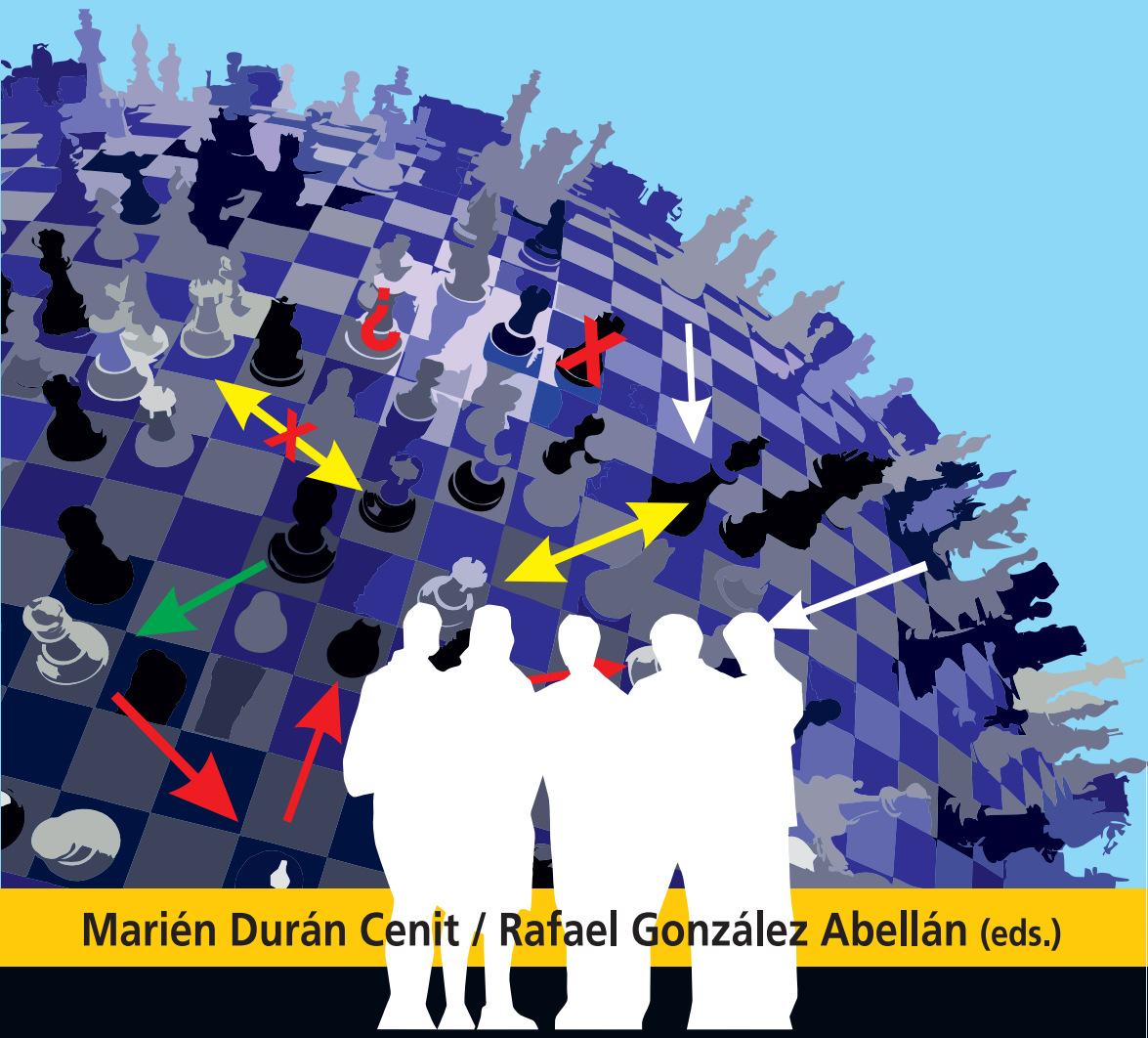


Marién Durán Cenit / Rafael González Abellán (eds.)

