LA INVERSIÓN EN TECNOLOGÍAS HABILITADORAS: HACIA UNA ESTRATEGIA DE DEFENSA

MARIO FERNÁNDEZ PANTOJA LUIS PARRILLA ROURE

Universidad de Granada

La implantación a nivel europeo del concepto que se ha venido a llamar «máquina de defensa tecnológica» (Gholz y Sapolsky, 2021) es un formidable reto estructural al que se han de enfrentar nuestras instituciones, de forma inaplazable a la vista de los recientes acontecimientos geoestratégicos. Este concepto, que supone una extensión de lo que de forma clásica vino a llamarse tecnología militar, engloba al conjunto de esfuerzos coordinados y sostenibles en el tiempo destinados a concebir, desarrollar e implementar todas aquellas iniciativas de potencial utilidad para los sistemas de defensa.

Para su consecución, resulta relevante destacar varios aspectos en este marco de trabajo. En primer lugar, se trata de un concepto transversal que comprende no solamente aquellos objetivos estratégicos que coyunturalmente se identifiquen como prioritarios, sino también a todos los conocimientos y aplicaciones que formen una base científica y tecnológica destinada a proporcionar una capacidad de respuesta rápida frente a la aparición de nuevos paradigmas y retos prioritarios a lo largo del tiempo. En segundo lugar, el carácter necesario de consecución de la propiedad intelectual del conocimiento o producto generado como sello distintivo entre los resultados de esta «máquina», respecto de otras inversiones en bienes y productos específicos en el campo de defensa que, si bien son absolutamente necesarios, no han de confundirse en términos presupuestarios ni organizativos por las notables diferencias que subyacen entre ambos. Por último, el carácter mixto civil y militar sobre el que ha de

apoyarse la implantación de la «máquina de defensa tecnológica», que proporcione la flexibilidad necesaria para resolver adecuadamente la porosidad histórica entre las invenciones civiles y militares (Peifer, 2021) (MacNeill, 1984), con numerosos ejemplos de uso cruzado entre ellas, más allá del origen y financiación de su descubrimiento.

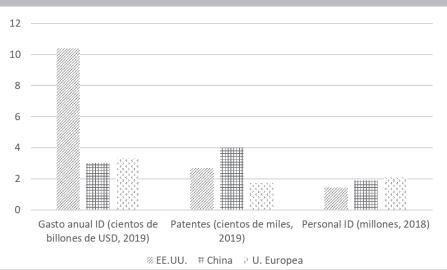
Sin duda, la mejor forma de afrontar las necesidades futuras concretas en términos de defensa es admitir un grado notable de incertidumbre en su predicción, y una certeza absoluta de la apuesta por tecnologías y conocimientos aplicados más generales como base sobre la que se sustentará la solución a dichas necesidades. En efecto, la previsión triunfalista «a diez años» de McCarthy, Minsky y Shannon (1) al idear la expresión «inteligencia artificial», en 1956, no ha sido identificada como estratégica hasta alcanzar un desarrollo suficiente de las habilidades de procesamiento de lenguaje y capacidades de

búsqueda de información propias de estos sistemas, sólidamente construidas a partir de conceptos más generales como los asociados al procesamiento de señal y almacenamiento electrónico de respuesta ultrarrápida. Por otro lado, pocos lectores de la revista «Popular Science» (2) hubieran imaginado en 1946 que la palabra «drone», usada en sus páginas por primera vez con el significado de «aeronave no tripulada», llegaría a ser varias décadas después una de las mayores revoluciones en términos de tecnología militar de los últimos siglos gracias, entre otros hitos de carácter más reciente, a la miniaturización de dispositivos electrónicos y el desarrollo de las comunicaciones inalámbricas. Y aún serían menos los visionarios que, aun siendo conscientes a mediados de la década de 1940 de la revolución que suponía el desarrollo de la máquina ENIAC (3) como punto de partida de la informática, podrían imaginar que la garantía de integridad funcional de dichas máquinas sería un objetivo indiscutible de defensa muchas décadas después, bajo el concepto de la palabra «ciberseguridad». Dicho objetivo no hubiera sido posible sin el desarrollo de las redes de computadores y otros conceptos tecnológicos asociados a la ingeniería telemática. Estos tres ejemplos ponen de manifiesto que la «máquina de defensa tecnológica» ha de construirse sobre un esquema coordinado de inversión estable en el tiempo así, como sobre tecnologías de carácter más fundamental, denominadas «tecnologías habilitadoras» (4), que permitan la evolución y adaptación rápida de los retos estratégicos concretos de defensa, y que poseen de forma inherente un carácter dinámico.

