Capítulo séptimo

I+D+i y ciberseguridad: análisis de una relación de interdependencia

Aurelio Hinarejos Rojo
Capitán del Cuerpo de Ingenieros Politécnicos del Ejército DGAM/SDGPLATIN

José de la Peña Muñoz
Director de la Revista SIC

Resumen

Los autores analizan la relación de interdependencia entre la I+D+i y la ciberseguridad, reivindicando el alineamiento de lo expresado en las Estrategias Españolas de Ciencia y Tecnología e Innovación (EECTI) y de Ciberseguridad Nacional (ECSN). Al tiempo exponen algunos de los frentes de I+D+i proyectados para sumergirse posteriormente en un análisis genérico que permite hacerse una idea razonable del esfuerzo internacional en I+D+i. En el capítulo se brinda también una visión de la colaboración público-privada y se exponen iniciativas significativas de alcance internacional y supranacional para finalizar con una aportación en la que se mencionan materias prometedoras para su tratamiento en los ecosistemas de CPP en I+D+i sobre ciberseguridad.

Palabras clave

investigación y desarrollo, innovación, ciberseguridad, ciberdefensa militar, resiliencia, independencia tecnológica, autonomía estratégica, ecosistemas de colaboración público-privada.

Abstract

The authors analyse the relationship of interdependence between research, development and innovation, and cybersecurity, while claiming the convergence of Spanish strategies for Science, Technology and Innovation (EECTI) and National Cyber Security (ECSN). At the same time, some of the hottest R&D&I areas are exposed just before delving into a generic analysis of the subject matter, which allows a reasonable picture of the international effort into cyber R&D&I to be provided. In addition, a perspective on public-private partnership in this realm, as well as significant initiatives at supra- and international level are exposed. Finally, an overview of promising matters on public-private partnership ecosystems focused on R&D&I on cybersecurity is also depicted.

Keywords

Research and development, innovation, cybersecurity, military cyberdefence, resilience, technological independence, strategic autonomy, public-private partnership ecosystems

Introducción

«*Politics is about crafting and picking alternatives. Politics matters, therefore, only if choices can be made and if making them has real consequences*».

—Dan Breznitz—

A principios del mes de enero de 2016, el Departamento de Seguridad Interior de los Estados Unidos (*DHS*, *Department of Homeland Security*) informaba acerca de la manipulación ilícita de vehículos aéreos no tripulados (*UAV*) del servicio de protección de fronteras[1]. Por medio del envío de señales GPS falsas que aparentaban ser genuinamente procedentes de los satélites NAVSTAR, lo que se conoce como *GPS spoofing*, narcotraficantes mejicanos lograban manipular la misión de los drones a fin de poder cruzar libremente la frontera entre Estados Unidos y México y así conseguir libertad de acción en su actividad criminal. Hoy por hoy no es posible acabar con esta vulnerabilidad, ya que la incorporación de un módulo anti-*spoofing*, tal como se hace en los sistemas militares, comprometería la autonomía de vuelo del *UAV*, por no mencionar el impacto económico que ello supondría. Sin embargo, se espera que la innovación tecnológica posibilite en el futuro inmediato la implantación de este tipo de módulos de forma asequible y con unas características físicas que no impidan su eficacia operativa. Este es solo un ejemplo, entre muchos otros que podrían mencionarse, de la confianza existente en que las actividades de investigación y desarrollo en curso conduzcan a innovaciones que permitan una mejora significativa en las condiciones de ciberseguridad actuales.

Más recientemente, el 16 de agosto de 2016, el diario *The New York Times* se hacía eco de la publicación en Internet por parte del grupo autodenominado *The Shadow Brokers*, de fragmentos de código fuente de *software* clasificado como «*Top secret*» aparentemente proveniente de la *National Security Agency* (*NSA*) de los Estados Unidos y que supuestamente habría formado parte del arsenal de ciberarmas atribuido a esta agencia[2]. Los *Shadow Brokers* afirmaban no obstante que el *software* pertenecía al *Equation Group*, nombre en clave con que la firma rusa Kaspersky Labs se refiere a la *NSA*. De hecho, Kaspersky Labs había identificado en el ciberespacio un grupo caracterizado por la complejidad de sus actividades y su apego al empleo de criptografía fuerte, imputándoles el desarrollo de *malware* como STUXNET[3]. Con

[1] Cimpanu, Catalin. «Drug Cartels are Hacking US Border Patrol Drones», Softpedia, Jan 1 2016, http://news.softpedia.com/news/drug-cartels-are-hacking-us-border-patrol-drones-498312.shtml

[2] Sanger, David E. «"Shadow Brokers" Leak Raises Alarming Question: Was the N.S.A. Hacked?», The New York Times, http://www.nytimes.com/2016/08/17/us/shadow-brokers-leak-raises-alarming-question-was-the-nsa-hacked.html?_r=0. Fecha de la consulta: 20 de agosto de 2016.

[3] GReAT, «A Fanny Equation: "I am your father", Stuxnet», Kaspersky Labs, February 17 2015, https://securelist.com/blog/research/68787/a-fanny-equation-i-am-your-father-stuxnet/. Fecha de la consulta: 24 de septiembre de 2016.

su anuncio, los *Shadow Brokers* aseguraban haber logrado golpear al hasta entonces invulnerable *Equation Group*. Lo que es importante resaltar en este contexto es que, recíprocamente, en el lado de las amenazas, se puede entrever que las más sofisticadas proceden de décadas de investigación y desarrollo de ciberarsenales por parte de actores supuestamente vinculados a entidades estatales.

Visto que, como ha venido ocurriendo a lo largo de miles de años de historia militar, el I+D está detrás de cada innovación, tanto en la vertiente ofensiva como en la defensiva, convendría, antes de entrar en materia, establecer una mínima clarificación terminológica con la intención de hacer más inteligible lo que más adelante se expondrá en este capítulo.

Por un lado, existe una frecuente confusión en la literatura especializada con los conceptos de ciberseguridad y ciberdefensa, cuestión abordada por Feliú[4]. En el ámbito de este capítulo sostendremos que la misión de la ciberdefensa es garantizar la ciberseguridad[5]. Igualmente, procede también diferenciar entre investigación y desarrollo (I+D) e innovación (i). Mientras que el I+D es el trabajo creativo emprendido sistemáticamente para incrementar el conocimiento científico, así como para utilizar este conocimiento con el fin de proyectar aplicaciones prácticas del mismo, la innovación tecnológica será el resultado de la transformación de una idea en un producto nuevo o mejorado que es introducido en un mercado y diseminado de manera que produzca un efecto en la sociedad o bien de un servicio nuevo o mejorado que ha sido insertado dentro de un proceso de producción[6]. De aquí que el objetivo del I+D+i en ciberdefensa será disponer de una capacidad defensiva avanzada que permita establecer de manera eficaz en cuanto a su coste las medidas de prevención, disuasión, protección y reacción necesarias para alcanzar el estado de ciberseguridad deseado.

Entendido que un proceso de I+D+i eficaz es necesario para dotarnos de mayor ciberseguridad, veremos que no es suficiente. Hasta la década de los ochenta del siglo pasado la mayoría de los avances tecnológicos procedían de la industria militar y aeroespacial, generosamente financiada con dinero público (en cierta medida como subproducto del complejo militar-industrial

[4] Feliú Ortega, Luis. «La ciberseguridad y la ciberdefensa». En: *El ciberespacio: nuevo escenario de confrontación*. Monografías del CESEDEN 126. CESEDEN, Madrid, febrero de 2012.

[5] En este trabajo se enfocará la seguridad en el dominio ciberespacial con una doble perspectiva: por un lado, estática, en la que la ciberseguridad es un estado a alcanzar y mantener; y, por otro lado, dinámica, en la que la ciberdefensa, activa o pasiva, será un proceso conducente al estado de ciberseguridad deseado. En síntesis, la ciberdefensa será el medio y la ciberseguridad el fin.

[6] Organisation for Economic Cooperation and Development. *Main definitions and conventions for the measurements of Research and Experimental Development (R&D). A summary of the Frascati Manual*. 1993. París: 1994, p. 4.

del que advirtió el presidente Eisenhower)[7], pero hoy día las innovaciones proceden mayoritariamente de la industria civil. Es por ello que las Administraciones Públicas se ven en cierta forma obligadas a llegar a acuerdos con operadores económicos no institucionales con el fin de acceder a los beneficios de una tecnología novedosa sin asumir los riesgos derivados de su investigación y desarrollo. Es decir, en este contexto, toma forma la colaboración público-privada (CPP) en I+D+i, aunque con el matiz de que será más exitosa en materia de innovación que en el puro aspecto de la investigación y desarrollo. Si bien lo descrito es aplicable a múltiples tecnologías, será la colaboración público-privada, por sus características específicas y que veremos en este capítulo, especialmente indicada en el caso del I+D+i en ciberseguridad. En este sentido, la creación en los Estados Unidos de *Defense Innovation Unit Experiment* (*DIUx*) supone una apuesta por la colaboración público-privada como medio para mantener el liderazgo tecnológico del Departamento de Defensa norteamericano en el ciberespacio, y constituye un nítido ejemplo de las iniciativas que en esta dirección se están impulsando en otros países[8].

Por otro lado, el asunto que se plantea no es trivial. Nos movemos en un espacio tridimensional en el que los ejes son el I+D+i, el nivel de ciberseguridad y el grado de colaboración público-privada, siendo necesario encontrar la zona de equilibrio donde se produce la sinergia suficiente como para sostener el sistema, produciendo al mismo tiempo beneficios para las partes.

Por lo que respecta a la dimensión de la ciberseguridad, partimos de la base de que esta presenta tres aspectos: el personal que la gestiona, los procesos que permiten garantizar su eficacia y los productos (tecnología) que soportan a estos últimos mejorando la eficiencia[9]. En cuanto a la colaboración público-privada, claramente existirá una diferencia de enfoque por parte del sector privado, que aspira a un legítimo retorno de inversión cuanto más generoso mejor, y un sector público que ha de atender en primer lugar a colmar las necesidades de seguridad y defensa de la población. En la práctica, ocurre que la colaboración público-privada no es una panacea y suscita suspicacias entre las partes. Existen numerosas ventajas y desventajas en su puesta en práctica. ¿Qué espera el sector público de una colaboración en I+D+i en ciberseguridad (transferencia de conocimien-

[7] Discurso del mensaje de despedida del presidente norteamericano Dwight Eisenhower, donde divulgó el concepto de «complejo militar-industrial», 17 de enero de 1961. Véase también: «The Military-Industrial Complex: The Farewell Address of President Eisenhower», Basements Publications, 2006.

[8] Creada en abril de 2015 por el secretario de Estado Ashton Carter, la *DIUx* es fruto de la *Defense Innovation Initiative*, cuyo objetivo es la generación de nuevas capacidades militares, así como del *Long Range Research and Development Plan*. Su finalidad es apoyar las propuestas tecnológicas de la industria civil estadounidense para madurarlas e integrarlas en el armamento y material, incluido el destinado a operaciones en el ciberespacio.

[9] Informe mensual de ciberseguridad CIBERelcano n.º 13, Real Instituto Elcano de Estudios Internacionales y Estratégicos, Madrid, abril de 2016, p. 12.

tos, acceso a tecnología novedosa, etcétera? Y qué puede esperar el sector privado de una cooperación con el público (financiación, ventajas fiscales, etcétera). ¿En qué aspectos debería ceder el sector público (relajación de las exigencias en materia de cesión de derechos de propiedad intelectual o flexibilidad en las relaciones contractuales) y en qué otros el sector privado (apuesta por el largo plazo en lugar de beneficios a corto)? Es necesario investigar dónde se encuentran los intereses comunes y dónde los particulares, de manera que el esfuerzo se centre en potenciar precisamente el logro de los intereses comunes. Cabe preguntarse también si existen casos documentados donde esa colaboración en I+D+i haya dado o esté dando resultados positivos.

Para abordar sistemáticamente el tema analizaremos progresivamente los diferentes planos definidos por cada pareja de ejes de este espacio: CPP y ciberseguridad, I+D+i y ciberseguridad y CPP e I+D+i. No nos detendremos mucho en el primer plano de la colaboración público-privada en ciberseguridad por ser el ámbito más general y cuyos pormenores se hallan exhaustivamente tratados en otros capítulos de este volumen. En cuanto al segundo plano, constituido por la I+D+i y la ciberseguridad, explicaremos someramente la diferencia entre investigación y desarrollo, y la innovación propiamente dicha, que será en lo que estemos más interesados en ciberseguridad. Presentaremos la necesidad y justificación de una estrategia de I+D+i en ciberseguridad plenamente en línea con la Estrategia Española de Ciencia y Tecnología y de Innovación y con la Estrategia de Tecnología e Innovación de la Defensa, por una parte, y con la Estrategia de Ciberseguridad Nacional, por otra. También repasaremos los retos actuales planteados al I+D en ciberseguridad, tales como el logro de la ansiada resiliencia de los sistemas en lugar de limitarnos a la mera protección de estos, avanzar en la capacidad de análisis forense para, entre otras cosas, lograr la atribución de los ciberataques, la gestión de identidades, innovación en productos, procesos y personas, etcétera.

El tercer plano, formado por la confluencia entre la colaboración público-privada y la I+D+i, en términos generales nos lleva a intentar responder las cuestiones antes formuladas. El papel general del Estado en los procesos de innovación ha sido ampliamente debatido por autores como Gerschenkron[10] y Breznitz[11]. En este sentido el resultado esperado de una exitosa colaboración público-privada será la transformación del conocimiento y experiencia generados a nivel académico e industrial (I+D) en productos innovadores aptos para un mercado abierto y competitivo.

[10] Gerschenkron, A. «Economic Backwardness in Historical Perspective: A Book of Essays». Belknap Press of Harvard University Press, Cambridge, 1962.

[11] Breznitz, Dan. «Innovation and the state: political choice and strategies for growth in Israel, Taiwan, and Ireland», Yale University Press, New Haven, 2007.

Investigación, desarrollo e innovación en ciberseguridad

La rápida evolución de las amenazas exige una inversión continua en I+D e innovación tecnológica para no quedarse atrás. Antes de examinar en detalle la especificidad de la I+D+i en ciberseguridad, procede volver a hacer hincapié en la diferencia entre I+D e innovación.

