La importancia de la I+D para potenciar una industria de seguridad competitiva

Ana I. Ayerbe | Directora del Área de Negocio TRUSTECH de TECNALIA | @AnaAyerbe

Tema

La investigación y el desarrollo de la ciberseguridad en la Unión Europea es necesaria para potenciar una industria de ciberseguridad competitiva y defenderse de las crecientes ciberamenazas.

Resumen

El reforzamiento de la investigación y desarrollo (I+D) de la ciberseguridad europea es imprescindible para que la Unión Europea pueda defenderse de las crecientes ciberamenazas y competir por el mercado industrial y tecnológico de la ciberseguridad. Este ARI describe el estado de la I+D en la UE y las medidas que se están adoptando para impulsarla en los distintos ámbitos de la inversión, la coordinación de los centros, los riesgos y las líneas de investigación prioritarias.

Análisis

La preocupación por la I+D europea en ciberseguridad es patente en la fragmentación existente en el ámbito de la I+D, con una industria que apenas cuenta con jugadores mundiales y una inversión pública a todas luces insuficiente —de entre 1.000 y 2.000 millones de euros— si se compara con la inversión en Estados Unidos —de 19.000 millones de dólares al año, incluyendo 900 millones para investigación e innovación— o frente al programa chino de tecnología cuántica enfocado a la ciberseguridad —de unos 10.000 millones—, lo que coloca claramente a Europa en una situación delicada a la hora de defenderse de las ciberamenazas.[1] En este contexto, es necesario trabajar en Europa tanto en aspectos organizativos que permitan crear masas críticas investigadoras de relevancia como coordinando las operaciones de las infraestructuras de laboratorios para no duplicar esfuerzos ya realizados o dotando a las diferentes iniciativas planteadas de presupuestos apropiados a la dimensión y relevancia de la ciberseguridad, con apuestas que se acerquen a las que se están realizando en otras partes del mundo.

[1] Comisión Europea, “Impact Assessment”, SWD (2018) 305, de 6 de abril de 2018, https://ec.europa.eu/commission/sites/beta-political/files/budget-june2018-digital-europe-impact-assessment-en.pdf.

(cont.)

En el caso de España, a pesar de que el Índice Global de Ciberseguridad, (Global Cybersecurity Index, GCI) la sitúa entre los países líderes en ciberseguridad,[2] la preocupación se refleja en la recientemente elaborada Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional el 12 de abril,[3] que señala que debe seguirse avanzando en reforzar capacidades que permitan afrontar las ciberamenazas y el mal uso del ciberespacio, planteando la I+D+i en ciberseguridad, junto con la gestión del talento tecnológico y el fomento de una base industrial de ciberseguridad, como pilares para incrementar la autonomía tecnológica.

En relación con la relevancia de la I+D+i, la Estrategia plantea líneas de acción específicas como las siguientes:

- "Potenciar la colaboración de los centros de excelencia e investigación en la lucha contra las ciberamenazas" y "asegurar la protección de las Infraestructuras Científico-Técnicas Singulares y los centros de referencia de I+D+i", dentro del Objetivo 1 de la Estrategia ("Seguridad y resiliencia de las redes y los sistemas de información y comunicaciones del sector público y de los servicios esenciales")

- "Potenciar la industria española de ciberseguridad y la generación y retención de talento, para el fortalecimiento de la autonomía digital", dentro del Objetivo 4 ("Cultura y compromiso con la ciberseguridad y potenciación de las capacidades humanas y tecnológicas").

Dentro de esta última línea de acción se plantean nueve medidas, todas ellas relacionadas con el desarrollo de la I+D+i, como un medio para lograr las competencias y tecnologías necesarias en ciberseguridad para obtener resiliencia a los ciberataques contra la Administración Pública, la industria y la sociedad y ayudar al desarrollo del mercado de la ciberseguridad. Destacan especialmente dos de las medidas:

- "Impulsar programas de apoyo a la I+D+i en seguridad digital y ciberseguridad en pymes, empresas, universidades y centros de investigación, facilitando el acceso a programas de incentivos nacionales e internacionales y mediante programas de compra pública innovadora".

- "Impulsar programas específicos de I+D+i en ciberseguridad y ciberdefensa".

[2] International Telecommunication Union, Global Cybersecurity Index (GCI) 2017, 2017, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf.

