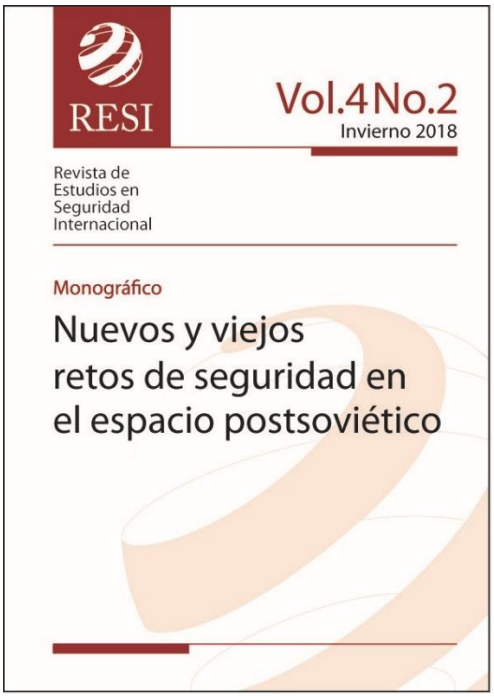

Revista de Estudios en Seguridad Internacional

Vol. 4, No. 2 (2018)

Editada por:
Grupo de Estudios en Seguridad Internacional (GESI)

Lugar de edición:
Granada, España

Dirección web:
http://www.seguridadinternacional.es/revista/
ISSN: 2444-6157
DOI: http://dx.doi.org/10.18847/1

Para citar este artículo/To cite this article:

José Díaz Toribio, "Ciencia y Tecnología en clave de Seguridad Nacional", *Revista de Estudios en Seguridad Internacional*, Vol. 4, No. 2, (2018), pp. 253-275.

DOI: http://dx.doi.org/10.18847/1.8.13

Si desea publicar en RESI, puede consultar en este enlace las Normas para los autores:

http://www.seguridadinternacional.es/revista/?q=content/normas-para-los-autores

Ciencia y Tecnología en clave de Seguridad Nacional

Science and Technology in Terms of National Security

JOSÉ DÍAZ TORIBIO

Asociación de Diplomados Españoles en Seguridad y Defensa

RESUMEN: Ciencia y Tecnología son elementos esenciales para la consecución de cualquier objetivo estratégico. Están en el núcleo de la competencia internacional, pero también son el motor de cambios sociales y políticos que dan lugar a desafíos para la seguridad. En este artículo estudiamos el papel que la Ciencia y la Tecnología desempeñan en la Seguridad Nacional. Sobre todo, intentamos analizar qué oportunidades ofrecen los avances científicos y tecnológicos actuales para la realización de los objetivos estratégicos de nuestro país. De acuerdo con el principio de que no es tan importante el conocimiento, sino cómo se utiliza, tratamos de descubrir cuál es la gestión del mismo que más favorece a los intereses españoles.

PALABRAS CLAVE: Ciencia; Seguridad Nacional; Sistema de Seguridad Nacional; Tecnología.

ABSTRACT: Science and Technology are essential elements to achieve any strategic objective. They are the core of the international competitiveness, but at the same time they are pursuing social and political transformations that are the origin of new challenges to our security. This article deals with the role played by science and technology in the Spanish national security. Above all we try to analyze the opportunities offered by the last scientist and technological progresses to reach our strategic objectives. According to the principle that it is not so important the knowledge as how we use it, we try to discover the best way of managing the knowledge to favor the Spanish interests.

KEYWORDS: National Security; National Security System; Science; Technology.

Recibido: 5 de abril de 2018

Aceptado: 11 de octubre de 2018

INTRODUCCIÓN

Aunque el término "Seguridad Nacional" aparece diseminado en diferentes textos jurídicos de nuestra historia (Zafra, 2016: 20-24), no es hasta 2011 cuando comienza a implantarse un auténtico Sistema de Seguridad Nacional en nuestro país. Y por tal hemos de entender aquel que desarrolla un concepto integrador y transversal del mismo, que supera la vieja distinción entre seguridad y defensa, y aglutina las dimensiones emergentes de la seguridad, como el ciberespacio.

Desde la publicación de la "Estrategia Española de Seguridad" en 2011 se puso en marcha un proceso que llevó a la creación de un Sistema de Seguridad Nacional. Dicho proceso culmina con la promulgación en 2015 de la Ley 36/2015, de 28 de septiembre de 2015, de Seguridad Nacional. El artículo 3 de la misma define Seguridad Nacional como:

> la acción del Estado dirigida a proteger la libertad, los derechos y bienestar de los ciudadanos, a garantizar la defensa de España y sus principios y valores constitucionales, así como a contribuir junto a nuestros socios y aliados a la seguridad internacional en el cumplimiento de los compromisos asumidos.

En el marco teórico que inspira esta definición y el desarrollo de las estructuras correspondientes nos mantendremos a lo largo de todo este artículo. Porque el enfoque integral de la Seguridad Nacional en el que se basan supone la superación de viejas distinciones teóricas -entre defensa y seguridad, o seguridad interna y seguridad externa- con repercusiones muy importantes en su gestión.

Todo este proceso ha coincidido en el tiempo con una revolución científica y tecnológica a nivel global que es fuente de una nueva competencia internacional (Torralba, 2018), y origen de nuevos desafíos para la seguridad.

En este artículo nos preguntamos fundamentalmente cómo se ha gestionado la Ciencia y la Tecnología en el marco del nuevo Sistema de Seguridad Nacional. En concreto nos hacemos tres preguntas básicas:

-1. ¿Qué papel desempeñan la Ciencia y la Tecnología en el ámbito de la Seguridad Nacional de España?

-2. ¿Cómo se han gestionado en los últimos años? Esta es la pregunta más importante que nos hacemos, y derivada de la misma nos hacemos la tercera,

-3. ¿Qué nivel de eficiencia ha tenido dicha gestión? Responder a esta pregunta nos obligará a descubrir si esta gestión ha sido congruente con el enfoque integral de la seguridad que se pretende desarrollar en los últimos años.

En este sentido, creemos que es perentorio enfocar la gestión científica y tecnológica en el ámbito de la Seguridad Nacional, ya que la bibliografía predominante ha abordado el tema desde la perspectiva de la Defensa (Instituto Español de Estudios Estratégicos, 2017) y de la Industria de Defensa (García Alonso, 2010; Jiménez Bastida, 2017), pero falta esa visión integral y holística.

Para llevar a cabo esta investigación se ha realizado, fundamentalmente, un análisis de la documentación oficial. Se han estudiado también textos de carácter estratégico, programático y presupuestario, a través de los que se materializa la gestión de los recursos y la consecución de los objetivos. Dichos textos oficiales son una fuente primaria y los completamos con las aportaciones de la literatura más reciente sobre la cuestión.

Es conveniente, antes de continuar, hacer algunas precisiones conceptuales. Utilizamos el concepto "Ciencia y Tecnología", como un todo. Engloba algo más que lo que tradicionalmente se entiende por I (Investigación) + D (Desarrollo) + i (innovación). También encontramos esta terminología, con un significado similar al nuestro, en la bibliografía más reciente (Fundación Alternativas, 2017).

Ciencia y Tecnología incluye la investigación científica básica con el fin de incrementar nuestro conocimiento, desarrollo tecnológico que aplique resultados novedosos de esta investigación, innovación en tecnologías y en procesos fruto de la aplicación de nuevos descubrimientos y nuevos sistemas de gestión. También engloba la modernización, entendiendo por tal la actualización tecnológica que se realiza a través de la adquisición de equipos, sistemas o programas con fin de dotarse de nuevas capacidades. Finalmente, y con carácter general, debemos añadir la gestión del conocimiento, con un espectro de actividades tan amplio que va desde la transferencia de tecnologías y saberes, la formación, la vigilancia tecnológica o la consultoría.

Ciencia y tecnología en la seguridad nacional de España

No se puede abordar desde un enfoque de la Seguridad Nacional la gestión científica tecnológica hasta que no se crea un Sistema de Seguridad Nacional propiamente dicho. Y esto ocurre en la práctica a partir del año 2013.

Desde ese año se abre un horizonte, al menos potencial, para analizar el contexto estratégico global y dar una respuesta integral desde una perspectiva holística. Hemos dicho potencial, y tal vez haya que decir teórica, porque precisamente el estudio de la gestión de las capacidades tecnológicas nos va a servir también para comprobar sobre el terreno si tales planteamientos se han implementado como estaba previsto, o han seguido predominando las tendencias anteriores en las que la respuesta a desafíos y amenazas se organizaba de manera cuasi autónoma y aislada por los distintos sectores concernidos: Defensa Nacional, Seguridad Pública y Relaciones Internacionales, principalmente.

Los documentos emitidos por el Sistema de Seguridad Nacional, que se componen, hasta la fecha, de dos Estrategias de Seguridad Nacional, tres estrategias sectoriales y cuatro Informes Anuales de Seguridad Nacional, expresan el análisis del contexto actual y la respuesta estratégica que se ofrece desde la perspectiva de la Seguridad Nacional de España. El objetivo que se persigue es intentar dirigir todos los esfuerzos y distribuir eficazmente los recursos del Estado para preservar la seguridad, en la forma de servicio público que mencionamos más arriba.

