ARI 80/2024
17 de junio de 2024

La ciberresiliencia: entre la ciberseguridad y la resiliencia

Félix Arteaga | Investigador principal, Real Instituto Elcano

Javier Alonso Lecuit | Investigador sénior asociado, Real Instituto Elcano

Tema

Resiliencia es un término que ha hecho fortuna en el campo de la seguridad, incluida la ciberseguridad. Todas las estrategias y políticas de seguridad fomentan la capacidad de recuperación, la resiliencia, también las de ciberseguridad, pero ¿en qué se diferencian la ciberseguridad y la ciberresiliencia?

Resumen

Resiliencia[1] es la palabra de moda en el campo de la seguridad. En sentido amplio se refiere a la capacidad de recuperación tras las crisis o incidentes y, en el estricto, a las medidas que se adoptan para asegurar esa capacidad. En este ARI se analiza la evolución de la resiliencia y su impacto en la ciberseguridad, la ciberdefensa y la ciberdiplomacia, junto a las principales aportaciones de cada iniciativa europea y nacional de los últimos años. El análisis plantea la duda de si la ciberresiliencia sirve sólo para designar la resiliencia de la ciberseguridad o si altera el modelo de gestión de la ciberseguridad y las funciones de sus responsables.

Análisis

Resiliencia se aplica a todo lo que tenga que ver con la capacidad de recuperación, tanto a las medidas preventivas como a las reactivas para minimizar daños y agilizar la recuperación. Como ejemplo, las estrategias españolas de Seguridad Nacional han asociado el término de resiliencia a la gestión de las crisis para normalizar cuanto antes el funcionamiento de los servicios esenciales. En su último informe de 2024, se considera la ciberresiliencia, la resiliencia de la ciberseguridad, como uno más de los componentes de la resiliencia nacional, para los que se ha creado un Grupo Permanente de Coordinación dentro del Comité de Situación del sistema de Seguridad Nacional.[2] Dentro de la ciberseguridad, la resiliencia se ha asociado a la protección de las infraestructuras críticas y la provisión de los servicios esenciales ofrecidos por éstas, mediante la aplicación de medidas de seguridad que han evolucionado desde un

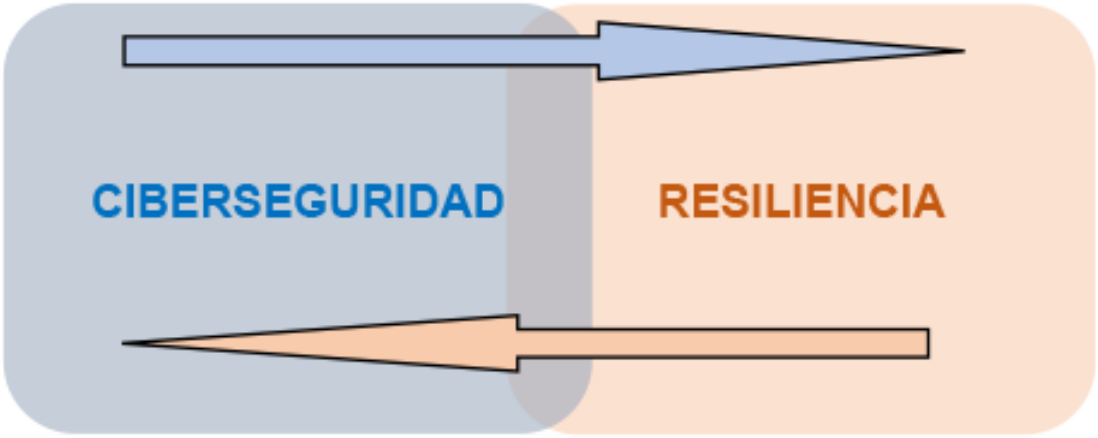
[1] Los autores desean expresar su agradecimiento a los miembros del Grupo de Trabajo sobre Ciberpolíticas, que revisaron el borrador y, en particular, a Carlos Galán y Pedro Pablo López por sus aportaciones.

[2] Presidencia del Gobierno (2024), “La resiliencia en el marco de la seguridad nacional”, marzo 2024, p. 10.

enfoque de cumplimiento de obligaciones regladas hacia otro orientado a la gestión de los riesgos (*risk-based approach*) en la que se incluyen toda clase de riesgos, como los tecnológicos, que no se contemplaban en la ciberseguridad.[3]

La ciberseguridad y resiliencia están significativamente relacionadas. Los modelos de evaluación de la ciberseguridad, tales como ISO 27001 o el Esquema Nacional de Seguridad, contemplan habitualmente medidas a caballo entre la ciberseguridad y la resiliencia, como la exigencia de desarrollar planes de contingencia. Sin embargo, estos modelos no suelen incluir otros elementos o acciones, más propios de la resiliencia, tales como las dirigidas a informar al público del incidente para recuperar la confianza en la organización, en el sector o en el propio Estado a través, por ejemplo, de la notificación a los organismos supervisores, a las Fuerzas y cuerpos de seguridad o medidas de respuesta de carácter social o económico.

