relacionados con la tecnología y la seguridad. Desde 2018, año en que se estableció el marco político común en materia de ciberdefensa para la UE, hemos comprobado cómo las aspiraciones de la comunidad europea ha ido a más de forma exitosa. Así, por ejemplo, se ha aprobado la primera norma de la UE relativa a la ciberseguridad, a saber: el Reglamento sobre la Ciberseguridad de 2019; y se han establecido extraordinarias medidas sancionadoras efectivas dentro del territorio de la UE aplicables a los ciberdelitos, que constituyen toda una innovación, siendo pioneras en este ámbito porque, si recordamos, una de las mayores desventajas del ciberespacio era la ausencia de una regulación normativa común.

Asimismo, mediante la constitución y delegación de responsabilidades sobre entes especializados en el estudio, comprensión y desarrollo de nuevas estrategias en materia de seguridad, en general, la UE consigue mantener la estabilidad en el interior del territorio, aunque puntualmente haya ciertos incidentes constitutivos de violaciones a los sistemas seguridad establecidos que, en algunas ocasiones, suponen la pérdida de activos inmateriales de gran valor y, en otras, se cobran la vida de muchos ciudadanos[89]. Por ejemplo, en 2017, el virus *WannaCry* fue el peor ataque producido por *Ransomware* producido en la historia. El *Ramsonware* es un tipo de virus informático que bloquea el acceso de los usuarios a sus archivos o sistemas mediante una encriptación muy compleja. A cambio del código de desencriptación, el virus pide una contraprestación monetaria. Se cataloga como el peor (o mejor, según se mire) ataque producido por *Ransomware* debido a que afectó a grandes compañías como las españolas *Telefónica, Iberdrola* y *Gas Natural*, así como a servicios

[89] Por ejemplo, los atentados yihadistas que han sucedido en el territorio europeo desde 2015, año en el cual tuvo lugar el primer ataque a la sede parisina de *Charlie Hebdo*.

nacionales de salud (el británico, por ejemplo), hospitales, universidades y organizaciones gubernamentales, alcanzando la cifra de más de dos millones de víctimas (Patil & Mohurle, 2017).

En cuanto a la evolución de las estrategias españolas con implicación en la ciberseguridad, a pesar de que hemos estudiado los esfuerzos desplegados por la Presidencia del Gobierno por acompasarse con la UE, soy de la opinión de que aún nos queda mucho camino para ser realmente competitivos en este ámbito[90]. En este sentido, Robles Carillo afirma que, en el ámbito del ciberespacio, los avances y desarrollos tecnológicos son imparables tanto en velocidad, como en impacto, hecho que contrasta con la "situación de relativo impasse" jurídica. El derecho internacional se ha ocupado de la regulación del ciberespacio a través de una "aproximación sectorial, coyuntural y fragmentaria" que a duras penas puede cubrir las necesidades reales de normación existentes. Como prueba de esta insuficiente regulación encontramos "el aumento de la criminalidad y de la conflictividad cibernética" (Robles Carrillo, 2016, p.1).

En los últimos años se ha empleado el acrónimo *VUCA*[91] para definir el mundo. *VUCA* se desglosa en *Volatility* (volatilidad), *Uncertainty* (incertidumbre), *Complexity* (complejidad), y *Ambiguity* (ambigüedad). El ritmo al que evolucionan las tecnologías es tan sumamente frenético que cualquiera que quiera estar al día ha de realizar grandes inversiones económicas, así como aquellas con incidencia en el capital humano objeto de formación en la materia. Esto es algo a lo que, por desgracia, no todos los países pueden hacer frente de forma idónea. Por otra parte, a lo largo de estos cinco años como estudiante de Derecho me he percatado de que, a rasgos generales, siempre se le da más importancia a la actuación o respuesta frente a los incidentes que tienen lugar, que a su prevención. Me parece que esto es un error muy común en cualquier ámbito porque, aunque un sistema de prevención, a simple vista, pueda parecer un despilfarro de dinero, resulta ser más económico si tenemos en cuenta los costes de todas las problemáticas que se pueden llegar a evitar. Si hablamos de