Desde el 2013 al 2018 hay una evolución, tanto en el diagnóstico como en la respuesta, en la visión que se tiene de la importancia del factor tecnológico y científico para la seguridad de España. De todas las variables que hemos identificado como componentes del concepto "Ciencia y Tecnología" (investigación básica, aplicación tecnológica, innovación, modernización y gestión del conocimiento), la que más parece interesar a los analistas de la Seguridad Nacional española es la tecnología y la modernización tecnológica. La innovación y la gestión del conocimiento quedan en un segundo plano, y la investigación básica está ausente del análisis del contexto y de la respuesta que se ofrece a amenazas, desafíos y riesgos.

En la Estrategia de Seguridad Nacional de 2013 (Gobierno de España, 2013) el uso nocivo de las nuevas tecnologías figuraba como uno de los potenciadores de riesgos. En lo que respecta al análisis pormenorizado de la influencia de la tecnología en amenazas y riesgos, prácticamente toda la atención se concentraba en las ciberamenazas, convirtiendo

la ciberseguridad en un ámbito nuevo de la Seguridad Nacional. De hecho, las tecnologías de la información pasan a situarse entre las infraestructuras críticas a proteger. El factor tecnológico también aparece de manera dispersa en dos amenazas. En el caso de espionaje, preocupaba mucho el espionaje económico, facilitado por las nuevas tecnologías, y se aseveraba que tiene gran relevancia para garantizar la competitividad de la economía española. Finalmente, se ligaba de manera vaga la innovación tecnológica, o la falta de ella, a la inestabilidad económica.

Aunque parezca sucinto, este catálogo de referencias agota el componente tecnológico en el ámbito de la Seguridad Nacional que se hacía en el documento del 2013. Ahora bien, en el año 2017, al menos en el planteamiento analítico del contexto, la variable tecnológica ocupa ya un lugar central.

Se menciona la tecnología como un factor transformador de la Seguridad Global y un elemento clave de la competitividad geopolítica, y, de hecho, esta vinculación entre tecnología y geopolítica es muy interesante. Se añade más sustancia y relevancia aún al elemento tecnológico cuando se asevera que es clave para el trabajo y, a través de él, para la Seguridad Nacional. En definitiva, los cambios tecnológicos, en la visión de esta nueva Estrategia de Seguridad Nacional, tienen repercusiones importantes para la seguridad de España. Incluso se concretan las tecnologías con más impacto para la Seguridad Nacional: Conectividad, Inteligencia Artificial, Ingeniería Genética y Robotización.

En este análisis, las tecnologías y los cambios tecnológicos aparecen más involucrados en las amenazas que en los desafíos. En relación a los conflictos armados se propugna que nuevos y sofisticados sistemas de armas están haciéndolos más peligrosos y duraderos. En el caso del terrorismo, se concluye que las nuevas tecnologías ponen a disposición de los grupos terroristas nuevos recursos. También estarían ampliando los horizontes del crimen organizado. Preocupa en el ámbito de la proliferación el material y la tecnología de doble uso (civil y militar). El espionaje industrial, sobre todo en el caso del acceso ilícito a conocimientos tecnológicos propios, se ubica como un eje central de la amenaza general que supone el espionaje en sí mismo. La vulnerabilidad del ciberespacio se convierte en una amenaza crucial, sobre todo teniendo en cuenta la transformación digital que experimentan las administraciones. También las nuevas tecnologías tienen una gran importancia para la seguridad marítima de España al permitir el acceso a recursos marítimos de manera ilícita. Finalmente, hay un aspecto al que se le concede una relevancia estratégica nueva, como es la protección del espacio aéreo y ultraterrestre. Aquí se concluye que las nuevas tecnologías son cruciales para esta protección, y algo también importante, serían un elemento básico de la competencia entre Estados (todo cuanto permita el acceso, uso y control de dichos espacios).

Como se puede observar, de la escueta mención en 2013 al uso nocivo de las nuevas tecnologías como potenciadores del riesgo (y su proyección sobre algunas amenazas), en 2017 se pasa a situar a la tecnología como factor crucial para la Seguridad Nacional y, en general, para la Seguridad Global.

Es posible, por tanto, detectar un salto muy importante en la Estrategia de Seguridad Nacional del 2017 sobre el papel de la tecnología con respecto a lo que venía siendo la línea marcada en 2013, y cuya coherencia teórica se había mantenido en los años sucesivos. En ese ejercicio 2013 se publicaron dos estrategias sectoriales: Estrategia de Ciberseguridad Nacional y la Estrategia de Seguridad Marítima Nacional. En la primera se mantenía el diagnóstico de la Estrategia de Seguridad Nacional, y se centraba en la ciberseguridad como un nuevo ámbito de relación y de la seguridad. Casi todo el análisis se centraba en los ciberataques, más que en la disección de su trasfondo tecnológico. En

el caso de la seguridad marítima también se recurría a la expresión de "*uso nocivo de las nuevas tecnologías como potenciadores de riesgos*" (Gobierno de España, 2013: 20). En el análisis de las amenazas se fijaba en el efecto de los ciberataques contra elementos esenciales para el desenvolvimiento de las actividades marítimas, y en el potencial de las nuevas tecnologías para prevenir catástrofes y accidentes.

En el año 2015, en la Estrategia de Seguridad Energética Nacional, sí que el factor tecnológico irrumpe con más fuerza en el análisis del contexto. Es el primer documento publicado por el Departamento de Seguridad Nacional en el que se vinculan transformaciones tecnológicas y variables geopolíticas en un mismo entorno, en este caso el energético. En el caso de la Seguridad Nacional de España se especifica que, al tratarse de una "isla energética", un vector importante de su seguridad es la disrupción tecnológica (tanto para la explotación de nuevas fuentes de energía autóctonas, como para obtener mejoras en el sector energético de cara a permitir su sostenibilidad económica y medioambiental y mejorar la eficiencia energética).

Es factible hacer un seguimiento de las consideraciones que han merecido los factores tecnológicos para los análisis del Departamento de Seguridad Nacional a través de los cuatro informes anuales que se han publicado hasta el momento. A través de ellos sí que vemos el creciente peso que se le va atribuyendo a la tecnología en la evolución de las distintas amenazas. En el informe del año 2013 había tres referencias claras al papel de las nuevas tecnologías en el auge de la ciberdelincuencia, en el ciberespionaje y en la seguridad energética. Pero en el informe siguiente (publicado en 2015) se extiende a nuevas amenazas: terrorismo (por uso creciente de nuevas tecnologías por grupos yihadistas), crimen organizado, protección de infraestructuras críticas, seguridad financiera, inmigración irregular, seguridad marítima y seguridad energética. Esta tendencia se mantendrá *in crescendo* en los dos años sucesivos, donde vamos viendo que cada vez se repara más en la importancia de aludir al impacto de las nuevas tecnologías para comprender mejor nuestro contexto de seguridad. Como hemos visto, la Estrategia de Seguridad Nacional del 2017 representa un salto cualitativo y cuantitativo incluso con respecto a la evolución de los dos años anteriores.

Esta creciente importancia que la tecnología tiene para la Seguridad Nacional se manifiesta también en la planificación de la respuesta a amenazas, desafíos y riesgos. Si la propia Estrategia de Seguridad Nacional del año 2013 define una estrategia de seguridad como un conjunto de directrices para reorganizar los recursos del Estado de manera eficiente para la provisión de este servicio público, al haber crecido la dimensión tecnológica en el análisis también lo hace en la respuesta. Pero en esto hay que matizar, porque, quizás, aquí está una de las debilidades del Sistema de Seguridad Nacional.

En el año 2013, a partir de la Estrategia de Seguridad Nacional, pero también de la Estrategia de Ciberseguridad Nacional y Estrategia de Seguridad Marítima Nacional, la respuesta estratégica principal que se ofrece a las amenazas, riesgos y desafíos identificados es la de optimización de los recursos existentes y la racionalización de las estructuras. En el campo de las capacidades, desde la Seguridad Nacional se alude genéricamente al desarrollo de las capacidades necesarias. Entre 2013 y 2015 encontramos referencias explícitas al desarrollo de capacidades tecnológicas en el campo de la Ciberseguridad (diseño de un Plan de I + D + i para impulsar la industria española de ciberseguridad y otras líneas de acción para promover la investigación), en contrainteligencia (dotación de capacidades tecnológicas a los órganos de inteligencia), protección ante emergencias (elaboración de un plan de alerta nacional frente a riesgos tecnológicos), proliferación (combate de transferencias de conocimientos y tecnologías), seguridad marítima (mejora capacidades de vigilancia y prevención de ciberataques) y

defensa (impulso de las capacidades tecnológicas de la industria de defensa). Junto al desarrollo de capacidades se aboga también por una mejora en la gestión del conocimiento que permita un intercambio más eficaz de información entre administraciones y entre el sector público y el privado.

En el año 2015, en la Estrategia de Seguridad Energética Nacional, con la creciente presencia en el análisis de factores como la disrupción tecnológica, la respuesta tecnológica es también más importante, englobando tanto investigación, aplicación tecnológica como innovación, para la explotación de nuevas fuentes de energía y promoviendo la sostenibilidad económica y medioambiental del sistema energético español.

Sin embargo, es en la Estrategia de Seguridad Nacional de 2017 donde uno de los cinco objetivos principales de la estrategia gira en torno a la respuesta tecnológica. En concreto, se habla de impulsar la dimensión de seguridad en el desarrollo tecnológico (apostando por una tecnología más segura). Y hay dos añadidos muy importantes a este objetivo: el Estado debe preservar determinadas capacidades tecnológicas de carácter estratégico y el desarrollo de la industria tecnológica propia se convierte en un ámbito de la soberanía nacional. El salto, como puede ver, es de magnitud.

