Revista CIDOB d'Afers Internacionals
ISSN: 1133-6595
ISSN: 2013-035X
publicaciones@cidob.org
Barcelona Centre for International Affairs
España

Munkøe, Malthe; Mölder, Holger
La ciberseguridad en la era de hipercompetitividad: ¿puede la Union Europea afrontar los nuevos retos?
Revista CIDOB d'Afers Internacionals, núm. 131, 2022, Mayo-Septiembre, pp. 69-94
Barcelona Centre for International Affairs
España

DOI: https://doi.org/10.24241/rcai.2022.131.2.69

Disponible en: https://www.redalyc.org/articulo.oa?id=695774517007

Revista CIDOB d'Afers Internacionals
n.º 131, p. 69-94
ISSN:1133-6595 | E-ISSN:2013-035X
DOI: doi.org/10.24241/rcai.2022.131.2.69

Fecha de recepción: 25.11.21
Fecha de aceptación: 20.04.22

La ciberseguridad en la era de hipercompetitividad: ¿puede la UE afrontar los nuevos retos?

Cybersecurity in the era of hypercompetitiveness: can the EU meet the new challenges?

Malthe Munkøe
Asesor sénior, BusinessEurope (escribe a título personal). *malthemunkoe@gmail.com.*

Holger Mölder
Profesor titular de Relaciones Internacionales, TalTech-Tallinn University of Technology.
holger.molder@taltech.ee. ORCID: https://orcid.org/0000-0003-2481-2735

Cómo citar este artículo: Munkøe, Malthe y Mölder, Holger. «La ciberseguridad en la era de hipercompetitividad: ¿puede la UE afrontar los nuevos retos?». *Revista CIDOB d'Afers Internacionals*, n.º 131 (septiembre de 2022), p. 69-94. DOI: doi.org/10.24241/rcai.2022.131.2.69

Resumen: En su discurso de 2021 sobre el estado de la Unión, la presidenta de la Comisión Europea, Ursula von der Leyen, recalcó la necesidad de mejorar la ciberseguridad de la UE. El panorama de las amenazas es diverso y cambiante: desinformación y noticias falsas, ataques informáticos contra infraestructuras gubernamentales, injerencia en elecciones de terceros países, etc. Ante ello, en diciembre de 2020, la UE dio a conocer una nueva Estrategia de Ciberseguridad que incluye iniciativas legislativas e institucionales: desde la revisión de la Directiva NIS –la primera legislación sobre ciberseguridad de la UE– hasta el establecimiento de un ciberescudo para identificar los ataques cibernéticos a gran escala. Para ser efectiva en este campo, en que participan una multitud de actores, la UE deberá garantizar la cooperación y el intercambio de información de forma sólida, tanto a escala nacional como europea, así como con la OTAN.

Palabras clave: Unión Europea, ciberseguridad, hipercompetitividad, integración europea, guerra informativa, seguridad económica

Abstract*: In her 2021 State of the Union address, European Commission President Ursula von der Leyen stressed the need to improve EU cybersecurity. The threat landscape is diverse and changing, and includes disinformation and fake news, cyber-attacks on government infrastructure and interference in elections in third countries. With this in mind, in December 2020 the EU unveiled a new Cybersecurity Strategy that includes legislative and institutional initiatives: from the revision of the NIS Directive – the EU's first cybersecurity legislation – to the establishment of a cybershield to identify large-scale cyber-attacks. To be effective in this field, which involves a multitude of actors, the EU will need to ensure robust cooperation and information exchange, both at national and European level, as well as with NATO.*

Key words*: European Union, cybersecurity, hypercompetitiveness, European integration, information warfare, economic security*

En la actualidad, la seguridad ha pasado de ser una cuestión relativamente opaca a convertirse en un tema de gran transcendencia política. El 15 de septiembre de 2021, la presidenta de la Comisión Europea, Ursula von der Leyen, dedicó un tiempo considerable a este asunto en su discurso sobre el estado de la Unión, señalando que: «No podemos hablar de defensa sin hablar de cibernética. En un mundo en el que todo está conectado, todo puede ser hackeado. Vista la escasez de recursos, debemos aunar nuestras fuerzas, y no darnos por satisfechos solamente con lidiar con la amenaza cibernética, sino que tenemos que trabajar para ser líderes en el ámbito de la ciberseguridad» (Von der Leyen, 2021). De esta forma, plenamente establecido lo cibernético en el discurso político de la Unión Europea (UE), no resulta sorprendente que una serie de iniciativas en forma de nueva legislación concerniente al campo cibernético y cambios institucionales estén listos para implementarse y desarrollarse. En su discurso, Von der Leyen incluso llegó a pedir una «política europea de ciberdefensa», lo que es un indicio de la centralidad otorgada a la ciberseguridad en la formulación de políticas de la UE.

La amenaza a la ciberseguridad a la que se enfrenta Europa es de naturaleza polifacética y procede tanto de bandas criminales, como de grupos con alguna supuesta relación con rivales geopolíticos, aunque también de fuerzas regulares cibersecuritarias desplegadas como parte del aparato militar que otros estados pueden usar en caso de conflicto.

La amenaza a la ciberseguridad a la que se enfrenta Europa es de naturaleza polifacética y procede tanto de bandas criminales, como de grupos con alguna supuesta relación con rivales geopolíticos, aunque también de fuerzas regulares *cibersecuritarias* desplegadas como parte del aparato militar que otros estados pueden usar en caso de conflicto, como se ha demostrado en la actual guerra ruso-ucraniana. Del mismo modo, la naturaleza de las ciberamenazas varía: desde las operaciones que persiguen deteriorar o interrumpir infraestructuras, hasta el ciberespionaje o los programas de extorsión, que incluyen desde la suplantación de identidad hasta la obtención de información comprometedora, por ejemplo, con fines de chantaje. Esta diversidad de amenazas surgidas del campo cibernético requiere un enfoque multidimensional, así como la colaboración institucional entre las fuerzas de orden público, de seguridad y de defensa, además de otros actores implicados. La rápida evolución de este fenómeno ha requerido una serie de desarrollos de políticas normativas, ya sean de ámbito estatal o europeo.

En este contexto hipercompetitivo, este artículo examina el desarrollo de las amenazas a la ciberseguridad de la UE y cómo sus élites han percibido el

cambiante panorama de dichas amenazas, sobre la base de lo cual han articulado la necesidad de ampliar la política europea de ciberseguridad para afrontar los retos a los que se enfrentan; a continuación, se focaliza en el desarrollo de la política de ciberseguridad desarrollada por la UE en respuesta a estas amenazas; y, por último, analiza los retos actuales para la UE y las perspectivas del trabajo normativo actualmente en curso que permitirán abordar estos desafíos de forma amplia y exitosa.

La era de la hipercompetitividad y la cibernética

En el discurso ya referenciado de Von der Leyen, esta subrayó que nos enfrentamos a un contexto de seguridad nuevo, hipercompetitivo y en rápido desarrollo, que se caracteriza por una rivalidad y competitividad entre potencias cada vez mayor, en el que las opciones de seguridad colaborativas posteriores a la Guerra Fría están siendo cuestionadas y el auge del nacionalismo y del proteccionismo amenazaría la paz estable de la que ha disfrutado Europa durante décadas. Así lo expresó, de forma cruda y reveladora, la presidenta de la Comisión Europea: «Nos adentramos en una nueva era, la de la hipercompetitividad, en la que hay quien está dispuesto a hacer lo que sea con tal de ganar influencia, ya se trate de prometer vacunas y proporcionar créditos a elevados intereses, o de recurrir a los misiles y a la desinformación. Es la era de las rivalidades regionales, en la que las principales potencias están reorientando sus atenciones mutuas» (Von der Leyen, 2021).