[90] Hay páginas web oficiales del Estado español que no disponen de certificación *Secure Sockets Layer* (SSL), que da fe de que el intercambio de datos que tiene lugar entre el usuario y la web está cifrado de extremo a extremo, impidiendo así vulnerabilidades respecto a la información que viaja. Por ejemplo, encontramos la página web del Ministerio de Educación y Formación Profesional y del Ministerio de Cultura y Deporte: http://www.mecd.gob.es/redirigeme/. (consultado a 31 de mayo de 2020). Las siglas "https" que preceden el vínculo de una página web significan *HyperText Transfer Protocol Secure* -en español: protocolo de transferencia de hipertexto seguro-. Si nos fijamos, al lado del "http" falta la "s" de seguro.

[91] Harvard Business Review, *What VUCA Really Means for You,* Vol. 92, Nº. 1/2, p. 1, 2014, en: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2389563 (consultada a 31 de mayo de 2020).

la seguridad (y, consecuentemente, de la ciberseguridad) no es distinto. Por ello, estoy convencida de que los Estados y, en concreto, España, deberían de dedicar más esfuerzos a prevenir ciberataques, empezando por la base: los ciudadanos. Creo que el Estado debería ofrecer cursos o acreditaciones sobre buenos hábitos de uso de los dispositivos electrónicos de manera obligatoria para toda persona que pretendiese conectarse a Internet. De esta forma, aumentaría la cultura general acerca de la higiene cibernética y cada individuo -en caso de tener la formación adecuada- podría actuar como un pequeño cortafuegos cuando se encontrase ante un delito cibernético o ante un ciberataque.

Por otra parte, en cuanto a los grupos no estatales organizados que operan en el ámbito de Internet, resulta muy complicado establecer una conclusión general para todos debido a la diversa naturaleza que estos poseen. A rasgos generales, podríamos decir que hay dos grandes grupos: los que tienen intenciones perversas y dañinas y los que no. En primer lugar, respecto a los que buscan cometer actos cibernéticos ilícitos, en mi opinión, los Estados miembros de la UE deberán actuar de forma conjunta para combatirlos porque es muy probable que no se encuentren en territorio europeo, sino dispersos en cualquier punto del globo terráqueo, hecho que los hace más peligrosos en cuanto que sus actuaciones pueden quedar impunes con mayor facilidad. Respecto a los que sólo buscan obtener conocimiento y/o entender el funcionamiento de la red, sin ningún ánimo de acritud, opino que no suponen una amenaza y que, lejos de perseguirles, los Estados deberían plantearse el invertir en la formación de estas personas físicas -mayoritariamente- y organizaciones tan curiosas y que se manejan tan bien en el mundo virtual, con el objeto de que trabajen a su servicio, luchando contra las del primer grupo.

Por último, en relación con el último epígrafe del trabajo en el que comparábamos las estrategias españolas de seguridad con las Francia y Alemania, hemos podido comprobar que, a pesar de que cada estrategia nacional define de manera diferente qué ha de entenderse por ciberseguridad, en todas ellas constituye un elemento muy importante. En conjunto, coinciden con la creencia de que existe la necesidad de garantizar un uso seguro de las redes cibernéticas y de los sistemas de información y comunicación, así como potenciar las capacidades de prevención, detección, análisis, reacción o respuesta, defensa y resiliencia frente a actos de terrorismo y de delincuencia cibernéticos.

ANEXOS

Anexo 1: El Caso de Edward Snowden. Un civil que destapó el ciberespionaje masivo acometido por algunos Estados contra sus ciudadanos y contra otros Estados. Texto obtenido de Joseph Verble (2014). Traducción propia

En mayo de 2013, Edward Snowden robó aproximadamente 1.700.000 documentos de la NSA clasificados como alto secreto y los entregó a un montón de agencias de información con el objeto de exponer muchos programas[92], secretos también, dirigidos contra sus propios ciudadanos, líderes de países extranjeros y distintos objetivos que se encontraban en el extranjero.

Muchos de estos archivos ponen de manifiesto y documentan los programas de espionaje doméstico en posesión de la NSA, los cuales recolectaban datos de la mitad[93] de la población americana mediante diferentes vías online.

