Asociación para las Naciones Unidas en España
United Nations Association of Spain

Marzo 2023

La evolución normativa de la ciberseguridad en la Unión Europea y su impacto político a nivel de actores, objetivos y recursos.

Alessandro Demurtas[1]

Resumen

Este artículo de reflexión quiere analizar la evolución normativa que la ciberseguridad ha tenido en los últimos años en la Unión Europea (UE), intentando determinar qué impacto ha tenido a nivel de actores, recursos y objetivos. La hipótesis de partida es que la ciberseguridad ocupa un lugar siempre más importante en la agenda de los decisores políticos europeos, por dos razones. La primera, más evidente, es la creciente importancia que la dimensión cibernética adquiere en las vidas cotidianas de todos los actores del sistema internacional: población, instituciones, empresas, organizaciones nacionales e internacionales, gubernamentales y no gubernamentales. La segunda razón es intrínseca al papel que el proceso de integración comunitaria otorga a las instituciones de la UE: la organización del marco para la cooperación intergubernamental en este ámbito, la coordinación de las acciones, los recursos y las estrategias de los veintisiete Miembros de la UE que, en la gran mayoría de los casos, comparten amenazas, retos y desafíos que afectan a su ciberseguridad.

Palabras clave: Ciberseguridad, ciberamenazas, ciberespacio, Unión Europea.

Abstract

This article of reflection analyses the normative evolution of cybersecurity in the European Union (EU) during the last years. It also seeks to determine its impact on actors, resources and priorities. The starting hypothesis is that cybersecurity is progressively becoming a priority in the European political agenda, for two reasons. The first is more evident and concerns the growing importance of the cyber dimension in the daily life of all actors of the international system: population, institutions, firms, national and international organizations, governmental and no governmental. The second reason is directly related with the role of the EU institutions in regional integration. EU must provide the framework for the intergovernmental cooperation, the coordination of national actions, resources and strategies of the twenty-seven Members. They share, in the great majority of cases, threats, risks and challenges against their cybersecurity.

Keywords: Cybersecurity, cyberthreats, cyberspace, European Union.

[1] Doctor cum laude en Relaciones Internacionales e Integración Europea por la Universidad Autónoma de Barcelona en 2014.
Profesor de Relaciones Internacionales en la Universidad Autónoma de Barcelona.
ID Orcid: orcid.org/0000-0002-1304-2221 Correo electrónico: alessandro.demurtas@uab.cat

Introducción

1 Marco teórico-conceptual y metodología

1.1 La seguridad del ciberespacio frente a las ciberamenazas

El ciberespacio ha adquirido, a lo largo de los últimos quince años, una importancia creciente – hoy en día, fundamental – para todos los actores del sistema internacional. Las principales tareas y funciones que permiten el mantenimiento de la vida cotidiana de Estados, sociedades, personas, instituciones y organizaciones nacionales e internacionales, gubernamentales y no gubernamentales, se llevan a cabo en la dimensión cibernética. Los sistemas de producción, de circulación y de mantenimiento de la gran mayoría de las infraestructuras, incluidas las críticas, son altamente dependientes del buen funcionamiento del ciberespacio, cuyo colapso podría tener consecuencias devastadoras bajo múltiples aspectos. De acuerdo con los datos emitidos por la Comisión Europea, "la incidencia económica de la ciberdelincuencia **se multiplicó por cinco entre 2013 y 2017**" (Consejo Europeo, 2020.) Por esta razón, Estados y organizaciones internacionales intergubernamentales, como la UE, buscan convertirlo y mantenerlo como un espacio "seguro", libre de amenazas.

El Departamento de Defensa de los EEUU define el ciberespacio como una "red interdependiente de infraestructuras de tecnologías de la información, incluyendo Internet, redes de telecomunicaciones, sistemas informáticos, procesadores embebidos y controladores" (Congressional Reserve Service, 2020). Es decir, un conjunto de dispositivos conectados por redes que almacenan y utilizan la información electrónica, así como un lugar de interacción entre múltiples actores, con el objetivo de facilitar y aumentar el flujo de comunicación e interacción entre individuos.

Los instrumentos utilizados para conseguir la seguridad en el ciberespacio pueden reagruparse bajo el concepto de políticas de ciberseguridad, un fenómeno propio del siglo XXI, que empieza a adquirir especial relevancia en la agenda de los decisores políticos nacionales e internacionales en los últimos quince años, como consecuencia de algunos acontecimientos que analizaremos más adelante. Este proceso se hace aún más evidente en los últimos siete años, especialmente a nivel europeo.

El objetivo último de las políticas de ciberseguridad es blindar los sistemas informáticos de tratamiento, almacenamiento, envío e intercambio de datos para evitar que puedan caer en manos de terceras personas.

De acuerdo con el Departamento español de Seguridad Nacional (DSN), el concepto de ciberseguridad nacional puede definirse como "la acción del Estado dirigida a proteger los intereses nacionales, vitales y estratégicos, referentes a:

- los sistemas de información y telecomunicaciones e infraestructuras comunes a todas las Administraciones Públicas, las infraestructuras críticas, las capacidades militares y de defensa y todos aquellos sistemas de interés para la Seguridad Nacional;
- la libertad y seguridad de los ciudadanos;
- la industria;
- el patrimonio tecnológico" (DSN, 2020).

La política de ciberseguridad de la UE se caracteriza por tener un carácter complementario a las políticas estatales porque, cómo se ha dicho antes, sus instituciones ejercen el papel fundamental de coordinación de las políticas de los Estados miembros. Por esto, la definición de ciberseguridad adoptada por las instituciones comunitarias es más amplia y difuminada si comparada, por ejemplo, con la definición adoptada por el Estado español.