Pero en el desarrollo de las líneas de acción no encontramos medidas prácticas que contribuyan de manera decisiva a cumplir dichos objetivos. Mientras que en la Defensa sí se habla de adquisición de capacidades estratégicas (en línea con la tradición anterior de este departamento), en las demás áreas de actuación predominan medidas para la mejora de capacidades, para su reforzamiento y para la promoción de la innovación[1]. Es decir, en el análisis global se reconoce la centralidad del cambio tecnológico en un contexto global competitivo, pero en el planteamiento de las medidas a implementar no se diseña una estrategia tecnológica que sea tan disruptiva y potente como el contexto que se describe. En el análisis de partida, la Estrategia de Seguridad Nacional 2017, como hemos visto, habla de las tecnologías disruptivas (inteligencia artificial, robótica, ingeniería genética, etc.), en cambio, en las líneas de acción se pierde toda referencia al desarrollo de cualquiera de estas tecnologías. Por supuesto, tampoco hay referencias a la investigación científica, muy involucrada en el impulso al potencial disruptivo de estas tecnologías.

Si desde el punto de vista del análisis estratégico hay cierta descompensación entre la creciente importancia en el análisis del factor tecnológico y la orientación que se desea dar a la distribución de los recursos, nos interesa ahora indagar sobre las realizaciones. Hemos querido saber si hay coherencia entre lo expresado estratégicamente desde la perspectiva de la Seguridad Nacional, y las medidas tomadas para implementar sus planteamientos sobre una realidad administrativa que es variada y celosa de conservar su autonomía.

LA GESTIÓN DE LA CIENCIA Y TECNOLOGÍA VINCULADA A LA SEGURIDAD NACIONAL

[1] En terrorismo: mejora de la capacidad de persecución, inteligencia y desarrollo tecnológico. En proliferación: control del tráfico ilícito de materiales y tecnología. En ciberseguridad: reforzar la capacidad de prevención, detección y reacción; mejora de capacidades tecnológicas mediante el impulso de la industria española de ciberseguridad; promover y retener las capacidades tecnológicas que España necesita para cumplir sus objetivos de ciberseguridad. En protección de infraestructuras críticas: favorecer la innovación en seguridad apostando por el I + D + i español. En seguridad económica: favorecer la innovación en la economía. En medio ambiente: apoyo a energías y tecnologías menos contaminantes y más sostenibles.

En este apartado describimos sintéticamente, dejando el análisis para un apartado posterior, cómo se ha llevado a cabo la gestión científico-tecnológica por la Seguridad Nacional de España.

Dirigiremos nuestro foco a tres de los ámbitos que engloba la Seguridad Nacional, donde, desde nuestro punto de vista, la gestión de Ciencia y Tecnología ha expresado más interés por su repercusión estratégica: las adquisiciones para la Defensa; el cambio de modelo productivo; y otras áreas de la seguridad relacionadas con la Seguridad Pública.

Ciencia y Tecnología en la política de adquisiciones para la Defensa

La gestión de Ciencia y Tecnología está incluida dentro de la gestión general de la adquisición de capacidades para la Defensa. Prácticamente en su totalidad se centra en la adquisición de capacidades tecnológicas a través de la provisión de equipos y materiales, ya que, en la propia Estrategia de Tecnología e Innovación para la Defensa, de 2015, se excluye la investigación básica o científica.

Por lo tanto, debemos detenernos en exponer cómo se articula la gestión de estas capacidades. Se han producido cambios importantes desde el año 2013, aunque más relacionados con las necesidades propias de la Defensa que fruto de la influencia o planificación desde el Sistema de Seguridad Nacional.

En la Estrategia de Seguridad Nacional de 2013 se fijaron dos objetivos en este campo. Uno era la provisión de capacidades militares para el cumplimiento de la misión de las Fuerzas Armadas y para la disuasión; el otro era el fortalecimiento de la industria española de defensa. En la siguiente estrategia, la del 2017, el planteamiento es similar, aunque añade un enfoque intelectual más propio de la Seguridad Nacional. Se habla de dotar a las Fuerzas Armadas de las capacidades que demanda el escenario de seguridad e impulsar una estrategia de industria de defensa autóctona para adquirir capacidades estratégicas y mejorar su competitividad (Gobierno de España, 2017: 83).

En la práctica, en estos cinco años el sistema de gestión de capacidades, entre ellas las tecnológicas, se ha modificado siguiendo los siguientes objetivos:

- Racionalizar unos recursos que son escasos para la actualización de capacidades
- Afrontar los problemas financieros derivados de los Programas Especiales de Armamento (PEA a partir de ahora).
- Proteger la industria de defensa (con medidas que posibiliten la invocación del artículo 346 del TFUE).

La gestión de las adquisiciones comienza a reformarse desde 2014 (García Montaño, 2015: 111-142). En estos últimos años se ha puesto en marcha un sistema en el que la Dirección General de Armamento y Material (dentro de la Secretaría de Estado de Defensa) es la proveedora de materiales, equipos y tecnologías para los Ejércitos y la Armada, que de este modo se convierten en sus clientes, estableciendo sus prioridades a partir del planeamiento periódico de la Defensa. En la DGAM se concentran estas funciones de gestor de adquisiciones y las de gestor de los PEA, así como de conexión entre la Defensa y la Industria, además de representar a España en las instancias y proyectos de la OTAN y la UE competentes en la materia. Esto coincide con el inicio de un nuevo ciclo inversor militar en el que comienzan a diseñarse los nuevos programas tecnológicos (en realidad de adquisición de equipos).

En el campo de la I + D se produce también un proceso de concentración de funciones. La DGAM se convierte en la planificadora de las capacidades tecnológicas requeridas (en

teoría, en base a las capacidades estratégicas planeadas) y el INTA (Instituto Nacional de Tecnología Aeroespacial) aglutina todos los procesos de ejecución e interlocución con los otros actores implicados: universidades, centros de investigación, industria de defensa e instituciones internacionales como la Agencia Europa de Defensa). El eje motor de estos cambios ha sido la necesidad de solventar las carencias y problemas de la Defensa.

En 2012 se publica la última Directiva de Defensa Nacional (Presidencia del gobierno, 2012) en vigor, que, por lo tanto, es anterior a las dos últimas estrategias de seguridad nacional. Dicha Directiva imponía una reforma de la Defensa, con especial interés en las capacidades para una nueva Fuerza (Fuerza Conjunta) y en la industria nacional de defensa. De hecho, en la Directiva se alude a la necesidad de involucrar a la Defensa en la revisión de la Estrategia de Seguridad Nacional, justificando en cierto modo ésta última en las necesidades de la Defensa. Es decir, se ha planteado influir en la Seguridad Nacional a través de la Defensa más que a la inversa.

En la práctica cotidiana de la adquisición de capacidades tecnológicas la vinculación de Defensa con la Secretaria General de Industria y la Secretaria de Estado de Ciencia e Innovación ha sido más importante que con el Sistema de Seguridad Nacional, en lo que atañe a la adquisición de capacidades tecnológicas. Tanto es así, que en los Informes Anuales de Seguridad Nacional de 2014 y 2015 ni tan siquiera se mencionan los cambios en el sistema de gestión de las capacidades.

De esta manera Defensa casi se ha identificado con las necesidades de capacidades tecnológicas que afectan al conjunto de la Seguridad Nacional. Tanto la "Estrategia Industrial de la Defensa" de 2015 (Secretaría de Estado de Defensa, 2015), (EID, a partir de ahora), como la "Estrategia de Tecnología e Innovación para la Defensa" de 2015 (Dirección General de Armamento y Material, 2015) (ETID, a partir de ahora) aluden siempre a capacidades tecnológicas para la Defensa, pero sin profundizar nunca en la transversalidad de las mismas para otras áreas de la Seguridad Nacional. Esto ha contribuido a reforzar el perfil de Defensa y, en general, la cultura de la autonomía dentro de la Seguridad Nacional, cuando la filosofía del concepto que se pretende materializar es de transversalidad, tanto para ser más eficaces para afrontar desafíos como para optimizar la distribución de recursos.

Y si el desarrollo del actual concepto de Seguridad Nacional encuentra en la política de adquisiciones un ámbito muy desarrollado y autónomo que se basta a sí mismo para la gestión de sus capacidades tecnológicas, por el contrario, la Seguridad Nacional no haya espacio de acción para el cumplimiento de otros de sus objetivos en relación a Ciencia y Tecnología: el cambio de modelo económico.

El cambio de modelo económico como elemento de la Seguridad Nacional

En la Estrategia de Seguridad Nacional de 2013 se advertía que la inestabilidad económica y financiera es uno de los principales riesgos y amenazas a nuestra seguridad, y que los riesgos económicos (tales como los desequilibrios macroeconómicos) reducen la resiliencia económica de España y su bienestar social. En la estrategia de 2017 la inestabilidad económica y financiera es uno de los desafíos para la Seguridad Nacional. Tanto en 2013, como en 2017, se propone como respuesta potenciar un modelo económico basado en la sostenibilidad, en la innovación y en la competitividad.

La potenciación de un sistema económico basado en la innovación recae fundamentalmente en el Sistema Español de Ciencia y Tecnología, que se organiza a partir de la Ley de Ciencia de 2011. En cambio, el Sistema de Seguridad Nacional no

participa directamente en la conexión entre la provisión y gestión de capacidades tecnológicas y su pretendido objetivo de contribuir a generar un modelo económico diferente.

