La industria de la ciberseguridad: ¡España y la UE deben ponerse las pilas!

Félix Arteaga | Investigador principal de Seguridad y Defensa, y coordinador del Grupo de Trabajo sobre Ciberpolítica del Real Instituto Elcano

La **ciberseguridad** no sólo presenta riesgos para la seguridad nacional; también ofrece oportunidades industriales y tecnológicas para la seguridad económica, pero, para aprovecharlas, España y la UE deben *ponerse las pilas* si no quieren seguir dependiendo de tecnología y productos de ciberseguridad de terceros. Esta obviedad se ha reconocido tarde en la UE y sigue pendiente todavía de reconocimiento en España, pero las cosas podrían estar cambiando si ambas se ponen manos a la obra y desarrollan sus respectivas bases industriales y tecnológicas de ciberseguridad.

> "España y la UE deben *ponerse las pilas* si no quieren seguir dependiendo de tecnología y productos de ciberseguridad de terceros".

La UE y sus Estados miembros han dado preferencia a la seguridad frente al negocio en sus agendas de ciberseguridad y han desarrollado estrategias, organizaciones y planes de respuesta. Las últimas medidas adoptadas en 2017 por la UE –el denominado el denominado ***cybersecurity package*** o 'paquete de ciberseguridad'– siguen la prioridad de proteger los activos digitales, reforzar la Agencia de Seguridad de las Redes y de la Información de la Unión Europea (ENISA, en sus siglas en inglés) y crear una infraestructura y procedimientos de certificación, así como un plan director para gestionar los incidentes y crisis de ciberseguridad a gran escala, incluido el relanzamiento del Plan de Ciberseguridad de la UE, ya analizado en el *CIBER Elcano* de diciembre de 2017.

Las medidas adoptadas eran una condición necesaria –pero no suficiente– para alcanzar el objetivo estratégico fijado en septiembre de 2017 por los jefes de Estado y de Gobierno europeos en la Cumbre Digital de Tallin de que la UE se convirtiera en "un líder mundial en ciberseguridad para 2025"[1]. Para ser suficiente, la UE y sus Estados miembros debían contar con una base industrial y tecnológica de ciberseguridad que les permitiera reducir su ciberdependencia tecnológica. El enfoque comenzó a cambiar en 2018 cuando, en su discurso sobre el estado de la Unión, el presidente de la Comisión reconoció la necesidad de "desarrollar y mantener las capacidades tecnológicas e industriales necesarias para asegurar de forma autónoma su economía digital", para lo que era necesario poner en común recursos y capacidades si se quería liderar la siguiente generación de tecnologías digitales y de ciberseguridad.

[1] A la Cumbre Digital de Tallin, celebrada el 29 de septiembre de 2017, no asistió el presidente del Gobierno español, Mariano Rajoy, debido a la proximidad de los sucesos en Cataluña.

Según la Comisión, los europeos son importadores netos de productos y soluciones de ciberseguridad, un mercado de 600.000 millones de euros que crece, aproximadamente, a un ritmo anual del 17%. Para acceder a ese mercado mundial, es preciso disponer de una base tecnológica e industrial que traduzca el conocimiento disponible en tecnologías aplicables y soluciones industriales comercializables que abarquen, en lo posible, la totalidad de la cadena de valor de la ciberseguridad. Sin embargo, la UE no ha movilizado todo su potencial investigador, que sigue disperso y sin orientación estratégica para alcanzar la deseable economía de escala, fragmentado en sectores que apenas comparten sinergias entre ellos (energía, espacio, civil, militar, seguridad, defensa y otros) ni con tecnologías polivalentes (inteligencia artificial, cadena de bloques, informática cuántica, automatización) y que, además, carecen de fuentes de financiación suficientes y estables.

Como resultado, la base industrial y tecnológica de la UE presenta las siguientes carencias principales:

- Las industrias que consumen ciberseguridad no cooperan suficientemente con las que la producen.
- Los sectores industriales y los de investigación no cooperan eficazmente entre ni dentro de ellos.
- Lo mismo ocurre entre los sectores dedicados a la ciberseguridad y a la ciberdefensa.
- Tampoco los Estados colaboran eficazmente entre ellos para desarrollar sus capacidades, programas e infraestructuras.

Para intentar remediar esta situación, la Comisión Europea presentó en junio de 2018 el primer programa Europa Digital para dedicar a la ciberseguridad 2.000 millones de euros de los 9.200 millones de los que dispondrá el programa entre 2021 y 2027 cuando se apruebe el próximo marco financiero plurianual de la UE. A estos fondos hay que añadir los que dedique el próximo Programa Marco de Investigación e Innovación Horizonte Europa a la investigación e innovación en materia de ciberseguridad, tecnologías duales y los que dedique el Fondo Europeo de Defensa a la ciberdefensa.