La Agencia de la Unión Europea por la Seguridad de las Redes y de la Información[1] (ENISA), afirma que la ciberseguridad es la seguridad del ciberespacio y que "la UE destaca la importancia de todos los portadores de intereses en el actual modelo de gobernanza de Internet, siendo partidaria del modelo de gobernanza con múltiples actores […] para conseguir estándares exitosos, especialmente en un área como la ciberseguridad donde las necesidades del sector público son implementadas, en gran medida, por proveedores de servicios del sector privado" (ENISA, 2015: 7).

La ENISA considera que la ciberseguridad es un concepto multidimensional que obliga a la UE y a sus Miembros a implementar medidas en cinco grandes ámbitos:

1. La seguridad de las comunicaciones frente a amenazas a las infraestructuras técnicas que podrían alterar su funcionamiento y provocar actividades indeseadas por parte de los usuarios.
2. La seguridad de las operaciones frente a amenazas que podrían desestabilizar o interrumpir los normales flujos y procedimientos entre usuarios.
3. La seguridad de la información frente a las amenazas de robos, cancelación o alteración de los datos almacenados o transmitidos a través del ciberespacio.
4. La seguridad física del ciberespacio frente a amenazas que podrían alterar su buen funcionamiento, a través de la inserción de malware, virus y otras herramientas malignas. Esta dimensión se centra en la seguridad y protección física de los servidores y de los nodos de transmisión de datos, que podríamos incluir dentro de la definición de "infraestructura crítica". En la UE, este concepto tiene una doble dimensión. Por un lado, hay las infraestructuras críticas estatales: "las infraestructuras estratégicas cuyo

[1] Cómo veremos más adelante, con la adopción de la primera Estrategia de ciberseguridad de la UE en 2013, la ENISA se convierte en la Agencia para la ciberseguridad europea, con mandato permanente.

funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales" (BOE - Boletín Oficial del Estado español, 2011: 3). Por otro lado, debido a la interdependencia compleja entre los Miembros de la Unión, a nivel comunitario se adopta la definición de infraestructura crítica comunitaria: "aquellas infraestructuras críticas situadas en algún Estado miembro de la Unión Europea, cuya perturbación o destrucción afectaría gravemente al menos a dos Estados miembros, todo ello con arreglo a la Directiva 2008/114, del Consejo, de 8 de diciembre, sobre la identificación y designación de Infraestructuras Críticas Europeas" (BOE - Boletín Oficial del Estado español, 2011: 3).

5. La seguridad pública o nacional frente a amenazas que buscan conseguir ventaja política, militar, estratégica para el atacante, como los ataques de larga escala contra los sistemas de comunicación, financieros u otras infraestructuras públicas críticas o infraestructuras industriales (ENISA, 2015: 10-11).

Los actos delictivos cometidos en el ciberespacio se conocen bajo los términos de ciberdelitos, cibercrimen o ciberdelincuencia y comparten cuatro características específicas. Primero, pueden cometerse más fácilmente porque el delincuente no se ve limitado por ninguna barrera física que proteja sus objetivos. Segundo, los recursos necesarios para llevarlos a cabo pueden ser infinitamente escasos, siendo necesarios, en algunos casos, exclusivamente un ordenador y una conexión a Internet. Tercero, bajo una perspectiva jurídico-legal, los ciberdelitos pueden cometerse en otras jurisdicciones, sin necesidad que quien los comete se encuentre físicamente en el territorio sujeto a esa jurisdicción. Cuarto y en parte relacionado con lo anterior, en muchos casos, los delincuentes se benefician de vacíos legales o zonas grises que dificultan su persecución y su punibilidad (Subijana Zunzunegui, 2008).

La posibilidad para el ciberdelincuente de mantenerse anónimo, la imposibilidad de acarrear daño físico directo e inmediato al objetivo, el fuerte sentido de impunidad y de no ser rastreable, debido a la distancia física de sus persecutores y a la falta de mecanismos internacionales de cooperación en este ámbito, hacen que el número de ciberdelitos vaya paulatinamente aumentando. En cuanto al sentido de impunidad, hay que añadir que muchos ciberataques son llevados a cabo con el apoyo de los Estados que ofrecen un refugio seguro a sus perpetradores, imposibilitando cualquier acción para poderlos perseguir.

A estas razones, como apunta la Agencia para la ciberseguridad europea, hay que sumar las ganancias económicas derivadas de los ciberataques relacionados con las cripto-monedas. Esta última tipología de ataques ya está catalogada por la UE como una de las quince ciberamenazas más graves. Todos estos factores representan una explicación del porqué, en los últimos años, el número de ciberataques haya crecido paulatinamente a nivel global: a nivel europeo, se estima que el 33% de la población haya sido víctima, como mínimo, de un ciberataque (ENISA, 2019a).

1.2 El contexto histórico de los últimos diez años: puntos de inflexión e impacto en las doctrinas y estrategias de seguridad en la posguerra fría

A pesar de que los primeros "incidentes" relacionados con el ciberespacio sucedan a principios de siglo, no es hasta el año 2007 que la comunidad internacional reacciona frente a los ciber-ataques. En este año, un ataque informático de hackers rusos provoca durante veintidós días la negación generalizada de servicios de las instituciones estatales de Estonia, Miembro de la UE desde el 1 de mayo de 2004. El ataque es una represalia rusa por la decisión del Gobierno estonio de trasladar un monumento en honor a los caídos soviéticos en la segunda guerra mundial hacia una plaza secundaria de la capital Tallin (Ottis, 2008).

