Documento
Análisis

04/2023 20 de enero de 2023

José Luis Pontijas Calderón *

Unión Europea: ciberseguridad y ciberdefensa

Unión Europea: ciberseguridad y ciberdefensa

Resumen:

La ciberseguridad y la ciberdefensa son campos íntimamente relacionados pero claramente diferenciados. La Unión Europea ha invertido un enorme esfuerzo en el primero y debe ser felicitada por ello. Sin embargo, los avances en el segundo ámbito se ven lastrados por las diferencias entre socios y sus distintos intereses, en ocasiones divergentes. El presente artículo reflexiona sobre el hecho de que la Unión debe realizar un esfuerzo por avanzar en sus capacidades de ciberdefensa si desea ser un actor relevante en el escenario mundial.

Palabras clave:

Unión Europea, ciberseguridad, ciberdefensa, ciberamenaza.

European Union: cybersecurity and cyberdefence

Abstract:

Cybersecurity and cyber defense are closely related fields, but clearly differentiated. The European Union has made an enormous effort in the first and should be congratulated for this, but progress in the second is hindered by the differences between the partners and their different and sometimes divergent interests. This article argues that if the Union wishes to be a relevant actor on the world stage, it must try to advance its cyber defense capabilities.

Keywords:

European Union, cybersecurity, cyberdefence, cyber threat

Cómo citar este documento:

PONTIJAS CALDERÓN, José Luis. *Unión Europea: ciberseguridad y ciberdefensa*. Documento de Opinión IEEE 04/2023. https://www.ieee.es/Galerias/fichero/docs_analisis/2023/DIEEEA04_2023_JOSPON_Europa.pdf y/o enlace bie[3] (consultado día/mes/año)

Las sociedades modernas —incluso los países en vías de desarrollo— están crecientemente expuestas a vulnerabilidades consecuencia de su exponencial dependencia de la tecnología basada en plataformas, a su vez basadas en el ciberespacio. Así, en las sociedades digitales aquellos ámbitos que coexisten en el ciberespacio precisan dotarse de sistemas y mecanismos que aporten la seguridad necesaria en dicho campo. Consciente de este hecho, la Unión Europea (UE) ha adoptado estándares de protección de datos y sistemas que intentan asegurar un funcionamiento sin sobresaltos.

Pero el ciberespacio es un dominio donde entidades estatales y no estatales actúan con gran impunidad en una confrontación que carece de los límites geográficos y temporales que afectan a otras que tienen lugar simultáneamente a nivel global. Por consiguiente, nunca se puede garantizar una seguridad absoluta. Además, dada la dificultad para la atribución de las acciones cibernéticas, cada vez son más numerosas las violaciones de las normas y leyes internacionales, lo que requiere dotarse de soluciones políticas relacionadas con la ciberseguridad y la ciberdefensa. Así, esta última se ha convertido en un nuevo campo de batalla multidimensional (ataques y defensas cibernéticos, desinformación, información dirigida, etcétera) y de competición estratégica que se puede situar con poco margen de error en el espectro de las herramientas del poder duro. En este sentido, las ciberoperaciones contra objetivos europeos llevadas a cabo por proxis y criminales que operan, entre otros lugares, desde China, Rusia, Corea del Norte e Irán no solo dañan seriamente la competitividad de la Unión, sino que también atentan contra la cohesión de su sociedad y del proyecto europeo en general. Ninguno de esos ataques ha llegado a alcanzar, por ahora, el nivel suficiente para que pueda considerarse una agresión armada en el sentido contemplado por la Carta de las Naciones Unidas, lo cual legitimaría el recurso al artículo 42.7 del Tratado de la Unión Europea (TUE), que alude a la obligación de prestarse ayuda mutua, o al artículo 5 del Tratado de Washington (OTAN). Aun así, los ataques mencionados suponen una amenaza permanente, por lo que las capacidades de ciberseguridad (término de significado amplio con connotaciones pasivas) y de ciberdefensa (término que abarca la posibilidad de acciones punitivas, ya sea de forma deliberada o en respuesta a ciberataques) son un componente fundamental de la panoplia de herramientas

necesarias para defender nuestros intereses y valores. Dicha defensa puede canalizarse también a través de la diplomacia, la economía y el imperio de la ley.