Pero, ¿qué diferencia a las tecnologías habilitadoras respecto de otros objetivos tecnológicos estratégicos y/o de las disciplinas tecnológicas fundamentales?. En primer lugar, y como rasgo más evidente, posee una concreción en su definición mucho mayor que el de las tecnologías fundamentales, pero un carácter mucho más global que un objetivo estratégico. Por ejemplo, la innovación en física cuántica posee un carácter muy general que ha venido siendo financiado casi en su totalidad por programas civiles, y contrasta con la concreción de un objetivo estratégico de defensa como es el desarrollo de comunicaciones militares seguras basados en sistemas cuánticos de encriptado y desencriptado (5). En segundo lugar, las tecnologías habilitadoras poseen un alto grado de transdisciplinariedad, ya que su desarrollo posee un carácter aplicado, que usualmente excede y las distingue de la innovación de carácter fundamental (un ejemplo de esto lo constituye el desarrollo de los dispositivos biotecnológicos, donde se fusionan necesariamente los avances en biología e ingeniería). En tercer lugar, como elemento diferenciador respecto de los objetivos estratégicos de defensa que requieren de una supervisión jerarquizada, las tecnologías habilitadoras poseen una capacidad de desarrollo deslocalizado y pueden desarrollarse a partir de la financiación de decenas o centenares de grupos no necesariamente coordinados (un paradigma de desarrollo este tipo puede encontrarse en los programas «Flagship» HUMANBRAIN(6) o GRAPHENE(7) del programa Horizonte de la Unión Europea, donde miles de investigadores independientes han puesto a Europa como líder mundial en las tecnologías asociadas a dichos campos). En cuarto lugar, mantienen un grado intermedio de madurez tecnológica (TRLS 4 y 5) (8), lo que les diferencia de las tecnologías fundamentales (usualmente entre los grados TRL 1 y 3) y los proyectos estratégicos (con objetivos situados en grados TRL 6 a 9), y además les confiere de una característica modular para el diseño de sistemas del que carecen el resto de los grupos de tecnologías, lo que a su vez les proporciona una versatilidad única en cuanto a las aplicaciones militares concretas que requieran de su uso. El concepto de versatilidad es clave para entender su quinta característica de identificación que es la capacidad múltiple de retorno de inversión en términos de ingresos de explotación de patentes (como, llegado el caso, podría suceder con el alto número de patentes desarrolladas en Europa en cuando a materiales nanotecnológicos avanzados en los últimos años, donde cualquiera de ellas podría identificarse como material clave y generar retornos de inversión en campos tan distintos como, por ejemplo, la medicina o la ingeniería aeroespacial). En sexto lugar, su grado en términos de inversión capital/riesgo es intermedio entre los desarrollos fundamentales, que rara vez generan retornos por sí mismos, y los estratégicos, donde el retorno previsible es cuantificable desde el inicio al tener un objetivo y mercado específicos en su propuesta. Y, por último, mencionaremos como elemento diferenciador las necesidades teóricamente intermedias en términos globales de presupuesto (menor que la de los programas fundamentales de innovación que requieren cubrir todo el espectro del conocimiento) y duración del programa (claramente mayor que la de los objetivos estratégicos que suelen marcarse a corto, o como mucho, medio plazo).

Una vez diferenciadas las características de las tecnologías habilitadoras, resulta adecuado plantear una comparativa en su trascendencia dentro de las estrategias de defensa de las dos potencias militares predominantes en la actualidad: Estados Unidos y China. Para analizar las distintas estrategias de inversión de ambas superpotencias es necesario recurrir a los conceptos que se han venido a denominar capacidades de innovación «duras» y «blandas» (Cheung, 2021). Dentro del primer tipo se engloban aquellos factores relacionados con infraestructura y disponibilidad presupuestaria, como son el número de centros de investigación y desarrollo, el número de personal involucrado en dichas actividades, la accesibilidad en términos de número de patentes en explotación tanto de desarrollo propio como externo, y la cuantía total presupuestaria en términos interanuales. Estos factores «duros» se caracterizan por tener una relativa facilidad de réplica, supuesta una disponibilidad presupuestaria adecuada. Por otro lado, los factores «blandos» dan cuenta de cuestiones contextuales heterogéneas cuya trans-