Los estudios militares y de seguridad en los albores del siglo XXI

volumen 1

UNIVERSIDAD DE GRANADA
MANDO DE ADIESTRAMIENTO Y DOCTRINA

LOS ESTUDIOS MILITARES Y DE SEGURIDAD EN LOS ALBORES DEL SIGLO XXI

Marién Durán Cenit
Rafael González Abellán
(Eds.)

LOS ESTUDIOS MILITARES Y DE SEGURIDAD EN LOS ALBORES DEL SIGLO XXI

VOL. 1

GRANADA
2017

Colección Conde de Tendilla

El Centro Mixto UGR-MADOC no se responsabiliza de las opiniones de los autores.

ISBN: 978-84-338-6103-0
Edita: Editorial Universidad de Granada
Campus Universitario de Cartuja. Granada
Colegio Máximo, s.n., 18071, Granada
Telf.: 958 243930-246220
Web: editorial.ugr.es
Fotocomposición: María José García Sanchis. Granada
Diseño de cubierta: José María Medina Alvea. Granada

INDICE

BLOQUE II:
TERRORISMO INTERNACIONAL

BLOQUE III:
CIBERSEGURIDAD Y CIBERDEFENSA

BLOQUE IV
CULTURA DE DEFENSA

BLOQUE V
ECONOMÍA E INDUSTRIA DE DEFENSA

BLOQUE VI
ENSEÑANZA, FORMACIÓN Y CONOCIMIENTO DE LAS FFAA

Prólogo

La Universidad de Granada viene manteniendo una intensa colaboración con el Ministerio de Defensa y con el Mando de Adiestramiento y Doctrina del Ejército (MADOC) gracias a la instalación en Granada de este último hace ya más de veinte años. Desde entonces, y a lo largo de estas dos dilatadas décadas, se han ido fortaleciendo unas estrechas y enriquecedoras relaciones que, movidas por una misma vocación de servicio a la sociedad, han dado como resultado la organización de una variada oferta de actividades dirigidas a la comunidad universitaria y a las Fuerzas Armadas.

Entre esas iniciativas culminadas con éxito destacan las de carácter formativo como congresos nacionales e internacionales, seminarios, jornadas, conferencias, workshops y cursos de verano; las de naturaleza científica plasmadas en múltiples proyectos de investigación en diferentes disciplinas y con importantes resultados académicos en el ámbito nacional e internacional; actividades culturales e institucionales, así como una línea propia de publicaciones dentro de la editorial de la Universidad de Granada.

Producto de esta amplia y provechosa colaboración fue el surgimiento del Centro Mixto UGR-MADOC (CEMIX) en el año 2010, que tiene como objeto coordinar esfuerzos, dirigir acciones y actividades, así como establecer una fértil colaboración entre ambas instituciones, fundamentada en el diálogo, el consenso y la complementariedad en las materias de seguridad y defensa.

Desde el CEMIX se canalizan todas las acciones del Plan Anual de Colaboración que año tras año tienen lugar en el seno de la Universidad y el MADOC. Entre las múltiples actividades desarrolladas, el CEMIX ha gestionado en octubre de 2016 uno de sus encuentros cumbre para difundir la Cultura de Defensa: la celebración del II Congreso Internacional de Estudios Militares

en el marco del Convenio de Colaboración suscrito en el año 2013 con el Banco de Santander.

El Congreso, con un marcado carácter internacional y con el título «Hacia una estrategia global de seguridad y defensa de la Unión Europea», acogió a una gran cantidad de participantes durante tres jornadas. Organizado con un exigente programa de conferencias y sesiones de comunicaciones, se contó, por un lado, con la participación de un nutrido grupo de expertos conferenciantes del ámbito político, diplomático, académico, jurídico y militar que proporcionaron un prestigioso elenco de análisis, con más de cien expertos que compartieron sus investigaciones en las diez sesiones que se organizaron con gran éxito de asistencia.