El triunfo de los sistemas políticos internacionales colaborativos e integracionistas iniciado tras el fin de la Guerra Fría ha resultado ser fugaz. Los nuevos desafíos a la seguridad que emergen de un contexto internacional mucho más adverso han evidenciado que una digitalización en rápida evolución no solo puede proporcionar grandes beneficios para nuestras sociedades, sino que también puede generar nuevos riesgos y vulnerabilidades. Ya sea por el intento de manipular los procesos electorales, por el espionaje industrial, por el hackeo de información clasificada de gobiernos extranjeros, o por el potencial para causar la destrucción de la infraestructura o las capacidades militares del enemigo, está claro que las ciberamenazas ya no pueden ignorarse. Las potencias revisionistas usan los ataques cibernéticos para favorecer sus ambiciones estratégicas y desafiar el statu quo en el sistema internacional (Tenembaum, 2012). El mundo se abre paso, así, hacia una nueva era de rivalidad entre

grandes potencias con tensiones cada vez mayores como, en particular, las guerras comerciales entre Estados Unidos y China. Rusia, China, Corea del Norte y otras potencias que desafían el statu quo han elaborado nuevas doctrinas estratégicas, especialmente sobre el uso de medios híbridos, para retar la hegemonía occidental. Una potencia revisionista puede tener ventaja a la hora de desafiar el statu quo del sistema internacional, ya que va más allá de las expectativas racionales (Krastev, 2014). Por lo tanto, el empoderamiento de ciertos actores y estados ha generado mayor inestabilidad y competitividad en las relaciones internacionales. Es más, encontrar soluciones duraderas para los problemas mundiales actuales –como la pandemia de la COVID-19 o el cambio climático– en un sistema internacional fuertemente polarizado resultará probablemente mucho más difícil que en un sistema caracterizado por la búsqueda de resultados mutuamente beneficiosos a través de la colaboración.

Este panorama de mayor rivalidad en las relaciones internacionales no solo tiene un impacto en la competencia por el liderazgo económico mundial entre Estados Unidos y China, sino que muy a menudo socava la unidad de las democracias liberales occidentales y erosiona la colaboración entre la UE y Estados Unidos, porque ambos son posibles competidores económicos. El pacto de seguridad y defensa AUKUS, firmado en septiembre de 2021 entre Estados Unidos, Reino Unido y Australia, derivó en una crisis diplomática entre Australia y Francia después de que Australia incumpliera el contrato por valor de 90.000 millones de dólares australianos para submarinos de diseño francés (Sheftalovich, 2021). El ministro de Asuntos Exteriores galo, Jean Yves Le Diran, calificó el anuncio de AUKUS de «brutal» e «imprevisible» y como una reminiscencia de la Presidencia de Donald Trump. Por su parte, la presidenta de la Comisión Europea, Ursula von der Leyen, mostraba su preocupación por el hecho de que «uno de nuestros estados miembros haya recibido un trato inaceptable» (Walden, 2021). Aquellos que desafían el sistema democrático liberal podrían sacar tajada de los acontecimientos que llevan a los estados occidentales a disputas y rivalidades entre ellos.

Puesto que los nuevos desafíos mundiales –COVID-19, cambio climático, guerra en Ucrania– amenazan nuestro planeta, sería sumamente importante que los países aunaran esfuerzos para elaborar políticas conjuntas y encontrar vías adecuadas para alcanzar soluciones comunes. En este entorno de seguridad cada vez más hostil, la UE todavía se manifiesta al viejo estilo, como una isla de relativa estabilidad, que se basa en activos cooperativos. En la 73ª Asamblea de la Organización Mundial de la Salud (OMS) celebrada en mayo de 2020, Von der Leyen (2020a) afirmó: «Es el momento de la colaboración. Es el momento de la ciencia y la solidaridad. Es el momento de que toda la humanidad se reúna en torno a una causa común. Y pueden contar con que Europa siempre trabajará para el conjunto».

Desde el Tratado de París de 1951, que estableció la Comunidad Europea del Carbón y del Acero (CECA), los avances realizados hacia la integración europea han sido impresionantes y han allanado el camino para una cooperación regional más estrecha, lo cual debería aumentar la probabilidad de que la integración socioeconómica se extendiese hasta la integración política, de modo que los gobiernos nacionales transfieran más autoridad a las organizaciones regionales (Schmitter, 2004: 47-48). En este sentido, ha habido intentos más o menos fructíferos de crear mecanismos integracionistas para resolver las crisis en la UE y sus estados miembros. Por ejemplo, a raíz de la crisis económica de 2007-2008, se creó el Mecanismo Europeo de Estabilidad (MEDE) intergubernamental para conceder préstamos a los estados miembros pertenecientes a la zona del euro con problemas financieros (Zeevaert, 2020). En materia de ciberseguridad, los ataques perpetrados en 2007 contra instituciones gubernamentales e infraestructura crítica en Estonia, presuntamente respaldados por Rusia, produjeron un efecto indirecto de mayor cooperación en ciberseguridad. De igual manera, la pandemia de la COVID-19 ha provocado un efecto indirecto similar en la seguridad sanitaria.

Los nuevos desafíos a la seguridad que emergen de un contexto internacional cada vez de mayor rivalidad y mucho más adverso han evidenciado que una digitalización en rápida evolución, aunque puede proporcionar grandes beneficios para nuestras sociedades, también puede generar nuevos riesgos y vulnerabilidades.

Sin embargo, el enfoque integracionista –que persigue conseguir ventajas racionales gracias a una mayor cooperación– no encuentra un contexto favorable en la actualidad, ya que el clima político está cambiando y puede ser adverso para una mayor integración regional. Asimismo, aunque la amenaza militar directa a la UE proveniente de otros estados se ha reducido enormemente, existen muchos otros desafíos a la seguridad: guerras comerciales, movimientos migratorios, ataques cibernéticos, propagación de la cultura del miedo, disturbios sociales, terrorismo y delincuencia de alcance internacional, así como pérdida de control sobre las armas de destrucción masiva, entre otras amenazas que podrían quebrantar de forma eficiente los principios y objetivos alcanzados en el marco del proceso de integración europea[1].

1. Además, la actual guerra entre Rusia y Ucrania pone en evidencia que queda pendiente abordar la seguridad militar.

Hoy en día, el término *cyber* o *ciber* se está convirtiendo en un elemento de marketing que puede adjuntarse prácticamente a todo (Whyte *et al.*, 2021: 4). Las nuevas tecnologías han alentado a variados movimientos populistas del espectro político –desde la extrema derecha hasta la extrema izquierda– a usar plataformas virtuales para difundir sus ideologías con las que han conseguido una gran fuerza, lo que nunca antes había sucedido. De esta forma, los movimientos populistas y extremistas, tanto dentro como fuera de la UE, propagan cada vez más la imagen de una Europa en declive e intentan desacreditar la democracia liberal, que describen como un sistema de gobierno «débil» que se encuentra en crisis (Krouwel y Önnerfors, 2021). Tras la elección de Donald Trump como presidente de Estados Unidos en 2016, su programa más proteccionista de «America First» (América, primero) alentó la rivalidad entre las grandes potencias y volvió más inestable el sistema internacional. De hecho, los patrones introducidos por la reciente oleada populista todavía influyen en el clima político y confirman que, si alguien decide desafiar el sistema internacional, podría tener ventaja sobre aquellos que deberían defenderlo.

Asimismo, está en auge la tendencia de llevar a cabo operaciones de injerencia en el campo cibernético, mediante las cuales algunos gobiernos revisionistas tienen como objetivo influir en ciertas emociones políticas o discursos públicos de otros países. Se ha usado propaganda digital para suprimir derechos humanos fundamentales, desacreditar a los oponentes políticos o silenciar las opiniones disidentes. Las democracias liberales pueden volverse especialmente vulnerables a estas operaciones de injerencia –incluida la propaganda digital–, porque el derecho a libertad de expresión y la libertad de prensa brindan a sus oponentes una puerta abierta para atacar sus valores. Al respecto, Bradshaw y Howard (2019) identificaron manipulaciones en las redes sociales en 70 países, de los cuales 26 han mostrado una tendencia autoritaria. Siete países (Arabia Saudí, China, India, Irán, Pakistán, Rusia y Venezuela) usaron plataformas de redes sociales (por ejemplo, Facebook o Twitter) para realizar operaciones de injerencia en el extranjero. Según los autores, Facebook ha sido la red más popular para dichas manipulaciones, puesto que 56 países habían usado esta plataforma para la propaganda digital. Estudios llevados a cabo en Taiwán y Ucrania han evidenciado que las campañas mediáticas de larga duración realizadas en prensa, radio, televisión y redes sociales pueden tener un impacto sobre la opinión pública para apoyar a candidatos respaldados por China o Rusia, respectivamente (Baterman *et al.*, 2021).

Las operaciones cibernéticas organizadas por actores revisionistas apuntan directamente al conocimiento y a la ciencia, mediante el uso ilegal, la

revelación, la interrupción, la eliminación, la corrupción, la modificación, la inspección, el registro o la devaluación de la información (Hamulák, 2018). La difusión masiva de ideologías extremistas y teorías conspirativas debido al fácil acceso al campo cibernético nos recuerda que la digitalización puede contener amenazas ocultas que pueden atentar contra los valores de la UE.