La investigación y desarrollo (I+D) es definida por Christopher Freeman como «el trabajo creador que, emprendido sobre una base sistemática, tiene por objeto el aumento del conocimiento científico y técnico, y su posterior utilización en nuevas aplicaciones»[12]. Por su parte, la innovación es, ante todo, un hecho fundamentalmente económico consistente en la aplicación comercial de una idea. Para el propósito de este capítulo, la innovación en ciberseguridad/ciberdefensa consistirá en la transformación de ideas y conocimiento en productos, procesos o servicios nuevos, o significativamente mejorados, que tendrán difusión y aceptación entre los actores comprometidos en la protección del ciberespacio. Así, una ciberdefensa eficaz se nutrirá de innovación procedente en gran parte del esfuerzo inversor en I+D.

La importancia actual de la investigación y desarrollo en ciberseguridad descansa, entre otras razones, en el hecho de que existe suficiente evidencia de la falta de eficacia de los métodos tradicionales de ciberdefensa. Estos se basan principalmente en el empleo de métodos heurísticos, detección de *software* dañino mediante reconocimiento de determinadas secuencias de código, protección mediante cortafuegos o medidas de prevención de pérdida de datos como las copias de seguridad, que no se encuentran ya a la altura de poder contrarrestar las modernas amenazas a la ciberseguridad[13]. Es por ello que urge adoptar una aproximación más científica al problema, que habrá de centrarse en tres áreas de actuación donde se concentran los principales desafíos: productos (tecnología), procesos y personal (*PPP*).

En cuanto a la primera de estas áreas, objetivo importante de la innovación tecnológica será la obtención de productos resilientes, así como el desarrollo y puesta en explotación de métodos de defensa más sofisticados, tales como el aprendizaje en profundidad (*deep learning*), que se van a basar en la inteligencia artificial y en el aprendizaje automático (*machine learning*) y que puede resultar de gran valor en la detección temprana de amenazas. Por su parte, la criptología, el análisis forense o la gestión de identidades continuarán constituyendo objetivos que también merecerán atención preferente. En todo caso, la ciberdefensa deberá ser efectiva en cuanto a su coste. Esto es, deberá centrarse en conseguir protección a un coste permisible, proporcionando defensas que sean capaces de, o bien impedir los ataques, o bien

[12] Freeman, Christopher. «The Economics of Industrial Innovation», The MIT Press, Cambridge, 1982.

[13] Greengard, Samuel. «Cybersecurity Gets Smart». En: *Communications of the ACM*, vol. 59, n.º 5, May 2016, p. 29.

hacerlos extremadamente difíciles, de manera que resulten muy costosos a los perpetradores. Sin embargo, según el investigador Daniel Genki y otros «el problema de crear *hardware* o *software* económicos que mitiguen adecuadamente toda clase de ataques, incluidos los ataques de canal lateral[14] sigue sin resolver»[15]. De aquí que aún quede un largo camino por recorrer en investigación en ciberseguridad.

La innovación en procesos es un concepto que lleva la innovación más allá de la transición tecnológica entre el espacio de la I+D y el de su uso práctico, al tratar de involucrar a los operadores en el proceso de cambio desde el principio. Ello es especialmente aplicable al ámbito de la ciberseguridad debido a la naturaleza cambiante de las tácticas empleadas por las amenazas.

Finalmente, área de especial atención de la innovación es la de los recursos humanos, el personal, por cuanto su disponibilidad con la adecuada formación, cualificación técnica y adiestramiento específico es clave tanto para mantener el estado deseado de ciberseguridad como para enfrentarse con éxito a las amenazas a la seguridad nacional en el ciberespacio.

La investigación y el desarrollo

Las ciberamenazas explotan en su favor la complejidad de las arquitecturas de los sistemas de información y telecomunicaciones existentes hoy día, que mediante sofisticadas técnicas informáticas como la computación en la nube y la virtualización proporcionan servicio a millones de dispositivos móviles y fijos. El carácter dinámico y distribuido de estas arquitecturas dificulta las actividades de ciberdefensa elementales como son la prevención, detección y respuesta en tiempo útil ante ciberataques. De aquí que resulte imprescindible un esfuerzo inversor en investigación y desarrollo de soluciones que permitan afrontar este desafío. Es de destacar en este sentido que la Agencia de Defensa Europea (EDA) ha identificado noventa y nueve proyectos de investigación y desarrollo de acuerdo con su *Agenda de investigación en ciberdefensa* (*CDRA, Cyber Defence Research Agenda*), que abordan asuntos tan variados como el aseguramiento del *software*, el establecimiento de repositorios de datos de investigación, la protección de sistemas móviles y empotrados, y la lucha contra la falsificación de identidades en el ciberespacio, entre otros.

[14] Conocidos en inglés como *side-channel attacks*, un «ataque de canal lateral» es un ataque criptológico a un criptosistema basado en la información obtenida de la implementación física del mismo, en lugar de explotar una debilidad algorítmica o de efectuar un ataque por fuerza bruta. Por ejemplo, las emanaciones electromagnéticas del criptosistema, su consumo de energía o incluso los sonidos que produzca podrían aportar información susceptible de ser explotada para romper el sistema.

[15] Hewitt, Carl. «Future Cyberdefenses Will Defeat Cyberattacks on PCs», en: *Communications of the ACM*, vol. 59, n.º 8, Aug 2016, p. 8.

A continuación efectuaremos un repaso de los temas prioritarios en investigación y desarrollo en ciberseguridad: resiliencia, consciencia situacional del entorno en cuanto a ciberseguridad, criptología, sistemas de detección de intrusiones y código dañino e intercambio de información sobre ciberseguridad.

Resiliencia

Últimamente se ha extendido el uso del término resiliencia en multitud de contextos diferentes. Entre otras definiciones, la Directiva de Política Presidencial de la Casa Blanca define resiliencia como «la capacidad de prepararse para y de adaptarse a condiciones cambiantes, y resistir y recuperarse rápidamente de las disrupciones», incluyendo «la capacidad para resistir y recuperarse de ataques deliberados, accidentes, incidentes y amenazas procedentes de la naturaleza»[16].

En ciberseguridad, la resiliencia tiene que ver con la robustez de los sistemas y su capacidad de recuperación frente a acciones hostiles. Asumiendo que los ataques a redes y sistemas de información, así como las entradas ilegítimas en los mismos, son inevitables, constituye todo un reto encontrar cómo lograr mantener inalteradas un conjunto mínimo predeterminado de funciones críticas, lo que denominaremos «resiliencia». Si hasta ahora se ha oído principalmente hablar de la protección de los sistemas, a partir de ahora el siguiente objetivo es disponer de sistemas resilientes, es decir, capaces de recuperarse frente a ciberataques. También se puede argumentar que la ciberresiliencia trata de la gestión, que no la eliminación, de los riesgos, una vez fijado un nivel de riesgo aceptable para el entorno considerado.

Imponer un requisito operativo de resiliencia a los sistemas implica que las nuevas tecnologías habrán de posibilitar el cumplimiento de la misión para la que han sido diseñados dichos sistemas, aun cuando se encuentren bajo ataque. De aquí que la investigación aplicada resulte fundamental para el desarrollo de estas tecnologías, sin olvidar que una resiliencia efectiva en cuanto al coste se logra, de nuevo, como conjunción óptima de tres factores: técnicos, humanos y procedimentales.

Consciencia situacional

La mejora de la consciencia situacional[17] del entorno en cuanto a ciberseguridad es uno de los objetivos más importantes que se fijan a la

[16] Presidential Policy Directive on Critical Infrastructure Security and Resilience (PPD-21), The White House, Washington DC, 2013.

[17] Conocida en inglés como *situation awareness* o *situational awareness* (*SA*), la consciencia situacional es el conocimiento inmediato del entorno mediante la percepción de los sucesos y elementos del mismo en relación con el tiempo o el espacio, la comprensión de su significado y la posibilidad de inferir su estado futuro tras el cambio de alguna variable como puede ser la ocurrencia de un suceso predeterminado o bien el mero transcurso del tiempo.

hora de adquirir una capacidad de ciberdefensa. Se trata de uno de los temas difíciles en la investigación en ciberseguridad y ciberdefensa, y abarca materias tan variadas como: métricas de consciencia situacional, valoración dinámica del riesgo para el aseguramiento de la misión, monitorización continua y análisis del tráfico de red, técnicas de visualización y análisis de las visualizaciones y evaluación de la efectividad de la consciencia situacional en ciberdefensa. Al igual que con la resiliencia, será necesario disponer de las herramientas, *hardware* y *software,* apropiadas, el personal adecuadamente formado y los procedimientos adaptados.

Existen numerosas iniciativas para fomentar la investigación y desarrollo en esta materia. Como botón de muestra mencionaremos las llevadas a cabo por dos organizaciones multinacionales comprometidas con el I+D en ciberseguridad: la Alianza Atlántica y la Agencia de Defensa Europea (*EDA*).

Por un lado, la Organización para la Ciencia y la Tecnología (*STO*) de la OTAN aprobó en 2015 una actividad denominada, no sorprendentemente, *Cyber Defence Situation Awareness* (IST-148), con la finalidad de investigar de manera colaborativa a escala internacional los temas antes citados para dar respuesta a esta apremiante necesidad operativa[18].

Y por el otro lado, también la Agencia de Defensa Europea ha identificado la consciencia situacional en ciberdefensa como una carencia que ha de ser abordada, a fin de proporcionar a las autoridades una visión clara del escenario de amenazas realmente existente, de manera que estas puedan dimensionar adecuadamente los recursos para combatirlas, así como para gestionar eficazmente los riesgos en ciberseguridad durante las fases de planeamiento y de conducción de las operaciones. Con este propósito la *EDA* está impulsando el proyecto *Cyber Situation Awareness Package* (*CySAP*)[19].

Criptología

Los productos criptológicos seguirán desempeñando un papel muy destacado en los métodos de ciberdefensa, por cuanto son esenciales para autenticar sujetos, mantener la confidencialidad y la integridad de la información, evitar el repudio y registrar las acciones ejecutadas en el sistema a efectos de imputación de responsabilidades. Al fin y al cabo, estos productos serán esencialmente implementaciones de funciones criptológicas emanadas de un proceso de investigación. Sin embargo, resulta curioso descubrir que, a pesar de que la criptología se encuentra latente en casi cualquier producto

[18] https://www.cso.nato.int/ACTIVITY_META.asp?ACT=8921. Fecha de la consulta: 10 de agosto de 2016.

[19] https://www.eda.europa.eu/info-hub/press-centre/latest-news/2016/02/24/business-case-on-cyber-situation-awareness-package-agreed. Fecha de la consulta: 10 de agosto de 2016.

o proyecto relativo a ciberseguridad, es difícil encontrar programas de investigación y desarrollo específicamente dedicados al avance de esta disciplina (investigación básica) o al desarrollo de nuevos sistemas o protocolos criptológicos propios[20]. Se puede considerar una excepción, no obstante, la iniciativa CriptoRed[21].

Volviendo al asunto de la protección contra los «ataques de canal lateral», que introducíamos anteriormente, en Estados Unidos, el experto Carl Hewitt ha defendido que sea el Departamento de Defensa quien inicie un programa de investigación y desarrollo de ciberdefensas potentes y económicas para ordenadores personales utilizando tecnologías como las jaulas de Faraday para procesadores, acopladores ópticos, filtros para las fuentes de alimentación eléctrica o el etiquetado de memoria[22].

Y para finalizar esta breve pincelada, quedaría reseñar que la introducción del concepto *Internet of Things* en el mundo militar hace especialmente importante y necesaria la continuación de la investigación en criptología.

Computación confiable

Un sistema confiable es aquel del que se tiene la seguridad de que puede hacer valer una política de seguridad especificada con un determinado nivel de confianza. La computación confiable[23] será pues aquella en la que el sistema informático se comportará consistentemente de la forma esperada. Una forma de lograr este objetivo consiste en la integración de un subsistema criptográfico conocido como *Trusted Platform Module* (*TPM*) cuyo *hardware* ha de ser capaz de almacenar una clave de cifrado de manera inaccesible al resto del sistema.

La protección de sistemas de mando y control militar, y de sistemas empotrados en plataformas como vehículos, equipos de radio y sistemas de armas es extremadamente importante para salvaguardar las misiones militares y la vida e integridad física de los participantes en las mismas. El empleo de técnicas de computación confiable proporciona en estos casos una garantía de seguridad difícilmente alcanzable por otros medios.

La implantación de la computación confiable basada en los *TPM* en plataformas computacionales ordinarias (ordenadores personales o dispositivos móviles) ha sido, no obstante, fuertemente criticada por voces prominentes

[20] DÁVILA MURO, Jorge. «Criptología y Seguridad». Cuadernos Cátedra ISDEFE-UPM n.º 4, ETSI de Telecomunicación, Madrid, 2008.

[21] Criptored es una red temática iberoamericana de criptografía y seguridad. http://www.criptored.upm.es

[22] HEWITT, Carl. «Future Cyberdefenses Will Defeat Cyberattacks on PCs», en: «Communications of the ACM», vol. 59, n.º 8, Aug 2016, p. 8.

[23] *Trusted computing*.

dentro de la comunidad científica[24] y del activismo en la Red[25], por considerarlo una amenaza contra la privacidad de los consumidores y una forma de encadenar a estos a los fabricantes de *hardware* y *software*. Es por ello necesario proseguir la investigación en computación confiable de manera que se pueda alcanzar una solución que incremente la ciberseguridad general en la sociedad sin socavar derechos considerados irrenunciables por los ciudadanos.

Sistemas de detección de intrusiones, código dañino y amenazas persistentes avanzadas.

La detección de amenazas persistentes avanzadas (*APT*, *Advanced Persistent Threats*) es otro asunto necesitado de investigación, ya que los productos comerciales alcanzan como mucho un 80 % de detecciones positivas de código dañino y ello no es suficiente. Además, es imperativo detectar estas *APT* en una escala de tiempos significativamente más baja: horas en vez de días o semanas.