Figura 1. Superposición y convergencia de la ciberresiliencia



Fuente: elaboración del Grupo de Trabajo sobre propuesta de Carlos Galán.

Ciberseguridad y resiliencia son dos conceptos superpuestos con una frontera más o menos difusa. Se puede considerar que son dos conceptos diferentes (ciberseguridad o resiliencia) cuya interacción se estrecha según la Figura 1, o que la resiliencia es un estado o cualidad aplicable a la ciberseguridad (la resiliencia de la ciberseguridad o ciberresiliencia). La relativa dificultad de deslindar ambos conceptos ha podido provocar una cierta inadecuación de la terminología, especialmente cuando se han empleado indistintamente, como en la Unión Europea (UE).[4]

El término ganó popularidad en Europa durante la pandemia del COVID-19, que desencadenó una oleada de crisis sanitarias, económicas, logísticas y digitales que obligó a la UE a reforzar sus mecanismos de preparación, respuesta y resiliencia ante

[3] Andrés Moisés Barrio (2023), "El cumplimiento basado en el riesgo o risk-based compliance, pieza cardinal del nuevo Derecho digital europeo", Real Instituto Elcano, ARI 34 (20/IV/2023).
[4] La denominación de la Cyber Resilience Act, tiene que ver poco con el concepto de ciberresiliencia.

futuras crisis.[5] El término se aplicó enseguida a la economía mediante el Fondo de Recuperación y Resiliencia (NextGenerationEU), lo que unido a la confrontación geopolítica con China y a la invasión rusa de Ucrania ampliaron aún más el interés por ella dentro de la Unión. En el ámbito de la seguridad y la defensa, la Brújula Estratégica incluyó un análisis de riesgos de la UE en el que se describían los retos y amenazas que afectaban a la seguridad europea y que obligaban a reforzar la resiliencia europea en sus distintos ámbitos, incluido el de la ciberseguridad.

A la "europeización" de la resiliencia, le siguió su "atlantización" en el Concepto Estratégico de la Organización del Tratado del Atlántico Norte (OTAN) de 2022. La Alianza tenía que protegerse frente a la hostilidad de las tácticas híbridas que obligan a reforzar todas las dimensiones de la resiliencia, tanto civiles como militares, incluidas la ciberseguridad y la ciberdefensa. La OTAN dispone de una Estrategia contra las Amenazas Híbridas desde 2015 y de un Centro de Excelencia al respecto desde 2017. También coopera con la UE para fomentar la resiliencia de las infraestructuras críticas, aunque corresponde a los Estados miembros supervisar su evolución.[6]

A la resiliencia colectiva y nacional se añade la corporativa. A medida que la resiliencia ha escalado posiciones en el enfoque de riesgo de las entidades privadas, se está convirtiendo en la medida de la continuidad del negocio. En ese sentido, proliferan los índices que miden la ciberresiliencia corporativa, como el Cyber Resilience Index del Foro Económico Mundial. Emplean variables que se corresponden, en líneas generales, con las que se utilizan para medir la ciberseguridad, pero enfocadas a permitir que las organizaciones continúen con su funcionamiento en las condiciones de ciberseguridad más difíciles (evalúan la resiliencia de la ciberseguridad o la ciberresiliencia).

1. La ciberresiliencia en la UE

Los riesgos afectan a la democracia, la seguridad económica y la energética, las libertades, las infraestructuras críticas, las políticas exterior, de seguridad y de defensa, los cinco dominios estratégicos, el cambio climático, emergencias, cadenas de suministro, tecnologías y asociaciones estratégicas de la UE. La Estrategia de Ciberseguridad de 2013 identificó la resiliencia de sus redes y sistemas de información como uno de sus cinco objetivos estratégicos y, para desarrollarla, se propuso incrementar las capacidades de prevención y respuesta mediante una Directiva con el fin de armonizar los niveles de seguridad de las redes y sistemas de información de la UE (conocida como Directiva NIS), así como los sistemas de control industrial y la colaboración público-privada. Progresivamente, y sin perjuicio de las competencias nacionales, la UE ha ido asumiendo el papel de dinamizador y regulador de la ciberresiliencia del mercado interior y dotándose de los instrumentos necesarios para ello.[7]

[5] Conclusiones del Consejo (14276/2021) sobre el reforzamiento de la preparación, capacidad de respuesta y resiliencia a futuras crisis de 23 de noviembre.