A finales de 2008 y durante todo el 2009, el virus *Conficker*, conocido también como *Downup*, consigue infectar millones de computadoras con el sistema operativo *Microsoft Windows*, provocando incidencias en el funcionamiento incluso de algunos buques de la Marina británica y del Parlamento de Londres (Radziwill, 2015: 72).

En 2009 se da el primer caso internacional de ciberespionaje. El virus *Ghostnet* – supuestamente de origen chino – ataca a las instituciones de más de cien países, provocando la negación de servicios en embajadas de numerosos países asiáticos, como India, Corea del Sur, Taiwán, Tailandia, Indonesia y Pakistán, y europeos: Rumanía, Chipre, Malta, Portugal y Alemania. EEUU y Reino Unido consiguen resistir al ataque sin reportar daños. El objetivo del ciberataque es conseguir información clasificada de carácter político, militar, diplomático y económico (Chang, 2009).

En este mismo año, ataques cibernéticos contra las instalaciones de Pentágono, Casa Blanca y Bolsa de Nueva York provocan el robo de información clasificada sobre técnicas de montaje de un nuevo modelo de caza de la Aviación estadounidense. El hecho de que algunas instituciones surcoreanas hayan sido víctimas del mismo ataque ha levantado sospechas sobre el origen norcoreano de este caso clasificado como ciber espionaje (Szoldra, 2016).

En 2010 se da el ciberataque más famoso de la historia de las relaciones internacionales, con consecuencias directas y duraderas para el sistema. El escándalo *WikiLeaks* provoca tensiones diplomáticas entre los partidarios de que su fundador, Julian Assange, fuera juzgado por espionaje y violación de secretos de Estados por parte de los países afectados – entre ellos los EEUU – y las personas e instituciones que ven en Assange un "paladín" de la libertad de información. Piénsese que *WikiLeaks* es nombrada por seis años consecutivos (2010-2015) como organización candidata al Premio Nobel para la Paz (WikiLeaks, 2020).

En 2012, los EEUU adquieren protagonismo cibernético. Por un lado, son los responsables de un caso de ciberespionaje: "los Estados Unidos e Israel han desarrollado el virus para ordenador *Flame* para ralentizar el programa nuclear iraní", a través del sabotaje de sus sistemas (Washington Post, 2012). Por otro lado, en mayo del mismo año, su Ministerio de Justicia se convierte en la víctima del robo y la difusión de 1,7 gigabytes de datos con información clasificada por parte la organización de hackers *Anonymous* (The Hill, 2012).

Otro ciber-ataque contra los EEUU se da en 2015, cuando un grupo de hackers – supuestamente relacionados con el Gobierno de Pekín – consigue robar información a la Oficina Federal de Administración del Personal, accediendo a información privada y autorizaciones de seguridad de veinte millones de empleados federales. Este ataque de ciberespionaje lleva la Administración Obama a anunciar represalias que quedan en el ámbito simbólico (Sanger, 2015). De hecho, después de este acontecimiento, las dos "ciber-superpotencias" empiezan unas negociaciones para cooperar en materia de lucha contra el cibercrimen y protección de los derechos de autor, alejando los fantasmas de una ciberguerra (Segal, 2016).

El año siguiente, los EEUU son víctimas de un ataque de ciberespionaje por parte de Rusia, con la intención de interferir en el voto en las elecciones presidenciales a favor del candidato republicano, Donald Trump (Comité Seleccionado de Inteligencia del Senado de los EEUU, 2019). Para concluir, el 2019 registra la mayor brecha de seguridad de la historia, con el robo de información de 2.200 millones de direcciones de correos electrónicos y contraseñas. Además, registra el robo de información relativa a 1.200 millones de cuentas de usuarios de Facebook – ya golpeada por el escándalo relativo a *Cambridge Analytica* – y LinkedIn. Las empresas no son exentas de los ciberataques: comparado con el año anterior, el 2019 registra un aumento del 500% da ataques con *ransomware* contra sus sistemas informáticos (Valle, 2020).

Esta breve reseña de ciberataques no pretende ser exhaustiva, sino que quiere demostrar dos tesis. Primero, como es de esperar, al crecer la dependencia de todos los actores del sistema internacional del mundo cibernético, hay un incremento notable del cibercrimen, motivado principalmente por razones económicas y geopolíticas (por lo que se refiere al ciberespionaje). El aumento de la ciber-dependencia y de los ciberataques obligan los Estados y las organizaciones internacionales a reaccionar – y, normalmente lo hacen a posteriori, sin adoptar un enfoque preventivo ni proactivo – para garantizar su ciberseguridad.

La extrema interdependencia de los Miembros de la UE, como veremos en el siguiente apartado, conlleva a un fortalecimiento del marco jurídico-normativo y político europeo. Esto para permitir dar una respuesta conjunta más eficiente a las ciberamenazas que pueden golpear indistinta y simultáneamente a todos los países europeos. A pesar de las reticencias estatales a ceder competencias en este ámbito tan sensible de su soberanía, los Gobiernos han tenido que otorgar, a lo largo del siglo XXI, ciertos poderes de decisión y actuación a las instituciones comunitarias.

1.3 Metodología

El objetivo de este artículo es delinear cuáles son los últimos avances en el discurso normativo y estratégico de la UE en relación con su ciberseguridad y, como consecuencia, analizar cómo ha evolucionado la implementación de políticas en este sector, especialmente en relación con los recursos utilizados y los actores responsables, sus objetivos y prioridades.

Para realizar este análisis, se seleccionan los principales documentos adoptados por las instituciones europeas en los últimos quince años, con especial énfasis en los avances realizados en los siete últimos años. Por razones de espacio, no es posible analizar en detalle todos los documentos oficiales adoptados por todos los actores comunitarios responsables de la ciberseguridad: el artículo se centra en los documentos que marcan los principales puntos de inflexión que determinan la actual configuración europea en este ámbito.