Por otra parte, debido a que los métodos tradicionales de protección contra estas amenazas (prevención de pérdida de datos mediante copias de seguridad, uso de herramientas defensivas como los cortafuegos, detección de código dañino en función de su firma digital o, simplemente, la heurística) resultan hoy día poco eficaces, la investigación está centrándose en adoptar nuevas técnicas basadas en inteligencia artificial y en aprendizaje automático con el fin de construir modelos defensivos radicalmente diferentes. El objetivo es mejorar la identificación de comportamientos y patrones sospechosos, y así poder construir entornos de seguridad auto-adaptativos con el fin de ganar resiliencia con la mínima intervención humana. Las técnicas empleadas se basan en tecnologías como *Big Data*, correspondencia de patrones, computación cognitiva y métodos de aprendizaje profundo que intentan simular la forma de funcionamiento de la mente humana[26].

Como muestra de la importancia que se concede a la mejora de la efectividad en la detección de las *APT*, la Agencia de Defensa Europea, al amparo del programa *Pooling & Sharing*, está impulsando el proyecto *MASFAD* (*Multi-agent System for Advanced Persistent Threat Detection*) consistente en un sistema de detección de amenazas persistentes avanzadas a integrar en sistemas de información para el mando y control militar[27]. Actualmente se

[24] Anderson, Ross. «Trusted Computing' Frequently Asked Questions. TC/TCG/LaGrande/NGSCB/Longhorn/Palladium/TCPA. Version 1.1 (August 2003)», disponible en: http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html. Fecha de la consulta: 1 de agosto de 2016.

[25] Stallman, Richard. «Can You Trust Your Computer?», disponible en: https://www.gnu.org/philosophy/can-you-trust.en.html. Fecha de la consulta: 1 de agosto de 2016.

[26] Greengard, Samuel. «Cybersecurity Gets Smart». En: *Communications of the ACM*, vol. 59, n.º 5, May 2016, p. 29.

[27] MEES, Wim, y DEBATTY, Thibault. «Multi-agent System for APT Detection». En: «Proceedings of the 2014 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW'14)», IEEE Computer Society, Washington DC, USA, 2014, pp. 401-406.

dispone de un demostrador tecnológico de *MASFAD* y se está trabajando en una segunda fase del proyecto denominada *MASFAD II*.

Intercambio de información sobre ciberseguridad.

Un reto importante que encara la comunidad de ciberdefensa a escala global es la adquisición, integración e intercambio de información sobre amenazas y ataques en tiempo real. Es más, este intercambio de información dentro de las propias organizaciones no suele estar automatizado, dependiendo en gran medida de la intervención de operadores humanos, siendo por ello que existe un margen para la mejora de la calidad y eficiencia de esta comunicación donde juega su papel la automatización de los intercambios de información. Por ejemplo, resulta muy ineficiente que la implementación de contramedidas frente a determinadas amenazas se haga de manera redundante por diferentes organizaciones que funcionan aisladamente, cuando podrían trabajar colaborativamente si dispusieran de un marco de trabajo normalizado.

Por ello existe la necesidad operativa de conseguir la integración coherente de representaciones normalizadas y estructuradas de la información relevante, incluyendo análisis de patrones de ciberataque. En este sentido encontramos dos iniciativas dignas de mención: *CYBEX* y *STIX*.

CYBEX (*Cybersecurity Information Exchange Framework*), como su propio nombre indica, es un marco de intercambio de información sobre ciberseguridad que está siendo estandarizado por la Unión Internacional de Telecomunicaciones (*ITU*). Este marco de trabajo describe la forma en que la información sobre ciberseguridad ha de ser intercambiada entre las entidades de ciberdefensa[28] a escala global y cómo se asegura este intercambio. Los proponentes de este estándar sostienen que la implementación de *CYBEX* a escala mundial minimizaría la dispersión de la información y posibilitaría una respuesta más rápida y eficaz contra las amenazas[29].

STIX (*Structured Threat Information eXpression*) es esencialmente un lenguaje estructurado para definir información e inteligencia sobre ciberamenazas[30]. Sus casos de uso incluyen el análisis, la especificación de patrones de indicación, la gestión de actividades de prevención y respuesta, así como la compartición de información sobre estas amenazas. Se trata de un producto resultante de I+D llevado a cabo por MITRE[31], entidad que, no obstante, lo

[28] Por ejemplo los CERT y CIRT.

[29] Rutkowski, Anthony, *et al.* «CYBEX: the cybersecurity information exchange framework (x.1500)». En: *SIGCOMM Computer Communications Review*, n.º 40, 5 de octubre de 2010, pp. 59-64.

[30] https://makingsecuritymeasurable.mitre.org/docs/stix-intro-handout.pdf. Fecha de la consulta: 17 de septiembre de 2016.

[31] La Corporación MITRE es una empresa pública estadounidense sin ánimo de lucro que gestiona centros de investigación y desarrollo financiados con fondos del Gobierno Federal de los Estados Unidos. Véase: http://www.mitre.org

licencia sin restricciones de uso[32]. Lo interesante de este proyecto es que, una vez iniciado por MITRE, es continuado en forma de esfuerzo colaborativo por los usuarios pertenecientes a la comunidad de interés en inteligencia de amenazas en el ciberespacio.

Innovación

La innovación en ciberseguridad se ha de abordar de manera coherente en tres áreas de actuación: tecnologías (productos), procesos y recursos humanos (personas).

Innovación en productos

La innovación tecnológica en ciberseguridad debe ser la consecuencia directa del esfuerzo en investigación y desarrollo. La gran ventaja de la que disfrutan estos productos es que se basan en tecnologías de uso dual y ello debería suponer un incentivo para que los distintos actores implicados en la seguridad del ciberespacio (Gobiernos y Adminstraciones Públicas, industrias y organismos de investigación) decidan compartir los riesgos y beneficios de encarar juntos los retos que se presentan en este terreno. Según Michael Sieber, antiguo jefe de la Unidad de Superioridad en la Información del Área de Capacidades y Armamento de la Agencia de Defensa Europea, el carácter dual de estas tecnologías brinda la oportunidad de compartir el esfuerzo de enfrentarse a los desafíos en ciberseguridad[33].

Detección de amenazas, análisis forense, plataformas de adiestramiento en ciberdefensa, así como de mando y control de operaciones en el ciberespacio son algunas de las áreas donde aún existe un gran espacio abierto para la innovación.

Innovación en procesos

En ciberdefensa, este tipo de innovación está relacionada con cambios en la dirección y organización bajo la que se desarrollan las actividades defensivas; se trata en esencia, de una innovación doctrinal que ha de posibilitar una mayor inteligencia de la situación y un mejor aprovechamiento de los recursos disponibles, humanos, financieros y materiales. En general, se distinguen dos tipos de innovaciones de procesos: a nivel externo y a nivel interno. En el contexto de la ciberdefensa, las de nivel externo se refieren a la constitución de redes de cooperación con otros agentes nacionales e internacionales empeñados en el esfuerzo ciberdefensivo y al intercambio real de información entre los mismos. A nivel interno se identifican las innovaciones dirigidas a mejorar el rendimiento del trabajo en equipo, de manera

[32] Se encuentra libremente disponible en: https://stixproject.github.io

[33] —, «Bricks to build a cyber shield», EuropeanDefenseMatters, issue 9, European Defense Agency, Brussels, 2015, p.10.

que resulte más eficiente la ciberdefensa (reducción de escalas de tiempo, de horas a minutos, por ejemplo).

Según MITRE, una ciberdefensa eficaz depende en gran medida de la rápida respuesta a las tácticas cambiantes de las amenazas[34]. Para su implementación se introduce la idea de «innovación en las operaciones», que no es más que una variante de la innovación en procesos. Es un concepto que lleva la innovación más allá de la transición tecnológica entre el espacio de la I+D y el de su uso práctico, al intentar involucrar a todos los participantes en el proceso defensivo: operadores, administradores de sistemas, desarrolladores o analistas de amenazas, de manera que todos deben ser innovadores con el fin de llevar la delantera a los creadores de ciberamenazas.

Innovación en recursos humanos

El hombre sigue siendo el elemento fundamental de la acción también en el ciberespacio. Las más avanzadas tecnologías son virtualmente inútiles si no son utilizadas por personal adecuadamente adiestrado en su manejo. En Estados Unidos el Consejo Asesor de Seguridad Interior considera que una amenaza de seguridad apremiante es la escasez de personal especializado en ciberseguridad, por el consecuente vacío defensivo que se produce y que aparece como una invitación al ataque y a la materialización de las amenazas[35].

Las políticas innovadoras en recursos humanos son muy variadas y van desde la incentivación de la profesionalización de la ciberseguridad a las que simplemente impulsan la capacitación del personal o promueven la captación de personal especializado a través de la organización de cibercompeticiones que atraigan a los más capaces y motivados. Tampoco se pueden olvidar las que promueven la educación y mentalización sobre riesgos de todos los usuarios del ciberespacio, trabajen o no en ciberseguridad.

Resulta, pues, imperativo atender este aspecto y desarrollar políticas innovadoras en relación con el personal especializado en ciberseguridad. Ello no es sencillo si se tiene en cuenta el elenco de ocupaciones que contempla esta disciplina, desde las tecnológicas, altamente especializadas, hasta las de carácter gerencial, enfocadas en la administración, dirección y control de las actividades.

En conclusión, la implantación con éxito de una idea novedosa implica una creación de valor, pero será solo la puesta en práctica de una política de innovación coherente en las tres dimensiones (productos, procesos y personas) la que sea capaz de crear la sinergia necesaria para afrontar con éxi-

[34] https://www.mitre.org/capabilities/cybersecurity/operational-innovation. Fecha de la consulta: 20 de septiembre de 2016.

[35] Homeland Security Advisory Council, «Cyber Skills Task Force Report», Department of Homeland Security, Washington, DC, 2012.

to retos de la talla de los planteados por organizaciones como *The Shadow Brokers* o el *Equation Group*.

Necesidad de una actuación específica de I+D+i en ciberseguridad

La defensa en el nuevo escenario de confrontación que constituye el ciberespacio[36] exige la disponibilidad de una capacidad ciberdefensiva, en cuya obtención la innovación continua en productos, procesos y recursos humanos desempeña un papel crucial. A su vez, esta capacidad de innovación vendrá principalmente determinada por la apropiada transición de productos y tecnología de ciberseguridad desde el espacio de la I+D al de su empleo operativo.

La adopción de una adecuada estrategia de investigación, desarrollo e innovación en materia de ciberseguridad deviene, pues, en una necesidad insoslayable. España cuenta con la Estrategia Española de Ciencia y Tecnología y de Innovación (EECTI)[37], en el marco de la cual se sitúa el planeamiento de la I+D+i en ciberseguridad, sin perjuicio de que, dado su carácter transnacional, también es abordada a nivel de Unión Europea. Por otro lado, circunscrita al ámbito exclusivo de los equipos y sistemas con finalidad específicamente militar, la Estrategia de Tecnología e Innovación de la Defensa (ETID) del Ministerio de Defensa contempla actuaciones en ciberdefensa, en línea con la EECTI.

Asimismo, la actuación en I+D+i específica para la ciberseguridad nacional debe ser coherente no solo con la estrategia global del Estado en tecnología e innovación, la EECTI, sino también con las estrategias de seguridad y ciberseguridad en vigor. A continuación repasaremos estos planteamientos, enfocados desde la perspectiva de la I+D+i.

La Estrategia de Seguridad Nacional

La Estrategia de Seguridad Nacional (ESN)[38] concibe la seguridad aplicando un enfoque integral, de manera amplia e interdisciplinar, a nivel nacional, europeo e internacional extraeuropeo, involucrando también a la sociedad civil en los ámbitos de interés prioritario de la Seguridad Nacional. Precisamente la ESN identifica el ciberespacio como uno de estos ámbitos de actuación preferente, al ser considerado un escenario accesible, poco regulado y de difícil control, donde pueden tener lugar amenazas contra la seguridad nacional[39].

---

[36] —, «El ciberespacio: Nuevo escenario de confrontación», Monografías del CESEDEN n.º 128, CESEDEN, Madrid, 2012.

[37] —, «Estrategia Española de Ciencia y Tecnología y de Innovación (2013-2020)», Ministerio de Economía y Competitividad, Madrid, 2013.

[38] —, «Estrategia de Seguridad Nacional: un proyecto compartido», Presidencia del Gobierno, Madrid, 2013.

[39] ESN, p. 26.

La ESN señala la relación de dependencia entre innovación y seguridad en el marco de la seguridad económica de la nación, de suerte que, para garantizar esta, propugne, entre otras medidas, la incentivación de un modelo de crecimiento económico sostenible que «potencie la productividad, el tejido empresarial, la innovación y la competitividad»[40]. En este sentido, es pertinente reseñar que ya la anterior Estrategia Española de Seguridad de 2011 (EES) declaraba explícitamente que «quedarse por detrás de nuestros competidores en capacidad de innovación tendrá un serio impacto en nuestra competitividad y desarrollo y, por tanto, en nuestra seguridad»[41].

También identifica la ESN la ciberseguridad no como un mero aspecto técnico de la seguridad sino como un eje fundamental de nuestra sociedad y sistema económico, ya que «España está expuesta a los ciberataques, que no solo generan elevados costes económicos, sino también, y lo que es más importante, la pérdida de confianza de los ciudadanos en unos sistemas que, en la actualidad, resultan críticos para el normal funcionamiento de la sociedad»[42].

En relación con la I+D+i, una de las actuaciones que propone la ESN para afianzar la seguridad en el ciberespacio a nivel nacional es la «promoción de la capacitación de profesionales en ciberseguridad» y el «impulso a la industria española a través de un Plan de I+D+i»[43], aunque sin abordar el asunto de la independencia tecnológica, como sí lo hiciera su antecesora, la Estrategia Española de Seguridad de 2011, al propugnar el apoyo al desarrollo de empresas privadas nacionales en un sector estratégico como el de la ciberseguridad, «en el que puede ser peligrosa la dependencia de empresas extranjeras»[44].