FIGURA 1
COMPARATIVA DE FACTORES «DUROS» EN CAPACIDAD DE INNOVACIÓN ENTRE BLOQUES DE DEFENSA



Fuente: Elaboración propia a partir de datos de Informe «UNESCO SCIENCE REPORT» 2021.

misión entre distintos modelos de sociedad es más complicada. Entre ellos podemos mencionar: factores culturales, como el reconocimiento del valor del individuo y su aportación al sistema global de defensa; factores competitivos, entendidos como una redundancia en la inversión que favorezca la competencia entre centros de desarrollo; factores administrativos, como la admisión de inmigración cualificada para el personal implicado en labores de innovación tecnológica; y factores económicos, que permitan las inversiones mixtas público-privadas favoreciendo la diversificación en apuestas de innovación. Este tipo de factores «blandos» no son directamente transmisibles entre bloques de defensa distintos, ya que el carácter político y humano es históricamente distinto en la geografía mundial (Hacker, 2005). Mucho se ha debatido sobre la predominancia a corto y medio plazo entre ambas superpotencias (Gholz y Sapolsky, 2021). Más allá de los indiscutibles progresos económicos de China, que le han permitido ser competitiva en términos de factores «duros» en unos plazos de tiempo extraordinariamente cortos (recordemos, por ejemplo, que China no ejecutó su primer vuelo espacial de forma independiente hasta 2003 y su programa de desarrollo de defensa aeroespacial es el segundo más activo en la actualidad (9)), no existe un consenso claro entre cuándo se producirá el cambio de bloque predominante (Ferguson, 2012). Mucho de este debate tiene que ver con los mencionados factores «blandos», cuya adquisición por parte de China está resultando más lento y complicado por su encaje dentro de un modelo organizativo basado en estructuras altamente jerarquizadas. En cualquier caso, existen actividades recientes destinadas a proporcionar soluciones alternativas al modelo estadounidense de forma efectiva. Por una parte, frente al origen del reconocimiento del valor de la tecnología como medio de preservación del individuo se propone una valorización centrada en la colectividad del más numeroso, en términos de población, bloque oriental (Sapolsky, 2017). Por otra parte, frente a la competitividad y aportación mixta de fondos públicos y privados inherente al modelo americano entre distintas empresas y centros de investigación, el bloque chino ha planteado una estructura que, dentro de un control gubernamental, fomenta las soluciones alternativas entre los denominados «laboratorios-clave» de su sistema de innovación y las pujantes empresas locales del sector de defensa. Por último, y en oposición a la tradicional admisión de la inmigración de la sociedad americana, con esquemas de promoción de inmigración cualificada en sus programas de visado, se ha planteado una agresiva respuesta de búsqueda y atracción de talento dentro de China en los últimos años (10).

En este contexto, y en buena parte debido a los recientes conflictos militares, ha tomado relevancia por fin la apuesta por una estrategia conjunta de defensa de los países que conforman el bloque europeo. La Figura 1 muestra una comparativa de datos ilustrativos de la competitividad europea en factores de innovación «duros». El presupuesto anual de inversión y desarrollo es similar al bloque chino y, aunque el dato total americano resulte superior, se estima que solo un 30% de los espectaculares 1000 billones de dólares corresponden al sector público, por lo que la diferencia real es menor si se suma la actividad de la empresa privada. En términos de patentes, y aunque las cifras globales siguen siendo hasta cierto punto competitivas, se aprecia que Europa necesita mejorar en este sentido. La cifra de producción de patentes contrasta aún más si se tiene en cuenta que la cifra de personal de investigación y desarrollo europeo es, en el año 2018, la más numerosa de entre los bloques. A la vista de estos datos, y si bien es innegable la existencia de una formidable base pública y privada para la innovación tecnológi-

FIGURA 2 SISTEMAS ESTRATÉGICOS DE DEFENSA Y TECNOLOGÍAS HABILITADORAS





Fuente: Elaboración propia.

ca, la heterogeneidad social y política de sus estados miembros complica el modelo de una estrategia clara de inversión de defensa, que aumente la productividad de la innovación mediante la implantación efectiva de mejoras en los factores «blandos». Dicha estrategia entendemos que ha de sustentarse también con programas europeos competitivos específicos de innovación a corto v medio plazo, coordinados a través de organismos supranacionales y destinados al desarrollo de tecnologías habilitadoras, abiertos a todos los centros I+D y que sirvan de complemento a aquellos existentes en el European Defence Fund para los objetivos definidos como estratégicos (11), con mayor TRL que las tecnologías habilitadoras pero menor potencial en términos de patentes tecnológicas. El planteamiento de programas sectoriales específicos ha sido explorado exitosamente para programas destinados a la industria europea (European Defence Industrial Development Programme (12)), y permitirían dotar de una base tecnológica conjunta al bloque europeo que proporcionara la versatilidad y dinamismo requeridos en futuras estrategias de defensa.