[6] EU-NATO Task Force (2023), "Resilience of Critical Infrastructure. Final Report", junio 2023.

[7] Entre otros, la Organización Europea de Ciberseguridad (ECSO), los Centros de Información y Análisis (ISAC), el Centro Conjunto de Investigación (JRC) y la Academia de Ciberseguridad.

La UE aprobó en 2016, la mencionada Directiva NIS para proteger las infraestructuras críticas y armonizar las obligaciones de los operadores de los servicios críticos.[8] Los Estados miembros tuvieron que designar autoridades nacionales, elaborar estrategias y planes de cooperación NIS y disponer de equipos de respuesta a los incidentes (*Computer Emergency Response Teams*, CERT), así como establecer mecanismos de prevención, mitigación y respuesta frente a incidentes. Los actores privados y públicos de la ciberseguridad en sectores críticos tuvieron que pasar de una cultura de cooperación voluntaria (*European Public Private Cooperation*, EP3R) a una cultura de gestión de riesgo cada vez más reglada en el plano nacional y europeo.

La UE estableció su propio CERT-EU y, aunque ya contaba con una agencia de ciberseguridad (ENISA) desde 2004, tuvo que reforzar sus competencias para apoyar a los Estados miembros y a las empresas en la implantación de las nuevas medidas de cooperación y resiliencia mediante la Cybersecurity Act de 2019, modificada en 2023. El nuevo reglamento incluyó los esquemas europeos de certificación, imprescindibles para garantizar un nivel adecuado de ciberseguridad de los productos, servicios y procesos europeos, tal y como se analizará más adelante.

En mayo de 2020, se aprobó la Estrategia de Ciberseguridad de la UE en la que se ampliaron y profundizaron las medidas para la "ciberresiliencia" de todos los sectores relevantes. La Estrategia puso en marcha la revisión de la Directiva NIS, una nueva Directiva sobre la resiliencia de las entidades críticas, una red de centros de operaciones (SOC) y la Unidad Conjunta de Ciberseguridad de la UE. La Estrategia europea siguió reforzando el papel de la UE como coordinador de las respuestas a incidentes a gran escala[9] y, también, se preocupó por canalizar inversiones aprovechando los fondos europeos de investigación para desarrollar competencias industriales[10], tecnológicas y de investigación europeas mediante un reglamento para establecer el Centro Europeo de Competencia en Ciberseguridad.

Posteriormente, en mayo de 2022, el Consejo hizo pública la ciberpostura de la UE, es decir la forma en la que la UE se propone combinar los distintos instrumentos y políticas de la UE para preservar un ciberespacio abierto, libre y seguro y defenderlo de las amenazas y ciberataques.[11] Esta doctrina de acción reivindica la necesidad de reforzar la ciberresiliencia de la UE, a través de todas las iniciativas normativas señaladas anteriormente, junto a la de sus aliados y socios mediante la cooperación y la construcción de capacidades. Comprende todas las fases de actuación, desde la

[8] El Consejo Europeo solicitó en junio de 2004 la elaboración de una estrategia para proteger las infraestructuras críticas. La Comisión estableció en 2006 el primer Programa Europeo para la Protección de las Infraestructuras Críticas (EPCIP) frente a la amenaza terrorista y en 2008 aprobó la Directiva 114/2008 para la identificación, designación y evaluación de las infraestructuras críticas europeas.

[9] Recomendación 2017/1584 de 13 de septiembre sobre la respuesta coordinada a incidentes y crisis de ciberseguridad a gran escala.

[10] Entre otros, InvestEU, Horizonte Europa, Digital Europe Programme y Connecting Europe Facility.

[11] Conclusiones del Consejo 9364/2022 de 23 de mayo sobre el desarrollo de la ciberpostura de la UE que desarrollan las comunicaciones JOIN(2017)450 de 13 de septiembre del alto representante sobre resiliencia, disuasión y defensa para fortalecer la ciberseguridad de la UE, la COM(2016)410 de 7 de mayo sobre el reforzamiento del sistema europeo de ciberresiliencia y las conclusiones 14972/19 de 10 de diciembre para reforzar la resiliencia y contrarrestar las amenazas híbridas.

prevención a las opciones de respuesta, incluidas las de responder "con firmeza" a los ciberataques.[12]

La Comisión puso en marcha un plan de acción en 2018 que ha llevado al reglamento de resiliencia operativa digital (*Digital Operational Resilience Act*, DORA) de diciembre de 2022.[13] Es un reglamento sectorial que se aplica a un gran número de entidades de crédito, de pago, de dinero electrónico, agencias de calificación, gestores de fondos, empresas de seguros y reaseguros, proveedores de servicios de criptoactivos o de servicios de Tecnologías de la Información y la Comunicación (TIC) tales como plataformas de *cloud* y análisis de datos. DORA incide en afrontar la gestión de riesgos tecnológicos y en particular de ciberseguridad.