A la financiación anterior hay que añadir las iniciativas de cooperación entre los distintos sectores públicos y privados europeos para paliar las carencias señaladas. Entre ellas, cabe destacar la de crear una Red de Centros Nacionales de Coordinación (Network of Cybersecurity Competence Centres) y un Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad (European Cybersecurity Industrial, Technology and Research Competence Centre) para coordinar y financiar esa red. Estas iniciativas tratan de sacar el máximo partido posible al ecosistema industrial, tecnológico y de innovación disponible, que cuenta con unos 665 miembros identificados en marzo de 2018 en una encuesta de opinión para un informe técnico de la Comisión y del Centro Común de Investigación.

Barriendo para casa

No se puede decir que España estuviera ajena a esta situación de dependencia tecnológica y precariedad industrial ni que no se haya intentado reaccionar para remediarlo. El estado de necesidad se ha denunciado desde el sector privado y desde el sector público. En su estudio de mayo de 2015 sobre la "Viabilidad, oportunidad y diseño de una red de centros de excelencia", el Instituto Nacional de Ciberseguridad (INCIBE) concluyó que España:

- no tenía un claro posicionamiento en I+D+i a nivel internacional ni figuraba entre los más destacados dentro de las áreas científico-tecnológicas asociadas a la ciberseguridad;

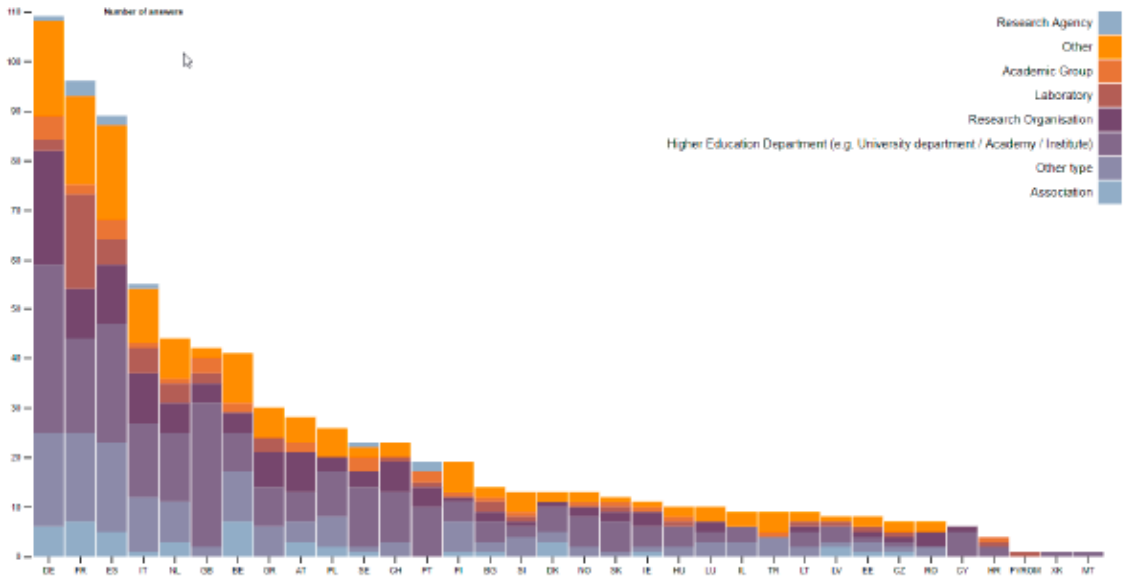
- estaba muy por detrás de líderes mundiales (Estados Unidos, Israel, Reino Unido) y europeos (Francia, Alemania y Países Bajos), sin políticas y focos de investigación claros ni inversiones en I+D+i a medio y largo plazo para madurar y obtener retornos, y que

- las carencias se asociaban a la debilidad del Sistema de Ciencia y Tecnología, a la restricción del crédito presupuestario en I+D+i y a factores culturales (aversión al riesgo, baja cultura colaborativa).

Como soluciones, el estudio del INCIBE propuso "establecer un foco o estrategia clara por parte del Estado sobre las prioridades a partir de las cuales articular la I+D+i, revertir la tendencia hacia la escasez de presupuestos y fomentar un mercado interno más amplio a través de una mayor tracción en la demanda de soluciones de ciberseguridad, principalmente por parte de las Administraciones Públicas y el Estado". También propuso crear la actual Red de Excelencia Nacional de Investigación en Ciberseguridad (RENIC), en sintonía con lo que ahora propone la Comisión y que se encuentra en fase de consolidación.