Ciberseguridad y ciberdefensa

Antes de proseguir conviene aclarar lo que entendemos por *ciberseguridad* y *ciberdefensa,* ya que existe cierta confusión al respecto, pues ambos términos son utilizados indistintamente. Es evidente que el rol de la defensa consiste en salvaguardar los intereses nacionales en el caso de que estos se vean amenazados de manera violenta por actores extranjeros. Así, la política de defensa de un Estado trata de protegerlo dentro de un entorno internacional que, dependiendo de la región, puede ser más o menos benigno o claramente amenazador e incluso hostil. Cuando el entorno internacional no consigue evitar el desarrollo de espirales de inseguridad y conflicto, la defensa de cada Estado debe estar dotada para afrontar la situación mediante el empleo de medios y capacidades operativas que garanticen la disuasión y, si esta fallase, la capacidad de respuesta.

Claramente, las alianzas entre socios aumentan la disuasión al incrementar la capacidad de respuesta. Pero incluso en dichos casos los Estados prefieren dotarse de medios nacionales que, dentro de las posibilidades de cada uno, garanticen la capacidad y la flexibilidad para actuar en solitario en defensa de los propios intereses. En el caso de la UE esto resulta todavía más cierto, ya que el proyecto de una defensa europea autónoma capaz de proporcionar una disuasión suficiente ha permanecido muy limitado en el campo operativo militar y se ha reducido a aspectos industriales e intentos de coordinación en el desarrollo de capacidades. En lo relativo al ciberespacio, la situación no es mucho mejor.

Sin embargo, resulta imperativo que las infraestructuras europeas críticas sean protegidas adecuadamente en el ciberespacio. Las sociedades avanzadas constituyen objetivos lucrativos y relativamente fáciles para los ciberataques y las operaciones de influencia. No obstante, la intersección entre digitalización exponencial y seguridad es un fenómeno complejo y muy exigente, con lo que la ciberseguridad conforma un campo más amplio que, a su vez, engloba la resiliencia y la ciberdefensa.

Así pues, aquí nos encontramos con que la ciberdefensa europea está sujeta a los mismos problemas y desafíos que la cooperación convencional en defensa. Y, además, resulta que la ciberdefensa no es el único ni el más importante modo de asegurar el ciberespacio europeo. En este sentido, el Marco Político de Ciberdefensa de la UE (CDPF, por sus siglas en inglés)[1] resalta la importancia de poseer capacidades que aseguren el rol estratégico de la Unión y la autonomía en su actuación, para lo que se requiere «más cooperación en el desarrollo de capacidades, impulsando la interoperabilidad de los medios civiles y militares». Ante esta afirmación, podemos preguntarnos cuál es el rol de la ciberdefensa en el conjunto más amplio de la ciberseguridad (que, como hemos dicho, engloba la resiliencia): la ciberdefensa debería alinearse con los acuerdos políticos y los mecanismos militares operativos para aportar un valor político-estratégico y enmarcarse en el marco más amplio de la ciberseguridad.

La respuesta de la Unión Europea

El pasado mes de noviembre la UE emitió un documento, titulado *EU Policy on Cyber Defence,* que representa un esfuerzo por plasmar sus objetivos estratégicos, políticos y operativos en el campo de la ciberseguridad[2]. Su propósito es aumentar la asertividad de la Unión y de sus Estados miembro mediante un incremento de la capacidad para prevenir, detectar y disuadir y, si esto falla, para defenderse contra los ciberataques. El documento se organiza alrededor de cuatro pilares: cooperación civil-militar, resiliencia del ecosistema de defensa, desarrollo de capacidades de ciberdefensa y partenariados. Además, se fijan objetivos ambiciosos y pragmáticos como la creación del Centro de Coordinación de Ciberdefensa de la UE (EUCDCC, por sus siglas en inglés), el desarrollo de recomendaciones sobre requerimientos de interoperabilidad o el deseo de mantener una ciberdefensa activa. Por consiguiente, podríamos afirmar que la UE intenta posicionarse en el ciberespacio como una potencia a la par con otras de categoría similar y capacitada para utilizar el poder duro en él, ya que una ciberdefensa activa implicar

[1] CONSEJO DE LA UNIÓN EUROPEA. EU Cyber Defence Policy Framework (14413/18). Bruselas, 19 de noviembre de 2018. Disponible en: https://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/en/pdf [consulta: 29/12/2022].