La información que se publicó gracias a Snowden se hizo eco a lo largo de todo el Mundo, acaparando gran parte de los titulares mediante los nuevos informes y detalles que se iban descubriendo poco a poco.

Desde que la historia se comunicó por primera vez a *The Guardian*, un famoso periódico británico, Snowden fue retenido en Hong Kong, se le retiró su pasaporte y, finalmente, fue reubicado en Rusia[94], país que le proporcionó asilo.

El 17 de enero de 2014, el presidente Barack Obama pronunció un discurso en el que mencionó la necesidad de reformar la NSA, al tiempo que insistía en la necesidad de disponer de programas como estos que -se supone- velan por la seguridad de los ciudadanos (Verble, 2014).

---

[92] Por ejemplo, *PRISM* y *XKeyscore*.

[93] Téngase en cuenta que este artículo de investigación data de 2014, pero Edward Snowden sacó a la luz todos estos documentos en 2013, momento en el que los usuarios con acceso a Internet eran menos en número y uso de los que son ahora. Por tanto, recopilar datos de la mitad de la población en años anteriores a 2013 es una cifra nada desdeñable.

[94] Para entender el asilo de Snowden en Rusia es necesario destacar que Rusia no tiene convenio de extradición con Estados Unidos. Además, históricamente Rusia y Estados Unidos han luchado por el dominio del Planeta Tierra. Por tanto, como Edward Snowden poseía información privilegiada acerca de la NSA, que era de gran interés para los rusos, y fue declarado "enemigo público" y "traidor" por los americanos, Rusia le abrió las puertas de su país y lo cobijó, quizás con la intención de mandar el mensaje de que toda persona con intención de traicionar a los Estados Unidos iba a tener un lugar en Rusia, y así incentivar este tipo de comportamientos.

Con todo lo expuesto sobre el caso Snowden, a lo largo de los años se han suscitado diferentes cuestiones de gran interés, que han puesto a colgar de un hilo la confianza de los ciudadanos en sus Estados:

- ¿Se está respetando nuestro derecho a la privacidad?
- ¿Se está recopilando masivamente información acerca de nosotros mediante los dispositivos con acceso a Internet (pulseras inteligentes, *smartphones*, *tablets*, ordenadores, etc.) o las aplicaciones que usamos habitualmente (redes sociales como *Facebook* o *Instagram*, apps de venta de ropa online, apps de música, etc.)?
- Si se estuviese recopilando información sensible sobre nosotros (pruebas e historiales médicos, creencias religiosas, orientación sexual), ¿cabría la posibilidad de vulneración del derecho humano de no discriminación en caso de emplearse dicha información para establecer filtros a la hora, por ejemplo, de contratar a una persona u otra?

Anexo 2. Índice del Código de Derecho de la Ciberseguridad

Nota: los textos normativos marcados con (*) se encuentran compilados de forma parcial en el Código.

CONSTITUCIÓN ESPAÑOLA*
NORMATIVA DE SEGURIDAD NACIONAL
Ley de Seguridad Nacional
Consejo Nacional de Ciberseguridad
Mecanismos para garantizar funcionamiento integrado Sistema de Seguridad Nacional
Estrategia de Seguridad Nacional
Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica
Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías
Comité de Seguridad de los Sistemas de Información de la Seguridad Social
Comité de Seguridad de las Tecnologías de la Información
Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica
Seguridad de las redes y sistemas de información
Ley reguladora del Centro Nacional de Inteligencia
Control judicial previo del Centro Nacional de Inteligencia
Ley sobre secretos oficiales
Desarrollo de la Ley sobre Secretos Oficiales
Ley Orgánica de los estados de alarma, excepción y sitio
Ley de Secretos Empresariales
Estrategia Nacional de Ciberseguridad 2019
INFRAESTRUCTURAS CRÍTICAS
Medidas para la protección de las infraestructuras críticas
Reglamento de protección de las infraestructuras críticas
Planes de Seguridad del Operador y Planes de Protección Específicos
NORMATIVA DE SEGURIDAD
Servicios Centrales y Periféricos de la Dirección General de la Policía*
Ley Orgánica de protección de la seguridad ciudadana
Ley de Seguridad Privada
Reglamento de Seguridad Privada
EQUIPO DE RESPUESTA A INCIDENTES DE SEGURIDAD
Ley de servicios de la sociedad de la información y de comercio electrónico*
Centro Criptológico Nacional
Organización básica de las Fuerzas Armadas*
Desarrollo de la organización básica de las Fuerzas Armadas*
Desarrollo de la organización básica del Estado Mayor de la Defensa*
TELECOMUNICACIONES Y USUARIOS
Ley de servicios de la sociedad de la información y de comercio electrónico
Medidas contra el tráfico no permitido y el tráfico irregular con fines fraudulentos
Distintivo público de confianza en los servicios de la sociedad de la información