TECNOLOGÍAS HABILITADORAS NOTABLES EN LA ACTUALIDAD \$

Analizaremos en este apartado algunas de las propuestas tecnológicas más prometedoras en la actualidad en el campo de la física y la ingeniería con un carácter multidisciplinar (electrónica, mecánica y metalúrgica). Cabe destacar que la lista de las aquí expuestas no incluye todas las posibles (13), destacando especialmente la omisión de aquellas relacionadas con la biotecnología e ingeniería química cuyo detalle exhaustivo requeriría de un análisis

complementario por parte de especialistas distintos a los firmantes de este trabajo. Con objeto de ilustrar la mencionada característica de modularidad de las tecnologías habilitadoras dentro de los sistemas estratégicos de defensa, se incluyen algunos ejemplos especulativos de potenciales aplicaciones, y se hace un resumen visual de los mencionados en la Figura 2.

Sistemas infrarrojos y ópticos. 🕹

Los sistemas de detección e identificación basados en frecuencias infrarrojas presentan una serie de ventajas asociadas a la longitud de onda a la que operan. Su focalización es mayor que las ondas radar, lo que aporta ciertas ventajas en su uso como detectores por ejemplo de vehículos no tripulados (UAVs) de pequeño tamaño. En España se es pionero en estas tecnologías, con el desarrollo de cámaras térmicas que son montadas habitualmente por la Guardia Civil en operaciones contra el narcotráfico en la zona del Estrecho de Gibraltar, pero también en los cazas Eurofighter, permitiendo la detección e identificación de otros aviones con sistemas de baja observabilidad radar (Gaitanakis, 2019). Un subconjunto de ellos, los denominados sistemas de infrarrojo lejanos o terahertzios aportan también una capacidad de detección de sustancias a nivel molecular, por lo que han sido objeto de inserción en cámaras de seguridad de aeropuertos para la detección e identificación remota de gases y líquidos que pongan en peligro la seguridad aérea (14). Por otro lado, los sistemas ópticos siguen siendo una fuente activa de novedades tecnológicas. La más notable de ellas a nivel de defensa lo constituyen los llamados sistemas de «invisibilidad», un hito que aún no está

completamente conseguido para sistemas de gran tamaño, pero con resultados sin duda espectaculares a nivel de pruebas de concepto (Lee, 2021).

Aplicaciones cuánticas 🗼

En los últimos años se ha producido un notable avance para conseguir el escalado de los sorprendentes efectos de la física cuántica al mundo macroscópico. El caso más conocido es el desarrollo de la computación cuántica (Ladd, 2010), que abre un gran abanico de posibilidades para desarrollar simulaciones de sistemas complejos, como sistemas financieros, investigación en nuevas moléculas para biomedicina o sistemas de inteligencia artificial, todos ellos con posibles aplicaciones relacionadas con defensa. Pero no es el único avance prometedor, pues existen, por ejemplo, prototipos de sensores basados en sistemas de transparencia electromagnética inducida cuya sensibilidad a la detección mejora a los receptores actuales en varios órdenes de magnitud. O pruebas de concepto de sistemas de intercambio de información basados en entrelazamiento cuántico, entre cuyas ventajas potenciales está la de soslayar la existencia de un canal de comunicación y, por tanto, obtener un objetivo recurrente en los sistemas de defensa: la imposibilidad de detección de la comunicación.

Criptografía hardware post-cuántica

Muy relacionado con el objetivo estratégico de la ciberseguridad (15), existen novedosas propuestas de sistemas criptográficos hardware orientados hacia la seguridad e inviolabilidad de los sistemas informáticos y de comunicaciones (Katz, 2020), eliminando las vulnerabilidades inherentes a los sistemas software. Entre ellas, y relacionada con las aplicaciones cuánticas anteriormente mencionadas, destacaremos los denominados sistemas criptográficos post-cuánticos, de mayor complejidad y que precisan de mayores recursos que los disponibles en la actualidad, pero que pretenden garantizar la seguridad de la información y las comunicaciones ante la computación cuántica, una de las principales preocupaciones de la ciberseguridad actual. De hecho, se están sustituyendo progresivamente todos los criptosistemas de llave pública basados en RSA, y se han estandarizado recientemente criptosistemas post-cuánticos por parte del NIST (National Institute of Standards and Technology) de EEUU (16), lo que ha llevado a los distintos bloques de defensa a prestar un gran interés en esta tecnología.