[2] COMISIÓN EUROPEA. *Joint Communication to the European Parliament and the Council: EU Policy on Cyber Defence* (JOIN[2022] 49 final). 10 de noviembre de 2022. Disponible en: https://www.eeas.europa.eu/sites/default/files/documents/Comm_cyber%20defence.pdf [consulta: 29/12/2022].

llevar a cabo acciones punitivas, es decir, ciberataques, aunque en el caso de la UE estos se produzcan en respuesta a otros sufridos previamente.

Aunque no se mencione expresamente en el documento, en consonancia con cuantas estrategias y normativas emite la Unión, es evidente que esta sobre ciberdefensa quedará supeditada a las normas y leyes internacionales relativas al comportamiento responsable de los Estados en el ciberespacio: la Unión es sin duda uno de los actores más activos a la hora de defender un orden internacional basado en normas.

En cualquier caso, el nuevo documento muestra que, a nivel estratégico, la UE ha evolucionado de una posición focalizada en las amenazas en el ciberespacio en general a otra donde se toman en cuenta las amenazas que pueden suponer los actores y los Estados considerados competidores. En este sentido, la Brújula Estratégica de marzo de 2022 considera dicho dominio un campo disputado y de competición estratégica donde el comportamiento está más regido por la defensa de pretendidos derechos históricos y el control de zonas de influencia que por el respeto al ordenamiento internacional acordado[3]. Este aspecto la diferencia claramente del enfoque de la Estrategia Global de la UE de 2016[4], que definía los desafíos en el ciberespacio en términos abstractos, como amenazas a la seguridad, la prosperidad y la democracia de la Unión. Así, la Estrategia de 2016 preconizaba que los Estados miembro se dotaran de las herramientas necesarias para protegerse por sí mismos contra las ciberamenazas (lo que incluía capacidades tecnológicas), mientras que la Unión como tal se convertía en un ciberactor encargado de proteger sus infraestructuras, componentes críticos y, a la vez, sus valores.

Con un enfoque diferente, la Brújula Estratégica preconiza una posición más asertiva y activa de la Unión, en la que esta se convierte en un proveedor de seguridad decisivo. Para ello, se asume que la UE debe ser capaz de responder de manera rápida y contundente ante ciberataques, sean estos esponsorizados por Estados o no. Por dicho motivo, en el documento se menciona expresamente el objetivo de desarrollar el

[3] SERVICIO DE ACCIÓN EXTERIOR EUROPEO. *A Strategic Compass for Security and Defence.* Marzo de 2022. Disponible en: https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf [consulta: 29/12/2022].

[4] ALTO REPRESENTANTE DE LA UE PARA LA POLÍTICA EXTERIOR Y DE SEGURIDAD. *Shared vision, common action: a stronger Europe – A Global Strategy for the European Union's foreign and security policy.* Junio de 2016. Disponible en: https://www.eeas.europa.eu/sites/default/files/eugs_review_web_0.pdf [consulta: 29/12/2022].

mencionado EUCDCC, que se ha cumplido diligentemente junto a otros propósitos: aumentar la investigación y la innovación; estimular la base industrial de la Unión; incrementar la cooperación entre la Unión, los Estados miembro y los socios y mejorar la interoperabilidad y el intercambio de información en la cooperación civil-militar —concretamente mediante los equipos de computadoras militares de respuesta ante emergencias (Mil-CERT, por sus siglas en inglés)— y en la conducción de ciberoperaciones (como hemos mencionado, con un carácter ofensivo-punitivo). Este último aspecto —las operaciones en el ciberespacio— está claramente ligado al desarrollo y uso de las nuevas tecnologías (inteligencia artificial, cuántica, 5G/6G, *big data*, etcétera), ya que de su actualización dependerá en gran medida la superioridad o no de las operaciones que se intenten llevar a cabo en el ciberdominio.

En el nivel político también se puede apreciar una evolución del papel otorgado a la ciberdefensa en la Unión. La Estrategia de Ciberseguridad de 2013[5] consideraba el desarrollo de una política de ciberseguridad y de las capacidades relacionadas con la misma una prioridad estratégica dentro de la Política Común de Seguridad y Defensa (PCSD). Sus objetivos eran la detección, respuesta y recuperación ante ciberamenazas sofisticadas y la búsqueda de sinergias entre los enfoques civil y militar para proteger elementos ciberdependientes críticos. Asimismo, el documento preconizaba la necesidad de un enfoque amplio y completo basado en tres pilares, cada uno de ellos con su correspondiente marco institucional y legal: seguridad de las redes y de la información, imperio de la ley y defensa. Por consiguiente, el desarrollo de una política de ciberdefensa iba claramente unido a la PCSD y se pretendían incentivar el desarrollo y la adquisición de tecnologías de la información y la comunicación dotadas de alta seguridad en cooperación con la Agencia de Defensa Europea (EDA, por sus siglas en inglés). De esta forma, se intentaba crear un ecosistema europeo autosostenible y muy competitivo en recursos de ciberseguridad.