Ley de acceso electrónico de los ciudadanos a los Servicios Públicos
Desarrollo parcial de la Ley de acceso electrónico de los ciudadanos a los servicios públicos
Ley de firma electrónica
Expedición del documento nacional de identidad y sus certificados de firma electrónica
Ley General de Telecomunicaciones
Reglamento sobre el uso del dominio público radioeléctrico
Protección del dominio público radioeléctrico
Ley de conservación de datos relativos a comunicaciones electrónicas y redes públicas
Formato de entrega datos conservados por los operadores
CIBERDELINCUENCIA
Ley Orgánica del Código Penal*
Ley Orgánica reguladora de la responsabilidad penal de los menores*
Ley de Enjuiciamiento Criminal*
PROTECCIÓN DE DATOS
Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales
Reglamento de la Ley Orgánica de protección de datos de carácter personal
Reglamento Europeo relativo a protección en el tratamiento de datos personales
RELACIONES CON LA ADMINISTRACIÓN
Ley del Procedimiento Administrativo Común de las Administraciones Públicas*
Ley de Régimen Jurídico del Sector Público*

Fuente: elaboración propia a partir de datos obtenidos en el BOE.

BIBLIOGRAFÍA

Alonso, C. (mayo de 2016). *Tu Blog Tecnológico*. Recuperado el 26 de mayo de 2020, de http://tublogtecnologico.com/chema-alonso-hacker-expande-limites-red/

Aucal Business School. (17 de diciembre de 2015). *Blog Ciberseguridad al día*. Recuperado el 26 de mayo de 2020, de https://www.iniseg.es/blog/ciberseguridad/que-diferencias-hay-entre-hacker-y-cracker/

Bennet, N., & Lemoine, J. (2014). What VUCA Really Means for You. *Harvard Business Review, 92*(1/2), 1. Recuperado el 31 de mayo de 2020, de https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2389563

Consejo de la Unión Europea. (9 de junio de 2016). Lucha contra las actividades delictivas en el ciberespacio: el Consejo acuerda medidas prácticas y los próximos pasos. *Consilium Europa*. Recuperado el 18 de mayo de 2020, de https://www.consilium.europa.eu/es/press/press-releases/2016/06/09/criminal-activities-cyberspace/

Consejo de la Unión Europea. (16 de abril de 2018). Actividades informáticas malintencionadas: el Consejo adopta unas Conclusiones. *Consilium Europa*. Recuperado el 18 de mayo de 2020, de https://www.consilium.europa.eu/es/press/press-releases/2018/04/16/malicious-cyber-activities-council-adopts-conclusions/

Consejo de la Unión Europea. (8 de junio de 2018). La UE establece un marco común de certificación de la ciberseguridad y refuerza su agencia: el Consejo acuerda su posición. *Consilium Europa*. Recuperado el 18 de mayo de 2020, de https://www.consilium.europa.eu/es/press/press-releases/2018/06/08/eu-to-create-a-common-cybersecurity-certification-framework-and-beef-up-its-agency-council-agrees-its-position/

Consejo de la Unión Europea. (19 de noviembre de 2018). Ciberdefensa: el Consejo actualiza el marco político. *Consilium Europa*. Recuperado el 19 de mayo de 2020, de https://www.consilium.europa.eu/es/press/press-releases/2018/11/19/cyber-defence-council-updates-policy-framework/