Los resultados de este Congreso han sido muy fructíferos gracias al interés y a la desinteresada participación de personalidades provenientes de una nutrida lista de centros y universidades. Por ello, uno de los objetivos prioritarios ha sido la publicación de estos trabajos de investigación en la colección Biblioteca Conde de Tendilla integrada en el catálogo de la Editorial de la Universidad de Granada, considerada una de las editoriales universitarias más prestigiosas de nuestro país. La Biblioteca Conde de Tendilla ha sido una colección muy activa desde que comenzase su andadura en el año 2010, manteniendo una línea constante de publicaciones en las materias de ámbito militar y de seguridad.

Para enriquecer esta interesante colección, la obra que se publica con el título «Los estudios militares y de seguridad en los albores del siglo XXI" constituye un material significativo, relevante, actual, minucioso y con aportaciones muy novedosas a los campos de la seguridad y de la defensa desde diferentes disciplinas como la Economía, la Ciencia Política, la Ingeniería y la Sociología. Además, otro valor añadido de esta edición lo constituye el hecho de contener trabajos realizados por destacados investigadores universitarios y por expertos militares.

Los dos volúmenes que componen la publicación conforman una obra de gran calidad por la recopilación de los múltiples aspectos que conlleva la seguridad y la defensa, así como por su decidido carácter científico que aborda temas como amenazas y riesgos para la seguridad a nivel general; terrorismo internacional; ciberseguridad y ciberdefensa; cultura de defensa; economía e industria de defensa; enseñanza, formación y conocimiento en las Fuerzas Armadas; Estrategia Regional Europea; estrategias y

problemas nacionales y regionales de seguridad; liderazgo, valores y procesos; e instrumentos, técnicas y modelos para la acción militar.

Los citados bloques temáticos se han abordado con una mirada científica, multidisciplinar, grupal y colectiva que reunió a ponentes de diferentes universidades españolas e iberoamericanas. Estas actas representan un fruto muy valioso en diversos sentidos: es obra de consulta de conceptos e ideas para temas actuales militares y de seguridad y defensa, además de muy útil para profesionales de la seguridad; y herramienta de trabajo para investigadores y docentes que quieran profundizar en las últimas líneas de investigación que se están desarrollando en el momento presente sobre las decisivas materias que este libro contiene.

Pilar Aranda Ramírez

Rectora de la Universidad de Granada

Prólogo

En octubre de 2016 el Mando de Adiestramiento y Doctrina (MADOC) acometió la celebración del II Congreso Internacional de Estudios Militares, en el marco del Convenio de Colaboración suscrito en 2013 con el Banco Santander. Esta segunda edición, cuya planificación y gestión recae en Centro Mixto Universidad de Granada-MADOC, se hace en un momento de madurez de un proyecto que nació con la finalidad de contribuir al fomento y difusión de la Cultura de Defensa

En las jornadas, que se desarrollaron bajo el título *Hacia una estrategia global de seguridad y defensa de la unión europea*, abordamos la posición geoestratégica de Europa ante el cambiante e inestable entorno de seguridad que estamos viviendo, entorno que nos recuerda que la paz, la libertad y la seguridad, que tan solo hace unos años parecía garantizada, parece ahora estar en serio peligro consecuencia de los conflictos que nos rodean en nuestra vecindad, oriental y meridional. Temática de rabiosa actualidad, las razones que nos llevaron a su elección fueron varias:

—Primera: La obligación de situar las estrategias de seguridad y defensa en un contexto internacional que, en el caso de España, viene dado por su condición de miembro de la Alianza Atlántica y de la Unión Europea.
—Segunda: Las corrientes de opinión partidarias de que la Unión Europea afronte de una manera decidida un nuevo marco estratégico de seguridad, acorde con la magnitud de los cambios producidos en esta materia en los niveles regional e internacional, especialmente los protagonizados por Rusia y el radicalismo violento.
—Tercera: El cumplimiento del 30 aniversario del ingreso de España en la Unión Europea y del referéndum de perma-

nencia en la OTAN, así como el 20 aniversario del ingreso en su estructura militar, ofrecía una justificación perfecta para reflexionar sobre el estado de la seguridad y la defensa en ambas estructuras internacionales.