Pero el ciberespacio evoluciona a tal velocidad que pocos años después se experimentó la necesidad de elaborar una nueva estrategia, que esta vez incorporaría los conceptos

[5] COMISIÓN EUROPEA. *Joint Communication to the European Parliament and the Council—Resilience, Deterrence and Defence: Building strong cybersecurity for the EU* (JOIN[2017] 450 final). 13 de septiembre de 2017. Disponible en: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:52017JC0450 [consulta: 29/12/2022].

de *ciberdisuasión* y *resiliencia* e incluiría las misiones y operaciones de la Unión: la Estrategia de Ciberseguridad de 2017[6].

No obstante, pocos años más tarde se precisó una nueva revisión de la citada estrategia: la denominada EU Cybersecurity Strategy for the Digital Decade (2020)[7], donde la ciberdefensa forma parte de una estrategia digital mucho más amplia y la ciberseguridad se integra en todo lo digital, particularmente en tecnologías como la inteligencia artificial, la encriptación y la computación cuántica. Además, dicha estrategia exhorta a que tanto la Unión como los Estados miembro proporcionen el ímpetu necesario para el desarrollo de capacidades de tecnología punta, desplieguen políticas e instrumentos como el Marco Político de Ciberdefensa de la UE (CDPF, por sus siglas en inglés)[8] y usen el potencial de herramientas comunes como la Cooperación Estructurada Permanente (PESCO, por sus siglas en inglés), el Fondo de Defensa Europeo (EDF, por sus siglas en inglés) o la Base Tecnológica e Industrial para la Defensa Europea (EDTIB, por sus siglas en inglés). La Estrategia de 2020 constituyó un paso decisivo para posicionar la ciberseguridad como una prioridad que acaba influyendo sobre otras áreas de la política europea: las amenazas híbridas, la autonomía estratégica, la estrategia industrial o incluso campos de estricto interés militar, como la movilidad militar, a la que también la OTAN otorga una importancia muy relevante. Así pues, la ciberseguridad se ha convertido en un vector horizontal de prioridad en áreas diversas y no necesariamente interdependientes.

En cuanto al nivel operativo, el mencionado CDPF contempla cinco áreas prioritarias: desarrollo de capacidades de ciberdefensa; refuerzo de la protección de las redes de comunicación; promoción de las sinergias en la relación civil-militar y en otras áreas de la política, las instituciones y las entidades relevantes de la Unión, así como en el sector privado; mejora de la preparación y la educación, incluyendo ejercicios, e impulso de la cooperación con socios internacionales clave, entre los cuales destaca la OTAN pero también la OSCE (Organización para la Seguridad y la Cooperación en Europa). En total, el documento contiene más de cuarenta propuestas que contemplan la coordinación entre los CERT y la Capacidad de Respuesta ante Ciberincidentes de la OTAN (NCIRC,

[6] *Idem.*
[7] COMISIÓN EUROPEA. *Joint Communication to the European Parliament and the Council: The EU's cybersecurity strategy for the digital decade* (JOIN[2020] 18 final). 16 de diciembre de 2020. Disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/%20PDF/?uri=CELEX:52020JC0018&from=EN [consulta: 29/12/2022].
[8] CONSEJO DE LA UNIÓN EUROPEA. *Op. cit.*

por sus siglas en inglés). De hecho, la ciberdefensa ya se ha convertido en un elemento destacado del sistema de gestión de crisis mediante la creación de los equipos de ciberrespuesta rápida (CRRT, por sus siglas en inglés), el proyecto de asistencia mutua en ciberseguridad y la Plataforma de Ciberamenazas e Intercambio de Información de Respuesta ante Incidentes[9,10].