2. El caso de la Unión Europea

2.1 Discurso estratégico y normativo sobre ciberseguridad: individuación de amenazas y objetivos

En cuanto a los distintos tipos de delitos en el ciberespacio, no hay a nivel internacional una clasificación común. Por otro lado, las autoridades europeas han procedido a clasificar las ciberamenazas de forma muy precisa. El último informe identifica quince categorías de amenazas para el ciberespacio (ENISA, 2019b), entre las cuales destacan:

1. El programa maligno o software malicioso es responsable del 30% de todos los ciberataques registrados. Desde 2017, no se registran incidentes a escala global, como fue el caso del *WannaCry*[2]. Hoy en día, su uso parece destinarse más al ciberespionaje y a la generación fraudulenta de cripto-monedas.
2. Los ataques a páginas y dominios web, o a sus aplicaciones, tienen el objetivo de sustraer información personal o datos bancarios de los usuarios.
3. El phishing es la técnica consistente en hacerse pasar por una persona o entidad de confianza de la víctima, con el objetivo de sustraerle información sensible, como sus datos bancarios. El 75% de los Estados de la UE has reportado a ENISA ataques de esta tipología.
4. La negación generalizada de servicios consiste en hacer caer los servidores y las páginas web de empresas o instituciones, que ya no pueden ofrecer servicios a sus clientes y usuarios.
5. El spam es "el abuso de correos electrónicos y de mensajes para llenar los buzones de los usuarios de mensajes no deseados". En 2008, el correo spam representaba el 85% de los correos totales. En 2017, gracias a las medidas de ciberseguridad adoptadas por los Estados, este porcentaje desciende hasta el 39,2% (ENISA, 2019b: 54).
6. La violación de datos (*Data breach*) es el resultado de un ciberataque que conlleva a la pérdida o a la sustracción de datos. Es una categoría muy general que puede abarcar el robo de datos a una institución sanitaria o de inteligencia, hasta llegar al escándalo conocido como *Cambridge Analytica* que afecta la

[2] "El ataque de ransomware *WannaCry* fue una epidemia global que tuvo lugar en mayo de 2017. Este ataque ransomware se propagó a través de ordenadores con Microsoft Windows. Los archivos del usuario se mantuvieron retenidos y se solicitó un rescate en bitcoins para su devolución" (Kaspersky, 2020).

compañía Facebook en 2018 y que obliga su fundador a declarar ante una comisión del Senado estadounidense.

7. La amenaza interna puede ser cualquier trabajador o socio de una empresa o institución que, voluntaria o involuntariamente, provoca una brecha de seguridad en el acceso a los datos confidenciales custodiados en los servidores internos. El 77% de las brechas de datos de las empresas mundiales son provocados por amenazas internas (ENISA, 2019b: 69).
8. La manipulación física, el daño, el robo o la pérdida son todos los posibles ataques físicos contra los servidores y las instalaciones donde están custodiados. En esta categoría se incluyen los atracos a los cajeros automáticos: en la UE, hay 1818 ataques en 2011, para llegar a 3584 en 2017 (ENISA, 2019b: 76).
9. El robo de identidad es el fraude cometido por el cibercriminal que consigue hacerse pasar por su víctima en el ciberespacio, generalmente con el objetivo de obtener ganancias económicas.
10. La minería de cripto-monedas maliciosas (*Crypto-Jacking*) consiste en el uso del ordenador de la víctima, sin su consentimiento, para "fabricar" cripto-monedas. "El 2018 fue el año del crypto-jacking" (ENISA, 2019b: 92), debido al incremento del valor de los *Bitcoins*. En apenas un año, el número de ataques relacionados con la minería de cripto-monedas se multiplicó por diez, pasando de 75547 a principios de 2017 a 787146 a principios de 2018 (ENISA, 2019b: 96).
11. El ciberespionaje es conocido también como el ciberataque "patrocinado por los Estados" y puede tener las finalidades más variadas: comprometer la infraestructura crítica o industrial de otro Estados, tener objetivos geopolíticos, buscar el robo de secretos comerciales e industriales, obtener información sensible política o diplomática, entre otros.

El análisis demuestra que las ciberamenazas son múltiples y a menudo conectadas entre ellas: debido a la paulatina digitalización de sociedades, empresas e instituciones, van adquiriendo siempre más importancia en las agendas de los decisores políticos, así como en los presupuestos de los Estados, que son los principales encargados de garantizar la ciberseguridad en sus jurisdicciones. Como ya se ha dicho, la UE adopta una perspectiva complementaria hacia este complejo fenómeno – consciente de su rápida evolución – debido a su papel de coordinación y de establecimiento del marco para la cooperación entre sus veintisiete Miembros y sus socios, como es el caso de la OTAN.

En relación con los objetivos planteados por la UE, hay que esperar hasta el año 2013 para verlos enumerados en la primera "Estrategia Europea de Ciberseguridad: un Ciber-Espacio abierto y seguro" (Comisión Europea, 2013, 4-14). La Estrategia individua cinco objetivos fundamentales para la cooperación multinivel entre actores público y privados:

1. Conseguir la ciber-resiliencia frente a todo tipo de ataque cibernético masivo, intentando concienciar más a los ciudadanos y a los sectores públicos y privados.