Los retos de la ciberseguridad

La revolución digital ha creado una plataforma propicia para iniciar y promover ciberguerras (o guerras tecnológicas) mediante el ataque deliberado a ordenadores y redes de estados soberanos u organizaciones internacionales (Troitiño, 2022). En abril de 2007, por ejemplo, el Gobierno de Estonia trasladó un monumento en recuerdo de los soldados rusos caídos durante la Segunda Guerra Mundial a un emplazamiento de Tallin más discreto y, como respuesta, estallaron disturbios entre la minoría rusófona. Poco después, empezaron cuatro oleadas de ciberataques, principalmente ataques de denegación de servicio distribuido (DDoS, por sus siglas en inglés), dirigidos a instituciones gubernamentales, medios de comunicación y bancos de Estonia. Si bien el impacto en cuanto a daños reales sobre la infraestructura crítica no fue notable, ello supuso una alerta para reconocer los riesgos y la necesidad de reforzar las capacidades en ciberseguridad.

Estos desarrollos alcanzaron un punto álgido con el aludido discurso de Von der Leyen (2021), cuando esta subrayó que la naturaleza de las actuales amenazas a la seguridad estaba evolucionando rápidamente, pasando de los ataques híbridos o cibernéticos a la escalada armamentística en el espacio: «La tecnología disruptiva ha venido a nivelar en gran medida el uso del poder por parte de estados 'canallas' [*rogue states*] o grupos no estatales, porque para causar daños a gran escala ya no hacen falta ni ejércitos ni misiles. Basta con un ordenador portátil o un teléfono para paralizar una fábrica, toda una administración municipal o un hospital. Con un simple teléfono inteligente conectado a Internet se puede alterar el curso de unas elecciones». Los ciberataques pueden apuntar eficazmente a la propiedad intelectual, a operaciones comerciales, a infraestructura crítica, así como a sistemas militares, pero también se utilizan en operaciones de información e injerencia para captar la mente de las personas y difundir la cultura del miedo y la incertidumbre. Asimismo, pueden afectar a estados, a empresas y a la ciudadanía en general, además de suponer una amenaza múltiple sobre nuestro bienestar y seguridad.

Alarmante aumento de la desinformación y las noticias falsas en el panorama mediático

En el contexto actual de *posverdad*[2], la información puede convertirse fácilmente en blanco de manipulaciones y en un mercado mediático para conseguir más atención y generar más beneficios. La cibercultura ha provocado el auge de medios y producción artificiales, manipulación y modificación de datos y medios de forma automatizada, así como una nueva oleada de *ultrafalsos* (o *deepfakes*)[3], por la que una persona que aparece en una imagen o un vídeo ya existentes es substituida por otra con un parecido razonable. La evolución de los medios artificiales puede conducir fácilmente a percepciones erróneas y promulgar nuevos mitos, creencias y conspiraciones que ayudan a aumentar la oleada populista.

Hackeos en infraestructuras gubernamentales

La digitalización provoca que los ataques contra otros gobiernos sean más rentables y ocultos, ya que el atacante puede permanecer fácilmente invisible y no ser identificado. Durante la pandemia de la COVID-19, varias agencias de los estados miembros y de la UE han sufrido ciberataques, encontrando los gobiernos dificultades para garantizar una protección total, por lo que han sido necesarias acciones coordinadas. Por ejemplo, en diciembre de 2020, la Agencia Europea del Medicamento anunció que había sido objeto de un ciberataque y, en marzo de 2021, el periódico neerlandés *De Volkskrant* publicaba un artículo que afirmaba que «fuentes cercanas a la investigación» habían revelado que detrás de los ataques estaban un servicio de inteligencia ruso y espías chinos (Reuters, 2021a). Aunque esa afirmación no fue confirmada oficialmente, es representativa del clima de inestabilidad actual.

---

2. El mundo contemporáneo de la posverdad describe una situación en la que «los hechos objetivos tienen menos influencia en la formación de la opinión pública que las apelaciones a las emociones y las creencias personales» (English Oxford Living Dictionaries, s.f.).
3. Los *ultrafalsos* se originan usando técnicas automatizadas de generación de contenido, incluida la inteligencia artificial, para crear imágenes de hechos falsos, manipular o generar texto, imágenes visuales (por ejemplo, retoques de fotos) o contenido de audio (por ejemplo, «voz clonada») (Kalpokas y Kalpokiene, 2021: 37; Sample, 2020).

Injerencias en elecciones de terceros países

Las injerencias en procesos electorales de terceros países se pueden producir ya sea a través de hackeos para alterar el escrutinio o revelar información confidencial sobre algún candidato, ya sea a través de diferentes campañas de desinformación, lo que se ha convertido en una amenaza constante para las democracias. Se ha descubierto recientemente que el grupo de hackers informáticos rusos *Ghostwriter* ha lanzado ataques contra cuerpos electos germanos con mensajes de correo electrónico falsos (Cerulus y Klingert, 2021).

Aplicación militar en la guerra directa

En 1988, Hashemi Rafsanjani, un portavoz del Parlamento iraní que más tarde sería el presidente, se refirió a las armas químicas y biológicas como «la bomba atómica de los pobres» (Headley, 2018). Hoy, su afirmación puede extenderse a la amenaza potencial del ciberarmamento, ya que desarrollar sus capacidades, aunque es menos costoso, es más eficiente. Los virus informáticos, el fraude electrónico o *phishing*, los gusanos informáticos y el *software* malintencionado o *malware* difundidos por instituciones militares pueden acabar con infraestructuras críticas, pudiendo los ataques de DDoS dañar redes y dispositivos informáticos (Andress y Winterfeld, 2014).

Ciberespionaje

Para el público, en general, los ciberataques suelen estar relacionados con ataques contra países con el fin de destruir su infraestructura crítica; sin embargo, la digitalización ha abierto nuevos caminos para tener acceso a nuevas tecnologías y secretos comerciales. Se lanzaron campañas anónimas de ciberespionaje contra varios funcionarios de gobiernos, incluyendo el ministro de Interior belga, políticos polacos y hospitales de Irlanda y Francia (Cerulus, 2021a). Asimismo, en este sentido, han surgido temores por la implicación de China en las redes inalámbricas 5G, debido a las acusaciones de que los equipos de redes móviles de proveedores chinos pueden contener puertas traseras que permitan la vigilancia por parte del Gobierno chino.

Guerra económica, espionaje industrial y el dilema de la desconexión

Esto puede incluir espionaje industrial (por ejemplo, robo de propiedad intelectual, información confidencial, planes comerciales diversos), presiones y amenazas sobre los clientes y el mero intento de sembrar cizaña para perjudicar a la competencia. La Administración estadounidense de Trump publicó una orden ejecutiva para restringir las transacciones de productos o servicios de tecnologías de la información y la comunicación (TIC) vinculados a un «adversario extranjero», lo que se relaciona con la acusación de que empresas chinas (por ejemplo, Huawei) usaban sus productos con fines de espionaje industrial (Lim y Ferguson, 2019). Esta cuestión también está relacionada con actuaciones delictivas, que en determinadas circunstancias pueden tener alcance gubernamental. Por ejemplo, Corea del Norte obtiene una parte de sus ingresos del robo cibernético (Reuters, 2019), lo que se está convirtiendo en una especie de modelo de negocios para los estados *canalla*, pero también para actores internacionales sin reconocimiento (como la organización Estado Islámico).

Delincuencia en el ciberespacio

Los ciberdelincuentes no necesariamente roban documentos o planes secretos guardados en cajas fuertes cerradas, sino que pueden simplemente hackear los sistemas informáticos de sus rivales. Informes recientes señalan que la ciberdelincuencia cada vez está mejor organizada y más extendida, lo que perjudica a compañías europeas –grandes y pequeñas– y amenaza con erosionar la confianza hacia la economía digital. Cabe mencionar que el 43% de los ciberataques se dirigen a pequeñas empresas que, obviamente, tienen menos recursos y capacidad financiera para invertir en ciberseguridad (Cyber Competence Network, 2021).