[3] Consejo Nacional de Seguridad, "Estrategia Nacional de Ciberseguridad", Orden PCI/487/2019, de 26 de abril, https://www.boe.es/boe/dias/2019/04/30/pdfs/BOE-A-2019-6347.pdf.

El panorama de la I+D+i en Europa

En la Unión Europea (UE), la necesidad de desarrollar la I+D+i quedó patente en septiembre de 2017 en el primer compromiso político de la UE para desarrollar una ambiciosa estrategia de ciberseguridad con la comunicación sobre ”Resilience, Deterrence and Defence: Building strong cybersecurity for the EU”,[4] donde se ponía el énfasis en apoyar el desarrollo de ciberresiliencia e I+D en ciberseguridad al mismo tiempo que reforzar la cooperación para prevenir, detectar y responder a ciberamenazas y poder responder de forma conjunta a ciberincidentes a gran escala en Europa. En la misma comunicación se anunciaba la intención de apoyar la creación de una red de centros de competencia en ciberseguridad, con un centro de competencia en ciberseguridad para estimular el desarrollo e implantación de tecnología de ciberseguridad.

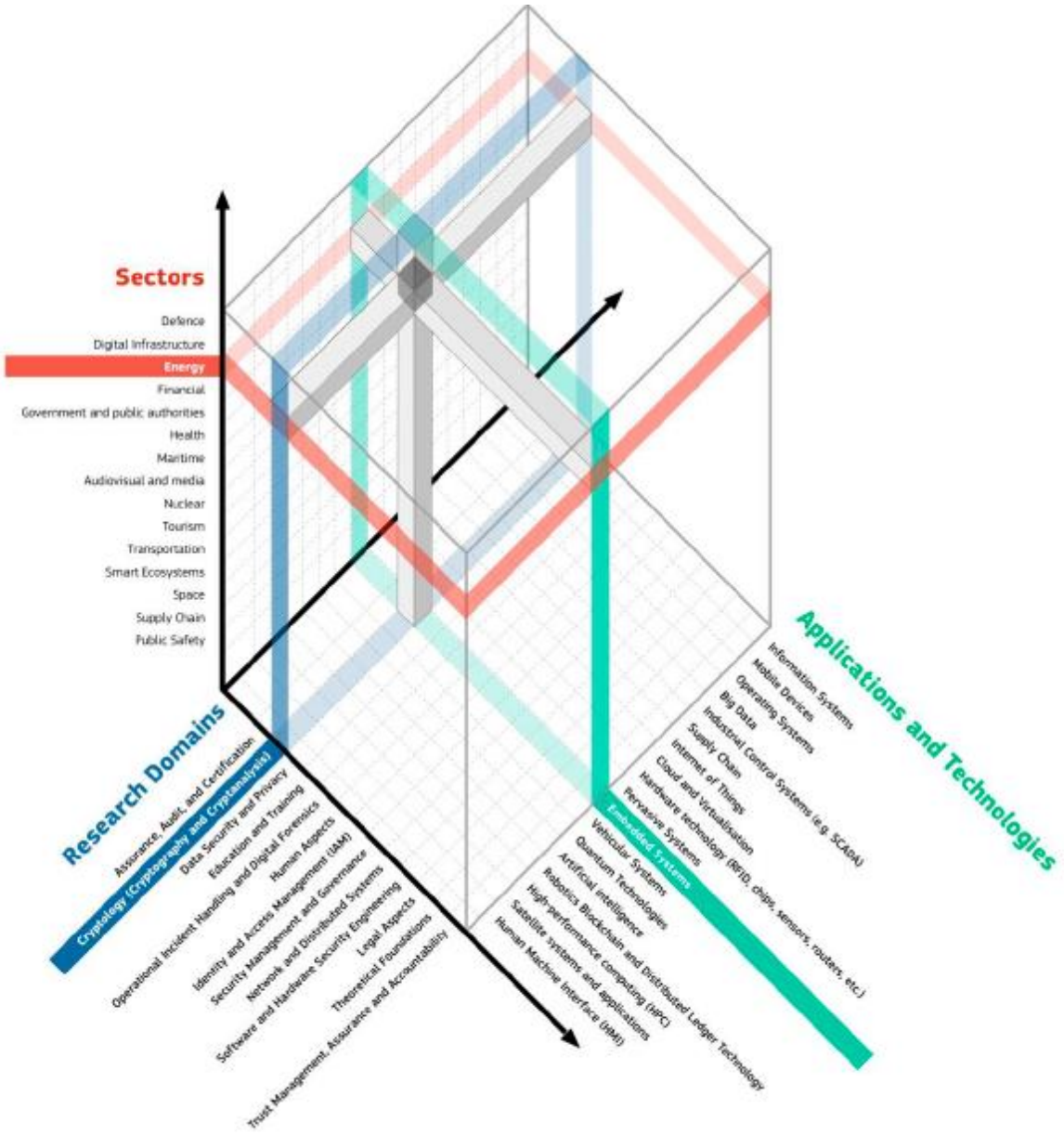
En este contexto, el Joint Research Centre, un centro de la Comisión Europea sobre ciencia y conocimiento, junto con la Dirección General para las Comunicaciones (DG Connect), inició la tarea de delimitar el complejo contexto de la ciberseguridad, sus dominios de aplicación, investigación y conocimiento, así como la de definir una taxonomía de la ciberseguridad y un esquema de clasificación que alineaba las terminologías de ciberseguridad, definiciones y dominios de la Figura 1.