La Estrategia de Ciberseguridad Nacional

La Estrategia de Ciberseguridad Nacional (ECSN) constituye un segundo escalón de desarrollo sectorial de la Estrategia de Seguridad Nacional[45]. Constituye una línea de respuesta a las ciberamenazas, una de las circunstancias que la EES identifica en su capítulo 4, sobre amenazas, riesgos y respuestas, como potencialmente atentatoria contra la seguridad nacional[46]. Como objetivo global, la ECSN se plantea «lograr que España haga un uso seguro de los sistemas de información y telecomunicaciones, fortaleciendo las capaci-

40 ESN, p. 44.
41 —, «Estrategia Española de Seguridad: una responsabilidad de todos», Gobierno de España, Madrid, 2011, p. 38.
42 ESN, p. 27.
43 ESN, p. 42.
44 EES, p. 68.
45 —, «Estrategia de Ciberseguridad Nacional», Presidencia del Gobierno, Madrid, 2013, p. 3.
46 EES, p. 65.

dades de prevención, defensa, detección y respuesta a los ciberataques»[47], para lo cual, entre otras medidas, establece que «será necesario potenciar, impulsar y reforzar las capacidades nacionales de investigación y desarrollo en ciberseguridad de las TIC[48]». En el caso de la defensa, la ECSN indica también que «además de mejorar las capacidades de los sistemas militares de defensa y de inteligencia es necesario reforzar la seguridad de los sistemas de información y comunicación estratégicos, adaptándolos a los nuevos riesgos y amenazas del ciberespacio»[49].

En lo que se refiere al I+D+i, la ECSN es explícita. Detalla que para alcanzar soluciones nacionales confiables «se requiere fomentar y mantener una actividad de I+D+i en materia de ciberseguridad de manera efectiva»[50]. En particular, la ECSN contempla una línea de acción, la sexta, que se ocupa precisamente del tema que nos interesa (conocimientos, competencias e I+D+i), con la intención de «promover la capacitación de profesionales, impulsar el desarrollo industrial y reforzar el sistema de I+D+i en materia de ciberseguridad»[51]. Merece la pena analizar esta línea de acción pues es donde convergen las diferentes estrategias: por un lado, la de seguridad nacional, de la que la estrategia de ciberseguridad nacional es solo una especialización sectorial, y, por otro lado, la estrategia española de ciencia, tecnología e innovación. Entre otras medidas, esta línea de acción contempla las siguientes actuaciones[52]:

1. Extender y ampliar los programas de captación de talento, investigación avanzada y capacitación en ciberseguridad en cooperación con universidades y centros especializados.
2. Fomentar el desarrollo industrial de productos y servicios en materia de ciberseguridad por medio de instrumentos, entre otros, como el Plan Estatal de Investigación Científica y Técnica y de Innovación e iniciativas de apoyo a su internacionalización.
3. Impulsar la coordinación nacional y la dinamización del sector industrial y de servicios de ciberseguridad para la mejora de la competitividad, la internacionalización, la identificación de oportunidades, la eliminación de barreras y la orientación normativa, entre otras actividades.
4. Impulsar las actividades de certificación de ciberseguridad de acuerdo con las normas y estándares de reconocimiento internacional, incluyendo estos criterios en los procesos de desarrollo y adquisición de productos o sistemas.

---

47 —, «Estrategia de Ciberseguridad Nacional», Presidencia del Gobierno, Madrid, 2013, p. 21.
48 ECSN, p. 22.
49 ECSN, p. 23.
50 ECSN, p. 26.
51 ECSN, p. 37.
52 *Idem. Ibid.*.

5. Impulsar modelos y técnicas de análisis de ciberamenazas y medidas de protección de productos, servicios y sistemas, así como su especificación, evaluación y certificación.

Como vemos, esta línea de acción es ambiciosa, está bien trazada, define adecuadamente el qué y apunta en algunos casos el cómo (Plan Estatal de Investigación Científica y Técnica y de Innovación), pero no han faltado voces críticas respecto a la misma. Por ejemplo, el investigador Dávila Muro considera que, declaraciones de intenciones aparte, los resultados permitirán evaluar si la ECSN tiene vocación de proporcionar soluciones al futuro cibernético de nuestra sociedad o si por el contrario, en sus propias palabras, este documento se trata tan solo de «un puente hasta la redacción del siguiente»[53]. Es decir, la sexta línea de acción de la ECSN delinea un conjunto de intenciones a nivel estratégico, pero es necesario pasar de la estrategia a la táctica: cómo, cuándo y con qué recursos acometer en la práctica todas esas iniciativas determinarán el éxito o el fracaso de la acción estratégica. Como mínimo, una financiación específica y adecuada a la magnitud del empeño sería condición necesaria, aunque no suficiente, para el éxito.

La Estrategia Española de Ciencia, Tecnología e Innovación.

La Estrategia Española de Ciencia, Tecnología e Innovación 2013-2020 (EECTI)[54] recoge en su objetivo general cuarto la necesidad de orientar la investigación hacia los grandes desafíos del futuro[55], y, más concretamente, hacia la ciberseguridad como parte del objetivo específico sobre seguridad, protección y defensa[56]. Además, prescribe que el I+D+i en ciberseguridad debe alinear la política española en esa materia con los objetivos perseguidos por la Unión Europea a través del programa Horizonte 2020, de manera que se facilite el acceso de los agentes españoles a las fuentes de financiación comunitarias.

En cuanto a su implementación, corresponde a los planes estatales de ciencia y tecnología y de innovación el desarrollo y financiación, por parte de la Administración General del Estado, de las actuaciones contenidas en la EECTI. El Plan Estatal de Investigación Científica y Técnica y de Innovación

[53] Dávila Muro, Jorge. «La estrategia de ciberseguridad nacional y otros buenos deseos». En: *Revista SIC*, n.º 108, febrero de 2014.

[54] —, «Estrategia Española de Ciencia, Tecnología e Innovación 2013-2020», Ministerio de Economía y Competitividad, Madrid, 2013. Disponible en: http://www.idi.mineco.gob.es/stfls/MICINN/Investigacion/FICHEROS/Estrategia_espanola_ciencia_tecnologia_Innovacion.pdf

[55] EECTI, p. 26. El apartado 4.4 formula el objetivo general IV: Investigación orientada a los retos de la sociedad.

[56] EECTI, p. 31. El apartado 4.4.8 plantea el objetivo específico 8: Seguridad, protección y defensa.

(PEICTI) para el periodo 2013-2016[57] contempla la ciberseguridad como un reto para «la economía y la sociedad digital»[58], así como para «la seguridad, protección y defensa»[59].

La Estrategia de Tecnología e Innovación de Defensa

La Estrategia de Tecnología e Innovación de Defensa (ETID)[60] es el marco general en el que se deben situar los distintos planes y actividades de los agentes dedicados a la I+D+i de la defensa, y nace con la intención de «mejorar la gestión de la I+D+i del Ministerio de Defensa, de forma que se tenga un mayor aprovechamiento de las oportunidades para potenciar su situación dentro del marco nacional e internacional de la innovación aplicable a la defensa»[61].

La I+D+i de la defensa, como parte de la I+D+i nacional, debe ser plenamente consistente con los objetivos de la EECTI. Por un lado, la ETID se encuentra alineada con las acciones programáticas y los objetivos tecnológicos del reto en seguridad, protección y defensa del Plan Estatal de Investigación Científica, Técnica y de Innovación[62]. Por otro lado, la ETID limita la ciberdefensa al ámbito de los sistemas de información y comunicaciones para el mando y control militar, para los que define dos metas tecnológicas: la automatización de las acciones ante ciberataques[63] y la inteligencia cibernética y disminución de la cibermovilidad del enemigo[64].

Estrategia de Ciberseguridad de la Unión Europea.

La Estrategia de Ciberseguridad de la Unión Europea (ECSUE)[65] se centra en dos áreas: tecnología y capacitación del personal. En lo referente a tecnología, la ECSUE identifica los siguientes temas abiertos a la innovación: criptología, protección de sistemas militares (plataformas y sistemas empotrados), sistemas autónomos y capacitación mediante adiestramiento y formación.

---

57 —, «Plan Estatal de Investigación Científica y Técnica y de Innovación 2013-2016», Ministerio de Economía y Competitividad, Madrid, 2013. Disponible en: http://www.idi.mineco.gob.es/stfls/MICINN/Investigacion/FICHEROS/Plan_Estatal_Inves_cientifica_tecnica_innovacion.pdf

58 PEICTI, p. 38.

59 PEICTI, p. 39.

60 —, «Estrategia de Tecnología e Innovación de Defensa», Ministerio de Defensa, Madrid, 2015. Disponible en: http://www.tecnologiaeinnovacion.defensa.gob.es/Lists/Publicaciones/Attachments/205/ETID %202015.pdf

61 ETID, presentación del secretario de Estado de Defensa.

62 PEICTI, p. 39; ETID, p. 22.

63 Meta tecnológica 6.5.1, ETID, anexo I, p. 62.

64 Meta tecnológica 6.5.2, ETID, anexo I, p. 62.

65 —, «Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. JOIN(2013) 1 final», European Commission, Brussels, 7/2/2013. Disponible en: https://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf.

Prioridades clave de esta estrategia son la ciberdefensa en el marco de la política común de seguridad y defensa de la Unión Europea, la necesidad de un marco de política de ciberdefensa de la Unión Europea, la mejora de las capacidades ciberdefensivas de los Estados miembros, sinergias cívico-militares y cooperación con otras partes interesadas, incluso más allá de las fronteras comunitarias. Como actuación derivada de la puesta en práctica de esta estrategia el Consejo de Europa adoptó en 2014 un marco para la definición de una política de ciberdefensa[66] que esboza principios generales para facilitar la cooperación con el sector privado en lo que se refiere al desarrollo de una capacidad de ciberdefensa, con un especial enfoque en el fortalecimiento de la investigación y el desarrollo tecnológico, así como de la base tecnológica e industrial europea de defensa[67]. Por último, cabría reseñar que la Unión Europea, por medio de la Comisión Europea, tiene prevista comenzar la financiación directa del I+D en ciberdefensa a través de la Acción Preparatoria del próximo programa marco de investigación y desarrollo, ya que la ciberseguridad es uno de los cuatro temas principales de dicha acción.

Consideraciones sobre el camino a seguir en I+D+i en ciberseguridad

La actuación en I+D+i en ciberseguridad ha de articularse en torno a los ejes prioritarios marcados en la EECTI y, a su vez, debe estar alineada con una política de ciberseguridad nacional, de manera que se oriente al logro del objetivo global de la Estrategia de Ciberseguridad Nacional, que no es sino «lograr que España haga un uso seguro de los sistemas de información y telecomunicaciones, fortaleciendo las capacidades de prevención, defensa, detección y respuesta a los ciberataques»[68].

En lo que respecta a la I+D de defensa se advierte que aún queda camino por recorrer. Por un lado, se observa que su carácter eminentemente finalista puede constituir en ocasiones un lastre en materia específica de ciberdefensa, por cuanto no promueve la investigación básica, que es un aspecto crítico en ciberseguridad. Por otro lado, la I+D de defensa está enfocada en las aplicaciones con un fin específicamente militar, mientras que los productos y tecnologías en seguridad cibernética tienen un carácter dual. Luego es imperativo atraer a la I+D+i militar a nuevos agentes que antes dirigían sus actividades hacia el mundo comercial civil, por lo que una actuación en este sentido solo puede tener éxito si se dan los suficientes incentivos para que ambas partes obtengan beneficios. A título de ejemplo, encontrar un adecuado equilibrio en términos de propiedad intelectual entre empresas y Administración es clave para incentivar la innovación.

En todo caso será preciso de nuevo diferenciar entre I+D (confinado a la comunidad investigadora tanto académica como industrial, tanto en el sector

66 EU Cyber Defence Policy Framework, noviembre de 2014.
67 *European Defence Technological and Industrial Base* (*EDTIB*).
68 ECSN, p. 21.

público como en el privado) e innovación, proceso en el que es necesario involucrar a mayor número de actores. Ambos deben ser abordados en sus respectivos contextos, debiendo identificar de manera temprana necesidades presentes y futuras en materia de ciberseguridad, tanto provenientes del sector público como del privado. Igualmente importante será también saber realizar la transición de productos y tecnología de ciberseguridad desde el espacio de la I+D hasta el mercado[69].

La inversión en I+D+i en ciberseguridad

Habida cuenta de que el escenario de la ciberdefensa es relativamente nuevo, que todavía se están conformando sus estructuras organizativas (algunas cambiarán en los Estados miembros de la Unión Europea con la trasposición de la Directiva NIS a más tardar en 2018) y que algunos países no tienen su modelo presupuestario preparado para reflejar las inversiones en ciberseguridad (menos todavía I+D+i en ciberseguridad), no existe mucha información identificable y contrastada sobre esta materia.

Sin embargo, sí hay datos suficientes en diversas esferas y partidas que permiten hacerse una idea razonable de la situación, tanto en algunos Estados como en organizaciones supranacionales e internacionales (por prudencia, y más a la velocidad a la que avanza la preocupación por la inseguridad digital, es pertinente señalar aquí que algunos de estos datos están sometidos a posible modificación).

En Europa, por ejemplo, se espera destinar cerca de 1.800 millones de euros de aquí al año 2020 para financiar la I+D+i en tecnologías, productos y servicios de ciberseguridad. El mecanismo utilizado ha sido la firma en 2016 de un acuerdo entre la Comisión Europea con la *European Cyber Security Organization* (*ECS*), un instrumento de CPP al que más tarde se aludirá.

Sin salir de Europa, es de obligada mención la carta que en octubre de 2016 remitieron los ministros de Defensa de Francia, Alemania, Italia y España a sus colegas del resto de países de la Unión Europea para, tras el *Brexit*, fortalecer la defensa europea, dotarla de autonomía estratégica y estudiar la creación de un Consejo de Ministros de Defensa europeos.

El movimiento tendrá consecuencias positivas para la ciberdefensa militar, la I+D+i y la CPP, por cuanto se apuesta por «consolidar una base tecnológica e industrial europea de defensa capaz de gestionar tecnologías clave, proveer las necesarias capacidades militares en el futuro y reforzar nuestra autonomía de decisión»[70].

[69] En Estados Unidos, la DHS S&T Cyber Security Division tiene por misión precisamente esto.

[70] González, Miguel. «Los cuatro grandes de la Unión Europea apuestan por una defensa común con "autonomía estratégica"», *El País*, 15 de octubre de 2016, http://internacional.elpais.com/internacional/2016/10/14/actualidad/1476449123_095969.html

Durante el desarrollo de la conferencia NITEC 2016 en el verano de 2016, la OTAN anunció la inversión de 3.000 millones de euros en ciberseguridad para reforzar capacidades frente a posibles ciberataques.