Nanotecnología 🕹

La nanotecnología ha sido un campo de novedades tecnológicas permanentes en las últimas dos décadas, con soluciones tecnológicas plenamente operacionales gracias a la habilidad adquirida de fabricación a escala nano y micrométrica, tanto en sus variedad «top-down», donde se van conformando diseños a partir de una muestra primaria de mayor tamaño mediante el uso por ejemplo de láseres de ablación, o en una aproximación «bottom-up» donde a partir de componentes fundamentales de tamaño incluso atómico se van obteniendo agregaciones para generar dispositivos de propósitos muy diversos, como son el suministro de fármacos para aplicaciones de biomedicina o el desarrollo de nanosensores y nanomotores para el campo de la electrónica. No es difícil pensar que este tipo de sistemas sean aplicables próximamente en objetivos concretos de defensa, como por ejemplo la localización de activos en entornos operativos o la atención médica remota en soldados (Barman, 2022).

Materiales avanzados 🗼

Muy relacionado con la nanotecnología, pero no exclusivo de ella, se encuentra el desarrollo de nuevos materiales con propiedades físicas distintas a las de los materiales encontrados en la naturaleza. Si bien el más conocido de todos es el grafeno, con múltiples aplicaciones en electrónica, medicina y desarrollo de baterías más eficientes, existen muchos otros (molibdenita o siliceno por ejemplo) que comparten unas características de espesor nulo y elevada reconfigurabilidad electrónica que los hacen una fuente activa de investigación aplicada. Dentro de este grupo, los superconductores de alta temperatura constituyen otro de los avances más sorprendentes reportados en pruebas de baja madurez tecnológica, y que podría tener aplicaciones indudables en los sistemas de defensa en los próximos años. Pero existen muchas propuestas, no tan conocidas, de materiales cuyas potenciales aplicaciones en ingeniería sobrepasan las fronteras actuales (Behera, 2022).

Sistemas autosuficientes energéticamente 🗼

Como último ejemplo, mencionaremos los logros mencionados para desarrollar sistemas cuyo funcionamiento no requiera de alimentación energética externa o sistemas energéticamente autónomos. Existen numerosos esfuerzos para conseguir soluciones destinadas a potencias y consumos energéticos elevados, que permita la independencia energética de un bloque de países, como son las células solares de alto rendimiento (apoyadas en buena medida con el desarrollo de materiales avanzados y de la nanotecnología), los sistemas de energía geotérmica de última generación, los recientes reactores de fusión (con un muy reciente hito destacable, la obtención de un balance de energía positivo en la práctica por primera vez), o los polémicos sistemas de «fracking». En cualquier caso, a un nivel de potencia y energía más reducido, los sistemas de recolección de energía o «Energy Harvesting» (Panda, 2022), con prototipos de desarrollo prácticamente a cualquier frecuencia del espectro electromagnético, constituyen un ejemplo de prototipos con aplicaciones potenciales en defensa, en cuanto que se podrían mantener unas habilidades defensivas con comunicaciones operativas

aun habiéndose producido ataques a las instalaciones críticas generadoras y distribuidoras de electricidad o las refinerías petrolíferas.