Los cambios en la gestión del Sistema Español de Ciencia, Tecnología e Innovación han tenido como objetivo principal gestionar recursos más escasos y conectar la Ciencia y la Tecnología con la realidad empresarial. En 2015 se crea la Agencia Estatal de Investigación para financiar todas las actividades de I + D + i en la Administración General del Estado. Mientras, el Centro para el Desarrollo Tecnológico Industrial concentra las tareas necesarias para conectar el conocimiento científico con la industria.

El principal obstáculo que las propias Estrategias de Seguridad Nacional reconocen para la transformación de nuestro modelo productivo es, precisamente, la desconexión entre el conocimiento científico y tecnológico y la realidad empresarial española. De la necesidad de cerrar esa brecha nacen iniciativas como la Agenda Industrial 2014 e inspira la "Estrategia Española de Ciencia y Tecnología y de Innovación (2013-2020)" (Ministerio de Economía y Competitividad, 2013), de la que se derivan dos planes estatales de investigación científica (Ministerio de Economía Industria y Competitividad, 2017), técnica y de innovación para planificar la aplicación de los recursos.

Pues bien, a pesar de reconocerse desde Seguridad Nacional la importancia de estos desafíos, no se hace eco de estas medidas en las Informes Anuales de Seguridad Nacional. En cambio, sí que se toma nota de otras medidas como la reforma del mercado laboral. Falta, por tanto, no ya la orientación, sino incluso cierto enfoque de Seguridad Nacional en los cambios de la gestión de la Ciencia y la Tecnología para generar un nuevo modelo económico. Tampoco encontramos recursos, ni de momento planificación, en el Sistema de Seguridad Nacional para avanzar en la adaptación a los grandes retos tecnológicos de la economía a los que se refiere la Estrategia de Seguridad Nacional de 2017, o al menos para trasladar la visión de Seguridad Nacional a un fin que requiere de medidas de índole transversal.

Ciencia y Tecnología en otras áreas de la Seguridad Nacional

El concepto moderno de Seguridad Nacional implica una planificación desde arriba de todos los recursos con el fin de afrontar de manera transversal y conjunta desafíos y amenazas. Dada la importancia que las Estrategias de Seguridad Nacional conceden al factor tecnológico, debemos rastrear también cómo se ha gestionado la respuesta en otras áreas de la seguridad y el papel que ha tenido el Sistema de Seguridad Nacional.

En la Estrategia de Seguridad Nacional de 2013 se habla genéricamente de un incremento de las capacidades en ciberseguridad y contrainteligencia. Las medidas más concretas que se mencionan son la aprobación de un Plan de I + D + i para impulsar la industria española de ciberseguridad, el control de las transferencias de conocimiento y tecnologías y la constitución de una red nacional de riesgos tecnológicos. Todas estas medidas se conciben como una racionalización del uso de los recursos disponibles más que como el impulso a la investigación y desarrollo tecnológico desde el punto de vista de la Seguridad Nacional. Y, por añadidura, la inclusión del apartado "retos a la seguridad" en la Estrategia de Ciencia y Tecnología y de Innovación 2013-2020 se hace a través de la acción de los departamentos ministeriales.

En la Estrategia de Seguridad Nacional de 2017 se es más explícito en cuanto al desarrollo de capacidades tecnológicas. Dispersas en las diferentes líneas de acción, hallamos medidas como la mejora de las capacidades tecnológicas para perseguir el

terrorismo, el desarrollo tecnológico de los órganos de inteligencia, el refuerzo de las capacidades frente a ciberataques y la potenciación de la innovación para la protección de las infraestructuras críticas.

En estos últimos cinco años, los Informes de Seguridad Nacional nos hablan de la implementación de diferentes acciones de carácter tecnológico en algunos ámbitos de la Seguridad Nacional. Las más importantes han sido:

- Ciberseguridad: Creación Mando Conjunto de Ciberdefensa, creación del CERT (equipo de respuesta ante emergencias informáticas) de Seguridad en Industria, creación de la Oficina de Coordinación Cibernética, mejora de las capacidades del Centro Criptológico Nacional, despliegue de sistemas de alerta temprana de cibertaques y fomento del emprendimiento de la industria.
- Inmigración: desarrollo del programa europeo "Fronteras Inteligentes" y proyectos de detección temprana de migrantes en el mar.
- Contrainteligencia: refuerzo de los recursos tecnológicos del CNI (Centro Nacional de Inteligencia) y del Centro de Inteligencia de las Fuerzas Armadas (CIFAS).
- Respuesta ante catástrofes: creación de una red de alerta nacional de distintos tipos de catástrofes.

La inclusión de estas medidas en los Informes Anuales de Seguridad Nacional debe concebirse más como una constatación de lo que los departamentos realizan que como fruto de la gestión y planificación de la Seguridad Nacional.

Así, la Estrategia de Ciencia y Tecnología e Innovación (2013-2020) no está alineada con los objetivos de la Estrategia de Seguridad Nacional 2017 en lo que respecta a seguridad, por cuanto es anterior. Si la Estrategia de 2017 se refiere a la importancia de la tecnología dual como elemento clave para constituir una industria de seguridad y defensa competitiva, en la primera este desarrollo está ausente.

RESULTADO DE LA GESTIÓN DE CIENCIA Y TECNOLOGÍA PARA LA SEGURIDAD NACIONAL

Hemos visto cómo se gestiona, dentro de sus posibilidades, el binomio Ciencia y Tecnología por el Sistema de Seguridad Nacional. Hemos destacado que, a pesar de ser este sistema la plasmación de un enfoque integral de la seguridad, perviven muchas inercias del pasado. En los documentos estratégicos emanados de Seguridad Nacional se hace hincapié en la importancia de las capacidades tecnológicas para la política de adquisiciones de la Defensa, en el cambio de modelo económico-productivo y en las capacidades tecnológicas de otras áreas de la seguridad.

Conviene que analicemos la eficacia de la gestión de las necesidades tecnológicas y científicas que el propio Sistema de Seguridad Nacional ha identificado desde la perspectiva de un concepto integral y transversal de la seguridad. Este análisis lo estructuramos en tres áreas de estudio: la planificación, la disponibilidad de recursos y los resultados tecnológicos.

La planificación

En primer lugar, sobresale la falta de una planificación estratégica de las necesidades científicas y tecnológicas para la seguridad de España.

En el caso de las adquisiciones para la Defensa hay dos problemas. Uno es de confusión conceptual. Así, en el "Acuerdo del Consejo de Ministros de 29 de mayo de 2015, por el que se determinan las capacidades industriales y áreas de conocimiento que afectan a los intereses esenciales de la Defensa y la Seguridad Nacional", en el tercer párrafo de su preámbulo[2], se dice que las necesidades para la Seguridad Nacional emanan de la Directiva de Defensa Nacional, cuando sabemos que es de la propia Estrategia de Seguridad Nacional. El otro problema es la ausencia de una revisión estratégica de la Defensa. Lo que tenemos es un acuerdo del Consejo de Ministros para proteger las capacidades industriales y áreas de conocimiento estratégicas para la Defensa, en el que de manera repetida se confunde la Defensa con la Seguridad Nacional. Pero desde 2003 se carece de una revisión estratégica, que debería abordar la provisión de las necesidades tecnológicas que puedan entrar en conexión con otros ámbitos de la Seguridad Nacional. Otro documento de planificación de la tecnología es la "Estrategia de Tecnología e Innovación para la Defensa", del año 2013, que mantiene como principal objetivo conectar la industria de defensa con las necesidades de las Fuerzas Armadas, pero no tiene el valor que tendría una revisión estratégica para la actualización de las capacidades tecnológicas.

Hemos visto que otro de los objetivos de la Seguridad Nacional ha sido el cambio de modelo productivo. Desde Seguridad Nacional se ha incidido en el carácter disruptivo de las transformaciones tecnológicas en la economía. Sin embargo, en las planificaciones realizadas a través de la Estrategia de Ciencia y Tecnología y de Innovación 2013-2020, y en los planes trianuales, el objetivo principal ha sido salvar el Sistema de Ciencia y Tecnología antes que utilizar la Ciencia y Tecnología para transformar el sistema económico. Los objetivos y los indicadores del apartado final de la Estrategia 2013-2020 no guardan estrecha relación con un fin transformador, al no incluir indicadores de creación de valor, comparaciones internacionales y de impacto socioeconómico.

El enfoque de Seguridad Nacional sí ha que ha influido más en la planificación de la respuesta estratégica a los desafíos actuales que se da en los campos de la ciberseguridad, seguridad marítima y seguridad energética. Ahora bien, esta planificación sectorial se produce en un contexto en el que no se dispone de una estrategia general de seguridad interior. Sería buen instrumento para plasmar en la planificación las relaciones evidentes que se producen en la realidad entre el crimen organizado, el terrorismo, la ciberseguridad, la proliferación etc. De esta manera se podrían haber alineado los tres ámbitos de la Seguridad Nacional que identifica la propia Ley de septiembre de 2015: Defensa, Seguridad Pública y Acción Exterior.

Los recursos

Desde nuestro punto de vista, el mayor problema al que se ha enfrentado la gestión de la Ciencia y Tecnología en los ámbitos de la Seguridad Nacional, en los últimos cinco años, ha sido la escasez de recursos.

En el caso de la Defensa, en los Presupuestos Generales del Estado de este período consta que los objetivos de los recursos asignados han sido el mantenimiento de las capacidades operativas mínimas, el mantenimiento de la disuasión y la reducción del déficit público. Con este propósito, los Programas Especiales de Armamento se han convertido en el principal instrumento para los dos primeros de ellos. Absorben el 90% de todo el esfuerzo inversor de Defensa, con una dotación de 1.824 millones de euros en

[2] Boletín Oficial del Estado, 6 de agosto de 2015, página, 70583.