Para el desarrollo programa académico hemos contado con la participación de expertos e ilustres conferenciantes del mundo diplomático, político, académico y de las Fuerzas Armadas con experiencia en esta materia. La participación, tanto en términos cuantitativos como cualitativos, cumplió todas las expectativas.

Conscientes de que lo realizado es una actividad más entre las muchas patrocinadas por otras instituciones, estamos sin embargo convencidos de que el principal instrumento para transmitir y generar conocimiento sobre cualquier materia es la comunicación. Por ello, finalizado el Congreso, nos fijamos como reto la publicación de este libro que viene a certificar, en línea con la finalidad del proyecto, el cumplimiento de uno de los principales objetivos que nos planteamos, que no es otro que la promoción y difusión de estudios y análisis sobre distintos aspectos relacionados con la Seguridad, la Defensa y las Fuerzas Armadas.

Este libro recoge, el esfuerzo de aquellos investigadores civiles y militares que canalizan sus energías y dedican su tiempo al estudio de estos temas. La obra constituye una aportación importante, concienzuda y de riguroso valor intelectual, que se pone a disposición de la sociedad como fuente de información y conocimiento. Como decía Abraham Lincoln, «El conocimiento es la mejor inversión que se puede hacer».

En el título elegido para la publicación *Los estudios militares en los albores del siglo XXI*, subyace la diversidad de campos en torno a los cuales los investigadores pueden desarrollar su tarea investigadora en materia de Seguridad y Defensa.

Queremos agradecer el trabajo llevado a cabo por los miembros del Comité Organizador, por la organización del Congreso y por el proceso de revisión del gran número de comunicaciones recibidas, que ha dado como resultado la selección de ponencias incluidas en este libro de actas. No hubiera sido posible este congreso sin la participación de los autores de los artículos que han llenado de contenido este libro y dan un paso más en la ordenación.

Por último señalar que, junto al trabajo que se desarrolla en otras instituciones tanto del ámbito civil como del militar que con

carácter casi exclusivo se dedican de forma destacada a esta tarea, tenemos la ilusión de que desde Granada se irradie interés y se fomente una rica red que permita profundizar en este campo tan importante como es la seguridad de España.

José Carrasco Gabaldón
Teniente General del MADOC

LOS ESTUDIOS MILITARES Y DE SEGURIDAD EN LOS ALBORES DEL SIGLO XXI

Marién Durán Cenit
Rafael González Abellán
(Eds.)

Los amplios volúmenes de los que consta esta obra son el producto de las comunicaciones y los trabajos presentados en el II Congreso Internacional de Estudios Militares, celebrado en la Universidad de Granada en octubre de 2016. Este Congreso es la continuación del I Congreso de Estudios Militares que tuvo lugar en septiembre de 2014 con gran éxito. Debido a los resultados y la acogida de este evento se ha continuado con este tipo de fructíferos encuentros con expertos y académicos del ámbito nacional e internacional. El resultado es que el II Congreso no ha sido menos exitoso que el primer encuentro. De ahí el reflejo en esta obra construida y diseñada con el cariño que merece gracias a una amplia, interesante y prestigiosa asistencia.

Estos congresos de carácter bienal tienen por objetivo los temas relacionados con la seguridad, la defensa y las Fuerzas Armadas. En ellos concurren investigadores, profesores y militares especialistas en temas que abarcan múltiples aspectos relacionados con los estudios de seguridad y defensa. El Congreso tiene un carácter tanto nacional como internacional. La presencia internacional es remarcable, especialmente de otros países europeos y muy especialmente de Iberoamérica.