2. Reducir drásticamente el cibercrimen, desarrollando una legislación más exhaustiva y eficaz contra estos delitos, que permita la interoperabilidad entre todos los actores involucrados en la política multinivel.
3. Desarrollar una política de ciberseguridad, con sus propios recursos, en el ámbito de la Política Común de Seguridad y Defensa, que provea mecanismos de cooperación más eficaces y eficientes, evitando la duplicación de esfuerzos. Para hacer esto, se recomienda que el Alto Representante para la Política Exterior y de Seguridad Común promueva los Estados miembros a cooperar con la Agencia Europea de Defensa.
4. Desarrollar nuevos recursos tecnológicos e industriales para la ciberseguridad, fomentando el mercado único para los productos y servicios de este sector, gracias a la adopción de certificaciones y estándares comunes y con recomendaciones y consejos ofrecidos por la ENISA a todos los *stakeholders* públicos y privados.
5. Establecer una política internacional para el ciberespacio que sea coherente y basada en los valores fundamentales de la UE y promoverla en el sistema internacional.

La "Estrategia Global para la Política Exterior y de Seguridad de la UE" de 2016 mantiene estos objetivos, además de poner el énfasis en la necesidad de "buscar el conseguimiento de sistemas innovadores para las tecnologías de información y comunicación (TIC), que garanticen la disponibilidad y la integridad de los datos", junto con la certificación de productos y servicios en el espacio digital europeo[3]. Además, hay que desarrollar nuevas plataformas digitales que permitan la cooperación en todas las políticas europeas, con especial énfasis en el fortalecimiento de la dimensión cibernética en la Política Europea Común de Seguridad y Defensa (Unión Europea, 2016: 22). De acuerdo con el documento estratégico, la ciberseguridad se configura como una política transversal que debe fortalecerse en todos los ámbitos de actuación de la UE, garantizando una mayor eficiencia, eficacia e interoperabilidad en todas las políticas implementadas, donde hay múltiples actores involucrados. Es decir, la UE debe fortalecer la ciber-gobernanza multinivel y transversal a todas sus políticas.

2.2 Actores involucrados, objetivos y prioridades políticas y recursos destinados a la ciberseguridad

El objetivo de este último apartado analítico es determinar las novedades más recientes en la política de ciberseguridad europea, intentando contestar a tres grandes preguntas:

1. ¿Cómo ha cambiado el mapa de los actores responsables de la ciberseguridad europea en los últimos años?

[3] Este objetivo se consigue con el Acuerdo entre Embajadores de la UE del 19 de diciembre de 2018, conocido como el "Acta de Ciberseguridad" (Consejo Europeo, 2018; Parlamento y Consejo Europeo, 2019).

2. ¿Qué funciones prioritarias desarrollan estos actores? Es decir, ¿cómo se estructura hoy en día la política de ciberseguridad de la UE en cuanto a objetivos?
3. ¿Cómo ha evolucionado el gasto europeo para la ciberseguridad en los últimos años?

El mapa de los actores que colaboran en el marco de la política de ciberseguridad se ha ido expandiendo paulatinamente a lo largo de los últimos años, siendo coherente con la expansión normativa antes analizada. Siguiendo la dinámica de *spill-over* (o "mancha de aceite"), la ciberseguridad ha ido adquiriendo siempre más importancia en un número creciente de políticas. Esto ha obligado a que haya más actores que cooperan en este ámbito. ENISA ofrece un mapa que identifica hasta veintidós actores (ENISA, 2020a) que podemos dividir en tres grandes categorías. En primer lugar, hay actores creados específicamente para garantizar la ciberseguridad europea, como la misma ENISA (Agencia de la Unión Europea para la Ciberseguridad), creada en 2004 con sede en Atenas o la Red Judicial Europea contra la Ciber-delincuencia de 2016.

En segundo lugar, a lo largo de los últimos años, aparecen organismos (llamados célula, comité, oficina, grupo de trabajo o centro) para la ciberseguridad en seno a las instituciones europeas, con el objetivo principal de agilizar la cooperación entre los actores pertenecientes a la red para la ciberseguridad. Ejemplos de este tipo son el Directorado General de la Comisión Europea para las Redes, los Contenidos y las Tecnologías de la Comunicación del año 2012; el Centro Europeo contra el Cibercrimen (EC3) de la Europol, creado en el 2013, la Célula de Fusión Híbrida de la UE del Servicio Europeo de Acción Exterior, creada en 2016 y a la que se le asigna una sede permanente en Helsinki en 2017; el Grupo de Trabajo Horizontal de las Partes sobre Ciber-delincuencia, creado en seno al Consejo de la UE en 2016. Estos organismos pueden ser definidos como nuevas secciones o departamentos de instituciones ya existentes, con la misión compartida de garantizar la "resiliencia, disuasión y defensa" (Consejo de la Unión Europea, 2017).

La tercera categoría de actores agrupa aquellos que ya existen con funciones propias y que, por su relevancia para la ciberseguridad, acaban adquiriendo paulatinamente funciones y competencias en este ámbito: piénsese a la Agencia de Defensa Europea, al Centro de Investigación Conjunta de la Comisión Europea, al CERT-EU (el organismo encargado de armonizar los estándares europeos de certificación), a EUROPOL y a EUROJUST. Estos veintidós actores constituyen las arenas para la cooperación, el diálogo y la interoperabilidad entre las cuatro "comunidades" de profesionales que trabajan para la ciberseguridad en la UE:

1. Comunidad para la justicia en el ciberespacio y contra el cibercrimen,
2. Comunidad para la ciber diplomacia y las ciber políticas,
3. Comunidad para la ciberdefensa,
4. Comunidad para la ciber-resiliencia.

Esto quiere decir que, en cada uno de los veintidós actores, hay un número variable de comunidades que interactúan para conseguir los mejores resultados en su ámbito de actuación. Para poner unos ejemplos aclaradores, en la ENISA cooperan las cuatro comunidades; en el Consejo Horizontal de las Partes para el Trabajo sobre Asuntos Cibernéticos están presentes la Comunidad para la ciber diplomacia y las ciber políticas

junto con la Comunidad para la ciber-resiliencia y, por último, en la Célula de Fusión Híbrida de la UE del Servicio Europeo de Acción Exterior sólo actúa la Comunidad para la ciber diplomacia y las ciber políticas (ENISA, 2020b).