Como es sabido, la OTAN dispone del Centro de Excelencia de Ciberseguridad en Tallin (Estonia), del que España es miembro fundador. Precisamente dicho Centro se ubicó allí por el ciberataque que sufrió hace años este país europeo, un suceso que marcó el inicio de la toma de conciencia por los Gobiernos y Estados occidentales de la importancia de la ciberdefensa.

El Centro de Excelencia de Ciberseguridad tiene información actualizada y precisa del estado de la ciberseguridad a gran escala.

En la Cumbre de Varsovia en julio de 2016, la OTAN expuso el estado del arte de su incubadora de proyectos en el ámbito de la ciberseguridad, que se desarrolla en el contexto de la relación de la propia OTAN con actores de la industria a través de la OTAN *Industry Cyber Partnership* (*NICP*)[71], y eje de sus espacios colaborativos orientados a la innovación.

La *NATO Industry Cyber Partnership* es una iniciativa formal, aprobada por los veintiocho países aliados durante la Cumbre celebrada en Gales (2014) y presentada días después en el encuentro de ciberseguridad celebrado en Mons (Bélgica). A través de *NICP* la Alianza busca impulsar la cooperación con el sector privado en base a los siguientes principios: mejorar la ciberseguridad en la cadena de suministro de defensa de la OTAN; aumentar la comprensión y el conocimiento sobre las ciberamenazas y riesgos mutuos, incluyendo el intercambio de información; contribuir a los esfuerzos de la Alianza en educación, formación y realización de ciberejercicios; mejorar el intercambio de las mejores prácticas y conocimientos sobre la preparación y recuperación; ayudar a la OTAN y aliados a aprender de la industria.

El acercamiento al sector privado establecido se guía por tres principios; a saber: cooperar con el sector privado con el objetivo principal de reforzar la protección de las propias redes de la OTAN; dar la bienvenida a la cooperación con las empresas más innovadoras de los países de la OTAN de forma abierta, transparente e inclusiva; y crear sinergias a través de la construcción, el esfuerzo y la garantía de una coherencia en las iniciativas existentes con la industria.

Estados Unidos[72], el país en el que se gestó y desarrolló Internet, y en el que la Administración Obama nombró en 2016 a un *CISO* (*Chief Information Security Officer*) Federal, viene destinando desde hace años ingentes cantidades de recursos para atender la ciberseguridad y perfeccionar en un ciclo continuo sus capacidades de ciberdefensa en prevención, explotación y ataque.

[71] http://www.nicp.nato.int
[72] https://whitehouse.gov

El aumento de la tensión en la campaña presidencial durante 2016 por la exfiltración de información de servidores del Partido Demócrata y posterior filtración masiva llevó a una escalada de ciberguerra fría, en la que Estados Unidos indicó públicamente que la autoría de estos hechos (ciberataque) era responsabilidad de Rusia, reservándose el derecho a responder mediante un ciberataque proporcionado. Al hecho, le sucedió —esté o no relacionado— un ciberataque de denegación de servicio de significativas proporciones a entidades privadas de Estados Unidos.

Para el año 2017 Estados Unidos ha presupuestado una inversión en ciberseguridad de 19.000 millones de dólares (17.183 millones de euros), lo que supone un incremento de 5.000 millones de dólares (alrededor de 4.520 millones de euros) respecto al presupuesto de 2016. De los 19.000 millones de dólares, 3.100 millones de dólares (2.804 millones de euros) se destinarán a la modernización tecnológica en varias agencias federales y 62 millones de dólares (algo más de 56 millones de euros) a la ampliación de esfuerzos para atraer y retener a profesionales cualificados en ciberseguridad que trabajen para la Administración estadounidense.

Por su parte, el Cyber Command de Estados Unidos está reforzando su fuerza cibernética con la estructuración de ciento treinta y tres equipos montados a partir de seis mil doscientos militares, civiles y personal de apoyo de todos los departamentos militares y componentes del área de defensa. Este cibercomando estaría plenamente operativo en 2018, aunque ya se están empleando mecanismos al servicio de los objetivos de la Administración en todo el espectro de sus operaciones cibernéticas.

Las operaciones en el ciberespacio motivadas por la amenaza del islamismo radical violento ha provocado que en abril de 2016 el secretario de Defensa, Ash Carter, afirmara que el Pentágono planeaba invertir 35.000 millones de dólares —alrededor de 32.000 millones de euros— en ciberseguridad para reforzar las capacidades militares ofensivas y defensivas.

Estados Unidos destina a I+D+i notables recursos, sabedor de que tales inversiones se traducen en ventajas a corto, medio y largo plazo. Su ecosistema le permite no solo alinear las sinergias del sector privado y del público, sino mantener continuamente engrasada la maquinaria de la innovación y su encaje en el mercado, nutriéndose, además, de iniciativas foráneas a las que metaboliza vía inversiones de capital-riesgo.

Canadá[73] dispone de un Plan de Acción en materia de ciberseguridad para el periodo 2015-2020. Como parte de este Plan, se prevé la inversión de 2.009 millones de dólares (1.393 millones de euros), de los cuales 1.513 millones de dólares (1.049 millones de euros) se destinarán a la defensa y 439 millones de dólares (304 millones de euros) al aumento de la seguridad nacional.

[73] http://budget.gc.ca

Otros Estados del continente americano también están planeando su esfuerzo para invertir en ciberseguridad, incluido el capítulo de alguna línea de I+D+i. Prácticamente todos manifiestan interés por este frente, aunque el estado de madurez en Latinoamérica y Caribe no es homogéneo.

Hay que reseñar que la Organización de Estados Americanos (OEA), con la que las estructuras de la ciberseguridad nacional española, particularmente a través de INCIBE, mantienen una creciente colaboración, tiene en su hoja de ruta acciones al respecto, aunque muy vinculada con la protección de infraestructuras críticas y la persecución del ciberdelito y no tanto en lo referente a la ciberdefensa militar. Los países de la «vieja Europa» también están realizando esfuerzos en varios frentes.

Reino Unido[74], hoy más de actualidad que nunca por el *Brexit*, es un Estado que considera la buena gestión de su ciberseguridad como un valor diferencial en lo social y lo económico. Invertirá, entre 2015 y 2020, 1.900 millones de libras esterlinas (2.225,5 millones de euros) en su protección frente a ciberataques y en el desarrollo de capacidades soberanas en el ciberespacio. Espera generar por ello más de cien mil empleos directos.

En abril de 2016, el Gobierno británico anunció una inversión de 40 millones de libras (46,8 millones de euros) para el *Cyber Security Operations Centre* (*CSOC*), como parte de sus planes para referenciar las capacidades de ciberseguridad operativa de su Ministerio de Defensa. Y en octubre de ese mismo año, el secretario de Defensa, Michael Fallon, asignó 265 millones de libras (293,4 millones de euros) a este Ministerio para fines de ciberseguridad.

Reino Unido dispone de un ramo industrial orientado a la ciberseguridad, que es un ingrediente esencial para gozar de una razonable independencia tecnológica en algunos frentes de la ciberdefensa.

En junio de 2016, Francia[75] anunció una inyección de 1,5 millones de euros para aumentar sus capacidades de defensa en la «guerra cibernética», algo señalado como estratégicamente prioritario por el ministro de Defensa del país galo. El presupuesto francés de 2016 para la defensa alcanza los 32.000 millones de euros, manifestándose un fuerte compromiso con la modernización.

Alemania[76] es otro Estado nuclear de la Unión Europea. Su ministra de defensa dio a conocer en abril de 2016 los planes para establecer una nueva fuerza cibernética para mejorar la eficacia de defensa de las Fuerzas Armadas, el *Kommando Cyber- und Informationsraum* (*KdoCIR*). Este Comando para la Ciberseguridad y la Información tendrá acceso a unos fondos de inversión de más de 1.000 millones de euros y sus operaciones tendrán el centro de mando en Bonn para supervisar las tareas operativas como la cibernética,

[74] http://blog.rielcano.org
[75] http://www.defense.gouv.fr
[76] http://faz.net

informática, de comunicaciones militares e información geológica. A tal fin, las capacidades TI existentes de la *Bundeswehr* (Fuerzas Armadas) se agruparán a partir de abril de 2017 dentro de la nueva rama de la cibernética e información espacial (CIR) y se asignará un total de trece mil quinientos puestos de otras ramas CIR, que será dirigida por un inspector con el grado de teniente general.

Para proveer de personal a este «ciberejército» se tiene previsto crear en 2018 un grado específico en la Universidad del Ejército alemán en Munich, donde se aspira a formar también un *cluster* de ciberdefensa con participación de empresas del sector privado.

Estas iniciativas se unen a la campaña de reclutamiento de efectivos en el campo de la ciberseguridad, que cuenta con un presupuesto de 3,6 millones de euros, y a la creación del Departamento Cyber/TI (CIT) dentro del Ministerio de Defensa con un director de la Información al frente que asumirá la responsabilidad.

Italia[77] destina menos recursos a TIC que Francia y Alemania. Su presupuesto en I+D+i orientado a la ciberdefensa y a la ciberdefensa en sí es limitado. En 2015 el presupuesto general militar alcanzó los 1.000 millones de euros y en 2016, según las informaciones disponibles, tiene presupuestados 2.000 millones para ciberseguridad, defensa y cultura. En abril de ese mismo año se presentó el «Framework Nazionale per la Cyber Security».

Si vamos a otro rincón del globo, llegamos a Australia[78]. En abril de 2016 se anunció el desarrollo de una nueva estrategia contra ciberataques para el periodo 2016-2017, que contará con un presupuesto de 230 millones de dólares (157,4 millones de euros) para la creación de cien nuevos puestos de trabajo y aumentar las capacidades gubernamentales de ciberseguridad. Esta inversión complementa la que se deduce de las medidas para la próxima década centradas en la mejora de las capacidades cibernéticas y de inteligencia de defensa, contenidas en el Libro Blanco de Defensa 2016.

La nueva estrategia también incluye el fortalecimiento de las ciberdefensas, la creación del ciberembajador y la designación de un especialista para asistirlo en la materia.

El esfuerzo en ciberseguridad de otros países, como Turquía o Japón, no es fácilmente cuantificable, y menos en I+D+i. Sí, ciertamente, puede afirmarse que el segundo mencionado, Japón, país altamente tecnificado y con un potente sector industrial de TIC, seguramente atenderá a través de su Plan Nacional del Ministerio de Defensa a diez años (dividido en dos periodos de cinco, 2014-2018 y 2019-2023) la potenciación de las capacidades de ciber-

[77] http://www.cybersecurityframework.it ; http://sicurezzanazionale.gov
[78] http://www.zdnet.com

defensa en el contexto de nuevas capacidades de guerra y la creación de una «Fuerza Dinámica Conjunta de Defensa» (*Dynamic Joint Defense Force*).

Rusia es una potencia que utiliza la fuerza militar. No es conocido su nivel de inversión en ciberseguridad y ciberdefensa; sin embargo, fuentes cercanas a su Ministerio de Defensa han declarado a una publicación especializada en ciberseguridad[79] que podría estar entre los 200 y 250 millones de dólares USA (entre 180 y 225 millones de euros) al año.

Sobre China tampoco hay demasiados datos contrastables. Este país dispone de un gran sector de TIC y los analistas no dudan en afirmar que sus inversiones en I+D+i en ciberseguridad son considerables y crecientes. China dispone de estructuras en consonancia con el tamaño del país.

En marzo de 2016, anunció la puesta en marcha de su primera organización pública para la ciberseguridad, *The Cyber Security Association of China*, compuesta por instituciones académicas, expertos y empresas de Internet. La organización se centra en promover la autodisciplina en la industria, a fin de acelerar el establecimiento de estándares en ciberseguridad y promover la cooperación internacional. El objetivo último es salvaguardar la ciberseguridad del país y la conversión de China como una gran potencia en Internet, atrayendo además a empresas de ciberseguridad vanguardistas y talento.

Ya en febrero de 2016, China aprobó una inversión destinada a ciberseguridad con un capital inicial de 300 millones de yuanes (alrededor de 41 millones de euros)[80].

Irán es mención obligada. Cuando en 2013 Hasan Rohani asumió el cargo de presidente de Irán, según un informe de la organización británica *Small Media*, titulado «Iranian Internet Infraestructure and Policy Report»[81], los fondos para ciberseguridad de este país para el bienio 2013-2014 alcanzaron los 42.073 millones de riales iraníes (algo más de 1 millón de euros). Al año siguiente se disparó hasta los 178.800 millones de riales iraníes (algo más de 5 millones de euros); y en 2015-2016 llegó a los 550.000 millones de riales iraníes (aproximadamente 15,5 millones de euros), lo que supone un incremento del 1.200 % en solo tres años.

Muy posiblemente, los ataques de Stuxnet (2010) y Flame (2012), y los escándalos de las filtraciones de la *NSA* en Estados Unidos, hayan jugado un papel relevante en la fortificación de las ciberdefensas iraníes frente a ciberataques, específicamente cibersabotajes. Y no es de dudar que hayan sido un estímulo para sentar las bases de una capacidad ofensiva, rasgo que hoy hay que entender como un indicador del grado de avance de un Estado. Sea

[79] http://ieee.es

[80] http:/www.gadgetsnow.com/tech-news/China-launches-first-cybersecurity-organization-report/articleshow/51561355.cms ; http://www.scmagazineuk.com

[81] http://europe.newsweek.com

con los productos, herramientas y servicios mediante una I+D+i propia o de terceros.

Y si Irán es cita obligada, también lo es Arabia Saudí[82], que en el año 2015 detectó más de 160.000 ataques al día, convirtiéndose en el país más atacado de Oriente Medio, según las cifras disponibles. La mayoría de los objetivos se concentraron en los sectores de las telecomunicaciones, el petróleo, el gas y la banca.

Se espera que el mercado de ciberseguridad de Arabia Saudí pase de los 1.510 millones de dólares de 2013 hasta los 3.480 millones de dólares en 2019, con una tasa de crecimiento anual del 14,50 %. Esta es una señal inequívoca del esfuerzo inversor de las agencias gubernamentales y Gobiernos locales de este país.

India es otro país que presta una extraordinaria atención a la ciberseguridad. En 2014-2015, su departamento de TI destinó 1.160 millones de rupias indias (15,7 millones de euros) a la seguridad cibernética. Además se ha propuesto establecer un Centro Nacional de Coordinación Cibernética (CNCC) con un presupuesto separado de 10.000 millones de rupias indias, más de 136 millones de euros[83].