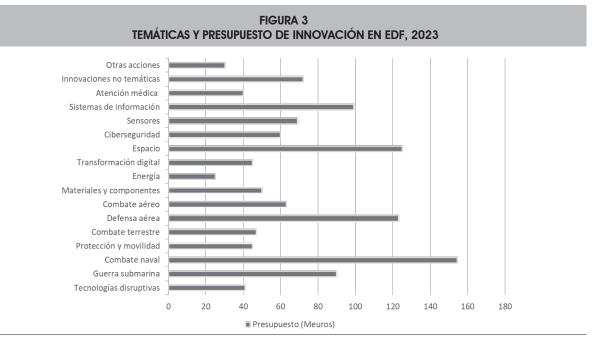
TECNOLOGÍAS HABILITADORAS EN LA ESTRATEGIA DE DEFENSA 🔹

Una vez reconocida la importancia de promover la innovación en tecnologías habilitadoras para aplicaciones de defensa, definidas sus características diferenciales respecto de otros programas de innovación, y mostrados algunos ejemplos prácticos de actualidad, es necesario abordar la oportunidad y su encaje en la estrategia de defensa europea. Como se desprende de los datos aportados en el primer epígrafe, Europa posee un problema de retención de propiedad intelectual que de ninguna forma puede atribuirse a la falta de factores «duros» en su sistema de innovación, puesto que el número de investigadores y el presupuesto total resultan competitivos. Por tanto, son los factores «blandos» los que poseen deficiencias cuya subsanación no ha de buscarse en ninguno de los otros modelos de defensa puesto que la estructura y cultura europea son distintas a las del resto de bloques. Un primer factor diferencial radica en la dificultad de coordinación a nivel tecnológico de las estrategias de defensa de los miembros de la Unión Europea. En efecto, la Agencia Europea de Defensa (EDA), creada en 2004, no posee ni los recursos ni las competencias de sus homólogas americana, la histórica DARPA, y el Comité Directivo de Investigación Científica Militar, creado por China en 2017, cuya labor en términos de coordinación resulta más sencillo por cuanto ambos actúan sobre una estructura de ejército única. Los esfuerzos de promoción de la innovación en defensa se superponen con los de coordinación entre los diferentes países miembros, y los de coordinación entre los sectores público y privado. Todo ello además a través de acuerdos que, para proyectos de medio y largo plazo como son los planes de innovación han de ser estables frente a los cambios constantes de gobierno en sus democracias. Es aquí donde surge el primer punto que supone una problemática para la adquisición de competencias «blandas»: los diferentes puntos de vista sobre el papel de la tecnología en defensa. Si bien existe unión sobre la identificación de objetivos estratégicos, la apuesta por tecnologías de base en defensa no está suficientemente asentada entre los distintos estados miembros, ni se percibe de igual forma su necesidad por los mismos. Existe también una deficiencia en términos de inmigración cualificada. La diversificación de universidades y centros de investigación entre los distintos países resta atractivo para que ejerzan directamente como agentes de innovación en defensa, y no existen organismos europeos supranacionales consolidados con capacidad de contratación y desarrollo de una carrera investigadora como puede ser el caso, por ejemplo, del Army Research Laboratory americano. Los esfuerzos de la EDA por fomentar la competencia público-privada del sector están dando sus frutos poco a poco, pero el grado de impacto de los programas europeos de innovación en defensa es muy diverso en función de los países participantes y, por tanto, queda mucho camino por recorrer en ese sentido. Si tomamos como referencia el existente programa EDF de la EDA solo entre un 4%-8% se destina a tecnologías disruptivas, pero en cualquier caso, las posibilidades de éxito de los aplicantes son mayores optando a TRLs altos y con consorcios numerosos, a los que se les deja una iniciativa de propuesta amplia, lo que en la práctica, resulta en proyectos más cercanos a objetivos estratégicos que a los propios de generación de una base tecnológica a largo plazo. El resto de financiación del programa trabaja sobre objetivos estratégicos (la Figura 3 muestra un resumen visual de los objetivos de EDF), en general más orientados al sector privado por cuanto existen organismos públicos de investigación en distintos países que, desgraciadamente, también reparan en desarrollos para defensa dentro de sus propios estatutos de creación. Por todo ello, no parece desacertado concluir que las posibilidades de éxito en propuestas de baja madurez tecnológica y alto riesgo en sus resultados, como son las de las tecnologías habilitadoras, son pocas dentro del actual formato del programa, donde solo 41 proyectos obtuvieron financiación en 2022.

Sin intención de resolver un problema tan complejo como el de la definición de la «máquina tecnológica europea», sí que parece claro que existen modelos europeos sobre los que apoyarse para la coordinación entre países y sobre objetivos únicos. Los progresos de la Agencia Espacial Europea, con personal cualificado estable en su estructuras, los esfuerzos del consorcio Eurofighter, con empresas multinacionales coordinadas en objetivos concretos, la diversidad de objetivos del programa Horizonte Europa, con una implicación muy repartida entre todos los socios europeos, son modelos de inspiración en los que desarrollar un propuesta para la adquisición de «factores blandos», que doten de un nexo de unión tecnológico a los distintos ejércitos europeos garantizado la diversidad en la unidad como principio de funcionamiento de la Unión Europea. Todo ello sin perjuicio de los programas existentes, sin duda acertados, y comenzando por establecer una conciencia sobre la apuesta tecnológica de base para el desarrollo de sistemas que eviten la extensión de desagradables experiencias al sector de defensa, como los recientes problemas de ciberseguridad en empresas civiles como Air Europa en 2023, o de Telefónica 2017, o como la incipiente problemática asociada inherente a la Inteligencia Artificial (17), con el potencial uso malintencionado de ChatGPT (Deng, 2022), o mediante torticeros planteamientos electorales, inspirados en la minería de datos a partir de esquemas de rendimiento electoral como los tristemente logrados por Cambridge Analytica en 2016.