Según todos los indicios, pues, hemos visto solo la punta del iceberg de lo que los actores de la ciberseguridad tienen que estar preparados para abordar en el futuro cercano, porque deberán gestionar situaciones de tensiones geopolíticas que conducirán a picos descomunales de incidentes y ciberataques completamente planificados.

La política de la UE ante los retos de la ciberseguridad

La labor de la UE en materia de ciberseguridad se inició en 2004, cuando se creó la Agencia Europea de Seguridad de las Redes y de la Información (ENISA, por sus siglas en inglés) en Heraclión (Grecia), cuyo mandato es realizar análisis e investigaciones sobre ciberseguridad, fomentar la cooperación y la confianza entre los estados miembros en la materia, proporcionar formación y contribuir a la sensibilización[4]. Luego, tuvo que pasar casi una década para tener lugar el siguiente gran avance en materia de ciberseguridad en la UE. Antes, sin embargo, en 2011, se creó la Agencia Europea para la Gestión Operativa de Sistemas Informáticos de Gran Magnitud en el Espacio de Libertad, Seguridad y Justicia (eu-LISA) para gestionar los sistemas informáticos de gran magnitud necesarios, en especial, para el espacio Schengen y la Agencia Europea de la Guardia de Fronteras y Costas (Frontex). Y ya en 2013, la UE dio a conocer su primera Estrategia de Ciberseguridad, señalando la diversidad de riesgos, desde las actividades cibernéticas patrocinadas por estados[5] hasta grupos políticos o criminales.

En 2013, la UE dio a conocer su primera Estrategia de Ciberseguridad, que hizo un gran hincapié en el trabajo de la que sería la conocida como Directiva NIS, la cual establecería unos requisitos mínimos comunes en torno a la ciberseguridad en todos los estados miembros, garantizando la coordinación y sirviendo de enlace con la ENISA y la Comisión Europea.

La Estrategia de Ciberseguridad 2013 hacía un gran hincapié en el trabajo de la que sería la conocida como Directiva NIS (siglas en inglés de «redes y sistemas de información»)[6], la cual establecería unos requisitos mínimos comunes en torno a la ciberseguridad en todos los estados miembros, garantizando la coordinación al constituir órganos de contacto para participar en las redes pertinentes y servir de enlace con la ENISA y la Comisión Europea. Se alcanzó el acuerdo político sobre la Directiva NIS en diciembre de 2015, aprobándose y entrando

4. Reglamento (CE) No 460/2004 (Parlamento Europeo, 2004)
5. Téngase en cuenta que «patrocinadas por estados» no presupone entender que los estados extranjeros estarían directamente involucrados.
6. Oficialmente, Directiva relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información de la Unión. Directiva (UE) 2016/1148 (Unión Europea, 2016).

en vigor la directiva final en julio de 2016. Se dieron 21 meses a los estados miembros para transponer completamente los requisitos NIS a la legislación nacional, aunque, de hecho, la implementación total no se consideró completa hasta 2020. NIS ha desarrollado, asimismo, una arquitectura institucional para la labor de la UE en materia de ciberseguridad, exigiendo a los estados miembros la designación de puntos de contacto para intercambiar información con los demás estados miembros y las instituciones de la UE, a fin de monitorizar y garantizar la implementación de los requisitos legales de la Directiva; también el establecimiento de Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRT, por sus siglas en inglés) para monitorizar incidentes de ámbito nacional y trabajar juntos a través de una red CSIRT para facilitar la cooperación y el intercambio de información; y, por último, el nombramiento de un representante nacional para un grupo de cooperación que se crearía con el fin de abordar el amplio abanico de asuntos en torno a la ciberseguridad en la UE.

Mientras tanto, Europol, la agencia de la UE en materia policial, abrió un nuevo Centro Europeo de Cibercrimen (EC3) en 2013. El EC3, que combina la investigación sobre amenazas de cibercrímenes con la cooperación operativa, es un centro neurálgico de cooperación para los servicios de los estados miembros, al tiempo que ofrece apoyo forense analítico (incluyendo soporte técnico y digital) para las investigaciones. Por su parte, la Agencia de la Unión Europea para la Cooperación Judicial Penal (Eurojust) también ha ido asumiendo progresivamente el papel de coordinación en casos jurídicos y asuntos judiciales relativos a la ciberseguridad, y la Agencia Europea de Defensa (AED) ha desarrollado programas de formación, llevado a cabo maniobras[7] y realizado investigaciones en el ámbito cibernético (European Defence Agency, 2021b).

En 2015, la UE dio a conocer un nuevo documento estratégico: la Agenda Europea de Seguridad, que analizaba ampliamente los retos de seguridad a los que se enfrentaba Europa e incluyó la ciberseguridad como una de las tres prioridades clave que requerían coordinación a escala comunitaria. En 2017, la Comisión Europea lanzó una versión actualizada de su Estrategia de Ciberseguridad (RTE, 2017), que sintetizaba una visión distinta del panorama. En este sentido, el entonces presidente de la Comisión, Jean-Claude Juncker (2017), señalaba en su discurso sobre el estado de la Unión de 2017 que «los ciberataques pueden ser más peligrosos para la

7. Por ejemplo, EU CYBRID de septiembre de 2017, organizado por la Presidencia estonia del Consejo de la UE, fue el primer ejercicio cibernético de ámbito ministerial de la UE que tuvo como objetivo en especial sensibilizar sobre la necesidad de coordinación ante incidentes de ciberseguridad y para la toma de decisiones estratégicas (Kerikmäe *et al.*, 2019).

estabilidad de las democracias y las economías que las armas y los tanques. (…) Por este motivo, la Comisión propone hoy nuevas herramientas, entre ellas una Agencia Europea de Ciberseguridad, que nos ayuden a defendernos de estos ataques». El hecho de equiparar la ciberseguridad con la seguridad cinética «del mundo real» supuso un paso importante para el desarrollo de una política de ciberseguridad de la UE, que pasó de ser una cuestión de nicho a otra dominante, tal y como sugería el hecho de tener una mayor percepción de amenaza.

Para implementar los diseños de la Estrategia de Ciberseguridad actualizada, la Comisión presentó el llamado Reglamento sobre Ciberseguridad y el marco para una respuesta diplomática conjunta de la UE a las actividades cibernéticas malintencionadas, la llamada «caja de herramientas de la ciberdiplomacia» (Bendiek *et al.*, 2017). Hasta ahora, ENISA tenía solo un mandato temporal que dependía del apoyo político y fiscal para su renovación, lo que frustró los intentos de planificación a más largo plazo. El Reglamento sobre Ciberseguridad finalmente le otorgó un mandato permanente y amplió el alcance de sus responsabilidades operacionales. Es importante señalar que también se le asignó la responsabilidad de implementar los programas de certificación de ciberseguridad de la UE (lo que incluye una serie de actividades como, por ejemplo, establecer estándares comunes para la industria de la computación en la nube).

En 2017, la Comisión Europea lanzó una versión actualizada de su Estrategia de Ciberseguridad, recogiendo las nuevas percepciones de las ciberamenazas. En este sentido, el entonces presidente de la Comisión, Jean-Claude Juncker, señalaba que «los ciberataques pueden ser más peligrosos para la estabilidad de las democracias y las economías que las armas y los tanques (…)».

Al respecto, la UE ha sido calificada como «superpotencia reguladora» (Bradford, 2020) y como «un gigante económico, pero un enano político» (véase, por ejemplo, Leonard, 2018). Como tal, la UE puede tener dificultades para desempeñar un papel decisivo en el campo sumamente politizado de la política de seguridad, pero debería estar bien posicionada para utilizar su poder regulador y económico para establecer programas de certificación y estandarización con una aceptación generalizada. Hay un importante trabajo en marcha sobre este asunto; por ejemplo, con el acuerdo alcanzado en enero de 2020 para establecer una nueva «caja de herramientas del 5G» para las clasificaciones de ciberseguridad del 5G (ENISA, 2020). Ello es fundamental para garantizar unos estándares de ciberseguridad adecuados en Europa, especialmente teniendo en cuenta, por ejemplo, el crecimiento y la generalización de la tecnología del Internet de las cosas; asimismo, puede ayudar a estimular el crecimiento de una industria europea de la ciberseguridad.