Para resumir la respuesta a la primera pregunta, a lo largo de los últimos años, el mapa de los actores responsables de la ciberseguridad en la UE ha ido creciendo exponencialmente, llegando a incluir veintidós actores de distinta tipología. Éstos establecen una red compleja de interacciones de cooperación entre las cuatro comunidades de profesionales portadoras de intereses y responsabilidades de un macro-ámbito de esta política. Hay un crecimiento evidente de actores pertenecientes a la segunda categoría antes mencionada, es decir secciones u oficinas dentro de organismos e instituciones comunitarias ya existentes, especialmente en los últimos cinco años.

Para contestar a la segunda pregunta, sobre el actual diseño de la política, hay que analizar las distintas funciones y prioridades llevadas a cabo por las cuatro comunidades antes mencionadas junto con la ENISA.

La misma ENISA (2020c) individúa dieciocho prioridades de las comunidades de profesionales que conforman los veintidós organismos europeos, que podemos reagrupar en las cuatro grandes categorías marcadas por la "Estrategia Europea de Ciberseguridad: un Ciber-Espacio abierto y seguro", analizada en la página 10. Cada una de estas categorías es perseguida por un número variable de comunidades de profesionales, como se detalla en la tabla a continuación.

Tabla 1: objetivos de la política de ciberseguridad europea y de las comunidades de profesionales responsables

GRANDES CATEGORÍAS según la primera Estrategia de ciberseguridad de la UE de 2013	OBJETIVOS Y PRIORIDADES según la ENISA en 2020	COMUNIDADES DE PROFESIONALES RESPONSABLES según la ENISA en 2020
Defensa y resiliencia	• Conciencia situacional • Construcción de la ciber-resiliencia • Construcción y desarrollo de capacidades • Aumentar la conciencia • Entrenamiento • Compartir información y cooperar	• Comunidad para la ciber-resiliencia • Comunidad para la ciberdefensa • Comunidad para la justicia en el ciberespacio y contra el cibercrimen
Reducción de la cibercriminalidad	• Persecución • Desarrollo de capacidades forenses cibernéticas • Respuesta a amenazas híbridas • Compartir información y cooperar	• Comunidad para la ciber-resiliencia • Comunidad para la ciberdefensa
Desarrollo e implementación de regulaciones y políticas	• Atribución de responsabilidades	• Comunidad para la ciber-resiliencia

	• Manejo de incidentes, respuestas y recuperación • Estandardización y certificación • Ciber-ejercicios y establecimiento de ciber-rangos • Compartir información y cooperar	• Comunidad para la ciberdefensa • Comunidad para la justicia en el ciberespacio y contra el cibercrimen • Comunidad para la ciber diplomacia y las iiber políticas
Desarrollo de recursos industriales y tecnológicos	• Investigación • Interoperabilidad • Compartir información y cooperar[4]	• Comunidad para la ciber-resiliencia

Fuente: elaboración propia a partir de ENISA, 2020a, 2020b, 2020c

La tabla muestra un entramado de objetivos y prioridades coherentes con la esquematización ofrecida por la UE en la primera Estrategia de ciberseguridad de 2013 y que sientan sus bases en la cooperación entre las distintas comunidades de profesionales encargadas de cooperar en los distintos ámbitos de la ciberseguridad europea.

La tercera pregunta que quiere contestar este apartado se relaciona con la evolución del gasto para la política de ciberseguridad de la UE en los últimos años. Un documento publicado en marzo de 2019 por la Corte Europea de Auditores afirma que los gastos europeos en ciberseguridad no son totalmente transparentes debido a que la mayoría de ellos se reparten en diferentes partidas del programa de la Comisión Europea "Horizon 2020" (H2020). A pesar de esto, el informe identifica, en 2018, 279 contratos financiados por la UE y relacionados proyectos para la ciberseguridad, por un total de 786 millones de euros. Los ámbitos de la ciberseguridad con más presupuesto son los fondos para las ayudas y los entrenamientos (183 millones de euros), las herramientas para la ciberseguridad y gastos de administración (143 millones), la protección de los datos de acceso y de la privacidad (101 millones) y la protección de la infraestructura crítica (80 millones) (European Court of Auditors, 2019: 23-24).

Este presupuesto de 786 millones de euros representa un notable incremento si comparado con los años 2015-2016, cuando el gasto para la ciberseguridad registrado es de 437 millones de euros. Esta tendencia al aumento notable del gasto se confirma para los años 2018-2021, debido al anuncio del Banco Europeo de Inversiones de querer invertir 6000 millones de euros en proyectos relacionados con la tecnología de doble uso, la ciberseguridad y la seguridad civil. Y, para terminar, y de cara al futuro, para el periodo 2021-2027, está previsto el lanzamiento del nuevo Programa Digital Europeo, cuya componente relativa a la ciberseguridad dispondrá de un presupuesto total de 2000 millones de euros (European Court of Advisors, 2019: 26).

[4] Este objetivo es el único realmente común a las cuatro categorías y por esta razón es repetido en cada una de ellas. Como se afirma en la introducción, éste puede considerarse como la función fundamental de la política europea de ciberseguridad. Desde 2018, la ciberdefensa se incluye en el Marco de la Cooperación Estructurada Permanente (PESCO) y la UE acuerda con la OTAN fomentar la cooperación en materia de investigación e innovación sobre ciberdefensa (Alonso Lecuit, 2017).