2017. En realidad, en los últimos veinte años han sido el eje de la modernización tecnológica, con una función económica también primordial para la industria del sector.

Los recursos destinados a I + D, y que complementan a los Programas Especiales de Armamentos (que estrictamente hablando no están destinados a la investigación y desarrollo, aunque impliquen resultados de este tipo) se distribuyen entre el INTA (137 millones) y otras partidas de 21 millones.

En conjunto, el gasto en I + D de Defensa representa desde 2014 el 1.3% de los gastos públicos en I + D, frente al 3.1 de 2008: (Calvo, 2018: 8). A la actividad pública deberíamos añadir la inversión en I + D de las empresas del sector, muy centrada actualmente en la revisión de los procesos, en una gestión más abierta del conocimiento y en un traslado más eficiente de los resultados científicos a los procesos de producción[3].

Para completar la imagen de los recursos disponibles para la Ciencia y Tecnología de Defensa, debemos añadir, por su importancia creciente, las posibilidades que se ofrecen en el ámbito europeo desde el Consejo Europeo de diciembre de 2013. Las fuentes de financiación para proyectos nacionales se han diversificado considerablemente: proyectos de diversas categorías de la Agencia Europea de Defensa, Fondos de la Comisión, *European Defence Fund*, *European Investment Bank*, etc.

Pero lo importante no es tanto la cuantía de los recursos, sino cómo se utilizan. Y esta utilización, complicada y deficiente, ha significado en la práctica una reducción de los recursos a disposición de proyectos y programas. Hay algunos ejemplos que lo ponen de manifiesto. En 2016 únicamente se aprobaron 25 proyectos dentro del programa COINCIDENTE. Otro de los mecanismos, la Compra Pública Innovadora, ha sido también infrautilizado por su complejidad. En el caso de los fondos europeos, programas de tecnología dual como COSME han visto una escasa participación española. La administración pública sí que ha acudido a la convocatoria de proyectos internacionales, pero la industria del sector, y sobre todo, la industria que potencialmente podría integrarse en él (con programas como HORIZONTE 2020), no ha estado presente, como debiera, para aprovechar estos recursos.

En resumen, como los Programas Especiales de Armamento siguen siendo el núcleo de la modernización tecnológica de las capacidades de la Defensa, en el campo de la Ciencia y la Tecnología se siguen utilizando los instrumentos ya tradicionales asociados a ellos. En el campo estricto de la I + D de la Defensa, se han reorganizado las estructuras, como hemos visto más arriba, para intentar racionalizar unos recursos que han sido más escasos.

También en la gestión de los recursos destinados a cambiar el modelo económico nos encontramos con los mismos problemas: escasez de recursos, reforma en lugar de transformación y dificultad para trasladar los compromisos de gastos a la realidad económica.

Los recursos destinados a I + D en España han descendido desde el 1.40% del PIB de 2010 al 1.19% del 2016, (Fundación COTEC para la innovación, 2018)**.** De ese gasto, el sector público gestiona el 47%, cuando la media europea es del 36%. Dentro del sector privado, el 54% de las inversiones en I + D las realizan pequeñas y medianas empresas, frente al 20% de Francia o Italia, y el 10% de Alemania. Esta cifra es relevante, porque

[3] Tomamos como ejemplo la empresa NAVANTIA, y el último informe de gestión, correspondiente a sus cuentas anuales del ejercicio 2016, pp: 87-92, sobre Investigación y Desarrollo. Disponible en la página web corporativa www.navantia.es .

el gasto destinado a este fin en el caso de las pequeñas empresas suele ser de dudosa calidad.

Se han reformado las administraciones para gestionar estos recursos menguantes. Desde 2015 la Agencia Española de Investigación administra el gasto en I + D de la Administración General del Estado, mientras que utiliza un instrumento antiguo como el Centro de Desarrollo Tecnológico Industrial (CDTI, creado en 1985) para canalizar recursos hacia las empresas.

Pero, por diversos motivos, solo una parte de los recursos asignados llegan a ejecutarse. En concreto, el 29% del presupuesto de la AEI fue ejecutado en 2017 (Domínguez, 2018).

En otras áreas de la Seguridad Nacional también se ha suplido la escasez de recursos con la reforma administrativa. La actualización tecnológica, también de carácter finalista (es decir, excluyendo la investigación básica), se ha llevado a cabo a través de la adquisición de equipos, formación, coordinación, reestructuración de la gestión y conexión entre actores para abrir el conocimiento.

Esto ha sido así en algunas áreas claves como la ciberseguridad. Se han creado equipos de respuesta a incidentes e instancias nuevas como la Oficina de Coordinación Cibernética, se han mejorado las capacidades de instancias claves como el Centro Criptológico Nacional y se han desplegado sistemas de alerta. En el campo de las reformas, el antiguo INTECO se ha transformado en el INCIBE. También se han reformado las estructuras encargadas de la protección de infraestructuras críticas, del control de fronteras y la lucha contra el terrorismo.

Pero la investigación científica y tecnológica propiamente dichas han quedado reducidas a algunos ámbitos más pequeños: programas del INCIBE (con un presupuesto total de 10 millones de euros), proyectos de I + D + i del Centro Nacional de Protección de Infraestructuras Críticas, proyectos de apoyo a la industria española a través del CDTI y la incorporación a proyectos europeos como en el caso de la protección de infraestructuras críticas.

Resultados tecnológicos: ¿más con menos?

Hemos visto que la gestión de la Ciencia y Tecnología para la Seguridad Nacional se ha gestionado siguiendo el principio de reformar estructuras para administrar unos recursos cada vez más escasos. En esta tarea, las estructuras del Sistema de Seguridad Nacional han ejercido funciones de análisis, mientras que en la planificación y ejecución el protagonismo ha sido para los departamentos ministeriales involucrados.

Analizaremos a continuación la eficiencia de esta gestión desde el punto de vista tecnológico, estableciendo comparaciones internacionales, con el objetivo de comprobar si en la práctica funciona la máxima seguida en los últimos años de "hacer más con menos".

El ámbito de la Defensa se enmarca en una creciente competitividad internacional, que se manifiesta claramente en el período que va desde la intervención de la OTAN en Libia a la crisis de Ucrania de 2013.

China y Rusia están intentando contrarrestar el liderazgo estadounidense con la aplicación de los nuevos avances científicos y tecnológicos al desarrollo de sistemas de armas de denegación de área y antiacceso (a partir de ahora, AD/A2). La respuesta de

Washington, que se materializa en la "tercera estrategia de compensación" (Colom, 2015), pretende extremar la optimización de la superior tecnología civil del país en su uso militar.

Esto está generando, en la vanguardia de la tecnología de defensa, unas tendencias que van a marcar el ritmo de la competencia entre los principales Estados.

Por un lado, se van a crear nuevos sistema satelitales y novedosos sistemas de navegación; se diseñarán redes autodefendibles; se sofisticarán los métodos de entrenamiento y simulación; se van a crear nuevos sistemas de armas; se potenciarán las capacidades furtivas y se crearán sistemas autónomos para todos los dominios de la guerra (The Defense Science Board, 2013). En definitiva, por parte de Estados Unidos se investigará y se invertirá en el desarrollo de capacidades que permitan la penetración y la superación de las medidas antiárea (Committee on Homeland and National Security and Technology Council, 2016)

Lo descrito es un pilar de una competencia en la que China aboga por sistemas AD/A2, apostando por sistemas antiespaciales, ciberdefensa, defensa antiminas, munición antibuque, actualización de armas nucleares, nuevas armas de espectro electromagnético, armas hipersónicas (más de 5 veces la velocidad del sonido) y tecnología de misiles (Cordesman & Colley, 2015; Office of Secretary of Defense, 2016). Por parte de Rusia se incide en nuevos sistemas de alerta y alarma (Gabner, 2016; Defense Intelligence Agency, 2017), actualización de todo el arsenal nuclear y convencional, guerra híbrida, sistemas autónomos y robotizados, aplicación de nuevas investigaciones en ingeniería genética, tecnologías cognoscitivas y nanotecnología (Covington, 2016).

Esta rivalidad tecnológica ya se está conjugando con una fuerte competencia económica (Babones, 2017) que es, a la postre, la que permitirá a los participantes mantenerse en la "carrera" (Béraud-Sudreau, 2017; Hunter, 2016). Es decir, se complementa con la implantación de nuevos procedimientos de producción, el diseño de tecnologías más versátiles y de uso dual (es decir, que puedan también ser rentabilizadas en el mercado civil) y la expansión de sistemas de producción de bajo coste, que reduzcan los precios unitarios.

A nivel más inmediato, nuestra pertenencia a la Unión Europea condiciona nuestro contexto estratégico de manera vital. El proceso europeo de integración tiene una vertiente muy importante en el campo de las capacidades tecnológicas. Desde el Consejo de noviembre de 2016, la cooperación en I + D se convierte en el motor de los avances que se producen en los campos de la seguridad y defensa. Así, el Fondo Europeo de Defensa se crea para financiar proyectos de investigación y desarrollo.

Pero esta corriente habrá que compaginarla con la acción de las grandes potencias. Desde el Brexit nos interesa sobre todo la política de Francia y Alemania. Ambos países, en sus últimas estrategias de seguridad (President of the French Republic, 2017; The Federal Government, 2016) han manifestado su intención de proteger su soberanía en el campo de la defensa, la protección de sus capacidades tecnológicas y de su industria de defensa (el "imperativo industrial" de Francia).