El sector financiero ha sido un pionero en la lucha contra la ciberdelincuencia y sigue siendo uno de los sectores más expuestos a los ciberataques de los grupos criminales organizados. La regulación es muy intensa y demandará cambios en la gestión del riesgo tecnológico y en la gobernanza interna de la ciberseguridad, incluidas las nuevas responsabilidades de los consejos de administración. El sector cuenta con actores públicos y privados dentro de un ecosistema de instituciones internacionales, europeas y nacionales de gobernanza bancaria como el Comité de Supervisión Bancaria de Basilea (BCBS), el Comité de Pagos e Infraestructura del Mercado (CPMI), entre muchos otros. La regulación sobre resiliencia ha pasado de un enfoque de prevención de los ciberataques dentro de la gestión de riesgos a otro que asume la posibilidad de un fallo (*breach mentality*) y está más alineado con el concepto de resiliencia operativa.[14] El Banco Central Europeo también ha adoptado este enfoque combinado para proteger los datos y sistemas de los ciberataques, minimizar las disrupciones y reanudar las operaciones cuanto antes, para lo que realiza pruebas de ciberresiliencia a entidades europeas de crédito.[15]

La Directiva sobre las medidas para aumentar el nivel de seguridad común en la UE (*Security of Network and Information Systems*, NIS2) de diciembre de 2022 revisó la Directiva NIS de 2016 y debe trasponerse en octubre de 2024.[16] Es una regulación transversal que establece exigencias mínimas comunes de ciberresiliencia a las entidades obligadas establecidas en la UE y que ofrecen servicios esenciales. Los Estados miembros deberán adecuar sus estrategias nacionales a la NIS2, definir autoridades competentes, designar equipos de respuesta (CSIRT.es) y habilitar regímenes de supervisión y sanciones. Las entidades implicadas, –las anteriores más las administraciones públicas, proveedores de servicios digitales, comunicaciones electrónicas, productos críticos, servicios postales y aguas–, aumentarán sus obligaciones de gobernanza, notificación, certificación y cadena de suministro, entre

[12] Recomendación del Consejo (2023/C, 20/01) para reforzar la resiliencia de las infraestructuras críticas.

[13] Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo de 14 de diciembre sobre la resiliencia operativa digital del sector financiero y por el que se modifican los Reglamentos (CE) 1060/2009, 648/2012, 600/2014, 909/2014 y 2016/1011.

[14] Juan C. Crisanto y Jefferson U. Pelegrini (2023), "Bank's cyber security. A second generation of regulatory approaches", Financial Instability Institute, junio 2023.

[15] Banco Central Europeo, nota de prensa (3/I/2024).

[16] Directiva 2522/2022 para reforzar el nivel de ciberseguridad común en la UE de 14 de diciembre.

otros. Además, la NIS2 formalizó la red europea para la gestión de crisis (*European Cyber Crises Liaison Organisation Network*, EU-CyCLONe) que funcionaba informalmente desde 2020 entre las autoridades nacionales y ENISA para mejorar la respuesta a los incidentes.

La Directiva sobre la resiliencia de entidades críticas (*Critical Entities Resilience*, CER) de enero de 2023 aportó una definición de la misma en la que se diferencian elementos cibernéticos y no cibernéticos, y dentro de los cibernéticos valoran capacidades desde la prevención a la recuperación.[17] Persigue la resiliencia de las entidades críticas frente a emergencias naturales o causadas por cualquier tipo de amenaza y deroga la Directiva 2008/114 sobre la identificación y designación de infraestructuras críticas europeas (conocida como Directiva PIC). Son entidades críticas las que proporcionan servicios de banca, transporte, salud, agua, residuos, infraestructuras digitales y financieros, espacio, administración pública y alimentos (10 sectores). Los países europeos deberán trasponer la Directiva en 2024 y disponer en enero de 2026 de una estrategia específica de resiliencia (no de ciberresiliencia), con objetivos, medidas de actuación y un marco de gobernanza, junto con una evaluación de riesgos específica y un listado de entidades críticas. Por su parte, las entidades críticas deberán disponer de un plan de resiliencia y ponerlo en práctica bajo la supervisión de las autoridades nacionales, mientras que la Comisión supervisará los resultados nacionales a través de su Grupo de Resiliencia de las Entidades Críticas (al igual que el Grupo de Cooperación supervisa los avances de la resiliencia en aplicación de la Directiva NIS).[18] De esta forma, la gestión de la resiliencia, y no sólo de la ciberseguridad, ha entrado en la gestión de riesgos corporativos de las entidades críticas.