Todo ello muestra que la UE contempla el ciberespacio como un ámbito donde se llevan a cabo operaciones defensivas y también ofensivas —además de una amplia panoplia de actividades humanas, diplomáticas y comerciales—, enmarcadas por las necesarias medidas, reglamentación y capacidades que proporcionen una amplia ciberseguridad. Además, la Unión ha fortalecido otro importante aspecto de esta última: el diplomático. En un esfuerzo por aumentar su capacidad de disuasión, ha lanzado *The UE Cyber Diplomacy Toolbox*[11], que le permite imponer sanciones a individuos, entidades y, llegado el caso, Estados que lleven a cabo actividades hostiles contra sus intereses.

Una Europa disonante

A la luz de lo dicho, pudiera parecer que la Unión disfruta de una armonía que le permite mirar al ciberespacio con gran confianza, pero desgraciadamente esto no sería del todo correcto. Resulta obvio que la actividad en el ciberespacio (ciberataques vs. ciberdefensa, información vs. desinformación, operaciones de influencia, actividades de inteligencia y contrainteligencia, poder blando, etcétera) forma parte de los intereses particulares de los Estados miembro, que, como ya sabemos, tienen puntos de vista diferentes y en ocasiones divergentes sobre las amenazas, la prioridad para afrontarlas y el modo de hacerlo (especialmente en su mayor o menor propensión a emplear medios punitivos). Así, la diversa cultura estratégica de cada socio, producto de la experiencia histórica y política particular, influye también en la manera de enfocar su ciberseguridad

[9] PESCO PROJECTS. *Cyber rapid response teams and mutual assistance in cyber security.* Disponible en: https://www.pesco.europa.eu/project/cyber-rapid-response-teams-and-mutual-assistance-in-cyber-security/ [consulta: 29/12/2022].
[10] PESCO PROJECTS. *Cyber threats and incident response information-sharing platform.* Disponible en: https://www.pesco.europa.eu/project/cyber-threats-and-incident-response-information-sharing-platform/ [consulta: 29/12/2022].
[11] MORET, Erica y PAWLAK,Patryk. «The EU Cyber Diplomacy Toolbox: towards a cyber sanctions regime?». European Union Institute for Security Studies, 21 de julio de 2017. Disponible en: https://op.europa.eu/en/publication-detail/-/publication/88cfb104-701b-11e7-b2f2-01aa75ed71a1/language-en [consulta: 29/12/2022].

y su ciberdefensa. Esto provoca un distanciamiento entre lo que el aparato burocrático bruselense ambiciona y las preferencias individuales de los Estados miembro que lastra la acción exterior de la Unión como tal, también en el campo de la ciberdefensa. Por ejemplo, mientras que Estonia y España han establecido mandos militares de ciberdefensa, Finlandia ha preferido no crear ninguno. El problema se agrava a causa de la predilección de ciertos socios europeos por la OTAN en lo que se refiere a seguridad y defensa: siguiendo la línea argumental de la Alianza Atlántica, los esfuerzos en el marco de la Unión deben ser complementarios de los impulsados en el de la OTAN, y ello necesariamente incluye la ciberdefensa.

Por otro lado, el Parlamento Europeo ha tomado cartas en el asunto. Su «Resolución sobre el estado de las capacidades de ciberdefensa europeas» resulta ambiciosa: afirma que una política de ciberdefensa común y un nivel de cooperación substancial son elementos centrales para el desarrollo e impulso de una unión más profunda en la defensa europea, que, a su vez, genere una común y también mejor capacidad de ciberdefensa[12]. Pero esta llamada general del Parlamento a una ciberdefensa europea que coadyuve a avanzar hacia el objetivo de la defensa común europea —contemplado en el artículo 24 del Tratado de la UE— de poco o nada ha servido para cambiar la dirección que cada socio ha seguido manteniendo en asuntos de ciberseguridad.

Alinear la ciberdefensa con otros instrumentos europeos relativos a la defensa requeriría un esfuerzo de coordinación sustancial, ya que la ciberseguridad y la resiliencia inherente a la misma se benefician enormemente de su carácter civil, en contraposición con la defensa convencional, de carácter masivamente militar. Combatir los delitos cibernéticos es una misión fundamentalmente civil, de la que se encargan las fuerzas policiales y el sistema judicial. Una parte importante de dicha misión consiste en la atribución de los delitos, para lo que se requiere la intervención de agencias de inteligencia y de autoridades civiles de nivel político. La unión en la defensa no es un objetivo compartido por todos los socios europeos, especialmente por aquellos colindantes con Rusia, que apuestan y seguirán apostando firmemente por la OTAN.