Así pues, la participación en proyectos de I + D europeos estará condicionada a lo que puedan aportar los candidatos a formar parte de ellos, tanto en términos de integración, como de competitividad internacional. La clave, pues, para jugar en esta primera liga europea va a estar en la habilidad para conjugar estas tres variables desde el punto de vista tecnológico: interés nacional; aportación al proyecto europeo; valor añadido para mejorar la competitividad global de los participantes.

En este contexto, hemos visto que los Programas Especiales de Armamento han aglutinado el grueso de la actualización de las capacidades tecnológicas de la Defensa Nacional. Paralelamente, y teniéndolos también en mente, el Gobierno ha definido las metas tecnológicas de la Defensa. Tal y como se ha dicho más arriba, en 2015, el Consejo de Ministros fijó las tecnologías y áreas de conocimiento estratégicas a proteger: sistemas S4I, ciberdefensa, ISTAR, control de tráfico, sistemas críticos embarcados en plataformas, sistemas especiales de tratamiento de datos, simuladores, sistemas de navegación, sistemas complejos integrados por otros sistemas de armas avanzados.

Por parte del Ministerio de Defensa las metas tecnológicas fijadas por la Estrategia ETID se centran en armas y municiones, sistemas electrónicos, plataformas, sistemas combatiente, NRBQ y CUI. En realidad, muchas de estas metas persiguen el desarrollo de capacidades a incorporar en los grandes proyectos de adquisición de armas. En síntesis, podemos concluir que los desarrollos tecnológicos aplicados a la Defensa en nuestro país se concentran en tres áreas:

- Incorporación de sistemas de armas a diferentes plataformas, pensando principalmente en los Programas Especiales de Armamento.
- Sistemas de mando, control y vigilancia.
- Desarrollo de nuevos sistemas de armas y protección de los efectivos humanos.

De los veintisiete programas de la Agencia Europea de Defensa en los que participa España, más de dos tercios están relacionados directamente con estas áreas. La mayoría de los proyectos del INTA tienen que ver también con ellas y con la interoperabilidad.

Algunos autores han comparado las capacidades actuales de las Fuerzas Armadas españolas con las de los países europeos más importantes de nuestro entorno (Instituto Español de Estudios Estratégicos, 2016) y como resultado de ello se pueden extraer algunas conclusiones previas:

- En capacidades navales, las Fuerzas Armadas españolas están a un nivel similar a Italia (con menos unidades, pero muy modernas gracias a las Fragatas F100, al buque de proyección estratégica y de transporte anfibio o a los buques de acción marítima), por debajo de Francia o Reino Unido, pero por encima de Alemania. Sin embargo, cuando concluyan los programas actuales en curso en todos estos Estados, quedarán muy por debajo de Italia.
- Cuentan con menos capacidades de transporte aéreo que Italia, Francia, Reino Unido y Alemania.
- En capacidades aéreas de combate están en línea con Italia o Alemania en lo que se refiere a cantidad, pero en franca desventaja cualitativa.
- En sistemas remotamente pilotados, en lo que se refiere a capacidades estratégicas, también están por debajo de estos países.
- Cuentan únicamente con dos satélites propios de observación, y participan en un 2.5% en el programa multinacional HELIOS (al 90% francés). Esta capacidad se va a modernizar en los próximos dos años.
- En capacidades terrestres mantienen un buen nivel en cuanto a cantidad de carros de combate de última generación, pero carencias en lo que atañe a vehículos blindados (algo a suplir con el programa tecnológico Vehículo de Combate sobre ruedas 8x8).

España ha hecho grandes esfuerzos por adaptar tecnológicamente sus Fuerzas Armadas, lo que le permite mantenerse, en el marco europeo, en un nivel inmediatamente por detrás de Italia. Ahora bien, hablamos de capacidades teóricas, porque las realmente

disponibles pueden ser inferiores, aunque se trata de información clasificada. Si el esfuerzo inversor y de actualización tecnológica no se mantiene se corre el riesgo de perder posiciones en los próximos años, como vemos al comparar las diferentes capacidades.

Esta reflexión última tiene una clara implicación para la Seguridad Nacional. De cara al futuro, las líneas de acción en esta área, para conservar la posición actual adaptándose al ritmo que impone la competencia internacional, pasa por seguir las siguientes políticas:

- Incorporarse definitivamente a la liga europea, combinando las tres variables a las que nos referíamos más arriba: interés nacional, proyección europea, contribución a la mejora de las capacidades del conjunto de participantes en los proyectos.
- Desarrollar tecnologías de vanguardia que serán el eje de las capacidades futuras: entrenamiento de vanguardia, sistemas autónomos, nuevas armas, sistemas alternativos de comunicación, vigilancia, inteligencia, nuevos sistemas de armas y potenciar la tecnología dual: tecnología blockchain, por ejemplo, para desarrollar redes más resistentes.
- Redacción de una nueva revisión estratégica de la defensa para saber por dónde ir, que establezca las prioridades tecnológicas, y, sobre todo, que queden bien justificadas estratégicamente.
- Orientar el futuro de la industria de defensa: sobre nuevos productos, nuevos procesos, mercados exteriores y precios competitivos. Por supuesto, determinar qué proteger y con qué medios.
- Explotar al máximo las tecnologías civiles que se encuentran en el mercado (nacional y exterior) que, entre otras cosas, puedan abaratar los costes de adquisición de equipos y material.
- Participar en grandes proyectos internacionales para el desarrollo de sistemas de armas, pero buscando la autonomía tecnológica para personalizar dichos sistemas (armas, sistemas electrónicos, etc.) según nuestras necesidades. Esto ya se está haciendo en programas tecnológicos como la Fragata F110 y el vehículo blindado sobre ruedas 8X8. En ambos se recogen desarrollos tecnológicos de vanguardia proporcionados por la industria española (redes autodefendibles, por ejemplo) (Pons, 2018a). Hay que seguir este camino, que es vital para mejorar las capacidades españolas y para proteger su autonomía estratégica, como sostiene la Estrategia de Seguridad Nacional 2017.

Como estamos viendo, la gestión de la Seguridad Nacional implica analizar y actuar en áreas de la vida de un país que aparentemente no tienen mucha relación. Pero, sin lugar a dudas, mantener los equilibrios económicos y sociales es uno de sus objetivos. Y hoy depende en gran parte de la adaptación al progreso tecnológico. La no aplicación de los avances científicos y técnicos conlleva vulnerabilidad desde el punto de vista de la competencia internacional, de la estabilidad social y de la propia posición estratégica de un Estado (Corte y Blanco, 2014: 72-75).

Así ha sido reconocido en las Estrategias de Seguridad Nacional, sobre todo en la del 2017. El deseo de transformar el modelo productivo español, dando lugar a uno de mayor valor añadido, ha resultado precariamente cumplido. En líneas generales, España ha mantenido sus posiciones a través de las reformas, con un gasto en I + D estancado y de baja calidad en el sector privado. Como en el caso de las capacidades defensivas, gastar menos en Ciencia y Tecnología ha sido útil para conservar unos niveles mínimos, pero no para hacer más.

En el "Índice de Competitividad Global 2017"[4] España ha subido hasta el puesto 32 (2017) desde el 35, donde se encontraba en 2014. Esta mejora se ha debido a la devaluación salarial, pues en el apartado de innovación el país se sitúa en el puesto 38, frente al 39 en el que estaba en 2014. Aquí conviene traer a colación dos ejemplos internacionales que representan dos modelos de lo que puede hacerse con el desarrollo tecnológico. Por un lado, tenemos el caso irlandés, que ha pasado del puesto 27 al 23 gracias al esfuerzo innovador, pues en este apartado se sitúa en la posición 19. Sus indicadores sociales son buenos y muestran un uso beneficioso para el conjunto del país de los avances tecnológicos. En el lado contrario está India. En términos globales de competitividad se ubica en la posición 39, pero en el apartado innovador llega al puesto 30. Sin embargo, en el capítulo de indicadores sociales baja al puesto 85. Es el paradigma de cómo los esfuerzos innovadores no se proyectan socialmente.

En España, la adaptación tecnológica no ha transformado su modelo productivo en profundidad, su economía es más competitiva gracias a otros factores que han provocado un incremento de la desigualdad social, aunque, desde luego, no es comparable a lo que sucede en India, a pesar de que este país pueda tener una economía supuestamente más innovadora.

Que no se ha transformado el modelo productivo en torno a un uso más intensivo de la aplicación de los avances científicos y tecnológicos lo demuestran algunos indicadores:

- En concesión de patentes España ocupa el puesto 31 (A partir de los Datos sobre la Propiedad Industrial 2016, elaborado por la Organización Mundial de la Propiedad Industrial.)
- El porcentaje de investigadores es de 6.8 por mil, por debajo de la media europea de 7.9 (Fundación Alternativas, 2017: 27)
- Ha habido un incremento de la producción científica (Docampo, 2016), pero también un descenso del liderazgo (Fundación CYD, 2016: 144)
- Únicamente se ha ejecutado el 29% del presupuesto de la Agencia Española de Investigación (Domínguez, 2018).
- Se ha producido una deficiente traslación de los resultados científicos a la realidad económica (Fundación COTEC, 2018: 64).

Dada esta situación para la Seguridad Nacional se plantean dos retos principales: adaptar la revolución tecnológica a la realidad económica y avanzar en una dimensión social y económica equilibrada.