De acuerdo con el informe del Consejo de Seguridad de Datos de la India (*SDIC*), el tamaño del mercado de la ciberseguridad de este país es de aproximadamente 4.000 millones de dólares (más de 3.500 millones de euros), y se espera que crezca hasta los 35.000 millones de dólares (32.000 millones de euros) en el año 2025[84].

Asimismo, India ha estado buscando ayuda para formarse en las mejores prácticas en seguridad cibernética. A principio de 2016, una delegación oficial encabezada por funcionarios del Gobierno indio y empresarios del país visitó Londres, La Haya e Israel. Según diversos medios, Israel ha ofrecido colaboración a la India para preparar un plan de ciberseguridad integral[85].

India, considerado por las multinacionales como un país atractivo para la deslocalización del desarrollo de aplicaciones, dispone de una ingente cantidad de profesionales muy bien formados en matemáticas y en ciencias de la computación. Su industria de ciberseguridad destaca en no pocos frentes, uno en especial es el de las herramientas IRM con seguridad de grado militar.

No sería de recibo concluir sin mencionar a Israel, el Estado que desde poco antes de la explosión del uso comercial de Internet es el símbolo del éxito del fomento estatal de la I+D+i en ciberseguridad y del triunfo comercial de

82 http://www.think-progress.com ; http://www.mcit.gov.sa
83 http://articles.economictimes.indiatimes.com
84 http://www.enterpriseinnovation.net
85 http://economictimes.indiatimes.com

empresas especializadas, hoy multinacionales sólidamente asentadas y/o adquiridas por las grandes multinacionales de la industria TIC.

En el ejemplo de Israel trasciende el hecho de la I+D+i, porque ha sabido construir un ecosistema que ha culminado en un modelo de CPP digno de elogio, motivo por el que se estudiará su caso en el siguiente apartado.

Conclusión

La inversión de los Estados, las organizaciones internacionales y las supranacionales en I+D+i orientada a la ciberseguridad y a la ciberdefensa no es, en líneas generales, un capítulo presupuestario asentado. Al menos no lo es como en otros frentes más experimentados en el contexto de los complejos industriales de las defensas y los centros de investigación y universidades.

Las estructuras públicas de la ciberseguridad y la ciberdefensa tienen pocos años de vida y en la mayoría de países todavía están sometidas a cambio y no han empezado a engranarse de modo óptimo en las maquinarias de I+D+i.

Si a ello le sumamos que el ciberespacio es especialmente dinámico, sus fundamentos no estuvieron orientados a la seguridad de la información (salvedad hecha de la disponibilidad de las comunicaciones) y al uso comercial generalizado, y que la criticidad de la ciberseguridad todavía no ha sido completamente metabolizada ni por los Estados ni por las industrias y los centros de conocimiento, y convertida en procesos ágiles que permitan a unos prever y saber qué quieren en grano fino y a otros servirlo y proponer avances en una suerte de mercado estable y creciente, la conclusión está a la vista: queda casi todo por hacer en una sociedad inmersa en un proceso imparable de transformación digital que traerá, sin duda, cambios en el proceso clásico de I+D+i, en la localización y aprovechamiento de las canteras de talento y en la forma en la que se manifiesten las amenazas y ataques, porque en un futuro no muy lejano casi cualquier persona tendrá medios a su disposición para ciberatacar, configurándose un escenario de asimetría extrema.

El papel de la colaboración público-privada en el proceso de I+D+i

La colaboración público-privada (CPP) está ligada a las sociedades que aspiran a lograr cotas crecientes y sostenibles de bienestar, guardando un equilibrio entre el alcance de los poderes del Estado y las capacidades de la iniciativa privada.

La base del modelo es, por tanto, la colaboración leal entre las estructuras públicas y las organizaciones que operan en el sector privado.

Las sociedades más evolucionadas son aquellas que se han dotado de un ecosistema sostenible para la CPP; es decir, uno en el cual ambas partes obtienen ventajas y beneficios directos e indirectos conforme a derecho y

a buenas prácticas. Este ecosistema, además, se extiende al escenario de relaciones exteriores y al de las organizaciones supranacionales e internacionales, como no puede ser de otra manera en la era de la globalización.

La CPP es un mecanismo nuclear en la ya mencionada Estrategia Española de Ciencia y Tecnología e Innovación 2013-2020. Y en lo que toca a la ciberseguridad, forma parte de la doctrina de la Estrategia de Ciberseguridad Nacional-ECSN, que el Gobierno de España define como «... El marco de referencia de un modelo integrado basado en la implicación, coordinación y armonización de todos los actores y recursos del Estado, en la colaboración público-privada y en la participación de la ciudadanía». Algo similar expresó la Unión Europea en su Estrategia Europea de Ciberseguridad, y lo mismo han hecho numerosos países en sus documentos correspondientes.

Si hay un frente de la ciberseguridad en el que la CPP adquiera una especial significancia, ese es el de la I+D+i. Así se expresa en el Objetivo V de la ECSN, centrado en «Alcanzar y mantener los conocimientos, habilidades, experiencia y capacidades tecnológicas que necesita España para sustentar todos los objetivos de ciberseguridad», al indicar que «... Se requiere fomentar y mantener una actividad de I+D+i en materia de ciberseguridad de manera efectiva». Y que para ello «... «Será necesaria una adecuada coordinación del conjunto de agentes implicados en las TIC, facilitando la colaboración entre empresas y organismos públicos de investigación...».

Más adelante, en la Línea de Acción 5, «Seguridad y resiliencia de las TIC en el sector privado», se resalta la necesidad de impulsar la seguridad y la resiliencia de las infraestructuras, redes, productos y servicios empleando instrumentos de cooperación público-privada.

Esta Línea de Acción está íntimamente ligada a la Línea de Acción 6, «Conocimientos, Competencias e I+D+i», en la que se expresa la necesidad de promover la capacitación de profesionales, impulsar el desarrollo industrial y reforzar el sistema de I+D+i en materia de ciberseguridad.

También hay referencias a la CPP y la I+D+i, ya directas ya indirectas, en la Agenda Digital para Europa, la Agenda Digital para España y el Plan de Confianza en el Ámbito Digital.

Por tanto, y en el caso de España, está sobradamente justificada la obligación de poner a punto un ecosistema de CPP para alcanzar una buena posición en I+D+i en la ciberseguridad a efectos generales y también en la defensa y en las operaciones militares. Y no hay que olvidar aquí que, al igual que la mayoría de las infraestructuras críticas existentes en España se gestionan por multinacionales cotizadas, también el mayor porcentaje de la inversión y el gasto en I+D+i en ciberseguridad la realizan compañías de ciberseguridad y de TIC (en general, también multinacionales cotizadas), cuyo beneficio mercantil no proviene de las adquisiciones de productos y servicios por la defensa, aunque el germen del ciberespacio fuera, en origen, una solución

académica para minimizar riesgos asociados con la indisponibilidad de la red de comunicaciones académico-militar ARPANET, y por mucho que ciertos desarrollos de fabricantes destacados de TIC y de ciberseguridad de la llamada «era Internet», hoy liberados para uso civil, hayan tenido su génesis en la cobertura de necesidades de la inteligencia y de la defensa militar.

En la actualidad, se tiene la sensación de que el llamamiento por parte de las áreas no civiles de los Estados al sector civil para que se propongan soluciones a necesidades de las defensas no es el motor principal que mueve la I+D+i y que, a la postre, se traduce en avance social. Quizá esta circunstancia, que pudiera ser no coyuntural, deba interpretarse como un rasgo de la transformación digital.

Iniciativas foráneas

Hay algunos ejemplos ilustrativos de iniciativas de CPP en I+D+i, o en los que la I+D+i encuentra acomodo. El más significativo por su dimensión, y en el que nos centraremos, es el emprendido por el Estado de Israel en el desierto del Neguev, en el que se ha creado un parque especializado en ciberseguridad, denominado CyberSpark[86], que aúna en una misma localización geográfica a instituciones académicas (la Universidad Ben Gurion), la industria tecnológica y las Fuerzas de Defensa de Israel (FDI).

La intención del Gobierno israelí es trasladar a las inmediaciones del Parque, inaugurado en 2016, a unos treinta mil soldados de la Unidad 8200 —incluidas las unidades de seguridad cibernética— que, a su vez, trabajarán estrechamente con la Autoridad Nacional de Seguridad Cibernética.

CyberSpark ya ha atraído a numerosas empresas multinacionales, con las que las instituciones públicas israelíes mantienen una relación *win to win*. Además, en el Parque se han instalado tres incubadoras y existen seis *startups* que dan empleo a unas mil doscientas personas.

Israel es un país que lleva a gala su potencial en ciberseguridad, una industria que se constituye en uno de los motores de su economía: genera más de 6.000 millones de dólares al año, exporta por valor de 3.500 millones de dólares y cuenta con unas cuatrocientas treinta empresas instaladas y cuarenta centros de ciberseguridad y de I+D de multinacionales extranjeras.

CyberSpark encuentra sitio en el Parque de Tecnologías Avanzadas (*ATP*), inaugurado en 2013 por el primer ministro Benjamin Netanyahu.

Esta experiencia es actualmente una de las más avanzadas a nivel mundial en lo que respecta a la CPP en I+D+i en ciberseguridad y ofrece notables ventajas a Israel, ya que potencia su industria de ciberseguridad en el circuito internacional y, al tiempo, la integra con otras áreas de las TIC, como las

[86] http://cyberspark.org.il

vinculadas con la *IoT*, las infraestructuras críticas, el sector financiero, el de telecomunicaciones o el espacio exterior.

En principio, «CyberSpark no está comprometido con cualquier operación o desarrollo ofensivo»[87].

Iniciativas supranacionales

En Europa se ha creado la Organización Europea de Ciberseguridad (European Cyber Security Organization, *ECS*)[88], una entidad autofinanciada y sin ánimo de lucro en la que participan asociaciones empresariales, grandes compañías y pymes, centros de investigación y universidades, que se cataloga como asociación público-privada sobre ciberseguridad europea.

La Comisión Europea firmó en julio de 2016 un acuerdo CPP con la *ECS* orientado a la promoción, la investigación y la innovación en seguridad cibernética. Para guiarse en los objetivos marcados se ha formado un órgano, denominado *Partnership Board*, integrado por miembros de la Comisión Europea y miembros de la *ECS*, que llevará a cabo un análisis exhaustivo del programa de trabajo en ciberseguridad del plan Horizonte 2020, la ejecución del gasto total y todas las materias relacionadas con la I+D, además de acomodar las actualizaciones necesarias del plan de trabajo plurianual y de realizar un seguimiento de los compromisos contraídos en el acuerdo público-privado firmado. La inversión total comprometida podría alcanzar los 1.800 millones de euros hasta 2020.

El Instituto Nacional de Ciberseguridad, INCIBE, se ha adherido a *ECS* como punto de contacto oficial de España junto a la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información (SETSI) y el Centro para el Desarrollo Tecnológico Industrial (CDTI), en esta asociación en la que hay entidades españolas participantes que han trabajado, trabajan o pueden trabajar en la ciberdefensa española.

INCIBE también ha promovido la creación en España de RENIC, la Red de Excelencia Nacional de Investigación en Ciberseguridad, que ya es miembro de pleno derecho de la *ECS*.

La *ECS* articulará sus acciones en base a las siguientes líneas de acción:

- Colaborar con la Comisión Europea y las Adminstraciones Públicas nacionales para promover la investigación y la innovación (I+I) en ciberseguridad.
- Desarrollar e invertir en proyectos piloto de demostración y de impulso al mercado para facilitar llevar la innovación al mercado de ciberseguridad.
- Favorecer la competitividad y el crecimiento de la industria de la ciberseguridad en Europa (grandes empresas y pymes) para facilitar a los

[87] Declaraciones a *SIC* (n.º 120) de Roni Zehavi, *CEO* de CyberSpark.
[88] ECS: www.ecs-org.eu

usuarios finales/operadores tecnologías innovadoras, aplicaciones, servicios y soluciones.
- Apoyar la implantación en el mercado de las mejores tecnologías innovadoras y servicios de ciberseguridad para su uso profesional y privado.
- Promover y ayudar en la definición e implementación de una política industrial de ciberseguridad para fomentar el uso de soluciones de ciberseguridad, así como soluciones TIC seguras y confiables a escala europea para aumentar la autonomía digital.
- Apoyar el desarrollo y los intereses de todo el ecosistema de la ciberseguridad y la seguridad de las TIC.

La financiación de esta iniciativa de CPP se hará del siguiente modo: por parte de la Unión Europea se fija una inversión de 450 millones de euros. Por parte de los actores representados en la *ECS* se liberarán tres euros por cada euro invertido por la Unión Europea. Se espera, por tanto, que este mecanismo desencadene una inversión total, como ya hemos comentado, de 1.800 millones de euros de aquí al año 2020.

España

La inversión en ciberdefensa es baja —y manifiestamente mejorable— para un país con la posición de España, al igual que la dedicada a I+D+i, no registrándose además iniciativas evolucionadas de CPP. Por decirlo de alguna manera: si se destinara a la ciberseguridad militar las decenas de millones de euros que cuesta adquirir un solo cazabombardero o un tanque o los elementos no ciber de un barco de guerra, España sería una potencia francamente destacada; hecho que es extrapolable a muchos otros países, incluso europeos. Aunque semejante decisión hoy debería estar avalada por un cálculo de riesgos en el que se analizaran las ciberamenazas, la probabilidad de materialización, el valor de los activos (entre los que está la información) que pudieran verse afectados, el impacto y el problema que pudiera causar a España, directa o indirectamente, disponer de un cazabombardero, un tanque o un barco menos (si es que el momento actual fuera propicio para las adquisiciones).

No obstante lo dicho, el Mando Conjunto de Ciberdefensa (MCCD) firmó en 2016 un acuerdo a tres años con opción de prórroga con INCIBE para, entre otras acciones, colaborar en la generación de conocimiento científico y tecnológico mediante el concurso de equipos de investigación del ámbito académico, apoyar la transferencia de los resultados de la I+D+i a las Administraciones y llevar a cabo iniciativas conjuntas de formación de profesionales en ciberseguridad y ciberdefensa.

Igualmente, el MCCD firmó en 2016 un acuerdo con el Centro Criptológico Nacional (CCN) por el que estableció un marco de colaboración en varios frentes, uno de ellos centrado en el desarrollo de proyectos tecnológicos.