Este estudio se complementó con la identificación y mapeo de los centros de ciberseguridad existentes (centros tecnológicos, laboratorios, asociaciones, grupos académicos, instituciones…) a nivel europeo (655 participantes en la encuesta)[5] utilizando la taxonomía propuesta y mostrando que en Europa existe una importante comunidad investigadora en ciberseguridad que presenta, en algunos casos, dificultades para lograr la masa crítica necesaria, falta de coordinación en dominios sinérgicos y ciertas dificultades para conectar con la industria.

[4] Joint Communication to the European Parliament and the Council: “Resilience, Deterrence and Defence: Building strong cybersecurity for the EU”, septiembre de 2017, https://ec.europa.eu/transparency/regdoc/rep/10101/2017/EN/JOIN-2017-450-F1-EN-MAIN-PART-1.PDF.

[5] “European cybersecurity centres of expertise – cybersecurity competence survey”, JRC Technical Reports, 2018, http://publications.jrc.ec.europa.eu/repository/bitstream/JRC111211/survey_report_1.6-final.pdf.

Figura 1. Taxonomía de la ciberseguridad (visión de alto nivel)

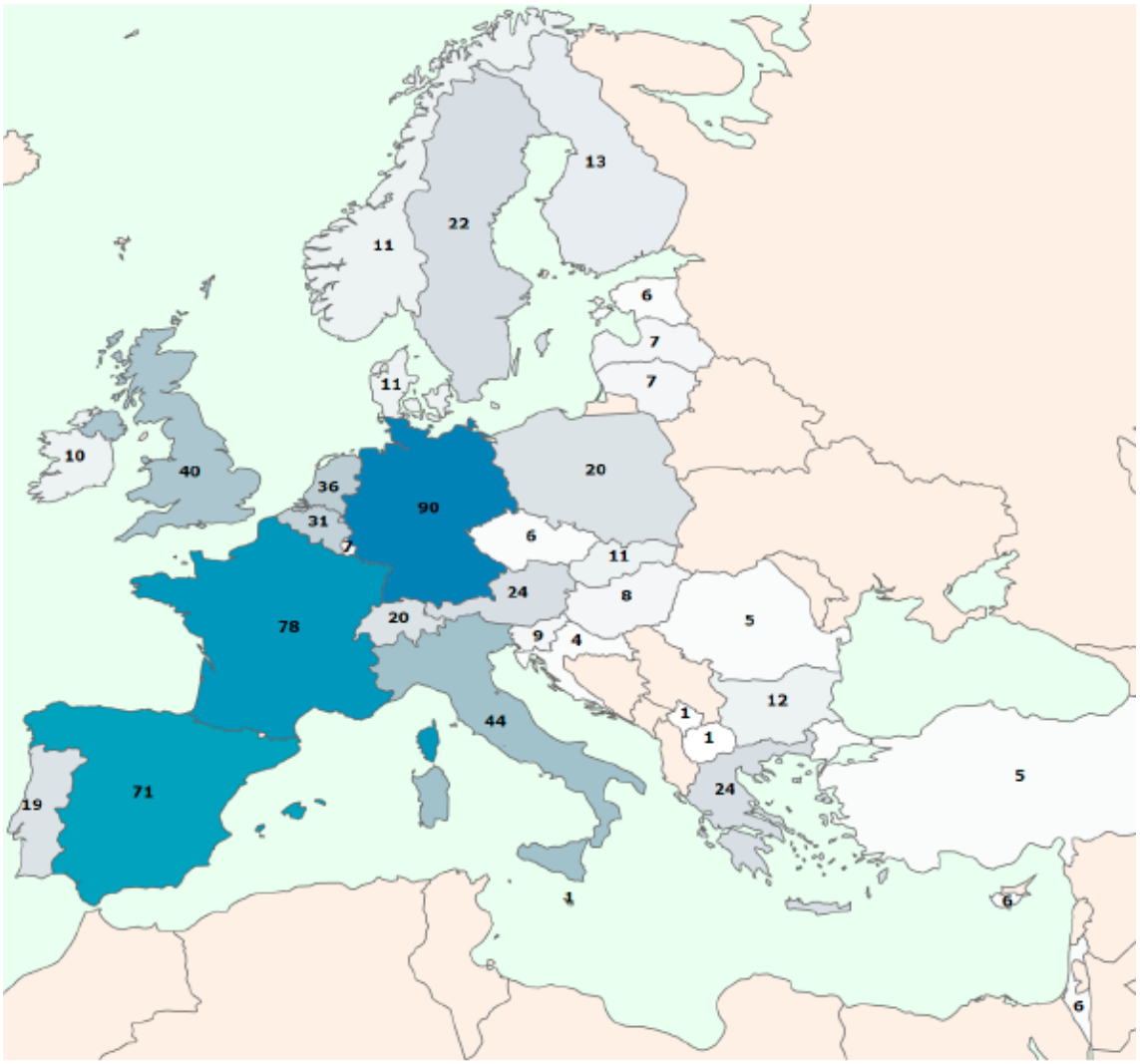


Fuente: Joint Research Centre (JRC), p. 26, http://publications.jrc.ec.europa.eu/repository/bitstream/JRC111441/taxonomy_final.pdf.[6]

Este estudio concluyó que existen dominios de importancia para la ciberseguridad que actualmente están escasamente apoyados por la comunidad investigadora, como son el de la criptografía cuántica y poscuántica, la investigación del cibercrimen y tecnologías para crear confianza y ciberseguridad en la inteligencia artificial. De las conclusiones del estudio se han extraído las Figuras 2 y 3, que reflejan el número, distribución y prioridades de investigación en la UE.

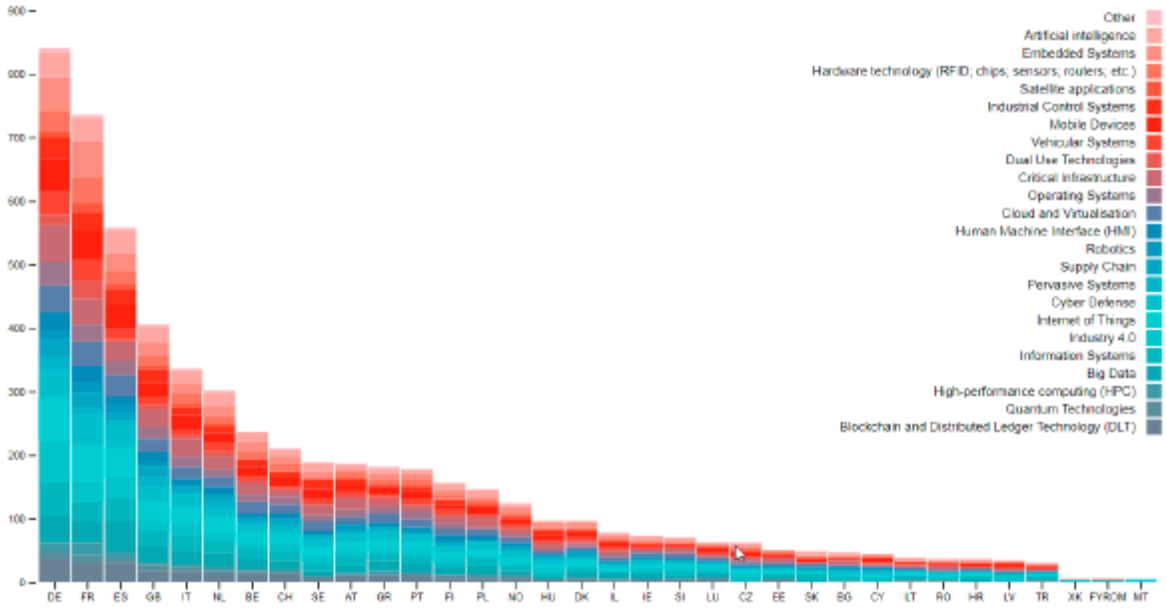
[6] "European Cybersecurity Centres of Expertise Map – Definition and Taxonomy", JRC Technical Reports, 2018, p. 26. http://publications.jrc.ec.europa.eu/repository/bitstream/JRC111441/taxonomy_final.pdf.