El Reglamento sobre cibersolidaridad (*EU Cyber Solidarity Act*, CSA) de abril de 2023 reforzó la conciencia situacional, el intercambio de información y el apoyo a la preparación ante ciberincidentes a gran escala que puedan afectar a varios Estados miembros. Para alcanzar estos objetivos se creó el denominado ciberescudo europeo (*European Cybersecurity Shield*) con una red de SOC interconectados junto a un mecanismo de emergencia (*cyber emergency mechanism*) y otro de revisión de incidentes (*cyber security review mechanism*). El ciberescudo se apoya en los SOC nacionales y en los SOC transfronterizos (consorcios de al menos tres países) para detectar incidentes y coordinar la respuesta con la Comisión, la red CSIRT y la red EU-CyCLONe.

El Reglamento de Ciberresiliencia (*Cyber Resilience Act*, CRA) extiende las obligaciones de resiliencia a los fabricantes de productos conectables, *software* y *hardware*. Anunciado en la Estrategia de Ciberseguridad de la UE de 2020, y a partir de su entrada en vigor en 2024, no se podrán comercializar productos que no cumplan los

[17] Resiliencia se define en la Directiva como “la capacidad de una entidad crítica para la prevención, la protección, la respuesta, la resistencia, la mitigación, la absorción, la adaptación y la recuperación en caso de un incidente, considerado éste un acontecimiento que tiene el potencial de perturbar significativamente, o que perturbe, la prestación de un servicio esencial, en particular cuando afecte a los sistemas nacionales que salvaguardan el Estado de Derecho” (art. 2).

[18] Entre las medidas establecidas en el Plan de Resiliencia, las entidades críticas deberán: (1) implantar medidas técnicas, organizativas y de seguridad adecuadas y proporcionadas; (2) elaborar y aplicar un plan de resiliencia; así como (3) designar un punto de contacto con las autoridades.

requisitos/certificación y los consumidores sabrán si compran o no productos protegidos y, además, si la protección se mantendrá o no durante la vida útil del producto.[19] En contrapartida, contarán con un etiquetado CE que contribuirá a la armonización y mejora de la competitividad dentro del Mercado Digital Único. El Reglamento CRA no incluye el *software* de código abierto o el proporcionado como parte de un servicio esencial, ya que la Directiva NIS2 atribuye su responsabilidad a las entidades esenciales que prestan esos servicios (sanidad, automoción, aviación…). Sí que impone requisitos de ciberseguridad obligatorios para el diseño, desarrollo y producción de productos digitales conectados (*Internet of Things*, IoT).

2. El papel de los esquemas de certificación y estándares en la ciberresiliencia

La gestión del riesgo en la ciberseguridad cuenta con esquemas de certificación y estándares que establecen principios básicos y requisitos mínimos para proteger la seguridad de la información de productos y servicios ofrecidos por las empresas, así como de su cadena de suministro. Se apoyan en estándares y normas consensuadas entre expertos y organizaciones que forman parte de los organismos de normalización. La certificación se realiza por una entidad reconocida como independiente de las partes interesadas y manifiesta la conformidad de una determinada empresa, producto, proceso, servicio o persona con los requisitos definidos en normas o especificaciones técnicas.

La Comisión incluyó en la *Cybersecurity Act* un marco europeo armonizado de esquemas de certificación válidos en la totalidad de los Estados miembros. Los esquemas establecen el alcance y categorías de productos y servicios, el nivel de seguridad, el tipo y los criterios de evaluación (mediante autoevaluación o realizado por terceras partes) y el grado de garantía o confianza esperado (bajo, sustancial y alto). La certificación UE es voluntaria, salvo excepciones regladas, y su vigencia máxima es de tres años (renovable). En la actualidad, ENISA desarrolla tres esquemas europeos: esquemas para la Comisión: el de Certificación de Servicios en la Nube (EUCS), el de Certificación de Servicios de Seguridad Gestionados[20] y el de Certificación de Ciberseguridad para 5G (EU5G) y ha propuesto para su aprobación el de Ciberseguridad sobre Criterios Comunes para productos TIC (EUCC 1.1.1). También está evaluando si las aplicaciones y servicios basados en inteligencia artificial podrían ser objeto de certificación en materia de ciberseguridad, aunque este trabajo es preparatorio porque la Comisión no ha solicitado un esquema europeo todavía.