El MCCD ha activado acuerdos con algunas universidades españolas para dotarse de algunos instrumentos esenciales para el cumplimiento de su misión. Hay dos iniciativas que podemos referenciar, una centrada en el desarrollo de una herramienta *software* de generación de escenarios de ciberdefensa, que se integre en el campo de maniobras del MCCD, y la otra enfocada al desarrollo de una solución orientada a la visualización completa de la situación de la ciberdefensa en un momento dado. Ambos proyectos fueron presentados en las II Jornadas del MCCD en mayo de 2016.

De otro lado, INCIBE, que ha lanzado diversas acciones para estimular el crecimiento de la I+D+i, y está potenciando la conformación de un Polo Tecnológico Nacional de Ciberseguridad, a modo de *atractor* de los distintos agentes involucrados, para apoyar la industrialización, I+D+i en la ciberseguridad, y conectarla con rutas de internacionalización, terreno en el que colabora ICEX España Exportación e Inversiones.

A estas iniciativas mencionadas se suman otras estrictamente privadas, llevadas a cabo por algunas multinacionales de origen español, principalmente centradas en promover y/o adquirir *startups* en nuevos frentes de la ciberseguridad. Estas iniciativas, aunque no se enmarquen en la CPP estrictamente, tienen implicaciones en parte del ecosistema en el que encuentra sitio esta y la I+D+i, puesto que algunas toman forma en el marco de la colaboración entre la industria privada usuaria de TIC, la industria proveedora de TIC y servicios, la universidad y la investigación, tratando de estimular nuevas ideas y enfoques que puedan cristalizar en futuras líneas de desarrollo industrial, principalmente en el control de ciberfraude, la identificación y autenticación enfocadas al *scoring*, la minimización de riesgos intencionales, la ingeniería de datos y la analítica predictiva.

Las multinacionales de sectores estratégicos (también las de origen español) están invirtiendo en I+D+i para ir dominando su transformación digital. Y en sus enfoques han incorporado la gestión de riesgos de ciberseguridad.

Estos movimientos, en principio ajenos en el momento presente a la ciberdefensa militar, quizá deban ser analizados por especialistas en la ciberseguridad militar porque van a delimitar el ecosistema digital de la sociedad a la que nos dirigimos, en la que la manifestación de conflictos ciberespaciales y ciberfísicos no entenderá de barreras conceptuales y potestativas, ni de la naturaleza de las organizaciones que han de defenderse y atacar en un marco de acuerdos intersupranacionales y cualquier investigación, disciplina, técnica o tecnología que facilite información y ventaja ha de valorarse.

Retos, riesgos y oportunidades

Las estructuras de la defensa están inmersas en el proceso de transformación digital que afecta a toda la sociedad y que trae consigo la analítica

avanzada de macrodatos, la robótica aplicada a casi todos los escenarios, la inteligencia artificial, la computación cognitiva, las tecnologías de comunicaciones avanzadas que soporten servicios de misión crítica incompatibles con la indisponibilidad y resilientes.

Por otro lado, gran parte de las estructuras de la defensa, a efectos generales, son usuarias de tecnologías de la información y comunicaciones de uso civil que padecen defectos de diseño en materia de seguridad, debido principalmente a los tiempos de mercado y la presión de los inversores.

En España (y a buen seguro también en otros países) la industria de la defensa en su conjunto no fue muy madrugadora a la hora de enarbolar la bandera de la ciberseguridad, que se configuró como ramo específico gracias a algunas pequeñas compañías especializadas muy competitivas y a algunos grupos pioneros de departamentos y áreas de grandes empresas. La facturación en 2015 de este ramo oferente en España supera los 1.000 millones de euros. Podemos formularnos la siguiente pregunta a modo de reflexión: ¿qué porcentaje de esa cifra se debe a inversiones de las estructuras del Ministerio de Defensa ampliamente entendidas y de la ciberdefensa militar en concreto?

El reto aquí es conformar en la industria de la defensa un ecosistema viable de empresas de ciberseguridad o con línea de ciberseguridad gestionadas por personas y equipos de personas que estén interesados en innovar y no en mantener el *status quo*. Tal ecosistema debería estar preparado para renovarse completamente (como el ave Fénix) sin empezar de cero. Y aquí juegan un papel esencial las empresas completamente establecidas, que son capaces de dar garantías financieras, continuidad a las líneas de industrialización, diagnosticar con una orientación a la mejora y la modernización, ayudar en la prescripción, facilitar la identificación de nuevos productos prometedores que aparecen en el mercado, realizar investigación y desarrollo... pero que hace ya tiempo dejaron de ser organizaciones punteras en innovación.

La oportunidad que se abre brinda la posibilidad de enfocar la fortaleza de la ciberseguridad de los sistemas TIC de la ciberdefensa, ampliamente entendidos, no en base al secreto y al número restringido de proveedores, sino en base a la verificación efectiva y formal del nivel de seguridad que se precisa. Y facilitar dichos sistemas, servicios y productos, y no otros, a quienes los tengan que usar.

Este hecho afecta a tecnologías concretas, que deberían estar holgadamente atendidas en los esfuerzos de I+D+i de la ciberdefensa[89]:

– Comunicaciones seguras, autenticadas y auditadas en las redes, más allá de las de combate.

[89] Los frentes tecnológicos aludidos han sido analizados por el profesor Jorge Dávila Muro a lo largo de los años en su sección fija de *SIC* (www.revistasic.com) denominada «En construcción».

- Equipos/*gadgets* personales y de entretenimiento certificados para su uso exclusivo en entornos militares. El BYOD por ahora no puede ser una opción.
- Sistemas inalterables, redundantes y a «toda prueba» para la auditoría de comunicaciones y de documentos digitales (toda la información debería estar clasificada en su justo nivel y poder ser «atribuida» a alguien y con el control de quién la ve y qué hace con ella). Los sistemas modernos IRM están tecnológicamente maduros.
- Sistemas de actualización y mantenimiento remotos de equipos a prueba de intrusos y de errores. No debería arrancar ningún artefacto TIC sin que todos los componentes del mismo estén activamente verificados (*secure boot*).
- Sistemas que aseguren la integridad de las redes IT.
- Sistemas de identidad digital y personal intransferibles.
- Técnicas IT de engaño que ayuden a eliminar «canales laterales» de ataque que pudiesen poner de manifiesto directa o indirectamente actividades de interés militar por su reflejo en las actividades de la red.
- Sistemas TIC de contrainteligencia militar (pasiva y activa).
- Sistemas de todo tipo redundantes a prueba de fallos, una resiliencia automática y puntual, así como todas las medidas que permitan siempre tener un plan B y otro plan C en tiempo.
- Sistemas para el entrenamiento ciber de usuarios de todos los niveles.
- Investigar los tipos de analistas, especialidades de ciberseguridad y de perfiles de especialistas que va a necesitar a largo plazo la ciberdefensa.

La viabilidad de llevar esto a efecto no puede conseguirse en un mercado clásico, sino en uno diversificado en el que realmente la ciberdefensa contribuya y participe en iniciativas CPP de I+D+i en cuyo contexto tengan un papel creativo esos expertos con habilidades especiales a los que llamamos *hackers* y que siguen evolucionando con los tiempos. En suma, estudiar fórmulas para suscitar en la sociedad civil el interés por compartir sus ideas/innovaciones en ciberseguridad con la ciberdefensa.

Hay cuatro campos, entre otros, que conviene tratar en iniciativas de CPP + I+D+i, uno es el de la atribución de acciones en el ciberespacio, se decida o no dar curso a la apertura de conflicto. Se requiere, por tanto, estudiar y poner a punto sistemas de reconocimiento de ataques (y su origen) en «tiempo real» que involucren a la ciberdefensa militar y a otras estructuras de la ciberseguridad nacional, o solo a la ciberdefensa militar.

El segundo, aunque esté en fases muy tempranas, es el de la computación cuántica y sus implicaciones en la ciberseguridad, muy concretamente en lo que atañe a la criptografía y el criptoanálisis.

El tercero presenta hoy un grado de complejidad notable: cómo hacer más eficiente el sistema de certificación funcional de la seguridad de productos TIC. En el estado actual, los tiempos requeridos y el esfuerzo inversor son,

en ocasiones, disuasorios en términos de mercado sin que exista certeza por parte de la empresa que pone en evaluación sus productos de que serán adquiridos.

El cuarto pasaría por estudiar con un enfoque interdisciplinar qué protocolos y sistemas de notificación serían los más adecuados para que las estructuras actuales de la ciberseguridad puedan funcionar del modo más eficiente posible como un sistema integrado de ciberseguridad nacional, y señalamos aquí la defensa militar, la inteligencia (Centro Nacional de Inteligencia-CNI), la protección de infraestructuras críticas (Centro Nacional para la Protección de Infraestructuras Críticas-CNPIC) y la seguridad interior.

Y en último término habría espacio en la I+D+i para estudiar muy por lo menudo, y aunque el asunto exceda con mucho lo ventilado en este capítulo, las implicaciones (técnicas, tecnológicas, sociales y económicas) que tendrá la puesta en explotación de sistemas de ciberseguridad desatendidos, autónomos y el uso de robots y asistentes cibernéticos de ciberseguridad.

Como es sabido, la mecanización esclaviza y la automatización excluye. Lo que está sucediendo en esta fase del *Homoceno* es que en los sistemas productivos de la sociedad global se puede prescindir de fuerza de trabajo. Y esos millones de personas, jóvenes en base a las expectativas de vida actuales, y con conocimientos y experiencia, antes de llegar a edades muy avanzadas, pueden ser útiles. La I+D+i y la CPP pueden ser instrumentos para aprovechar la sabiduría y la destreza que atesoran y, ya que hablamos de ciberseguridad, ganarlos para la noble causa de la concienciación.

Interdependencia entre innovación y ciberseguridad

En las modernas economías basadas en el conocimiento, este es reconocido como el propulsor de la productividad y la creación de valor a través de la innovación, que se configura así como la piedra angular del crecimiento económico y por ende del bienestar material de la sociedad[90]. Hoy día el ciberespacio es el soporte fundamental de los procesos de innovación tanto en bienes como en servicios. La existencia de redes de comunicaciones universales, abiertas e interoperables, hace posible una potencial creación de valor de gran magnitud[91], solo condicionada a la existencia de suficiente confianza en esas redes. En otras palabras, un ciberespacio seguro significa una garantía para los agentes económicos y ello se ha de traducir en mayor inversión, mayor transparencia y dinamización de los mercados y, en

[90] —, «The Knowledge-based Economy», Organisation for Economic Co-Operation and Development, París, 1996. Disponible en: https://www.oecd.org/sti/sci-tech/1913021.pdf

[91] La Ley de Metcalfe establece que el valor de una red de telecomunicaciones es proporcional al cuadrado del número de usuarios o nodos conectados a dicha red. Atribuida a Robert Metcalfe, esta ley explica muchos de los efectos económicos producidos por las redes de comunicación como Internet o sus derivados la *World Wide Web* y las redes sociales.

consecuencia, crecimiento económico y prosperidad. Recíprocamente, es la innovación en ciberseguridad una de las actividades que permiten conservar la estabilidad del ciberespacio en términos de seguridad, de manera que sea confiable para los usuarios del mismo. Se da, pues, una realimentación positiva entre los procesos de innovación y de ciberdefensa.

La idea de que un ciberespacio seguro significa una ventaja económica competitiva para España ya había sido apuntada por la antigua Estrategia Española de Seguridad de 2011[92]. La actual Estrategia de Seguridad Nacional va más allá al señalar al «espionaje económico», que aprovecha las posibilidades que ofrecen las tecnologías de la información y las comunicaciones, como una amenaza cuyo «impacto potencial es cada vez mayor por su capacidad de dañar el sistema económico y afectar al bienestar de los ciudadanos»[93].

Pero será en particular la Estrategia de Ciberseguridad Nacional la que recoja explícitamente y en mayor extensión estos planteamientos. En su prólogo, el presidente del Gobierno afirma que «para España, los avances en el ámbito de la ciberseguridad contribuyen además a incrementar nuestro potencial económico, ya que promueven un entorno más seguro para la inversión, la generación de empleo y la competitividad»[94] y que «únicamente si nos comprometemos de forma decidida con la seguridad del ciberespacio, la competitividad de nuestra economía y la prosperidad de España serán una realidad posible»[95]. Más aún, la Estrategia considera la ciberseguridad como «una necesidad de nuestra sociedad y de nuestro modelo económico»[96] y llama a la unidad de acción entre los diferentes actores, tanto públicos como privados, con el fin de alcanzar ese estado de ciberseguridad que a todos ha de beneficiar. Así, sostiene que «el fortalecimiento de la ciberseguridad proporcionará a las Adminstraciones Públicas, al tejido industrial y empresarial, a la comunidad científica y a los ciudadanos en general una mayor confianza en el uso de las TIC» y que «para ello, los organismos públicos responsables trabajarán en coordinación con el sector privado y con los propios ciudadanos para garantizar la seguridad y la confiabilidad de los sistemas que sustentan la llamada Sociedad de la Información»[97].

Pioneros en este concepto han sido países como Reino Unido y Estados Unidos. El primero aprobó en noviembre de 2011 su Estrategia Nacional de Ciberseguridad, cuyo primer objetivo consistía precisamente en «luchar contra el cibercrimen y convertir al Reino Unido en el lugar más seguro del mundo para hacer

92 EES, pp. 65 y 68.
93 ESN, p. 34.
94 ECSN, p. iv.
95 ECSN, p. v.
96 ECSN, p. 10.
97 ECSN, p. 21.

negocios en el ciberespacio[98]». En Estados Unidos, la Casa Blanca hizo pública en 2011 su «Estrategia Internacional para el Ciberespacio», la cual defendía que «el ciberespacio sirve a las necesidades de la economía y de los innovadores», siendo la ciberseguridad un factor crítico no solo para la seguridad nacional en términos generales sino para la seguridad económica en particular[99]. Por su parte, el Departamento de Comercio del Gobierno de los Estados Unidos reconocía que internet es una pieza central en la política norteamericana de promoción del crecimiento económico de la nación y de orientación del modelo económico al mantenimiento del liderazgo de Estados Unidos durante el siglo XXI. De ahí que ese departamento ministerial oriente su esfuerzo normativo, aunque limitándose a Internet sin abarcar la totalidad del ciberespacio, a encarar los grandes retos que puedan minar la confianza en la Red, retos entre los que se encuentra la mejora sustancial de la ciberseguridad[100].