Junto con la estrategia actualizada y el Reglamento sobre Ciberseguridad, la Comisión también lanzó el Plan director de la respuesta coordinada a los incidentes y crisis de ciberseguridad a gran escala de la Unión (Comisión Europea, 2017) y presentó una caja de herramientas de ciberseguridad que fundamentalmente ha conseguido que los ministros de asuntos exteriores acepten la posibilidad de desplegar «medidas restrictivas» (es decir, sanciones de la UE) ante «actividades cibernéticas malintencionadas». Esta opción se pondría en práctica en julio de 2020, cuando la UE impuso sus primeras sanciones –prohibición de viajar y congelación de activos– contra seis individuos de China y Rusia, así como tres entidades de China, Rusia y Corea del Norte, en respuesta a una serie de incidentes, incluido el tan publicitado ataque con el criptogusano WannaCry (Unión Europea, 2020b); posteriormente, estas se complementaron con sanciones de prohibición de viajar y congelación de activos contra la unidad militar rusa conocida coloquialmente como «Fancy Bear», también para dos miembros de esa unidad, por el ataque informático de 2015 contra el Parlamento alemán (Unión Europea, 2020a).

A finales de 2019, tras asumir el cargo de presidenta de la Comisión Europea, Ursula von der Leyen declaró la transición digital (junto con la transición verde) como el eje principal de su mandato, lo que preparó el terreno para un aluvión de iniciativas legislativas relativas a políticas digitales, incluido el campo cibernético (Von der Leyen, 2020b). A mediados de 2019, había presentado las orientaciones políticas (*Political Guidelines*) –que describen los objetivos y las visiones de cada nueva Comisión–y, en este caso, destacaba la intención de crear una Unidad Cibernética Conjunta. Así, en diciembre de 2020, la Comisión Von der Leyen publicó una nueva Estrategia de Ciberseguridad que describía un panorama de amenazas bastante oscuro y preveía un número de iniciativas mucho más ambiciosas que las contenidas en la estrategia anterior de 2013.

En este sentido, la Estrategia de Ciberseguridad 2020 exigía revisar la Directiva NIS, puesto que una evaluación de su impacto había revelado que su implementación había sido muy dispar en los diferentes estados miembros, lo que había llevado a la fragmentación de las prácticas y los estándares de seguridad. La directiva revisada, conocida como «NIS2», ampliaría su alcance hasta abarcar todas las medianas y grandes empresas de un abanico más amplio de sectores (entre los que ahora se incluiría el de las telecomunicaciones); también abarcaría las pequeñas empresas si se consideraba que presentaban un perfil de alto riesgo de seguridad. El objetivo sería optimizar los requisitos impuestos sobre las empresas abarcadas, incluyendo la obligación legal de notificar los incidentes de ciberseguridad a las autoridades competentes en los plazos establecidos (Comisión Europea, 2020b). NIS2 avanzará más hacia la armonización de las sanciones entre los estados miembros y también creará un registro de vulnerabilidades de

la UE en ENISA (Comisión Europea, 2020b). Además, se establecerá la Red Europea de Organización de Enlace de Crisis Cibernéticas (Red CyCLONE)[8] para facilitar la cooperación entre los estados miembros en torno a los incidentes críticos (ENISA, 2021).

Formando parte de su paquete de medidas de ciberseguridad, la Comisión también presentó una propuesta para una Directiva relativa a la resiliencia de las entidades o actores considerados críticos, la llamada Directiva CER (Comisión Europea, 2020d), cuya principal novedad es el aumento de los sectores que cubre y el refuerzo de la cooperación transfronteriza. De esta forma, irá más allá del ámbito de aplicación de la actual Directiva relativa a la infraestructura crítica, al abarcar no solo la energía y el transporte, sino también la banca, los mercados financieros, la Administración pública y el espacio. Asimismo, esta directiva exige a los estados miembros que identifiquen las entidades críticas, establezcan una estrategia para reforzar su resiliencia, evalúen periódicamente los riesgos que les pueden afectar y fijen obligaciones para las entidades críticas con el fin de garantizar su resiliencia, por lo que enumera una serie de medidas que dichas entidades deberían llevar a cabo para aumentarla.

En diciembre de 2020, la Comisión Von der Leyen publicó una nueva Estrategia de Ciberseguridad que describía un panorama de amenazas bastante oscuro, preveía un número de iniciativas mucho más ambiciosas y exigía revisar la Directiva NIS.

Complementariamente a estas acciones legislativas, la Estrategia de Ciberseguridad 2020 también exige una serie de cambios institucionales: el desarrollo de un servicio de resolución de sistemas de nombres de dominio (DNS, por sus siglas en inglés)[9], una nueva infraestructura de comunicación cuántica (QCI, por sus siglas en inglés) para que las autoridades públicas transmitan la información confidencial, y mayor ciberseguridad para las propias instituciones europeas (en este sentido, se trabaja en un reglamento para actualizar la normativa actual). Quizá lo más destacado sea que la Comisión tiene la intención de crear un *ciberescudo* –una red de centros de operaciones de seguridad en toda la UE– para detectar muy rápidamente las amenazas y anticiparse a los daños con acciones proactivas, usando inteligencia artificial, entre otras medidas (Comisión Europea, 2020c).

8. La red se creó en 2021 basándose en la cooperación francoitaliana con el fin de servir de enlace entre los ámbitos tecnológico (es decir, los CSIRT) y político durante las crisis cibernéticas a gran escala (ENISA, 2020).
9. Los DNS son fundamentales para el funcionamiento del Internet moderno, y la UE está preocupada por las interrupciones o los ataques contra uno o más de los proveedores clave para empresas.

Simultáneamente, la UE está avanzando con una serie de iniciativas legislativas no horizontales que tendrán importantes repercusiones en materia de ciberseguridad y que incluyen nuevas reglas para los operadores de energía, nuevas reglas relativas a la infraestructura energética y a los flujos transfronterizos de electricidad y una ley de resiliencia operativa digital para entidades financieras (el Reglamento DORA) (Krüger y Brauchle, 2021). Por lo tanto, la UE prepara nuevos avances institucionales en un panorama de la ciberseguridad ya de por sí complejo: una Unidad Cibernética Conjunta, que se establecerá en Bruselas, y un nuevo Centro Europeo de Competencia en Ciberseguridad, que lo hará en Bucarest. Complementando estos avances institucionales en el ámbito de la UE, se ha establecido una Organización Europea de Ciberseguridad (ECSO, por sus siglas en inglés) con el fin de colaborar con la UE estableciendo alianzas público-privadas en materia de ciberseguridad.

Puesto que, de un modo u otro, todas las agencias, empresas y ciudadanos usan herramientas digitales, la ciberseguridad también es en cierta medida esencial para cada sector y ámbito de las políticas. En consecuencia, el número de actores que trabajan en ciberseguridad en la UE es elevado y va en aumento, incluyendo numerosas direcciones generales (DG) y agencias especializadas. De un modo similar, las iniciativas legislativas en otras áreas se van solapando cada vez más con la ciberseguridad, como el trabajo para abordar las responsabilidades jurídicas de los intermediarios digitales, por ejemplo, las redes sociales –a través de la nueva Ley de Servicios Digitales (DSA, por sus siglas en inglés)–, que también tendrá importantes ramificaciones para hacer frente a la difusión de desinformación en Europa (Krüger y Brauchle, 2021). En la misma línea, la UE se prepara para desplegar recursos económicos procedentes de una gran variedad de programas y fuentes propias con diferentes alcances y objetivos para apuntalar su labor en materia de ciberseguridad. Junto con las inversiones de los estados miembros, la Comisión Europea espera inversiones en ciberseguridad por un valor total de 4.500 millones de euros para el período 2021-2027[10].

Todo ello implica que, para abordar con éxito las amenazas a la ciberseguridad, serán necesarios la coordinación efectiva y el enlace entre un gran número de actores e instituciones a diferentes escalas (Singh, 2018; Ilves *et al.*, 2016).

10. Para un resumen de las políticas de ciberseguridad en la UE, véase Domenico Ferrara, funcionario de políticas de la Comisión Europea, DG CNECT.H.1 Tecnología de Ciberseguridad y Creación de Capacidad (en Gonzalez-Sancho, 2021).

Desafíos y obstáculos en el desarrollo de la ciberseguridad en la UE

Una conclusión destacada que se desprende de la Estrategia de Ciberseguridad 2020 es que la UE centra sus esfuerzos en ser capaz de «prevenir, desalentar e impedir ciberataques y responder de forma efectiva ante ellos» (Comisión Europea, 2020c). Sin embargo, para que las capacidades de la ciberseguridad actúen como una forma de disuasión efectiva, por lógica, la disuasión también se debe potencialmente poder desplegar con fines ofensivos. Esto supone desviarse significativamente de la postura tradicional de la UE en política de seguridad e inevitablemente suscita una serie de preguntas sobre el papel que deben desempeñar la UE, la OTAN y los propios estados miembros en un panorama complejo que tiene múltiples capas y actores (European Court of Auditors, 2019).