CONCLUSIÓN ±

La inversión para promocionar la innovación en tecnologías habilitadoras es imprescindible para cualquier estrategia de desarrollo autosuficiente en sistemas de defensa a medio y largo plazo. El



Fuente: Elaboración propia.

establecimiento de programas que fomenten la innovación a nivel intermedio permite una mayor versatilidad para el cumplimiento de objetivos estratégicos, y un ahorro en tiempo y costes de sistemas con objetivos tecnológicos muy definidos, cuya implementación se basa en tecnologías habilitadoras que, caso de no haber sido previamente adquiridas, suelen tener asociados costes de patente y, frecuentemente, restricciones de propiedad intelectual que impiden su rediseño y adaptación al sistema global en desarrollo.

Estas estrategias de promoción en la innovación de tecnologías habilitadoras están contempladas dentro de los bloques de defensa estadounidense y chino, si bien con diferentes aproximaciones como corresponden a los denominados factores «blandos» de una máquina de defensa tecnológica. A nivel europeo está aun por definir una estrategia conjunta de innovación en tecnologías habilitadoras, lo que constituirá un reto notable por cuanto las soluciones han de basarse en una idiosincrasia de innovación en defensa que aún se encuentra disgregada entre sus componentes. Si bien es evidente que las diferencias históricas, culturales, organizativas y de idioma entre las sociedades europeas juega un papel en contra, existen otros argumentos que permiten ser optimistas para el éxito del desarrollo de una innovación en sistemas de defensa autosuficiente y competitiva a nivel mundial. Entre estos argumentos están la alta capacidad de innovación de sus centros tecnológicos, la demostrada capacidad de su industria para formar consorcios supranacionales, y las exitosas experiencias de desarrollo de programas Horizonte de promoción de la innovación fundamental y la European Defence Fund para el desarrollo de sistemas estratégicos de defensa.

Solamente bajo este prisma decidido de promoción de la innovación tecnológica coordinada en sistemas de defensa, podrá obtenerse la propiedad intelectual de desarrollos necesarios en tecnologías habilitadoras, como elementos clave a emplear en futuros objetivos estratégicos. Como ejemplo de tecnologías de nivel intermedio, los autores han seleccionado y expuesto la base de un subconjunto de campos muy prometedores a nivel de defensa: los sistemas infrarrojos y ópticos, las aplicaciones cuánticas, los materiales avanzados, la nanotecnología, la criptografía hardware o los sistemas autosuficientes energéticamente. El liderazgo europeo parcial o total en la innovación de las tecnologías habilitadoras constituiría un motor de arranque del modelo inversión-producto-retorno en los sistemas de defensa, permitiendo ingresos adicionales de otros bloques de defensa con el objetivo de consolidar la sostenibilidad a medio y largo plazo, que es imprescindible para mantener la competitividad frente a la pujanza económica de otras superpotencias mundiales.

NOTAS \$

- [1] http://www-formal.stanford.edu/jmc/history/dartmouth/dartmouth.html
- (2) «Drones, as the radio-controlled craft are called, have many potentialities, civilian and military. Some day huge mother ships may guide fleets of long-distance, cargo-carrying airplanes across continents and oceans. Long-range drones armed with atomic bombs could be flown by accompanying mother ships to their targets and in for perfect hits». [Popular Science, November 1946]
- [3] Freiberger, P.A. y Swaine, Michael R. ENIAC. Encyclopedia Britannica. https://www.britannica.com/technology/ENIAC