[12] PARLAMENTO EUROPEO. «Resolución del Parlamento Europeo de 7 de octubre de 2021 sobre el estado de las capacidades de ciberdefensa europeas» (2020/2256). 7 de octubre de 2021. Disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021IP0412&from=EN [consulta: 29/12/2022].

También hay que contemplar el hecho de que no todos los socios están capacitados para llevar a cabo ciberoperaciones, pues carecen de los medios, las capacidades e incluso de los marcos organizativo, legal y doctrinal para ejecutarlas: la ciberseguridad y la ciberdefensa precisan de un amplio abanico de conceptos, recursos, autoridades y organizaciones, que a su vez exige un alto grado de coordinación y convergencia tanto a nivel doméstico como internacional.

Quizás pudiera parecer que todas las medidas puestas en funcionamiento por la UE distan mucho de la disuasión convencional o nuclear, que, tal y como las conocemos, combinan denegación y castigo. No obstante, sin duda contribuyen a la construcción de una cierta disuasión, ya que combinan también la denegación (que incluye la resiliencia ante ciberataques) con una creciente capacidad para la atribución de la autoría de actividades hostiles y la disposición para la respuesta (ciberoperaciones ofensivas), además de adaptarse constantemente a la evolución de las ciberamenazas, con lo que las vulnerabilidades disminuyen. Si la respuesta ante las ciberacciones hostiles es conjunta, su eficacia estratégica, operativa y política contribuirá sin duda a disminuir el clima de impunidad y la disuasión aumentará.

Quizás una de las características de la UE sea defender ambiciosas propuestas pero implementar otras más modestas para alcanzar objetivos factibles que sean aceptados por los veintisiete socios. La actual política de ciberseguridad bascula así entre lo que desea ser y lo que se consigue a nivel de organización, en contraposición a lo que algunos Estados miembro han logrado individualmente, muy por encima de dicho nivel. Si la Unión desea intervenir asertivamente en el diseño del escenario internacional que se está fraguando, debería ser capaz de materializarse como un actor de peso y reconocido en el campo de la ciberdefensa, capaz de ejecutar ciberoperaciones y no simplemente de fijar estándares de seguridad cibernética, muy necesarios pero insuficientes para alcanzar una mayor autonomía estratégica.

Ciberdefensa en los contextos OTAN y Unión Europea

Partiendo de la base de que ambas organizaciones poseen cláusulas similares referentes a una necesaria solidaridad mutua que garantice la disuasión (artículo 5 en el Tratado de la OTAN y artículo 42.7 en el de la UE), podríamos preguntarnos cuál está

situada en mejor posición para responder ante un ciberataque a uno o varios de sus socios. Ambas cláusulas han sido invocadas solo una vez por los EE. UU., en el caso de la Alianza, y por Francia, en el caso de la Unión, y en sendas ocasiones ha sido con motivo de un ataque terrorista, es decir, de un ataque no perpetrado por ningún Estado, sino por organizaciones terroristas. Si bien las dos cláusulas parecen similares, no solo difieren en su formulación léxica, sino que también lo hacen en la amplitud de la respuesta que se espera y que obliga a cada uno de los socios, pues cualquier reacción por parte de la OTAN estará necesariamente confinada a la esfera militar. Por el contrario, el amplio abanico de respuestas que la Unión puede ofrecer abarca ámbitos como la economía, la diplomacia, la información, la legislación, el comercio y la cultura, entre los más destacables.

No podemos olvidar que las agresiones y actividades ilícitas en el ciberespacio quedan por debajo del nivel del uso de la fuerza, es decir, fuera del ámbito militar. El reino cibernético no es un arma como tal, sino un ambiente que permite los ciberataques, un dominio operacional en el que la información y otras dimensiones interaccionan continuamente. Así pues, los ciberataques difieren de los ataques convencionales al poder ejecutarse desde lugares remotos. Este hecho, junto a la compleja identificación del perpetrador o perpetradores, hace que difícilmente pueda acudirse al artículo 51 de la Carta de las Naciones Unidas para invocar el derecho a la defensa propia ante un ataque armado, tal y como también contempla el artículo 5 del Tratado de Washington.

A diferencia de lo expuesto, la UE, como hemos visto, no solamente posee un mayor abanico de posibles respuestas: el artículo 42.7 del TUE menciona la solidaridad mutua ante cualquier «agresión armada». Así, la palabra *agresión,* más amplia, abarca cualquier acción hostil de variada graduación, incluidas las que se pudieran producir por debajo del mencionado nivel del uso de la fuerza.