Figura 2. Distribución geográfica y número de participantes



Fuente: “Cybersecurity Competence Survey”, JRC, p. 12, http://publications.jrc.ec.europa.eu/repository/bitstream/JRC111211/survey_report_1.6-final.pdf.

Figura 3. Aplicaciones y tecnologías de ciberseguridad por país



Fuente: "Cybersecurity Competence Survey", JRC, p. 27, http://publications.jrc.ec.europa.eu/repository/bitstream/JRC111211/survey_report_1.6-final.pdf.

Durante 2018, la Comisión Europea lanzó una fase piloto para la creación de una red de centros de ciberseguridad europeos a cargo del Programa Horizonte 2020.[7] Esta fase comprendía tres programas piloto para que, por un lado, escalasen la investigación existente en ciberseguridad con soluciones cercanas al mercado y, por otro lado, pusiesen en marcha y probasen una red de competencia en ciberseguridad con un *hub* central de competencia. Finalmente fueron aprobados cuatro proyectos piloto en lugar de tres (Concordia, Sparta, CyberSecurity4Europe y ECHO). Estos pilotos han iniciado su ejecución en 2019 y persiguen aunar a la comunidad investigadora de cada uno de los proyectos en la realización de hojas de ruta sobre ciberseguridad, certificación, entrenamiento, educación y *cyber ranges*.[8] La Comisión está poniendo especial énfasis en la coordinación entre los cuatro pilotos como un medio de avanzar hacia la futura red de centros. Los resultados de los pilotos, junto con la participación de la Organización Europea de Ciberseguridad (ECSO) y los Estados miembros, ayudarán a sentar la base para la construcción de la nueva estructura de la red de centros de competencia en ciberseguridad y plantear los asuntos sobre los que Europa deba investigar.

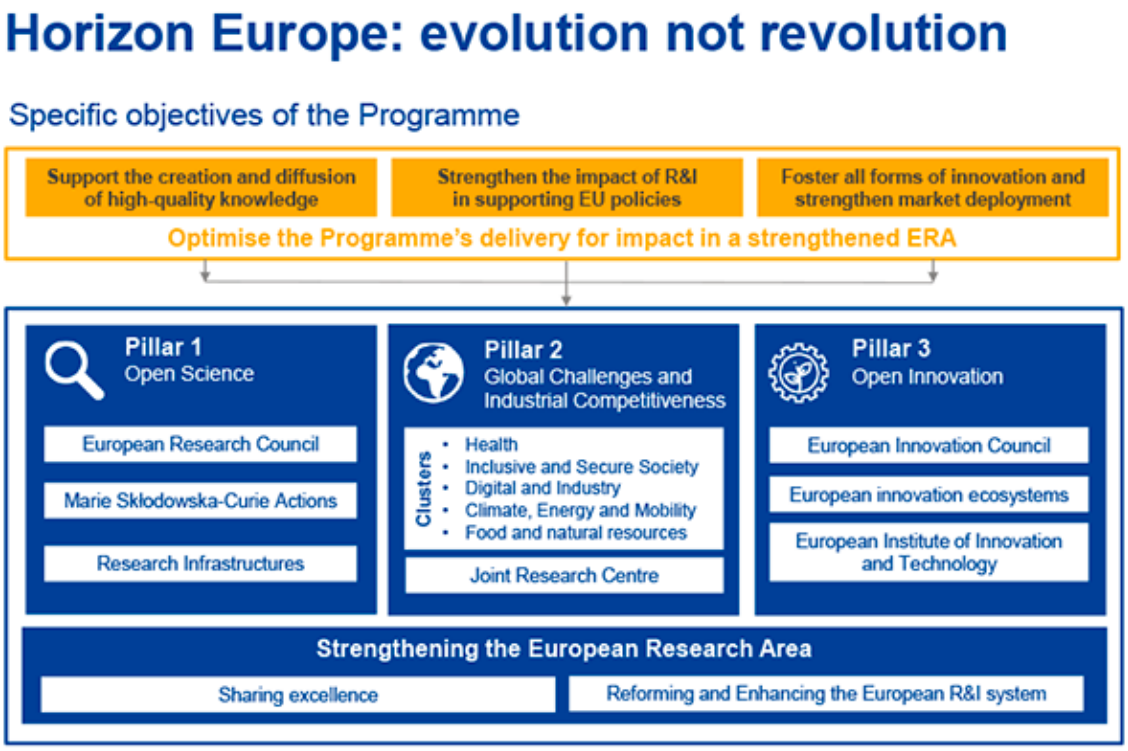
[7] Horizonte 2020, "Establishing and operating a pilot for a cybersecurity competence network to develop and implement a common cybersecurity research & innovation roadmap", marzo de 2018, https://ecs-org.eu/calls-for-proposals/66.