Consejo de la Unión Europea. (19 de noviembre de 2018). Marco político de ciberdefensa de la UE (actualización de 2018). Bruselas, Bélgica. Recuperado el 22 de mayo de 2020, de http://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/es/pdf

Consejo de la Unión Europea. (16 de mayo de 2019). Decisión del Consejo relativa a medidas restrictivas contra los ciberataques que amenacen a la Unión o a sus Estados miembros. Bruselas. Recuperado el 22 de 05 de 2020, de http://data.consilium.europa.eu/doc/document/ST-7299-2019-INIT/es/pdf

Consejo de la Unión Europea. (3 de diciembre de 2019). Conclusiones sobre la importancia de la tecnología 5G para la economía europea y la necesidad de mitigar los riesgos para la seguridad relacionados con la 5G. (M. Jurado del Águila, Trad.) Bruselas. Recuperado el 26 de mayo de 2020, de https://www.consilium.europa.eu/media/41595/st14517-en19.pdf

Consejo Europeo. (20 de diciembre de 2017). Ciberseguridad: las instituciones de la UE refuerzan la cooperación para combatir los ciberataques. *Consilium Europa*. Recuperado el 18 de mayo de 2020, de https://www.consilium.europa.eu/es/press/press-releases/2017/12/20/cybersecurity-eu-institutions-strengthen-cooperation-to-counter-cyber-attacks/

Consejo Europeo. (18 de octubre de 2018). *Consilium Europa*. Recuperado el 18 de mayo de 2020, de Reunión del Consejo Europeo de 18 de octubre de 2018: https://www.consilium.europa.eu/es/meetings/european-council/2018/10/18/

Consejo Europeo. (9 de abril de 2019). *Ciberseguridad en Europa: normas más estrictas y mejor protección*. Recuperado el 26 de mayo de 2020, de https://www.consilium.europa.eu/es/policies/cybersecurity/

Federal Ministry of Defence. (2016). *White Paper 2016 on Germany Security Policy and the future of the Bundeswehr*. Recuperado el 31 de mayo de 2020, de https://www.dsn.gob.es/sites/dsn/files/2016_German_WhitePaper_SecurityPolicy_13jul2016.pdf

Federal Ministry of the Interior. (2011). *Cyber Security Strategy for Germany*. Recuperado el 1 de junio de 2020, de https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-for-germany/view

German Ministry of Defence. (2011). *Guidelines: Safeguarding National Interests, Assuming International Responsibility, Shaping Security Together.* Recuperado el 1 de junio de 2020, de https://www.bmvg.de/resource/blob/16136/0c1b6d8d0c0e6ba0aed5f0feb0af81d8/g-03-110527-vpr-engl-data.pdf

Guttal, S. (2007). Development in Practice. *Routledge. Taylor & Francis Group*, 523-531.

INCIBE. (22 de abril de 2014). *Ciber-Resiliencia: Aproximación a un marco de medición*. Recuperado el 22 de mayo de 2020, de https://www.incibe.es/protege-tu-empresa/blog/ciberresiliencia-marco-medicion

INCIBE. (2020). Red Teaming. *Catálogo de empresas y soluciones de ciberseguridad*. Recuperado el 25 de mayo de 2020, de https://www.incibe.es/protege-tu-empresa/catalogo-de-ciberseguridad/listado-soluciones/red-teaming

Kemp, S. (2019). *Digital 2019: Global Internet Use Accelerates.* We Are Social. Recuperado el 08 de 05 de 2020, de https://wearesocial.com/blog/2019/01/digital-2019-global-internet-use-accelerates

Martí, A. (2017). *Xataka*. Recuperado el 27 de mayo de 2020, de https://www.xataka.com/seguridad/the-shadow-brokers-su-historia-desde-el-hackeo-a-la-nsa-hasta-la-venta-de-exploits-por-suscripcion-mensual

Ministerio de Defensa Español. (1970). *Libro Blanco Alemán 1970, acerca de la seguridad de la República Federal de Alemania y de la situación de las fuerzas armadas federales.* Recuperado el 31 de mayo de 2020, de https://dialnet.unirioja.es/descarga/articulo/4771880.pdf