Por otro lado, los artículos de defensa mutua tanto de la OTAN como de la UE tienen una dimensión geográfica, es decir, se aplican al territorio de ambas organizaciones, lo que excluye todos los demás territorios no contemplados en el tratado del Atlántico Norte. Esto es especialmente relevante para España, ya que Ceuta y Melilla no se encuentran bajo el paraguas de la OTAN, por mucho que el señor Stoltenberg, actual secretario general de la Alianza, intentara alcanzar un difícil equilibrio diplomático durante la Cumbre de Madrid, el cual no ha tenido reflejo en documentos oficiales. Sin embargo, el

artículo 42.7 del Tratado de la UE abarca el territorio nacional de todos los socios, estén estos en el Caribe o en el Pacífico, lo que evidentemente cubre a nuestras plazas de soberanía africanas.

Otra ventaja en manos de Bruselas es la capacidad de invocar la denominada «cláusula de solidaridad», contemplada en el artículo 222 del Tratado de Funcionamiento de la UE (TFUE). Esta se diseñó específicamente para el caso de ataques terroristas o desastres naturales, sean estos provocados o no por seres humanos. El artículo 222 es especialmente importante, ya que el significado de *desastre* es bastante amplio e incluye cualquier situación que resulte o pudiera resultar en un grave impacto sobre la población[13]. Es evidente que dicho artículo cubre sobradamente cualquier fleco que pudiera quedar al descubierto por el artículo 42.7, lo que configura un campo de actuación en el ciberespacio solamente limitado por el imperio de la ley y, en principio, capacita a Europa para actuar en respuesta ante un mayor abanico de acciones hostiles que la OTAN.

Conclusiones

La creciente vulnerabilidad cibernética de las sociedades modernas obliga a estas a dotarse de capacidades y desarrollar estándares de seguridad, protección y respuesta ante las complejas y crecientes amenazas en dicho ámbito.

Ciberseguridad y ciberdefensa se configuran así como campos que, si bien están relacionados, se diferencian claramente. La ciberseguridad, más amplia y fuertemente vinculada con la resiliencia, parece abarcar los aspectos que tratan de garantizar el normal funcionamiento de la sociedad en un amplio sentido, mientras que la ciberdefensa parece estar más dirigida a la capacidad de atribución y respuesta punitiva ante ciberataques o a la posibilidad de llevarlos a cabo de manera ofensiva.

Consciente de ello, la UE trata de no perder la capacidad de garantizar su autonomía y funcionamiento, para lo que ha confeccionado estrategias, doctrinas, instituciones y legislación que aumentan su seguridad y disuasión.

[13] Consejo de la UE, 'Decision on the arrangements for the implementation by the Union of the solidarity clause', op.cit., Article 3 (a), pag, 55; 'Cybersecurity and cyberdefence: EU solidarity and mutual defence clauses', pag. 4.

La ciberseguridad y la ciberdefensa precisan de un amplio abanico de conceptos, recursos, autoridades y organizaciones, que a su vez exige un alto grado de coordinación. Con ello se contribuye a una mayor disuasión que se beneficia de la acción conjunta, pues esta aumenta la eficacia estratégica, operativa y política. En este sentido, las herramientas de la Unión como tal no son desestimables (sanciones económicas, declaraciones políticas de atribución, acciones legales, etcétera): unidas a las capacidades individuales de sus socios pueden formar un conjunto de efectividad considerable.

A pesar de la mayor capacidad de la Unión para hacer frente a actividades hostiles por encima y por debajo del nivel de ataque armado en el ciberespacio, la diferente percepción de la amenaza por parte de los Estados miembro de la Unión —así como los intereses diferentes y en ocasiones divergentes de los socios— dificulta avanzar en el campo de la ciberdefensa y progresar hacia el objetivo contemplado en el artículo 24 del TUE: una defensa común europea también en el ciberespacio.

Así pues, si la Unión desea avanzar en su autonomía estratégica y ser reconocida como un actor internacional de peso, debe hacer un esfuerzo para avanzar en el campo de la ciberdefensa, más allá de la ciberseguridad.

*José Luis Pontijas Calderón**
Doctor en Economía Aplicada por la UAH
Profesor de Geopolítica y Estudios Estratégicos en la UC3M
@JoseLuiPontijas