- [4] Este concepto de «tecnología habilitadora» es recurrente en diferentes ámbitos (por ejemplo, puede referirse a digitales como https://portalayudas.mineco.gob.es/THD a las referentes a la industria 4.0 como en https://www.grupocibernos.com/blog/12-tecnologias-habilitadoras-dentro-del-marco-de-la-industria-4-0). En este artículo se referirá este concepto como a aquellas orientadas a las aplicaciones de defensa
- [5] https://www.nationaldefensemagazine.org/articles/2021/12/27/quantum-and-the-future-of-cryptography
- [6] https://www.humanbrainproject.eu/en/
- [7] https://graphene-flagship.eu/
- [8] https://www.mincotur.gob.es/Publicaciones/Publicacionesperiodicas/Economialndustrial/RevistaEconomialndustrial/393/NOTAS.pdf
- [9] https://www.bbc.com/mundo/noticias-internacional-61709355
- [10] https://www.brookings.edu/articles/chinas-national-talent-plan-key-measures-and-objectives/
- [11] https://defence-industry-space.ec.europa.eu/eu-defence-industry/european-defence-fund-edf en
- [12] https://bianor.com/blog/edidp-for-innovative-eu-defense-industry/
- [13] Pueden consultarse otras adicionales, de carácter más específico, en https://www.defense.gov/Spotlights/Engineering-in-the-DoD/
- [14] https://www.nist.gov/programs-projects/terahertz-imaaing-and-sources
- [15] https://www.secureit.es/mas-de-la-mitad-de-las-empresas-espanolas-aumentara-su-inversion-en-ciberseauridad-en-2023/
- [16] https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization
- [17] https://futureoflife.org/open-letter/pause-giant-ai-experiments/

REFERENCIAS \$

Barman, J., Tirkey, A., Batra, S., Paul, A. A., Panda, K., Deka, R., & Babu, P. J. (2022). The role of nanotechnology based wearable electronic textiles in biomedical and healthcare applications. *Materials Today Communications*, 104055

Behera, Ajit (2022). Advanced Materials: An Introduction to Modern Materials Science. Springer DOI: 10.1007/978-3-030-80359-9

Cheung, Tai Min (2021) A conceptual framework of defence innovation, Journal of Strategic Studies, 44:6, 775-801, DOI: 10.1080/01402390.2021.1939689

Deng, J., & Lin, Y. (2022). The benefits and challenges of ChatGPT: An overview. Frontiers in Computing and Intelligent Systems, 2(2), 81-83

Ferguson, N. (2012) Civilization: The West and the Rest. Penguin Press.

Gaitanakis, G. K., Vlastaras, A., Vassos, N., Limnaios, G., & Zikidis, K. C. (2019). Infrared search & track systems as an anti-stealth approach. *Journal of Computations & Modelling*, 9(1), 33-53.

Gholz, Eugene, & Sapolsky, Harvey M. (2021) The defense innovation machine: Why the U.S. will remain on

the cutting edge, Journal of Strategic Studies, 44:6, 854-872, DOI: 10.1080/01402390.2021.1917392

Hacker, Barton (2005). «The Machines of War: Western Military Technology 1850–2000». History & Technology. 21 (3): 255–300. doi:10.1080/07341510500198669. S2CID 144113139.

Katz, Jonathan, & Lindell, Yehuda (2020). Introduction to Modern Cryptography (3 ed.). Chapman & Hall/CRC.

Ladd, T. D., Jelezko, F., Laflamme, R., Nakamura, Y., Monroe, C., & O'Brien, J. L. (2010). Quantum computers. Nature, 464(7285), 45-53.

Lee, Kyu-Tae, Ji, Chengang, lizuka, Hideo, & Banerjee, Debasish (2021); Optical cloaking and invisibility: From fiction toward a technological reality. J. Appl. Phys. 21; 129 (23): 231101. https://doi.org/10.1063/5.0048846

McNeill, William H. (1984) The Pursuit of Power: Technology, Armed Force, and Society since A.D. 1000. University of Chicago Press.

Panda, S., Hajra, S., Mistewicz, K., In-na, P., Sahu, M., Rajaitha, P. M., & Kim, H. J. (2022). Piezoelectric energy harvesting systems for biomedical applications. *Nano Energy*, 100, 107514.

Peifer, Douglas Carl (2021), Transfer of Military and Naval Technology 1325–1650, in: European History Online (EGO), published by the Leibniz Institute of European History (IEG), Mainz 2019-05-03. URL: http://www.ieg-ego.eu/peiferd-2019-en

Sapolsky, Harvey M., Gholz, Eugene, & Talmadge, Caitlin (2017) U.S. Defense Politics: The Origins of Security Policy. New York:Routledge.