Sea para reforzar un modelo de gestión de ciberseguridad o de ciberresiliencia, su madurez depende de la implantación de esquemas de certificación armonizados en la UE para evitar el riesgo de fragmentación del mercado y la pérdida de competitividad de

[19] A partir de su aprobación en 2024, la entrada en vigor será de 36 meses con carácter general y 21 meses para las notificaciones de incidentes.

[20] Los *servicios de seguridad* gestionados, prestados por empresas especializadas, son cruciales para la prevención, detección, respuesta y recuperación de incidentes de ciberseguridad, así como para realizar pruebas de penetración o auditorías de seguridad.

las empresas transfronterizas[21]. Sin embargo, la adopción de esquemas internacionales del tipo ISO 27001 o específicos europeos por las empresas choca con los distintos esquemas nacionales ya implantados por las administraciones nacionales. Por ejemplo, en España son referencia el Esquema Nacional de Seguridad (ENS) de aplicación a todo el sector público, así como a los proveedores que colaboran con la Administración, el esquema LINCE que ofrece una metodología simplificada de evaluación de productos TIC basada en los principios de criterios comunes orientada al análisis de vulnerabilidades y pruebas de intrusión u otros sectoriales como, por ejemplo, la calificación de ciberseguridad Pinakes de aplicación al sector financiero.

3. Ciberdiplomacia y ciberdefensa

En la acción exterior de la UE y de sus Estados miembros confluyen diversas variantes como la diplomacia verde, la ciberdiplomacia o la diplomacia digital, que contribuyen a su comunicación estratégica. La Estrategia para la Política Exterior y de Seguridad de la UE de 2016 no hizo referencias a la ciberdefensa, pero sí a la ciberdiplomacia y a la ciberseguridad. Ciberdiplomacia se refiere a los aspectos diplomáticos de las relaciones internacionales de la ciberseguridad, tanto la cooperación con socios y aliados para robustecer el derecho internacional y la gobernanza multilateral aplicable al ciberespacio como la construcción de capacidades con ellos. La construcción de la ciberdiplomacia europea comenzó en 2015 con la declaración de principios y objetivos del Consejo.[22] En 2017, el Consejo aprobó un conjunto de medidas (*EU Cyber Diplomacy Toolbox*) de prevención, disuasión o respuesta, incluidas las restrictivas frente a las actividades maliciosas de terceros.[23] En 2019, se adoptó el régimen de sanciones y las primeras sanciones se adoptaron en 2020 dentro de la Política Exterior y de Seguridad Común (PESC).[24]

A la ciberdiplomacia de la UE le siguió la diplomacia digital, un enfoque geopolítico de la ciberseguridad que tiene que ver con sus dimensiones tecnológicas y económicas.[25] En términos prácticos de resiliencia, la ciberdiplomacia trata de fortalecer la UE frente a los ciberataques y acciones híbridas de terceros, mientras que la diplomacia digital trata de preservar la soberanía tecnológica y digital (por ejemplo, el Plan de Acción 5G). La diplomacia digital comparte con la ciberdiplomacia la protección y libertad del mercado digital único y de internet, así como la participación en instituciones y normas internacionales de gobernanza.[26]

[21] Manuel Carpio (2021), “La calificación de la seguridad de los sistemas de información en Europa”, Real Instituto Elcano, ARI 77 (9/IX/2021).

[22] Conclusiones del Consejo 6122/2015 de 11 de febrero sobre ciberdiplomacia.

[23] Conclusiones del Consejo 9916/2017 de 7 de junio sobre una respuesta diplomática conjunta de la UE a actividades maliciosas y decisiones del Consejo 2019/796 y 2019/797 de 17 de mayo sobre las medidas restrictivas contra los ciberataques que amenacen a la UE o sus Estados miembros.

[24] Decisión del Consejo 1127/2020 de 30 de julio sobre sanciones.

[25] Conclusiones del Consejo 11406/22 de 18 de julio sobre la diplomacia digital de la UE.

[26] Annegret Bendiek y Matthias C. Ketterman (2021), “Revisiting the EU Cybersecurity Strategy: A Call for EU Cyber Diplomacy”, SWP Comment 16, febrero de 2021.