Una conclusión que se desprende de la Estrategia de Ciberseguridad 2020 es que la UE centra sus esfuerzos en ser capaz de «prevenir, desalentar e impedir ciberataques y responder de forma efectiva ante ellos»; sin embargo, para que las capacidades de la ciberseguridad actúen como una forma de disuasión efectiva, esta también se debe potencialmente poder desplegar con fines ofensivos. Esto supone desviarse significativamente de la postura tradicional de la UE en política de seguridad.

La ciberseguridad abarca un amplio abanico de esferas: desde el crimen convencional e investigaciones penales hasta las actuaciones de estados extranjeros, o desde el fraude electrónico (*phishing*) y el fraude de hacerse pasar por director ejecutivo (*CEO fraud*) hasta el hackeo, la obtención de información, la desactivación de sistemas y la difusión de desinformación. Por lo tanto, la UE debe garantizar rutinariamente la coordinación y el enlace no solo entre la Comisión y sus agencias, sino también entre los 27 estados miembros y los socios externos (como, por ejemplo, la OTAN en cuestiones relativas a defensa y seguridad militar) (Carrapico y Barrinha, 2017). Sin embargo, aunque la UE ha podido establecer una gran variedad de puntos de contacto, redes y agencias de ciberseguridad, ello no necesariamente garantiza que estos consigan una capacidad operativa efectiva (European Court of Auditors, 2019). Además, lograr un intercambio de información fluido y una cooperación efectiva constituye un desafío en este panorama complejo. Otro factor de confusión es el hecho de que las relaciones con la OTAN no se caracterizan necesariamente por presentar un alto grado de confianza, sobre todo tras los casos de espionaje estadounidense contra aliados europeos, ni por una división de tareas y responsabilidades clara y de refuerzo mutuo en el

campo emergente de la ciberseguridad (Reuters, 2021b). También complica la situación el hecho de que los estados miembros de la UE hasta ahora se han mostrado reacios a cualquier aspiración de mayor cooperación e integración de ámbito europeo en cuestiones de defensa y seguridad, ya que muchos prefieren mantener la plena soberanía nacional sobre dichas cuestiones o seguir cooperando con la OTAN en vez de con la UE.

En cambio, las potencias revisionistas, que potencialmente pueden tener como blanco a los países de la UE, tienden a presentar una unidad de organización y dirección mucho mayor que la configuración con múltiples instituciones que caracteriza a Europa, lo que puede colocar a los europeos en situación de desventaja. Un tema controvertido en los últimos años ha sido que la tecnología china y el gigante del 5G Huawei pueden construir «puertas traseras» en sus sistemas y en su *hardware* que podrían usarse para infiltrarse (Pancevski, 2020), lo cual ha motivado los intentos estadounidenses de que Europa prohiba Huawei como han hecho ellos.

Los responsables políticos europeos ya no pueden ignorar los riesgos que plantea el hecho de que la infraestructura digital sea de propiedad extranjera, por lo que deben decidir qué acciones reguladoras emprender para contener esa dependencia y ese riesgo. Al respecto, los estados miembros han adoptado posturas dispares, especialmente ante las acusaciones que se han vertido contra Huawei, aunque con miras a avanzar hacia medidas más restrictivas (Cerulus, 2021b) e iniciativas para disminuir la dependencia externa, como la reciente creación de una Alianza Europea sobre Datos Industriales y Nube. Un reflejo de estos desarrollos y avances en materia de políticas es que la UE ha establecido un Reglamento de control de inversiones extranjeras directas en la Unión[11], que prevé la coordinación en torno al control de las inversiones nacionales, lo que puede llevar al bloqueo de las inversiones extranjeras sobre la base de los intereses estratégicos (Comisión Europea, 2020a). En cualquier caso, las inversiones extranjeras y el acceso de las empresas extranjeras a tecnologías clave seguirá siendo un asunto espinoso fundamental del debate sobre ciberseguridad de la UE en los próximos años.

Ante este escenario, la UE debe gestionar sus iniciativas con un gran número de actores e instituciones, los cuales tendrán que colaborar entre ellos para garantizar la efectividad de los esfuerzos realizados. También debe navegar en un contexto en que la ciberseguridad está pasando rápidamente de ser una cuestión de nicho a otra dominante, de formar parte de un área política para especialistas a otra con una importancia política crucial que ocupa un lugar muy destacado

11. Véase: https://eur-lex.europa.eu/legal-content/es/TXT/?uri=CELEX%3A32019R0452

en la agenda. Asimismo, debe lidiar con la creciente inquietud por la dependencia de proveedores extranjeros de soluciones tecnológicas, así como por el tema cada vez más complejo del libre flujo de los datos con una tendencia hacia la regionalización de Internet (Chernaskey, 2021; Sherman, 2019).

Conclusiones

La UE ha respondido a la rápida proliferación de amenazas a su ciberseguridad adaptando y ampliando su enfoque estratégico. Este proceso se inició en 2013, cuando dio a conocer su primera estrategia de ciberseguridad, ha continuado en la última década y ha culminado con una nueva y ambiciosa estrategia lanzada en diciembre de 2020, lo cual se ha visto confirmado en el discurso sobre el estado de la Unión que Von der Leyen pronunció en 2021. En respuesta a la percepción cambiante de la amenaza, la UE ha desarrollado un marco institucional con una agencia de ciberseguridad totalmente desarrollada, varias redes, puntos de contacto y organismos coordinadores, y ahora va más allá con nuevas iniciativas, como los planes para crear un *ciberescudo,* que pretenden aportar un alto grado de seguridad para la UE y sus estados miembros. Al mismo tiempo, la UE ha establecido un régimen normativo con una serie de directivas que establecen estándares y normas comunes, además de trabajar también en programas de certificación y estandarización.

Para la UE, encontrar un reparto adecuado de responsabilidades y un modus operandi que garantice la colaboración efectiva entre un gran número de actores de diferentes niveles se antoja difícil, pero ello, a su vez, es fundamental para garantizar una respuesta apropiada en Europa ante unas ciberamenazas cada vez más acuciantes.

Sin embargo, la ciberseguridad seguirá siendo un asunto espinoso para la UE en los próximos años. Y aunque la UE se considere una gran «potencia reguladora», sigue siendo un actor relativamente insignificante en cuestiones de políticas de seguridad, ya que muchos estados miembros prefieren arreglárselas por su cuenta o en el marco de la OTAN. La ciberseguridad abarca desde la cooperación judicial y operativa para el cumplimiento de la ley hasta la defensa militar real contra otros estados o grupos respaldados por estados. Para la UE, encontrar un reparto adecuado de responsabilidades y un modus operandi que garantice la colaboración efectiva entre este gran número de actores de diferentes niveles se antoja difícil, pero ello, a su vez, es fundamental para garantizar una respuesta apropiada en Europa ante unas ciberamenazas cada vez más acuciantes.

Referencias bibliográficas

Andress, Jason y Winterfeld, Steve. *Cyber Warfare. Techniques, Tactics and Tools for Security Practitioners*. Amsterdam: Elsevier, 2014.