Después de haber hecho el cuadro del aumento del gasto europeo para la ciberseguridad, sólo cabe remarcar, a nivel más concreto, el lanzamiento del "Plan Estratégico de Ciberseguridad Europeo", presentando al Parlamento y Consejo, el 13 de septiembre, por parte de la Comisión Europea. Este plan otorga un mandato permanente a la ENISA, transformada definitivamente en la Agencia de Ciberseguridad Europea: el presupuesto de ENISA se ve incrementado hasta 2021 de 11 a 23 millones de euros y su plantilla sube de 84 a 125 personas (Alonso Lecuit, 2017). Según los últimos datos oficiales publicados, el presupuesto anual de ENISA para 2019 asciende a 16.932.952,05 euros (ENISA, 2019), mientras que en 2018 registraba 11.449.000 euros (ENISA, 2018).

Por lo tanto, para concluir y para contestar a la tercera pregunta de este apartado, el gasto europeo en ciberseguridad ha ido paulatinamente aumentando y, para los próximos años, se confirma un aumento considerable de los recursos financieros de los que dispondrán los actores involucrados en la política de ciberseguridad. Cabe recordar que, junto con los veintidós actores europeos, antes analizados, en los cuales colaboran las cuatro grandes comunidades de profesionales para conseguir los dieciocho objetivos y prioridades, hay una miríada de actores estatales y subestatales, públicos y privados. Todos ellos se reparten el presupuesto comunitario y contribuyen al diseño y a la implementación de esta política multinivel a través de los proyectos financiados especialmente por la Comisión Europea y el Banco Europeo de Inversiones.

Conclusiones

El objetivo de este artículo de reflexión es corroborar si la creciente importancia de la ciberseguridad y la consecuente evolución estratégica y normativa en seno a la UE se traduce en cambios visibles en cuanto a actores y diseño e implementación de la política europea en este ámbito. Cómo hemos visto al principio, la cadena de ataques cibernéticos del siglo XXI demuestra que las ciberamenazas constituyen un abanico siempre más amplio y multidimensional al que la UE y sus Miembros se deben enfrentar. C, ciberseguridad y ciberdelincuencia tienen definiciones siempre más detalladas y precisas, y acaban adquiriendo aquella multidimensionalidad que es típica de otros ámbitos de la seguridad en la posguerra fría.

El discurso estratégico y normativo de la UE, llamada a jugar el papel fundamental de arena de la cooperación multinivel entre actores públicos y privados, tiene una marcada evolución, especialmente después de la primera Estrategia de ciberseguridad, publicada en 2013. Los hoy en día dieciocho objetivos y prioridades – pertenecientes a cuatro grandes categorías - son responsabilidad de cuatro comunidades de profesionales que podemos etiquetar como Justicia, Defensa, Resiliencia y Diplomacia/Política. Estas comunidades buscan un nivel siempre más alto de cooperación, compartición de la información e interoperabilidad, utilizando como bases de trabajo los veintidós actores europeos que componen el mapa europeo de la ciberseguridad, entre los cuales destaca la ENISA que, desde 2017, tiene un mandato permanente como Agencia para la Ciberseguridad Europea. El aumento del presupuesto y de la plantilla de la ENISA en los últimos años confirma la tendencia

generalizada en seno a la UE de destinar siempre más recursos financieros y personales a la ciberseguridad europea, como confirmado por los datos reportados en el párrafo anterior.

Para resumir, la política de ciberseguridad europea está viviendo y vivirá en los próximos años una expansión considerable en todos los ámbitos: normativo, político, en términos de actores y recursos. Este fenómeno es coherente con los mismos procesos que se dan a nivel estatal y es necesario debido al importante rol de la UE de coordinar y de fomentar la eficiencia y eficacia de coordinación entre sus Miembros.

Referencias bibliográficas

Alonso Lecuit, J. (2017), "Relanzamiento del plan de ciberseguridad de la UE", ARI 97/2017, *Real Instituto Elcano,* disponible en http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/ari97-2017-relanzamiento-plan-ciberseguridad-ue-union-europea [consultado el 03/07/2020]

BOE - Boletín Oficial del Estado español (2011), "Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas", disponible en https://www.boe.es/buscar/pdf/2011/BOE-A-2011-7630-consolidado.pdf [consultado el 20/05/2020]

Chang, G. G. (2009), "Busting the Ghost Hackers", *Forbes*, 30 de marzo, disponible en https://www.forbes.com/2009/03/30/ghostnet-spyware-hackers-opinions-columnists-china-obama.html#3c08af40e242 [consultado el 21/05/2020]

Comisión Europea (2013), "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace", 7 de febrero, disponible en https://eeas.europa.eu/archives/docs/policies/eu-cybersecurity/cybsec_comm_en.pdf [consultado el 25/06/2020]

Comité Seleccionado de Inteligencia del Senado de los EEUU (2019), "Report on Russian Active Measures Campaigns and Interference in the 2016 U.S. Elections", disponible en https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf [consultado el 21/05/2020]

Congressional Research Service (2020), "Defense Primer: Cyberspace Operations", disponible en https://fas.org/sgp/crs/natsec/IF10537.pdf [consultado el 19/05/2020]

Consejo de la Unión Europea (2017), "Plan de acción para la aplicación de las Conclusiones del Consejo sobre la Comunicación conjunta al Parlamento Europeo y al Consejo titulada «Resiliencia, disuasión y defensa: fortalecer la ciberseguridad de la UE", 12 de diciembre, disponible en http://data.consilium.europa.eu/doc/document/ST-15748-2017-INIT/es/pdf [consultado el 03/07/2020]