La ciberresiliencia tiene un ámbito civil –la ciberseguridad– y otro militar –la ciberdefensa– en la UE. La Estrategia de Ciberseguridad de 2013 reivindicó la necesidad de desarrollar una política de ciberdefensa asociada a la Política Común de Seguridad y Defensa (PCSD). Para ello se elaboró el *Cyber Defence Policy Framework* de 2014, actualizado en 2018[27], para reforzar la resiliencia de los sistemas y redes de información de la Defensa, sus necesidades operativas y la defensa frente a los ataques más sofisticados, aprovechando el apoyo y la experiencia de los responsables de la ciberseguridad de la UE [28] y de otros socios internacionales como el Centro de Excelencia de Ciberdefensa (CCD COE) de la OTAN.

Aunque la Estrategia de Política Exterior y de Seguridad de 2016 no hizo referencia a la ciberdefensa, la alta representante recuperó el término mediante su comunicación de septiembre de 2017 en la que se recogieron las posibles sinergias entre las capacidades de ciberseguridad de la UE y las capacidades en construcción de la PCSD. En 2018, el Estado Mayor Militar de la UE elaboró las directrices para la utilización del ciberespacio como un dominio de operaciones y misiones militares.[29] En el mismo sentido, tanto la Estrategia de Ciberseguridad de 2020 como la presidenta de la Comisión en 2021 urgieron la presentación de una política de ciberdefensa. [30] La posterior Brújula Estratégica de 2022 propuso desarrollar la política de ciberdefensa de la UE en colaboración con los Estados miembros y la OTAN de acuerdo con la ya mencionada ciberpostura de la UE en todos los dominios estratégicos (tierra, mar, aire, espacio y ciberespacio) y en todas las dimensiones de la PCSD (lucha contra el terrorismo, la proliferación, el control de armamento y otras). También quiso mantener el espacio de colaboración entre la ciberseguridad y la ciberdefensa, además de codificar las iniciativas para hacer frente a los ciberataques y proporcionar ciberseguridad, solidaridad y asistencia mutua a la Unión, sus instituciones, Estados miembros y socios en las cibercrisis.

En noviembre de 2022, el alto representante propuso al Parlamento y al Consejo la aprobación de una Política de Ciberdefensa de la UE orientada a la resiliencia del ecosistema de defensa de la UE que incluye entidades militares, industria y operadores privados. Para ello propuso desarrollar e invertir en capacidades, consolidar el ecosistema de ciberdefensa y cooperar con socios afines.[31] Las capacidades se refieren a las necesarias para operar en todo el espectro de la ciberdefensa y a las sinergias con el ecosistema de ciberseguridad para aumentar la resiliencia de la UE, incluido el sector de la defensa. También para apoyar las operaciones y misiones de la PCSD, aprovechando los instrumentos financieros y tecnológicos de la UE. A partir de entonces, el Consejo valora periódicamente el desarrollo de la política de ciberdefensa.[32]

[27] Consejo, 14413/2018 de 19 de noviembre sobre la actualización del marco de la política de ciberdefensa.

[28] La Agencia Europea de Defensa (EDA), el Servicio Europeo de Acción Exterior (SEAE), ENISA y EUROPOL.

[29] Doc. EEAS (2021)706 de 15 de septiembre su visión y estrategia del ciberespacio como un dominio de operaciones militares.

[30] Discurso sobre el estado de la Unión (15/IX/2021).

[31] Alta Representante, comunicación JOIN (2022) 49 de 10 de noviembre.

[32] Conclusiones 9618/23 de 22 de mayo del Consejo sobre la política de ciberdefensa de la UE.

España no cuenta con un concepto de ciberdiplomacia en su Estrategia de Acción Exterior 2021-2024. El Ministerio de Asuntos Exteriores, Unión Europea y Cooperación sí que considera la diplomacia digital como un instrumento de su diplomacia pública que realiza a través de los sitios web y los perfiles de las redes sociales de su red diplomática y consular. Por su parte, el Ministerio de Defensa sí que cuenta desde 2018 con un Concepto de Ciberdefensa para orientar el desarrollo doctrinal de las operaciones militares en el ciberespacio.[33] En sentido contrario, queda pendiente de definición y ejecución el concepto de "ciberdefensa activa" implantado en la Estrategia Nacional de Ciberseguridad de 2019 para que el sector público pueda mejorar la resiliencia del sector privado. La clarificación y desarrollo de los conceptos es importante para delimitar la entidad de las amenazas y la asignación de responsabilidades en fenómenos de riesgo novedosos como la desinformación o la guerra híbrida.