[8] Un cyber range es una plataforma virtual que permite simular entornos operativos reales —estáticos o desplegables, clasificados o no clasificados— para la formación y el entrenamiento —individual o colectivo— de profesionales, así como la experimentación, el testeo y la validación de nuevos conceptos, tecnologías, técnicas y tácticas de ciberseguridad y ciberdefensa. Enrique Fojón Chamorro, "Cyber Range: una capacidad estratégica", Blog RIE, 12 de diciembre de 2016, https://blog.realinstitutoelcano.org/cyber-range-una-capacidad-estrategica/.

(cont.)

Dentro del próximo Marco de Financiación Plurianual de la Comisión Europea (2021-2027), el futuro programa de I+D europea se denomina Horizon Europe y cuenta con una propuesta de presupuesto de 100.000 millones de euros, pendiente de un acuerdo sobre el siguiente presupuesto total a largo plazo de la Unión Europea.[9] La I+D de Horizon Europe se articulará en función de misiones que permitan ligar la I+D a las necesidades de la sociedad y los ciudadanos de forma visible y con impacto. La ciberseguridad aparece mencionada explícitamente en el reto "Sociedad segura e inclusiva", aunque estará presente transversalmente en el resto de los retos.

Figura 4. Objetivos y pilares del programa Horizon Europe de la UE



Fuente: Presentación de la Comisión Europea, https://ec.europa.eu/info/sites/info/files/horizon-europe-presentation_2018_en.pdf.[10]

Para complementar el programa Horizon Europe, la Comisión Europea ha propuesto la creación del primer programa Digital Europe, con un presupuesto de 9.200 millones de euros para alinear el próximo presupuesto de la UE para el periodo 2021-2027 con los crecientes retos digitales.[11] Digital Europe se centrará en cinco áreas: ciberseguridad, inteligencia artificial, supercomputación, competencias digitales y fomento de la utilización de tecnologías digitales por parte de la economía y sociedad. Estas cinco áreas no son estancas, sino que presentan múltiples interacciones y puede considerarse

[9] Comisión Europea, "Horizon Europe, the next research and innovation framework Programme", 20 de marzo de 2019, https://ec.europa.eu/info/designing-next-research-and-innovation-framework-programme/what-shapes-next-framework-programme_en.

[10] Presentación de la Comisión Europea, "Commission Proposal for HORIZON EUROPE", 25 de junio de 2018, https://ec.europa.eu/info/sites/info/files/horizon-europe-presentation_2018_en.pdf.

[11] Comisión Europea, "Digital Europe", 6 de junio de 2018, https://www.digitaleurope.org/.

la ciberseguridad de forma transversal a todas ellas. Por ejemplo, la inteligencia artificial se utiliza en ciberseguridad, pero al mismo tiempo hay que garantizar la ciberseguridad de la inteligencia artificial; la supercomputación puede utilizarse para la ciberseguridad y, al mismo tiempo, hay que asegurar su ciberseguridad, por no hablar de desarrollar competencias digitales en ciberseguridad.