Patil, M., & Mohurle, S. (2017). *A brief study of Wannacry Threat: Ransomware Attack 2017*. Recuperado el 27 de mayo de 2020, de https://sbgsmedia.in/2018/05/10/2261f190e292ad93d6887198d7050dec.pdf

Presidencia del Gobierno. (2017). *Estrategia de Seguridad Nacional 2017.* Madrid. Recuperado el 27 de mayo de 2020, de https://www.boe.es/boe/dias/2017/12/21/pdfs/BOE-A-2017-15181.pdf

Presidencia del Gobierno. (2019). *Estrategia Nacional de Ciberseguridad 2019.* Madrid. Recuperado el 26 de mayo de 2020, de https://www.boe.es/buscar/pdf/2019/BOE-A-2019-6347-consolidado.pdf

République Française, Premier Ministre. (2015). *Estrategia nacional francesa para la seguridad del ámbito digital.* Recuperado el 1 de junio de 2020, de https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_es.pdf

République Française, Président de la République. (2008). *Défense et Sécurité nationale: Le Livre Blanc.* Recuperado el 1 de junio de 2020, de https://www.vie-publique.fr/sites/default/files/rapport/pdf/084000341.pdf

République Française, Président de la République. (2013). *Livre blanc sur la défense et la sécurité nationale.* Recuperado el 1 de junio de 2020, de https://fr.calameo.com/read/000331627d6f04ea4fe0e

Revista UNIR. (7 de enero de 2020). Red Team, Blue Team y Purple Team, ¿cuáles son sus funciones y diferencias? *UNIR Revista*. Recuperado el 25 de mayo de 2020, de https://www.unir.net/ingenieria/revista/noticias/red-blue-purple-team-ciberseguridad/549204773062/

Robles Carrillo, M. (enero-abril de 2016). El ciberespacio: Presupuestos para su ordenación jurídico-internacional. *Revista Chilena de Derecho y Ciencia Política, 7*(1). doi:10.7770/RCHDYCP.V7N1.1025

Robles Carrillo, M. (9 de septiembre de 2016). Amenaza y uso de la fuerza a través del ciberespacio: un cambio de paradigma. *Revista Latinoamericana de Derecho Internacional*, 1-62. Recuperado el 23 de mayo de 2020

Robles Carrillo, M. (2018). Seguridad de redes y sistemas de información en la Unión Europea: ¿un enfoque integral? *Revista de Derecho Comunitario Europeo*(60), 563-600. Recuperado el 23 de mayo de 2020, de https://recyt.fecyt.es/index.php/RDCE/article/download/64023/40424

Segura Serrano, A. (2017). La estrategia española de ciberseguridad: análisis comparado. En J. Roldán Barbero, *La seguridad nacional de España: un enfoque geoestratégico* (págs. 522-553). Valencia: Tirant Lo Blanch.

Sierra, D. (2012). 'Anonymous', ¿quiénes son y cómo actúan? *RTVE*. Recuperado el 25 de mayo de 2020, de https://www.rtve.es/noticias/20120228/anonymous-quienes-son-como-actuan/438765.shtml

Signaturit. (26 de 04 de 2017). ¿Qué leyes regulan la ciberseguridad en la Unión Europea y en España? Recuperado el 08 de 05 de 2020, de ¿Qué leyes regulan la ciberseguridad en la Unión Europea y en España?: https://blog.signaturit.com/es/que-leyes-regulan-la-ciberseguridad-en-la-union-europea-y-en-espana

Townsend, C. (2020). (In)Famous Hacking Groups. *United States Cibersecurity Magacine*. Recuperado el 27 de 05 de 2020, de https://www.uscybersecurity.net/infamous-hacking-groups/

United Nations Development Programme. (2019). *Human Development Reports: Human Development Index (HDI).* Recuperado el 28 de mayo de 2020, de http://hdr.undp.org/en/indicators/137506

Verble, J. (2014). The NSA and Edward Snowden: surveillance in the 21st century. *Association for Computing Machinery. Digital Library.*, 14. Obtenido de https://dl.acm.org/doi/abs/10.1145/2684097.2684101

Wikipedia. (2020). *Anonymous*. Recuperado el 25 de mayo de 2020, de https://es.wikipedia.org/wiki/Anonymous