Bateman, Jon; Hickok, Elonnai y Shapiro, Jacob N. «Measuring the Effects of Influence Operations: Key Findings and Gaps from Empirical Research». *Carnegie Endowment for International Peace*, (28 de junio de 2021) (en línea) [Fecha de consulta: 30.09.2021] https://carnegieendowment.org/2021/06/28/measuring-effects-of-influence-operations-key-findings-and-gaps-from-empirical-research-pub-84824

Bendiek, Annegret; Bossong, Raphael y Schulze, Matthias. «The EU's Revised Cybersecurity Strategy». *SWP Comments*, n.º 47, (2017) (en línea) [Fecha de consulta: 01.10.2016] https://www.swp-berlin.org/publications/products/comments/2017C47_bdk_etal.pdf

Bradford, Anu. «When It Comes to Markets, Europe Is No Fading Power. The EU Sets the Standards for the Rest of the World». *Foreign Affairs*, (3 de febrero de 2020) (en línea) [Fecha de consulta: 11.09.2021] https://www.foreignaffairs.com/articles/europe/2020-02-03/when-it-comes-markets-europe-no-fading-power

Bradshaw, Samantha y Howard, Philip N. «The Global Disinformation Disorder: 2019 Global Inventory of Organised Social Media Manipulation». *Oxford Internet Institute – Working Paper*, *(*2019) (en línea) [Fecha de consulta: 12.09.2021] https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/09/CyberTroop-Report19.pdf

Carrapico, Helena y Barrinha, André. «The EU as a Coherent (Cyber)Security Actor?». *Journal of Common Market Studies*, vol. 55, n.º 6 (2017), p. 1.254-1.272. https://doi.org/10.1111/jcms.12575

Cerulus, Laurens. «EU to launch rapid response cybersecurity team». *Politico*, (21 de junio de 2021a) (en línea) [Fecha de consulta: 02.10.2021] https://www.politico.eu/article/eu-joint-cyber-unit-rapid-response-cyberattacks/

Cerulus, Laurens. «Germany falls in line with EU on Huawei». *Politico,* (23 de abril de 2021b) (en línea) [Fecha de consulta: 02.10.2021] https://www.politico.eu/article/germany-europe-huawei-5g-data-privacy-cybersecurity/

Cerulus, Laurens y Klingert, Liv. «Russia's 'Ghostwriter' hacker group takes aim at German election». *Politico*, (21 de septiembre de 2021) (en línea) [Fecha de consulta: 02.10.2021] https://www.politico.eu/article/russia-brash-hackers-turn-to-german-election/

Chernaskey, Rachel. «The World Wide Web's Break Up: State-Backed Media's Role in Supporting Internet Fragmentation». *Foreign Policy Research Institute*,

(28 de febrero de 2021) (en línea) [Fecha de consulta: 30.09.2021] https://www.fpri.org/fie/internet-break-up-russia-china/

Comisión Europea. «Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises». *European Commission*, (13 de septiembre de 2017) (en línea) [Fecha de consulta: 04.10.2021] ttps://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017H1584&from=EN

Comisión Europea. «EU foreign investment screening mechanism becomes fully operational». *European Commission*, (9 de octubre de 2020a) (en línea) [Fecha de consulta: 04.10.2021] https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1867

Comisión Europea. «Impact assessment Proposal for directive on measures for high common level of cybersecurity across the Union». *European Commission*, (16 de diciembre de 2020b) (en línea) [Fecha de consulta: 04.10.2021] https://digital-strategy.ec.europa.eu/en/library/impact-assessment-proposal-directive-measures-high-common-level-cybersecurity-across-union

Comisión Europea. «New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient». *European Commission*, (16 de diciembre de 2020c) (en línea) [Fecha de consulta: 04.10.2021] https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391

Comisión Europea. «The Commission proposes a new directive to enhance the resilience of critical entities providing essential services in the EU». *European Commission*, (16 de diciembre de 2020d) (en línea) [Fecha de consulta: 04.10.2021] https://ec.europa.eu/home-affairs/news/commission-proposes-new-directive-enhance-resilience-critical-entities-providing-essential_en

Comisión Europea. «Decision on establishing the office of the European Union Agency for Cybersecurity (ENISA) in Brussels». *European Commission*, (22 de junio de 2021a) (en línea) [Fecha de consulta: 04.10.2021] https://digital-strategy.ec.europa.eu/en/news/decision-establishing-office-european-union-agency-cybersecurity-enisa-brussels

Comisión Europea. «Joint Cyber Unit». *European Commission*, (23 de junio de 2021b) (en línea) [Fecha de consulta: 04.10.2021] https://digital-strategy.ec.europa.eu/en/policies/joint-cyber-unit

Consejo Europeo. «EU imposes the first ever sanctions against cyber-attacks». (30 de julio de 2020) (en línea) [Fecha de consulta: 30.09.2021] https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/

Cyber Competence Network. «Four EU pilot projects to prepare the European Cybersecurity Competence Network». *Cyber Competence Network*, (2021) (en línea) [Fecha de consulta: 30.09.2021] https://cybercompetencenetwork.eu/about/

EMA – European Medicines Agency. «Cyberattack on EMA - update 5». *EMA*, (15 de enero de 2021) (en línea) [Fecha de consulta: 04.10.2021] https://www.ema.europa.eu/en/news/cyberattack-ema-update-5

English Oxford Living Dictionaries. «Post-truth». *Lexico.com*, (s/f) (en línea) [Fecha de consulta: 04.08.2021] https://en.oxforddictionaries.com/definition/post-truth

ENISA – European Network and Information Security Agency. «EUCS – Cloud Services Scheme». *ENISA*, (22 de diciembre de 2020) (en línea) [Fecha de consulta: 04.10.2021] https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme/

ENISA – European Network and Information Security Agency. «EU Member States test rapid Cyber Crisis Management». *ENISA*, (19 de mayo de 2021) (en línea) [Fecha de consulta: 04.10.2021] https://www.enisa.europa.eu/news/enisa-news/eu-member-states-test-rapid-cyber-crisis-management

Eurojust. «Overview Report Challenges and best practices from Eurojust's casework in the area of cybercrime». *Eurojust*, (noviembre de 2020) (en línea) [Fecha de consulta: 04.10.2021] https://www.eurojust.europa.eu/sites/default/files/2020-11/2020-11_Cybercrime-Report.pdf

European Court of Auditors. «Challenges to effective EU cybersecurity policy». *European Union*, Briefing Paper, (marzo de 2019) (en línea) [Fecha de consulta: 04.10.2021] https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf

European Defence Agency. «EDA's Growing Role in Cybersecurity». *European Defence Matters*, n.º 18 (2021) (en línea) [Fecha de consulta: 04.10.2021] https://eda.europa.eu/webzine/issue18/focus/eda-s-growing-role-in-cybersecurity

European Union Agency for the Cooperation of Energy Regulators. «Framework Guideline on sector-specific rules for cybersecurity aspects of cross-border electricity flows». *European Union Agency for the Cooperation of Energy Regulators*, (22 de julio de 2021) (en línea) [Fecha de consulta: 04.10.2021] https://documents.acer.europa.eu/Official_documents/Acts_of_the_Agency/Framework_Guidelines/Framework%20Guidelines/Framework%20Guideline%20on%20Sector-Specific%20Rules%20for%20Cybersecurity%20Aspects%20of%20Cross-Border%20Electricity%20Flows_210722.pdf

Gonzalez-Sancho, Miguel. «Standardisation supporting the Cybersecurity Act». *ENISA Cybersecurity standardization conference 2021*, (3 de febrero de 2021) (en línea) [Fecha de consulta: 30.09.2021] https://www.enisa.europa.eu/events/cybersecurity_standardisation_2021/presentations/03-04-gonzalez-sancho

Hamulák, Ondrej. «La carta de los derechos fundamentales de la Union Europea y los derechos socuales». Estudios constitucionales, vol. 16, n.º 1 (2018), p. 167-186

Headley, Tyler. «Introducing "the Poor Man's Atomic Bomb": Biological Weapons». *National Interest*, (2 de diciembre de 2018) (en línea) [Fecha de consulta: 04.10.2021] https://nationalinterest.org/blog/buzz/introducing-poor-mans-atomic-bomb-biological-weapons-37437

Ilves, Luukas K.; Evans, Timothy J.; Cilluffo, Frank J. y Nadeau, Alec A. «European Union and NATO Global Cybersecurity Challenges: A Way Forward». *PRISM*, vol. 6, n.º 2 (2016), p. 126-141.

Juncker, Jean-Claude. «State of the Union Address». *European Commission*, (13 de septiembre de 2017) (en línea) [Fecha de consulta: 04.08.2021] https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_17_3165

Kalpokas, Ignas y Kalpokiene, Julija. «Synthetic media and information warfare: Assessing potential threats». En: Mölder, Holger *et al. The Russian Federation in Global Knowledge Warfare*. Springer, Cham, 2021, p. 33-50.

Kerikmäe, Tanel; Troitiño, David R., y Shumilo, Olga. «An idol or an ideal? A case study of Estonian e-Governance: Public perceptions, myths and misbeliefs». *Acta Baltica Historiae et Philosophiae scientiarum*, vol. 7, n.º 1 (2019), p. 71-80.