En septiembre de 2018 y ya habiéndose lanzado la fase piloto para la creación de una red de centros de ciberseguridad, la Comisión Europea realizó una propuesta para una regulación que permitiese crear un Centro Europeo de Competencia en Ciberseguridad Industrial, de Tecnología e Investigación y una Red de Centros de Coordinación Nacionales.[12] El Centro de Competencia sería el principal organismo para gestionar los recursos financieros europeos dedicados a la investigación en ciberseguridad de los futuros programas de Horizon Europe y Digital Europe.

En este sentido, cabe mencionar que España fue pionera en detectar la necesidad de la creación de una red de centros de ciberseguridad, ya que en 2015 el Instituto Nacional de Ciberseguridad (Incibe) publicó un estudio en el que detectó, tras analizar el contexto y las dinámicas de la investigación en ciberseguridad en España, la necesidad de la creación de una red,[13] que, posteriormente, se materializó en la creación de la Red de Centros de Excelencia Nacional de Investigación en Ciberseguridad (Renic). Esta red abierta está constituida por 16 socios fundadores y tiene como objetivo ser una asociación sectorial nacional que represente al ecosistema investigador nacional en ciberseguridad. Cabe mencionar que el Incibe también publicó en enero de 2017 el "Catálogo y mapa de conocimiento de la I+D+i en ciberseguridad".[14]

En relación con las líneas de investigación en I+D, el Grupo de Trabajo 6 de la ECSO tiene como objetivo definir la hoja de ruta de la I+D en ciberseguridad para fortalecer y construir un ecosistema europeo resiliente, diseñando y desarrollando tecnologías de confianza que aborden los retos de digitalización de la sociedad y sectores industriales para promover la autonomía digital europea. En la Agenda Estratégica de Investigación y Desarrollo (SRIA) publicada por la ECSO en junio de 2017, y como aportación al Programa de Trabajo 2018-2020 de H2020, se incluían cuatro tipos de proyectos:

- Ecosistema: proyectos con componente sociotécnico para el desarrollo de ecosistemas que favorezcan una mejor implementación y utilización de soluciones innovadoras de ciberseguridad, contemplando ámbitos como la simulación, educación, entrenamiento, certificación y estandarización, *cyber ranges* y un apoyo a las pymes.

[12] "Proposal for a regulation establishing the European Cybersecurity Industrial Technological and Research Centre and the network of National Coordination Centres", 12 de septiembre de 2018, https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-establishing-european-cybersecurity-industrial-technology-and-research.

[13] Incibe, "Estudio de viabilidad, oportunidad y diseño de una red de centros de excelencia I+D+i en ciberseguridad", mayo de 2015, https://www.incibe-cert.es/sites/default/files/contenidos/estudios/doc/informe_resumen_estudio_red_centros_excelencia.pdf.

[14] Incibe, "Catálogo y Mapa de Conocimiento de la I+D+i en Ciberseguridad", enero de 2017, https://www.incibe.es/sites/default/files/paginas/red-excelencia/estudios-caracterizacion/201701_catalogo.pdf.

- Demostración: proyectos de demostración de soluciones existentes en dominios verticales concretos, como industria 4.0, energía, *smart buildings* y *smart cities*, transporte y salud.

- Infraestructuras transversales: proyectos que permitan integrar tecnologías transversales a varios dominios en ámbitos como el del cumplimiento de la seguridad y la gestión del riesgo, prevención y protección, compartición de información, analítica de seguridad, detección y gestión de amenazas.

- Componentes tecnológicos: proyectos para el desarrollo de tecnología de ciberseguridad que permita eliminar las barreras a la confianza de aplicaciones y servicios guiados por datos manteniendo una infraestructura ICT segura y de confianza.

Actualmente, la ECSO está trabajando sobre prioridades potenciales para Horizon Europe y Digital Europe y ha identificado como tecnologías básicas y disruptivas con impacto en la ciberseguridad las siguientes:

- Inteligencia artificial y ciencias cognitivas.
- Robots y cíborgs.
- *Blockchain* y tecnologías de registro distribuidas.
- Gemelos digitales.
- Internet de las cosas y sistemas ciberfísicos.
- Criptografía cuántica y poscuántica.
- Biotecnologías y mejoramiento humano.