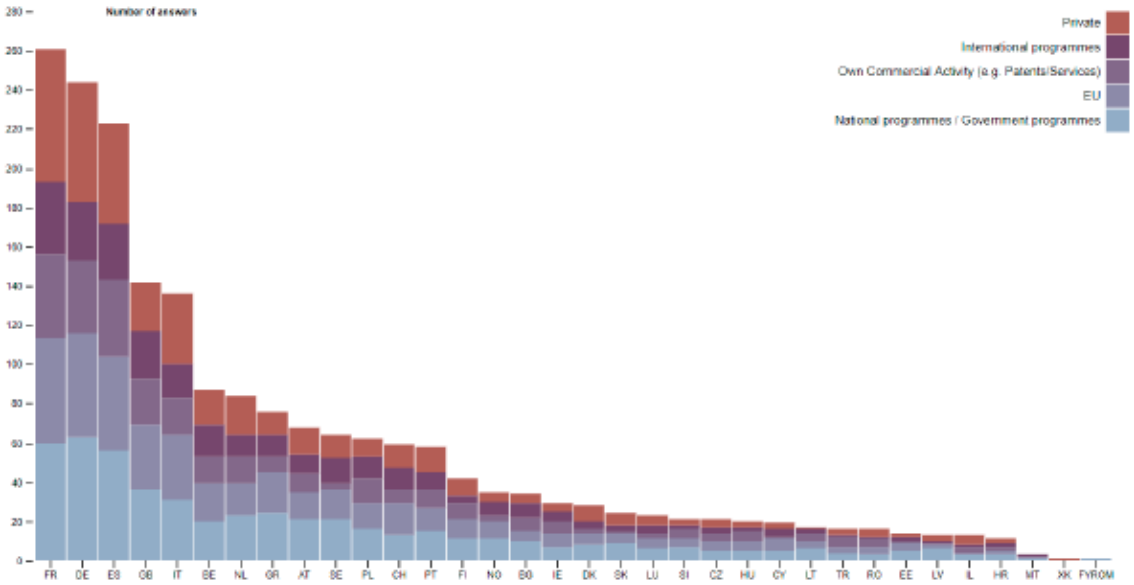
Muchos de los miembros consultados por INCIBE en 2015 (71 sobre un total de 665 participantes) participaron en la encuesta posterior del mencionado informe de la Comisión y del Centro Común de Investigación de 2018. El nuevo informe refleja una posición de ventaja cuantitativa del ecosistema español, no muy alejada en participantes de países como Alemania (90) y Francia (78) y por encima de Italia (44) o Reino Unido (40). En el mismo sentido, las Figuras 1 y 2 muestran una variedad de actores y de fuentes de financiación, respectivamente, muy similares a los países del entorno europeo.

Figura 1. Distribución de los encuestados según la modalidad de organización



Fuente: Cybersecurity Competence Survey 2018, European Cybersecurity Centre of Expertise, http://publications.jrc.ec.europa.eu/repository/bitstream/JRC111211/survey_report_1.6-final.pdf.

Figura 2. Distribución de los encuestados según la modalidad de financiación



Fuente: Cybersecurity Competence Survey 2018, European Cybersecurity Centre of Expertise, http://publications.jrc.ec.europa.eu/repository/bitstream/JRC111211/survey_report_1.6-final.pdf.

De la similitud entre las comparaciones anteriores y otras del informe se deduce que el ecosistema español dispone de una buena situación de partida para superar la ciberdependencia tecnológica e industrial de España, pero que no acaba de despegar por la falta endémica de liderazgo, organización y recursos. ¿Qué porcentaje del mercado mundial de la ciberseguridad aspira a ocupar España? ¿Y qué porcentaje de los fondos europeos de I+D+i para ciberseguridad? ¿Cuántos fondos está dispuesta a invertir de su presupuesto nacional para conseguir los anteriores? ¿Cómo piensa potenciar su ecosistema industrial y tecnológico? ¿Y quién será el responsable de hacerlo?

La Estrategia de Ciberseguridad Nacional de 2013 no logró pasar de los buenos deseos de fomentar la I+D+i en su línea de acción 6 y traducirla en acciones y presupuestos concretos. Lo aprendido en Europa y en España nos obliga a tomarnos en serio el desarrollo y sostenimiento de nuestras bases industriales y tecnológicas de la ciberseguridad si no queremos, primero, perder una oportunidad de negocio y, segundo, debilitar nuestra economía digital. La revisión de la Estrategia de Ciberseguridad Nacional, en curso, ofrece una oportunidad para desbloquear las reformas estructurales pendientes, pero lo difícil no es realizar el diagnóstico, sino aplicar los remedios. O se aprovechan ahora las iniciativas europeas o dejamos que otros lo hagan, así que lo dicho: ¡a ponerse las pilas!.

“Lo aprendido en Europa y en España nos obliga a tomarnos en serio el desarrollo y sostenimiento de nuestras bases industriales y tecnológicas de la ciberseguridad”.