4. La ciberresiliencia desde la perspectiva de los gestores corporativos de ciberseguridad

Para los gestores consultados, la ciberresiliencia es parte de la resiliencia corporativa y califica un estado de la ciberseguridad: se es más o menos ciberresiliente si la ciberseguridad es más o menos capaz de asegurar la recuperación. Para ser ciberresilientes, las corporaciones necesitan que su ciberseguridad cubra todas las fases de gestión, desde la prevención a la recuperación, y todos los riesgos de ciberseguridad. Pero para ser resilientes, las corporaciones necesitan –además– que también sean resilientes el resto de los componentes de riesgo distintos de la ciberseguridad a los que se enfrentan, en particular su cadena de suministro.

La ciberresiliencia de las corporaciones contribuye a su resiliencia global, pero ésta depende de muchos factores y procesos que no son exclusivamente de ciberseguridad. La ciberresiliencia es algo más que reponerse tras un ciberataque porque incluye medidas anticipatorias que disminuyen la exposición de las corporaciones y mitigan sus daños. También es algo más que cumplir las obligaciones de ciberseguridad y que preservar la seguridad de la información y los sistemas, porque existen riesgos transversales que afectan al estado de la ciberresiliencia.

La ciberresiliencia no amplia los ámbitos de la ciberseguridad. Los responsables de seguridad de la información (CISO) son conscientes de que han aparecido nuevos riesgos transversales como los tecnológicos o los geopolíticos, entre muchos otros, que se gestionan mediante comités multisectoriales de crisis o mediante gestores de riesgos múltiples. Las corporaciones aspiran a contar con una resiliencia integral que se gestiona integrando todos los gestores de riesgos, incluido el de ciberseguridad, y con modelos de gestión que dependen del ámbito y apetito de riesgo de cada empresa. A diferencia del pasado, y para contribuir a la resiliencia general, los CISO deben ahora colaborar en los distintos comités, ejercicios y simulacros con otros responsables de riesgos. En este sentido, las corporaciones siguen el patrón de integración y gestión de riesgos de los gabinetes de crisis nacionales y multinacionales: incluir todos los vectores de riesgo y todas las fases del proceso de gestión. Para ello, desarrollan estructuras y

[33] Centro Conjunto de Desarrollo de Conceptos (2018), "Concepto de Ciberdefensa", CESEDEN (28/IX/2018).

procesos de coordinación permanentes, que permiten acumular la experiencia de cada crisis puntual e implantan planes y ejercicios de ciberresiliencia. De este modo, aseguran la continuidad del negocio, la resiliencia corporativa.

Conclusiones

Resiliencia, ciberseguridad y ciberresiliencia son términos afines, pero no idénticos que comparten fronteras difusas. La preocupación por prevenir los riesgos (ciberseguridad) se ha ampliado a la recuperación si se producen ciberataques (ciberresiliencia) o crisis complejas en las que entran componentes cibernéticos y no cibernéticos (resiliencia). La ciberresiliencia es un prerrequisito del ciberespacio y del ecosistema de ciberseguridad asociado a una economía digitalizada madura. Abarca todos los ámbitos de la ciberseguridad, incluida la recuperación, y tiene su propia dinámica de adaptación. Se incluye por diseño en las políticas europeas, nacionales y corporativas de ciberseguridad y dispone de un creciente conjunto de instrumentos.

Por su parte, la resiliencia ocupa un lugar preferente entre las prioridades de los responsables de las seguridades colectiva, nacional y corporativa, La resiliencia tiene vocación omnicomprensiva, gestionar todos los componentes relevantes y evitar rupturas sistémicas. Que un Estado, organización o corporación sean resilientes significa que pueden resistir mejor los riesgos y amenazas que afectan a los servicios esenciales y, también, que pueden recuperar su funcionamiento si los ataques se producen en entornos degradados.

La ciberresiliencia, la resiliencia de la ciberseguridad, obliga a los CISO y autoridades responsables a gestionar los riesgos de ciberseguridad y a colaborar en la gestión de los riesgos no cibernéticos. Para lo primero, la ciberresiliencia ha evolucionado desde el cumplimiento de unas medidas de seguridad establecidas *ex ante* hacia la obligación de anticipar y evaluar los riesgos individuales a los que se ve expuesto cada agente, proceso o producto y adoptar por diseño una estrategia de gestión del riesgo embebida al mismo. Para los segundos, la ciberresiliencia debe formar parte de los mecanismos de gestión de crisis y continuidad de negocio para asegurar la resiliencia global/integral. Según el volumen y la vulnerabilidad de las empresas a la continuidad de negocio, los CISO continuarán ocupándose de la ciberseguridad, de la ciberresiliencia o de la resiliencia si participan en la gestión de los riesgos no cibernéticos.