Por su parte, Enisa también ha propuesto una serie de recomendaciones sobre prioridades para la I+D en ciberseguridad con la intención de convertir Europa en un líder mundial en ciberseguridad para 2025, asegurando la confianza y la protección de ciudadanos, consumidores y empresas.[15] Entre las prioridades se mencionan:

- Reto social: La utilización de la tecnología provoca cambios sociales y puede llevar riesgos asociados en términos de ciberseguridad de los que la sociedad debe ser consciente. Vivimos en un mundo híbrido y es necesario aprender a vivir en el mundo digital, lo mismo que hemos aprendido a vivir en el mundo real.

- Reto educativo: Partiendo de la base de la carencia de expertos en ciberseguridad, se hace necesario crear capacidades de ciberseguridad adaptando la educación en los diferentes niveles para reducir dicho desfase.

[15] Enisa, “Analysis if the European R&D priorities in cybersecurity”, 19 de diciembre de 2018, https://www.enisa.europa.eu/publications/analysis-of-the-european-r-d-priorities-in-cybersecurity.

- Amenazas existenciales: Amenazas que si se convierten en realidad tienen el potencial de dañar en diferente medida la parte de la sociedad, industria o negocio que sea vea afectada:

    - La inteligencia artificial genera nuevas oportunidades y nuevos riesgos (la IA forma parte de la solución en ciberseguridad, pero también del problema) ¿Podemos confiar en que los datos o los algoritmos no hayan sido manipulados y forzados en la toma de una determinada decisión?

    - Las tecnologías cuánticas pueden utilizarse tanto en ataques hacia los métodos de protección criptográficos actuales como en el desarrollo de nuevos modelos computacionales más seguros.

    - La complejidad de las interconexiones puede conducir a fallos en cascada de múltiples sistemas a lo largo de la cadena de suministro.

    - Los cibercriminales van a ser pioneros (*early adopters*) en la utilización de medios digitales y nuevas tecnologías, por lo que se debe trabajar en preservar las identidades digitales y activos de valor.

    - Las amenazas a la privacidad aumentan con el *big data* y las inferencias asociadas que pueden llevarse a cabo por lo que es necesario identificar fórmulas para preservarla.

Conclusión

El estado de la I+D en la ciberseguridad europea que se ha mostrado confirma la necesidad de impulsarla de forma más decidida para paliar su fragmentación, aumentar su presencia entre los jugadores mundiales e incrementar la inversión para evitar quedarse en una situación delicada a la hora de defenderse de las ciberamenazas o de competir con países como Estados Unidos o China. En este contexto, es necesario trabajar en Europa tanto en aspectos organizativos que permitan crear masas críticas investigadoras de relevancia e interoperando infraestructuras de laboratorios para no duplicar esfuerzos ya realizados como dotando a las diferentes iniciativas planteadas de presupuestos apropiados a la dimensión y relevancia de la ciberseguridad, con apuestas que se acerquen a las que se están realizando en otras partes del mundo.

Por otro lado, no debemos olvidar que cualquier proyecto que implique conectividad a la red —que va prácticamente implícito en cualquier proyecto de digitalización con independencia del sector— puede enfrentarse a un problema de ciberseguridad, por lo que debe tener en cuenta aspectos de seguridad y privacidad como elementos esenciales desde la concepción del proyecto si queremos avanzar en la seguridad y privacidad desde el diseño y no intentando poner parches de ciberseguridad, como hasta ahora.

Dado que cualquier nueva tecnología puede utilizarse desde un punto de vista ético para el fin para el que fue desarrollado o para otros fines no éticos y dado que en el ámbito de la ciberseguridad los ciberatacantes están siendo *early adopters* con un uso

evidentemente no ético de tecnologías como la inteligencia artificial, la internet de las cosas y la computación cuántica, debemos realizar, desde el punto de vista de la I+D+i y en coordinación con la industria, los esfuerzos investigadores necesarios en nuevas tecnologías para hacerles frente.

Finalmente, a pesar de que España ocupe actualmente lugares de privilegio en la I+D europea en ciberseguridad junto con países como Estonia, Francia o el Reino Unido, entre otros, y dado el elevado número de entidades trabajando en la I+D+i, deben llevarse a cabo las acciones necesarias para mantenernos en posiciones relevantes en un ámbito tan tecnológico y con tanta necesidad de I+D+i como es el de la ciberseguridad.