Krastev, Ivan. «Putin's world». *Project Syndicate*, (1 de abril de 2014) (en línea) [Fecha de consulta: 30.04.2019] www.project-syndicate.org/commentary/ivan-krastev-blamesthe-west-s-weak-response-in-crimea-for-empowering-russia#AK0vzVbmtIUQCseG.99

Krouwel, Andre y Önnerfors, Andreas (eds). *A Continent of Conspiracies: Conspiracy Theories in and about Europe*. Abingdon-on-Thames: Routledge, 2021.

Krüger, Philipp S. y Brauchle, Jan-Philipp. «The European Union, Cybersecurity, and the Financial Sector: A Primer». *Carnegie Endowment for International Peace*, (16 de marzo de 2021) (en línea) [Fecha de consulta: 12.09.2021] https://carnegieendowment.org/2021/03/16/european-union-cybersecurity-and-financial-sector-primer-pub-84055

Leonard, Mark. «Europe for itself». *European Council of Foreign Relations,* (24 de julio de 2018) (en línea) [Fecha de consulta: 12.09.2021] https://ecfr.eu/article/commentary_europe_for_itself/

Lim, Darren y Ferguson, Victor. «Huawei and the decoupling dilemma». *The Interest*, (28 de mayo de 2019) (en línea) [Fecha de consulta: 30.09.2021] https://www.lowyinstitute.org/the-interpreter/huawei-and-decoupling-dilemma

Maurer, Lucas. «Europe in the post-COVID-19 world». *Atlantic files*, (19 de mayo de 2021) (en línea) [Fecha de consulta: 22.07.2021] https://www.orfonline.org/expertspeak/europe-post-covid19-world/

NATO – North Atlantic Treaty Organization. «Brussels Summit Communiqué». *NATO*, (14 de junio de 2021a) (en línea) [Fecha de consulta: 30.09.2021] https://www.nato.int/cps/en/natohq/news_185000.htm?selectedLocale=en

NATO – North Atlantic Treaty Organization. «Cyber defence». *NATO*, (2 de julio de 2021b) (en línea) [Fecha de consulta: 30.09.2021] https://www.nato.int/cps/fr/natohq/topics_78170.htm?selectedLocale=en

Pancevski, Bojan. «U.S. Officials Say Huawei Can Covertly Access Telecom Networks». *The Wall Street Journal*, (12 de febrero de 2020) (en línea) [Fecha de consulta: 04.10.2021] https://www.wsj.com/articles/u-s-officials-say-huawei-can-covertly-access-telecom-networks-11581452256

Parlamento Europeo. «Regulation (EC). No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency». (10 de marzo de 2004) (en línea) [Fecha de consulta: 30.09.2021] https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=LEGISSUM:l24153

PESCO – Permanent Structured Cooperation. «Cyber exercise provides readiness to respond to cyber threats». *Cyber Rapid Response Teams (CRRTs) y PESCO*, (28 de mayo de 2021) (en línea) [Fecha de consulta: 30.09.2021] https://pesco.europa.eu/wp-content/uploads/2021/05/PRESSSTATEMENT-CRRT.pdf

Reuters. «North Korea took $2 billion in cyberattacks to fund weapons program: U.N. report». *Reuters*, (5 de agosto de 2019) (en línea) [Fecha de consulta: 03.10.2021] https://www.reuters.com/article/us-northkorea-cyber-un-idUSKCN1UV1ZX

Reuters. «Russian, Chinese hackers targeted Europe drug regulator: newspaper». *Reuters*, (6 de marzo de 2021a) (en línea) [Fecha de consulta: 03.10.2021] https://www.reuters.com/article/us-eu-cyber-idUSKBN2AY0F1

Reuters. «U.S. spied on Merkel and other Europeans through Danish cables - broadcaster DR». *Reuters*, (30 de mayo de 2021b) (en línea) [Fecha de consulta: 30.09.2021] https://www.reuters.com/world/europe/us-security-agency-spied-merkel-other-top-european-officials-through-danish-2021-05-30/

RTE – Raidió Teilifís Éireann, Ireland's National Public Service Media. «Plans unveiled for EU to step up cyber security efforts». *RTE*, (19 de septiembre de 2017) (en línea) [Fecha de consulta: 12.09.2021] https://www.rte.ie/news/2017/0919/905989-eu-cybersecurity

Sample, Ian. «What are deepfakes – and how can you spot them?». *The Guardian,* (13 de enero de 2020) (en línea) [Fecha de consulta: 03.10.2021] https://www.theguardian.com/technology/2020/jan/13/what-are-deepfakes-and-how-can-you-spot-them

Schmitter, Philippe C. «Neo-Neofunctionalism». En: Diez, Thomas y Wiener, Antje. (eds.). *European Integration Theory*. Oxford: Oxford University Press, 2004, p. 45-75.

Sheftalovich, Zoya. «Why Australia wanted out of its French submarine deal». *Politico,* (16 de septiembre de 2021) (en línea) [Fecha de consulta: 12.03.2022] https://www.politico.eu/article/why-australia-wanted-out-of-its-french-sub-deal/

Sherman, Justin. «Russia and Iran Plan to Fundamentally Isolate the Internet». *Wired*, (6 de junio de 2019) (en línea) [Fecha de consulta: 09.10.2021] https://www.wired.com/story/russia-and-iran-plan-to-fundamentally-isolate-the-internet

Singh, Rajnish. «Cybersecurity: Defending the digital wall». *The Parliament Magazine*, (4 de junio de 2018) (en línea) [Fecha de consulta: 30.09.2021] https://www.theparliamentmagazine.eu/news/article/cybersecurity-defending-the-digital-wall

Tenembaum, Yoav D. «International Relations: It's Time to Revise How We Talk About Revisionist Powers». *OXPOL Blog*, (6 de noviembre de 2012) (en línea) [Fecha de consulta: 22.07.2021] https://blog.politics.ox.ac.uk/international-relations-its-time-to-revise-how-we-talk-about-revisionist-powers/

Troitiño, David R. «The European Union Facing the 21st Century: The Digital Revolution». *TalTech Journal of European Studies*, vol. 12, n.º1 (2022), p. 60-78.

Unión Europea. «Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union». *Official Journal of the European Union*, (19 de julio de 2016) (en línea) [Fecha de consulta: 12.09.2021] https://eur-lex.europa.eu/eli/dir/2016/1148/oj

Unión Europea. «Of implementing Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States». *Official Journal of the European Union*, L 351 I, (22 de octubre de 2020a) (en línea) [Fecha de consulta: 30.03.2022] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2020:351I:FULL&from=FR

Unión Europea. «Amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States». *Official Journal of the European Union*, L 246 12, (30 de julio de 2020b) (en línea) [Fecha de consulta: 30.03.2022] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32020D1127&from=EN

Von der Leyen, Ursula. «Speech at World Health Organization's 73rd Assembly». *European Commission*, (19 de mayo de 2020a) (en línea) [Fecha de consulta: 30.09.2021] https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_20_1655

Von der Leyen, Ursula. «State of the Union Address». *European Commission*, (16 de septiembre de 2020b) (en línea) [Fecha de consulta: 30.09.2021] https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_20_1655

Von der Leyen, Ursula. «State of the Union 2021». *European Commission*, (15 de septiembre de 2021) (en línea) [Fecha de consulta: 30.09.2021] https://ec.europa.eu/info/strategy/strategic-planning/state-union-addresses/state-union-2021_en

Walden, Max. «How can Australia repair its relationship with France after the AUKUS submarine row?». *ABC News*, (23 de septiembre de 2021) (en línea) [Fecha de consulta: 04.10.2021] https://www.abc.net.au/news/2021-09-23/how-can-australia-repair-its-relationship-with-france-aukus/100480270

Whyte, Christopher; Thrall, A. Trevor y Mazanec, Brian M. (eds). *Information Warfare in the Age of Cyber Conflict*. Abingdon-on-Thames: Routledge, 2021.

Zeevaert, Marius. «Spillovers versus Bargaining – Which Integration Theory Explains the EU's Coronavirus Recession Response?». *The Yale Review of International Studies*, (octubre de 2020) (en línea) [Fecha de consulta: 30.09.2021] http://yris.yira.org/global-issue/4325#_ftn8

Traducción del original en inglés: Maria Gené Gil y redacción CIDOB.

Este artículo forma parte del proyecto de investigación de la Cátedra Jean Monnet "La Europa Digital y su influencia en la integración futura". N.º identificación: 101082988. ERASMUS-JMO-2022-HEI-TCH-RSCH. Programa: ERASMUS2027.