Hasta aquí observamos una concepción utilitarista del ciberespacio: se protege porque es garantía de beneficio económico, de lo que se deriva su utilidad social. Sin embargo, *sensu contrario*, encontramos que la innovación constituye un factor necesario, aunque obviamente no suficiente, para hacer posible el estado de ciberseguridad deseado. A escala global se aprecia que alcanzar un determinado estado de ciberseguridad es imposible sin innovación, y se desprende que a escala nacional alcanzar el deseado estado de ciberseguridad es inviable sin una I+D+i propia. Dicho de otra manera, sin una industria nacional de ciberseguridad puntera no es posible la construcción de un sistema nacional de ciberseguridad[101].

Consciente de ello, aunque sin particularizarlo en el caso de la ciberseguridad, el Ministerio de Defensa en su Estrategia de Tecnología e Innovación de la Defensa (ETID) defiende que la innovación «supone, asimismo, una pieza fundamental para promover el crecimiento, la competitividad y la internacionalización de la BTID[102], favorece su capacidad de respuesta ante nuevas necesidades tecnológicas y ayuda a evitar posibles dependencias tecnológicas futuras que condicionen la capacidad de respuesta ante situaciones sobrevenidas o que impliquen un coste excesivo en las adquisiciones»[103].

En este sentido, se constata que los países que están desarrollando un mayor esfuerzo inversor en ciberseguridad están obteniendo un rápido retorno de inversión (ROI) y se están convirtiendo en la referencia en exportación de tecnología, procesos y recursos humanos. Sin embargo, es una realidad que

98 —,«The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world», UK Government, Londres, 2011, p. 8.

99 —, «International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World», The White House, Washington DC, 2011, p. 18.

100 —, «Cybersecurity, Innovation and the Internet Economy», The Department of Commerce Internet Policy Task Force, Washington DC, June 2011.

101 Ciberelcano n.º 14, p. 5.

102 Base Tecnológica e Industrial de la Defensa.

103 ETID, p. 15.

España presenta un déficit en este aspecto, derivado en gran medida del hecho de que los sistemas de transferencia de resultados de la investigación y, en general, las relaciones entre las universidades, los centros de investigación teórica y aplicada, Gobierno y empresa están más desarrolladas y son más fluidas en otros países de lo que lo son en España[104].

Concluimos, pues, que la relación entre ciberseguridad e innovación es de mutua interdependencia, ya que si bien el I+D+i conduce a un entorno ciberespacial más seguro, este, recíprocamente, contribuye favorablemente a la innovación y al crecimiento económico. Por ello, disponer de una industria nacional potente en materia de ciberseguridad no solo es beneficioso para el sistema de ciberseguridad nacional *per se*, sino que la confianza, factor clave en economía, que podría aportar al espacio nacional como lugar seguro, favorecería la inversión y el crecimiento económico, así como, por realimentación, la propia I+D+i en seguridad cibernética.

Conclusión

Tras nuestro análisis de la situación, concluimos que la relación entre I+D+i y ciberseguridad es de mutua interdependencia, en presencia o no de la colaboración público-privada. En este contexto ciberespacial, si bien por una parte el propósito de la innovación es el de fortalecer un estado de ciberseguridad, *sensu contrario*, la ciberseguridad será soporte, garantía de innovación en diferentes ámbitos, lo que constituye un factor de crecimiento económico y bienestar de nuestra sociedad.

Una ciberdefensa eficaz depende no solo de la capacidad de innovación en tecnología, sino además de la capacitación técnica del personal y de la idoneidad de las operaciones defensivas.

El I+D+i en ciberseguridad debe estar alineado con la Estrategia Española de Ciencia, Tecnología e Innovación y orientarse a la consecución de los objetivos fijados por la Estrategia de Ciberseguridad Nacional. En todo caso, se hace preciso definir métricas o indicadores de rendimiento del esfuerzo realizado en I+D+i en ciberseguridad, en base a los resultados obtenidos[105].

El problema de medir, de fijar un patrón de medida y de saber qué medir y cómo, se presenta habitualmente. El ejemplo más claro es la propia ciberseguridad a la hora de establecer controles e invertir en medidas en base al valor de los activos que hay que proteger. El escollo se agrava cuando aparecen en los cálculos los temidos intangibles, que se resisten al análisis «eurométrico» (o «dolarométrico», si lo prefiere el lector).

---

104 Ciberelcano, n.º 13, p. 16.

105 —,«Oslo Manual: The Measurement of Scientific and Technological Activities. Proposed guidelines for collecting and interpreting technological innovation data», OCDE, 1993.

Medir el rendimiento del esfuerzo en I+D+i en ciberseguridad en base a los resultados obtenidos en tiempos parece lo razonable, siempre y cuando presupongamos que los que hayan realizado el esfuerzo en I+D+i hayan justificado la pertinencia de ese esfuerzo, hecho que se encuentra con la misma problemática de medición antes aludida.

Dado que hoy en día el motor de los avances tecnológicos no es la cobertura de necesidades militares sino el rendimiento económico en la sociedad civil, los planes de desarrollo de nuevas capacidades ciberdefensivas deberían contemplar algún esquema de colaboración público-privada ágil y bien preparado para sintonizar con los negocios de la industria.

Ya hay, como hemos mencionado, alguna experiencia (OTAN, por ejemplo, para el aprovechamiento de la propia Alianza, de los aliados y de sus industrias y expertos). En España no se detectan iniciativas completas al respecto, ni parece que el nivel de inversión del comprador sea lo suficientemente elevado como para cerrar el círculo y unir de modo más estrecho a la industria y a los investigadores. Sí hay acuerdos entre compañías y universidades, pero no tenemos ecosistema. Las acciones de CPP emprendidas por la Unión Europea deberían dar un impulso a la creación de un ecosistema sostenible de CPP para la I+D+i en España en el que la ciberdefensa habría de participar de modo destacado, y no exclusivamente en el descubrimiento y/o la obtención de vulnerabilidades no documentadas, sea cual sea el fin.

El compromiso del Estado con la I+D+i en materia de ciberseguridad (línea de acción 6 de la ECSN) debería estar respaldado con una adecuada dotación presupuestaria, que tendría que ser gestionada de manera centralizada por el organismo competente dentro de la estructura de ciberseguridad del Estado.

La ciberdefensa debe escuchar con atención los ecos del futuro en lo que toca a la transformación a la que pueden verse sometidos algunos actores del sector privado; es el caso de los operadores de telecomunicaciones, en contraposición a las grandes compañías digitales (las denominadas informalmente como GAFA: Google, Apple —aunque sea una histórica de las TIC—, Facebook y Amazon), que más allá de las barreras regulatorias, pudieran ir asumiendo un papel dominante en las comunicaciones globales y en la transformación de sectores nucleares como el financiero, el de contenidos y, en general, en la distribución digital de bienes y servicios. Esta circunstancia también tendría consecuencias en el ciberespacio y en la ciberdefensa.

España goza de un tejido profesional de ciberseguridad muy competitivo en todos los estratos, que se ha ido cultivando y curtiendo desde finales de la década de los noventa; hay, por tanto, continuidad intergeneracional y expertos situados en estratos de dirección estratégica, dirección organizativa y en toda la cadena de valor de la gestión técnica y la operación en casi todos los sectores privados y en las Adminstraciones Públicas. Las generaciones

más jóvenes de expertos siguen valorando la labor del *hacker* y su filosofía primigenia, contexto en el que atesoran conocimientos vivos día a día en un ecosistema colaborativo al que se van incorporando los *millennials*. Merece la pena estudiar, en un enfoque de I+D+i, la forma en la que estas personas pueden contribuir de forma más activa, no ya solo a la ciberseguridad, sino también a la ciberdefensa militar. Todo un reto.

Un alto porcentaje del conocimiento de elevado nivel de ciberseguridad en España se localiza en los departamentos de ciberseguridad de grandes compañías estratégicas del sector público y el privado: sector de banca y seguros, eléctrico, telecomunicaciones, combustibles, transportes, farmaquímico, aguas, logística, construcción, gestión de infraestructuras... Estos responsables de seguridad de la información y responsables de seguridad tecnológica pueden brindar a la defensa su experiencia y conocimiento de la gestión de riesgos de seguridad y ayudar y sugerir numerosas líneas de modernización y mejora dignas de incluirse en programas de I+D+i, entre otras razones porque los servicios que operan son objetivos en el marco de cualquier confrontación, y no solo pueden verse desde la óptica de la ciberseguridad interior.

La ciberseguridad puede permitir a España alcanzar en un tiempo razonable y con una inversión proporcionada y bien dosificada cotas de competitividad elevadas a escala internacional. Pero el paso previo es construir una plataforma de CPP estable entre los agentes involucrados —la defensa como uno de los más importantes—, saber potenciar nuestros mercados exteriores y ser capaces de ganarnos una imagen prestigiosa en consonancia con el alto nivel de nuestras habilidades y capacidades.

La relación de interdependencias que caracteriza hoy al mundo, y el proceso de globalización, todavía no ha provocado que los Estados-nación dejen de aspirar, en defensa de su soberanía (aunque algunos hayan cedido alguna parte de la misma para preservar su grueso), a la independencia tecnológica como apoyo a la autonomía en la decisión responsable.

Esa independencia tecnológica no ha de confundirse con autarquía, comportamiento extremo que llevaría al empobrecimiento tecnológico. Esto es algo muy estudiado. Las TIC fluyen para todos, y cada vez será más difícil tener una supremacía estrictamente tecnológica que dure algo más que días, semanas y, en ocasiones, horas.

Pero siendo posiblemente así, la circunstancia permite tener alguna esfera de independencia, y en lo tocante a la ciberseguridad este hecho toma especial relevancia, ya que no requiere un esfuerzo cuantitativo desproporcionado en I+D+i y en P (de producción), y sí planes de mucha calidad y con perspectiva no cortoplacista.

Como es sabido, la ciberdefensa militar, —especialmente en algunos países— y en algunas organizaciones internacionales, como es el caso de la

OTAN, está revolucionando el esfuerzo industrial y la atención que las empresas proveedoras y la estructuras de I+D+i han de prestar a este asunto.

Hay numerosos aspectos, tratados ya[106]: la gestión del conocimiento, la *IoT* en la ciberfedensa, los agentes inteligentes, el *Big Data* y la computación cognitiva aplicada a la ciberinteligencia en apoyo del analista, la gestión de identidades, la ciberdefensa aplicada a las plataformas militares (este epígrafe, concretamente, es nuclear para las defensa y donde la innovación juega un papel determinante), la conciencia situacional, el intercambio de información, la gestión de configuración evolucionada para la seguridad TIC, la gobernanza en la ciberseguridad, la CPP en formación, la orientación a servicios de la ciberseguridad...

Sobre este último punto basta decir que la orientación de los procesos y actividades privados y públicos a la prestación de servicios gestionados por terceros y el pago por uso es un rasgo de la transformación digital. La ciberdefensa debe adaptarse a este modelo, adaptar el modelo a sus necesidades o dejarlo en tablas. Y para ello hay que investigar los cambios que se avecinan en la ciberdefensa y en los procesos TIC, porque el ciberespacio actual no siempre será así, y la requisitoria de ciberseguridad de la ciberdefensa podría cambiar.

La ciberseguridad es una disciplina y una práctica. Las personas que han de gestionarla y operarla deben ser expertas y sus conocimientos han de entrar en ciclos continuos de instrucción y actualización. Uno de los frentes en los que se ha de invertir es en la I+D en nuevas formas de instrucción, de actualización y reciclaje. Tradicionalmente, y a efectos presupuestarios, no se suele incluir este epígrafe en las inversiones en la I+D+i. En nuestra opinión, mal no vendría reflexionar sobre la pertinencia de modificar esta situación.

En prácticamente todas las zonas del mundo ha empezado a aparecer legislación relacionada directamente con la ciberseguridad y la privacidad. La ciberdefensa militar debe estudiar cómo le afectan dichas leyes y normas. Por decirlo de algún modo: los profesionales de letras también cuentan en el mundo de la I+D+i.

En el caso de Europa, la Directiva NIS y el Reglamento General de Protección de Datos –y antes la normativa de protección de infraestructuras críticas y la de telecomunicaciones–, aunque no sean específicas para la ciberdefensa militar, sí la afectan, por cuanto atañen al intercambio de información de amenazas y ataques y a su notificación. Las estructuras de ciberseguridad de un país deben discriminar si una amenaza o un ciberataque notificado son de interés para la ciberdefensa. Y la defensa ha de tener información para estudiar profesionalmente si dicha amenaza y dicho ciberataque pudie-

[106] Los expertos españoles en ciberseguridad militar José Ramón Coz y Vicente Pastor han escrito sobre la mayoría de estos puntos en diversas ediciones de *SIC* (ww.revistasic.com).

ra tener implicaciones en su campo de actuación. Es un terreno más para la I+D+i. y para la cooperación.

La ciberseguridad está precipitando, quizá de un modo soterrado, un debate más profundo y que afecta a la organización de las muy asentadas estructuras de seguridad de los Estados, que todavía están intentando encajar en su seno las estructuras nacientes de ciberseguridad.

En el caso de la defensa, hay polémica en lo que toca a decidir, a la luz de la transformación, si procede en un futuro centralizar la función de ciberseguridad de los sistemas tecnológicos de la defensa, debate que sobrepasa la propia ciberseguridad por afectar a la raíz organizativa de la defensa. Lo mismo sucede con la pertinencia o no de crear un ciberjército. Obviamente, un ciberejército no debe confundirse con una organización dedicada a la gestión de riesgos de seguridad de los sistemas tecnológicos de la defensa.

Sea como fuere, nadie pondrá en duda que se sugiera incluir en la maquinaria de la I+D+i el estudio pormenorizado de las transformaciones organizativas que tendrá que ir adoptando la defensa para ir adaptándose a la transformación digital. A buen seguro que del estudio profundo y sin cargas del pasado del papel de la ciberseguridad (a todos los efectos) dependerá que España disponga de una defensa militar adaptativa y con las capacidades siempre adecuadas para operar en un ciberespacio cambiante.