Consejo Europeo (2020), "Ciberseguridad en Europa: normas más estrictas y mejor protección", disponible en https://www.consilium.europa.eu/es/policies/cybersecurity/ [consultado el 19/05/2020]

Consejo Europeo (2018), "EU to became more cyber-proof as Council backs deal on common certification and beefed-up agency", 19 de diciembre, disponible en https://www.consilium.europa.eu/en/press/press-releases/2018/12/19/eu-to-become-more-cyber-proof-as-council-backs-deal-on-common-certification-and-beefed-up-agency/ [consultado el 28/06/2020]

DSN - Departamento de Seguridad Nacional de España (2020), "Ciberseguridad", disponible en https://www.dsn.gob.es/es/sistema-seguridad-nacional/qu%C3%A9-es-seguridad-nacional/%C3%A1mbitos-seguridad-nacional/ciberseguridad [consultado el 19/05/2020]

ENISA (2020a), "Cybersecurity institutional map. Actors", disponible en https://www.enisa.europa.eu/cybersecurity-institutional-map/results?root=actors [consultado el 30/06/2020]

ENISA (2020b) "Cybersecurity institutional map. Communities", disponible en https://www.enisa.europa.eu/cybersecurity-institutional-map/results?root=communities [consultado el 30/06/2020]

ENISA (2020c), Cybersecurity institutional map. Priorities", disponible en https://www.enisa.europa.eu/cybersecurity-institutional-map/results?root=priorities [consultado el 03/07/2020]

ENISA (2019a), "Press Release. Exposure to cyber-attacks in the EU remains high – New ENISA Threat Landscape report analyses the latest cyber threats", disponible en https://www.enisa.europa.eu/news/enisa-news/exposure-to-cyber-attacks-in-the-eu-remains-high [consultado el 20/05/2020]

ENISA (2019b), "ENISA Threat Landscape Report 2018. 15 Top Cyber Threats and Trends", disponible en https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018 [consultado el 20/05/2020]

ENISA (2019c), "Statement of Estimates 2019", disponible en https://www.enisa.europa.eu/about-enisa/accounting-finance/files/annual-budgets/enisa-2019-annual-budget/view [consultado el 03/07/2020]

ENISA (2018), "Statement of Estimates 2018", disponible en https://www.enisa.europa.eu/about-enisa/accounting-finance/files/annual-budgets/enisa-2018-annual-budget/view [consultado el 03/07/2020]

ENISA (2015), "Definition of Cybersecurity. Gaps and overlaps in standardisation", disponible en https://www.enisa.europa.eu/publications/definition-of-cybersecurity [consultado el 19/05/2020]

European Court of Auditors (2019), "Challenges to effective EU cybersecurity policy", disponible en https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf [consultado el 03/07/2020]

Kaspersky (2020), "¿Qué es el ransomware WannaCry?", disponible en https://www.kaspersky.es/resource-center/threats/ransomware-wannacry [consultado el 20/05/2020]

Ottis, R. (2008), "Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective", Cooperative Cyber Defence Centre of Excellence of Tallinn, disponible en https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf [consultado el 21/05/2020]

Parlamento Europeo y Consejo Europeo (2019), "Reglamento UE 2019/881 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»)", 17 de abril, disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32019R0881&from=EN [consultado el 30/06/2020]

Radziwill, Y. (2015), "Cyber-Attacks and the Exploitable Imperfections of International Law", Ed. Brill – Nijhoff.

Sanger, D. E. (2015), "U.S. Decides to Retaliate Against China's Hacking", *The New York Tymes,* 31 de julio, disponible en https://www.nytimes.com/2015/08/01/world/asia/us-decides-to-retaliate-against-chinas-hacking.html [consultado el 21/05/2020]

Segal, A. (2016), "The U.S.-China Cyber Espionage Deal One Year Later", *Council of Foreign Relations,* 28 de septiembre, disponible en https://www.cfr.org/blog/us-china-cyber-espionage-deal-one-year-later [consultado el 21/05/2020]

Subijana Zunzunegui, I. J. (2008), "El ciberterrorismo, una perspectiva legal y judicial", *Eguzkilore: Cuaderno del Instituto Vasco de Criminología*, n. 22, 169-187, disponible en https://www.ehu.eus/documents/1736829/2176658/08+Subijana.indd.pdf [consultado el 20/05/2020]

Szoldra P. (2016), "A US Army General says North Korea has some of the world's best hackers", *Business Insider,* 10 de mayo, disponible en https://www.businessinsider.com/north-korea-worlds-best-hackers-2016-5?IR=T [consultado el 21/05/2020]

The Hill (2012), "Anonymous hacks DOJ server, releases data", 22 de mayo, disponible en https://thehill.com/policy/technology/228839-anonymous-hacks-justice-department-releases-data [consultado el 21/05/2020]

Unión Europea (2016), "A Global Strategy for the European Union's Foreign And Security Policy. Shared Vision, Common Action: A Stronger Europe", junio, disponible en https://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf [consultado el 26/06/2020]

Valle, M. (2020), "Estos fueron los mayores ciberataques en 2019", *Bit Life Media,* 16 de enero, disponible en https://bitlifemedia.com/2020/01/estos-fueron-los-mayores-ciberataques-de-2019/ [consultado el 21/05/2020]

Washington Post (2012), "U.S., Israel developed Flame computer virus to slow Iranian nuclear efforts, officials say", 19 de junio, disponible en https://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html [consultado el 21/05/2020]

WikiLeaks (2020), "What is Wikileaks", disponible en https://wikileaks.org/What-is-WikiLeaks.html [consultado el 21/05/2020]

Análisis Jurídico-Político, 2(3) 2020, 93–114 (https://doi.org/10.22490/26655489.3908)

Publicado por

Con el apoyo de