A pesar de que la inversión en I + D en otras áreas de la seguridad ha sido insignificante (no hay partida para ello en el presupuesto del Ministerio del Interior), se han adoptado novedades tecnológicas a través de las adquisiciones de equipo y formación de personal que han mejorado las posibilidades de hacer frente a algunos retos. Los mayores progresos se han conseguido en ciberseguridad y control de fronteras.

En el primer caso, la Unión Internacional de Comunicaciones (Balañá, 2018) sitúa a España en el puesto 19, a la altura de Alemania. Se han mejorado las capacidades del Centro Criptológico Nacional (capacidades como CARMEN, LUCIA, REYES, MARIA) que han dado resultados muy positivos en la gestión de la respuesta a incidentes concretos como el sucedido en 2017 (WANACRY), y se han configurado estructuras de respuesta

[4] World Economic Forum, (2018), *The global competitiveness report 2017-2018*, Ginebra: World Economic Forum. Para elaborar nuestra argumentación hemos utilizado este reporte en su conjunto.

y equipos en organismos como INCIBE, Centro Nacional de Protección de Infraestructuras Críticas, Mando Ciberdefensa, etc.

En el ámbito del control de fronteras, las Fuerzas y Cuerpos de Seguridad del Estado disponen de instrumentos innovadores como el *Automatic Border Crossing* (Díaz, 2017 y Montero, 2015), y sistemas de vigilancia como SIVE (Sistema Integral de Vigilancia Exterior), en funcionamiento desde 2002. La participación de España en el Programa de Fronteras Inteligentes de la UE, desde 2008, es útil también para la actualización de dichas capacidades. Aún así, se necesita mejorar el desarrollo de las tecnologías de vigilancia desde el Aire (Díaz, 2017). También hay retos pendientes como la necesidad de regular la inclusión de las nuevas tecnologías en sus diferentes ámbitos: tanto en el aire (Gudín, 2017), como en tierra (coche autónomo).

De igual manera, se han conseguido progresos en la lucha contra el terrorismo mediante las nuevas tecnologías, como en la identificación de usuarios de redes sociales mediante el uso de BOTS (Brezo y Rubio, 2016).

Pero en lo que sí es necesario avanzar es en la delimitación de las funciones derivadas del uso de tecnologías que son civiles y militares en áreas como el control del espacio aéreo (Martín, 2014; Martín, 2015). También hay ámbitos en los que, si bien España ha mejorado, precisa perfeccionar su gestión, como el de las tecnologías espaciales y gestión del espacio ultraterrestre (Pons, 2018b). Aquí se deberá aprovechar la oportunidad de negocio que se ofrece a la industria española de incrementar la representación española ante organismos internacionales y desarrollar respuestas a desafíos emergentes.

Las necesidades que nacen del uso del espacio ultraterrestre sí que deben entrar en una dinámica de implicación de los diferentes actores, como se ha hecho en la protección de infraestructuras críticas. No en vano, es en la Ley de Protección de Infraestructuras Críticas de 2011 (Ley 8/2011, de 28 de abril) donde este autor ha encontrado la primera referencia en un texto jurídico a un concepto moderno de Seguridad Nacional, donde se habla de transversalidad y se asignan responsabilidades entre los implicados.

En conjunto, hay un gran camino por delante para la Seguridad Nacional en la gestión de Ciencia y Tecnología en áreas tradicionalmente relacionadas con la Seguridad Pública. Es vital contar con un catálogo de recursos, que incluya las capacidades tecnológicas disponibles, que permita visualizar duplicidades, tecnologías de uso transversal, tecnologías base y áreas de investigación.

También hay que culminar los procesos de asignación y regulación de responsabilidades tecnológicas, en línea con la aspiración de una tecnología segura y respetuosa con los derechos ciudadanos. En concreto:

- La inclusión de nuevas tecnologías en sus nuevos ámbitos: especialmente Internet de las cosas.
- La coordinación tecnológica con las empresas privadas.
- El impacto y regulación de tecnologías nuevas como la inteligencia artificial.
- La protección de los derechos individuales ante las nuevas tecnologías debe ser, singularmente, objetivo de la Seguridad Nacional.

En definitiva, el Sistema de Seguridad Nacional debe ser un recurso imprescindible en todos los procesos de regulación que tengan que ver con las nuevas tecnologías.

CONCLUSIONES

Presentamos las conclusiones de este estudio desde una doble perspectiva: desde el interés estratégico que actualmente tienen la Ciencia y la Tecnología para España (en línea con las preguntas que nos hacíamos al comienzo de este artículo), y, finalmente, ofrecemos una visión general sobre las necesidades de mejora que se plantean en su gestión.

Hemos visto que la Ciencia y la Tecnología tienen importancia creciente para la seguridad, y se ve cómo afecta a aspectos muy diversos de la misma con influjo en números ámbitos de la vida del país, de sus relaciones exteriores y de sus intereses estratégicos. Por esa razón se debe abordar su gestión de manera transversal, y desde el enfoque moderno que define hoy a la Seguridad Nacional. La persistencia de particularismos resta eficiencia, tanto en lo que respecta a la utilización de recursos, como a los resultados tecnológicos obtenidos.

La evolución científica y tecnológica de la última década afecta especialmente a tres áreas de la seguridad: las capacidades defensivas, el modelo productivo y a diferentes campos de la seguridad pública.

En cuanto atañe a la Defensa, los resultados de la gestión de las capacidades de los últimos años nos permiten concluir que se han mantenido unas capacidades tecnológicas mínimas, y que se han conservado a duras penas las posiciones con respecto a los países de nuestro entorno. En cambio, si proyectamos hacia el futuro las tendencias que marcan los programas en marcha, previsiblemente, esta situación se deteriorará y se ampliarán las brechas con respecto a países como Italia, Alemania o Francia, y, también, se reducirán las que existen ahora con respecto a países como Marruecos.

Es de interés para la Seguridad Nacional, como hemos visto, el cambio de modelo productivo: será la clave para mantener el Estado del Bienestar, reducir la desigualdad social y económica y fortalecer la cohesión social. En este terreno podemos concluir que no se ha tenido éxito. De hecho, se ha deteriorado la capacidad para trasladar los resultados de la investigación científica y del desarrollo tecnológico a la realidad económica. La competitividad se ha mantenido gracias a otros factores que no ayudan a consolidar los objetivos económico-sociales de los que hemos hablado.

En áreas de la seguridad como ciberseguridad, control de fronteras, protección de infraestructuras críticas, etc., la adaptación tecnológica se ha producido a través de la adquisición de equipos, de capacidades y de formación. Ha habido buenos resultados en ciberseguridad y control de fronteras. Es necesario mejorar en el control del espacio aéreo y ultraterrestre y en la adaptación a los cambios que anuncian nuevas tecnologías: vehículos autónomos, inteligencia artificial o robotización.

Al presentar estas breves conclusiones nos interesa destacar que de ellas se derivan análisis fundamentales para la gestión de la Ciencia y Tecnología en clave de Seguridad Nacional.

En la adaptación a los cambios científicos y tecnológicos que se están produciendo en estos momentos es imprescindible evitar duplicidades, aprovechar bien la dualidad de las tecnologías y su carácter transversal. Estas características de nuestro entorno tecnológico propician una gestión de la adaptación al mismo en línea con lo que significa el moderno concepto de Seguridad Nacional.

En la práctica seguida en los últimos años han persistido confusiones conceptuales (por ejemplo, entre Defensa y Seguridad Nacional) y líneas de actuación independientes y autónomas.

Desde las estructuras de Seguridad Nacional se deben planificar las respuestas tecnológicas si se desea estar a la altura de los desafíos que describe la propia Estrategia de Seguridad Nacional de 2017. Dado que se reconoce la dinámica del profundo cambio que está teniendo lugar, así como su valor en términos geoestratégicos y de competencia entre Estados, se debe incluir en esa planificación la iniciativa y la anticipación, ampliando el marco de la respuesta tanto a nivel tecnológico como científico, es decir, en términos de conocimiento en general.

Lo analizado en este artículo demuestra que, en cierto modo, el Sistema de Seguridad Nacional centra sus funciones más en el análisis que en la propuesta y coordinación, desaprovechando lo que contempla el artículo 19 de la Ley de Seguridad Nacional. Para completar tales funciones, la gestión de la Ciencia y la Tecnología demuestra la necesidad de nombrar a un Consejero de Seguridad Nacional, potenciando su figura al más alto nivel. Sería la mejor manera de implementar en la práctica un concepto integral de la seguridad.

En los ámbitos estudiados, ello debería acompañarse de un incremento de sus recursos propios, que servirían de manera inmediata para:

- Elaborar un catálogo de recursos tecnológicos, científicos y de conocimiento disponibles para la Seguridad Nacional.
- Elaborar un catálogo de tecnologías transversales disponibles en el mercado con interés para la Seguridad Nacional.
- A partir de los anteriores, realizar otro catálogo de recursos tecnológicos y científicos requeridos y accesibles para el cumplimiento de los objetivos de Seguridad Nacional.
- Fomentar el uso de las tecnologías duales.
- Diseñar sistemas de cooperación más estrechos con el sector privado.
- Evitar duplicidades y adquirir tecnologías básicas que puedan dar lugar a su adaptación a distintos campos de la Defensa y la Seguridad Pública.
- Completar la visión desde la que se está emprendiendo la adaptación a la revolución tecnológica en curso, principalmente en el caso del modelo productivo, añadiendo el enfoque de Seguridad Nacional.

A nivel internacional hoy se nos enseña que hay mucha tecnología civil que puede ser útil para mejorar la respuesta a los desafíos a la seguridad. De hecho, la mejor manera de no convertir la adaptación estratégica a la competencia internacional en un esfuerzo oneroso, será recurrir siempre a tecnologías que sean rentables económicamente.

Con este artículo queremos demostrar la utilidad de un enfoque como el de Seguridad Nacional para gestionar un área como el de la Ciencia y la Tecnología. Principalmente, porque permitirá aclimatarse a un contexto estratégico de competencia con una reducción de los recursos propios. También, porque sirve para orientar una gestión que se desenvuelve en ámbitos tan diversos como la Defensa, la Economía y la Seguridad Pública.

NOTA SOBRE EL AUTOR: ***José Díaz Toribio****, es Licenciado en Historia Moderna, Máster en Administración y Dirección de Empresas y Doctor en Seguridad Internacional. Es Director Financiero de varios grupos de empresas y miembro de la Junta Directiva de la Asociación de Diplomados Españoles en Seguridad y Defensa (ADESyD).*

REFERENCIAS

Babones, Salvatore (2017), "China can´t afford to keep challenging America on military spending", *The National Interest*, March 7. Recuperado de: https://nationalinterest.org/feature/china-cant-afford-keep-challenging-america-military-spending-19703

Balañá, Javier (2018), "Estrategia de Seguridad Nacional y ciberseguridad", en ADESyD, *Actas IV Congreso ADESyD*, Madrid: ADESyD, pp. 46-64.

Béraud-Sudreau, Lucie (2017), "Russia`s defence spending: the impact of economic contration", *International Institute for Strategic Studies*. Disponible en: https://www.iiss.org/en/militarybalanceblog/blogsections/2017-edcc/march-f05a5/russias-defence-spending-7de6.

Brezo, Félix y Rubio, Yaiza (2016), "El uso de BOTS por parte de DAESH en las redes sociales", en ADESyD, *Actas II Congreso ADESyD*, Madrid: ADESyD, pp. 212-230.

Calvo, Carlos (2018)," Innovación", *Documento Opinión Instituto Español de Estudios Estratégicos*, 44/2018, pp.8.

Colom, Guillem (2015), "Runsfeld revisited: La tercera estrategia de compensación estadounidense", *Revista UNISCI*, No. 38, pp. 69-89.

Corte, Luis de la y Blanco, José María (2014), *Seguridad Nacional, amenazas y respuestas*, Madrid: LID editorial.

Committee on Homeland and National Security of the National Science and Technology Council (2016), *A 21st century science, technology and innovation for America`s National Security*, Washington: Executive Office of the President of the United States.

Cordesman, Anthony & Colley, Steven (2015), *Chinese strategy and military modernization in 2015: a comparative analysis*, Washington: Center for Strategic and International Studies.

Covington, Stephen (2016), *The culture of strategic thought behind Russia`s modern approaches to warfare*, Cambridge: Belfer Center for Science and International Affairs.

Defense Intelligence Agency (2017), *Russia Military Power*, Washington: Defense Intelligence Agency.

Díaz, José Antonio (2017), "Desafíos en la vigilancia de las fronteras nacionales y exteriores de la Unión Europea: demanda operativas y necesidades irrenunciables de innovación", en ADESyD, *Actas III Congreso ADESyD*, Madrid: ADESyD, pp. 57-67.

Dirección General de Armamento y Material. Subdirección General de Planificación Tecnología e Innovación (2015), *Estrategia de Tecnología e Innovación para la Defensa*. *ETID 2015*, Madrid: Dirección General de Armamento y Material. Subdirección General de Planificación Tecnología e Inovación.

Docampo, Domingo (2016) "Financiación, educación e investigación en la universidad española: ¿Lo hacemos peor o mejor de lo que algunos quieren hacernos creer?", *Blog de Studia 21*, 7 de junio. Recuperado de: http://:universidadsi.es/financiacion-educacion-e-investigacion-la-universidad-española-lo-hacemos-peor-mejor-lo-que-quieren-hacernos-creer.

Domínguez, Nuño (2018), "Las sociedades científicas denuncian que sólo se gastó el 29% del presupuesto de ciencia en 2017", *El País*, 12 de julio.

Fundación Alternativas (2017), *Informe sobre la Ciencia y la Tecnología en España*, Madrid: Fundación Alternativas. Recuperado de: http://fundacionalternativas.org/public/storage/publicaciones_archivos/1f6da6b4e2fa0bb773bc48b456e972ee.pdf

Fundación COTEC para la Innovación (2018), *Informe COTEC 2018: Innovación en España*, Madrid: Fundación COTEC PARA LA INNOVACIÓN. Recuperado de: http://informecotec.es/media/Informe-Cotec_2018_versi%C3%B3nweb.pdf

Fundación CYD (2016), *Informe CYD 2015: la contribución de las universidades españolas al desarrollo*, Madrid: Fundación CYD. Recuperado de: http://fundacioncyd.org/publicaciones-cyd/informe-cyd-2015/

Gabner, Alexander, (2016) "Deciphering China´s security intentions in northeast Asia: a view from Russia", en Joint US-Korea Academic Studies, *Rethinking Asia in Transition: Security Intentions, Value Gaps and Evolving Economic Relations*, Washington: Joint-US Korea Academic Studies, pp 59-75.

García Alonso, José María (2010), *La base industrial de la Defensa en España*, Madrid: Ministerio de Defensa.

García Montaño, Juan Manuel (2015), "La política industrial de defensa", en Instituto Español de Estudios Estratégicos, *Industria Española de Defensa: Riqueza, tecnología y seguridad*, Madrid: Ministerio de Defensa, pp. 111-142.

Gobierno de España, Presidencia del Gobierno (2013), *Estrategia de Seguridad Nacional. Un proyecto compartido*, Madrid: Presidencia del Gobierno.

Gobierno de España, Presidencia del Gobierno (2017), *Estrategia de Seguridad Nacional. Un proyecto compartido de todos y para todos*, Madrid: Presidencia del Gobierno.

Gudín, Manuel (2017), "Disimetría de sustentación en la seguridad privada con el uso de nuevas tecnologías de aparatos no tripulados", en ADESyD, *Actas III Congreso ADESyD*, Madrid: ADESyD, pp. 296-303.

Hunter, Edward (2016), "Does Russia have the financial means for its military ambitions?", *NATO Review Magazine*. Recuperado de: https://www.nato.int/docu/review/2016/also-in-2016/Does-Russia-have-the-financial-means-for-its-military-ambitions/EN/index.htm.

Instituto Español de Estudios Estratégicos (2016), *Análisis comparativo de las capacidades militares españolas con las de los países de su entorno*, Madrid: Ministerio de Defensa.

Instituto Español de Estudios Estratégicos (2017), *La gestión del conocimiento en la gestión de los programas de Defensa*, Madrid: Ministerio de Defensa.

Jiménez Bastida, José Lorenzo (2017), *Un análisis macroeconómico de los efectos de la inversión en defensa nacional sobre la base industrial y tecnológica en España*, Madrid: Ministerio de Defensa.

Martín, Miguel (Coord.) (2014), *Capacidades futuras de las Fuerzas Armadas*, Madrid: Ministerio de Defensa CESEDEN.

Martín, Miguel Ángel (2015), "Contribución a la Seguridad Nacional de las capacidades ISR (Inteligencia, Vigilancia y Reconocimiento)", en ADESyD, *Actas I Congreso ADESyD*, Madrid: ADESyD, pp. 23-39.

Ministerio de Economía y Competitividad (2013), *Estrategia Española de Ciencia y Tecnología y de Innovación, 2013-2020*, Madrid: Ministerio de Economía y Competitividad.

Ministerio de Economía Industria y Competitividad (2017), *Plan Estatal de Investigación Científica, Técnica y de Innovación 2017-2020*, Madrid: Ministerio de Economía Industria y Competitividad.

Montero, Luis (2015), "EGLos Sistemas de información y comunicación para la seguridad", en ADESyD, *Actas I Congreso ADESyD*, Madrid: ADESyD, pp. 194-200.

Office of the Secretary of Defense (2016), *Military and Security developments involving the People´s Republic of China 2016*, Wroclaw: Amazon Fulfillment.

Pons, Juan (2018a), "Dos programas de Vanguardia", *Revista Española de Defensa*, No. 347, pp. 44-49.

Pons, Juan (2018b), "El largo y tortuoso camino hacia la Agencia Española del Espacio", en ADESyD, *Actas IV Congreso ADESyD*, Madrid: ADESyD, pp. 70-86.

Presidencia del Gobierno (2012), *Directiva Defensa Nacional 2012. Por una defensa necesaria, por una defensa responsable*, Madrid: Presidencia del Gobierno.

-President of the French Republic (2017), *Defence and National Security Strategic review*, París: President of the French Republic.

Secretaría de Estado de Defensa. Dirección General de Armamento y Material (2015), *Estrategia Industrial de Defensa. EID, 2015*. Madrid: Secretaría de Estado de Defensa.

The Defense Science Board (2013), *Report on Technology and Innovation enablers for superiority in 2013*, Wroclaw: Amazon fulfillment.

The Federal Government, (2016), *White Paper 2016 on German Security Policy and the future of the Bunderwehr*, Berlín: The Federal Government.

Torralba, Carlos (2018). "Nuevos nacionalismos, nuevos arsenales", *El País*, 20 de mayo.

Zafra, Manuel (2016), "La Ley 36/2015, de 28 de septiembre, de Seguridad Nacional", en ADESyD, *Actas II Congreso ADESyD*, Madrid: ADESyD, pp. 20-25.