El Congreso constituye a su vez un foro multidisciplinar donde los investigadores y expertos civiles y militares, a nivel particular, de las instituciones organizadoras y colaboradoras y de muy diferentes universidades, puedan intercambiar experiencias, conocimientos y resultados de sus investigaciones en el ámbito de la seguridad y la defensa. En definitiva, constituir redes tanto nacionales como internacionales, así como redes mixtas entre civiles y militares.

El II Congreso Internacional de Estudios Militares ha llevado por título *el análisis de las estrategias de seguridad y defensa en el marco*

euroatlántico y europeo y en el contexto general de la seguridad internacional. Son varios los motivos justifican este elección.

En primer lugar, la obligación de situar las estrategias de seguridad y defensa en un contexto internacional que, en el caso de España, viene dado por su condición de miembro de la Alianza Atlántica y de la Unión Europea que, a su vez, están implicadas en el modelo general de seguridad internacional. Los cambios continuos y profundos, los nuevos desafíos, la aparición de nuevos conflictos y la incertidumbre sobre las amenazas y las necesidades de seguridad, se explican en clave internacional y en los distintos niveles de cooperación en los está implicada España en su contribución a la seguridad internacional.

En segundo lugar, la importancia de abordar un análisis de las estrategias euroatlántica y europea en términos de experiencia y lecciones aprendidas aprovechando la conmemoración del 30 aniversario del ingreso de España en la Unión Europea y del referéndum de permanencia en la OTAN, así como el veinte aniversario del ingreso en su estructura militar. Esta coincidencia de efemérides ofrece una justificación perfecta para reflexionar y exponer trabajos sobre el estado de la seguridad y la defensa en ambas estructuras internacionales y su participación en el contexto de seguridad internacional.

Cada vez son más numerosas y coincidentes las corrientes de opinión partidarias de que la Unión Europea afronte de una manera decidida un nuevo marco estratégico de seguridad, acorde con la magnitud de los cambios producidos en los niveles regional e internacional, desde la publicación, en 2003, de la Estrategia de Seguridad Europea. A ello se suman los cambios incorporados por el nuevo contexto normativo que ofrece el Tratado de Lisboa. En la misma línea se plantea la necesidad de una nueva estrategia de seguridad de la OTAN en Europa. Apuntando en esa misma dirección de renovación, se encuentran los importantes cambios que introdujo Estados Unidos en su nueva estrategia de seguridad, publicada a principios del 2015. Además a todo ello se suma el actual contexto de seguridad internacional, donde la UE participa con diversas misiones internacionales.

En tercer lugar, y como consecuencia de los cambios que se avecinan a esos efectos, nos encontramos con la necesidad de realizar un análisis prospectivo de esas nuevas tendencias estratégicas teniendo como perspectiva el primer cuarto de siglo (2025).

Por último, el reconocimiento del valor del análisis multidisciplinar y el carácter multidimensional de las cuestiones de seguridad y defensa ha de permitir a los investigadores analizar y reflexionar sobre las distintos aspectos y dimensiones que comprende esta materia, desde sus componentes tradicionales vinculados a la defensa territorial hasta los más actuales como el terrorismo, la delincuencia organizada transnacional, la proliferación armamentística, la seguridad energética o la ciberseguridad, entre otros. Los académicos e investigadores provienen de múltiples campos como la Ciencia Política, el Derecho, la Economía, Sociología, Historia, Ingeniería, etc.

Para reflexionar sobre estas cuestiones el Congreso se organizó en sesiones de conferencias y mesas redondas durante la mañana y en sesiones de comunicaciones durante la tarde. Durante las tres sesiones de mañana se contó con la presencia de especialistas de referencia nacional e internacional que nos ofrecieron brillantes conferencias sobre las temáticas referidas. Las dos sesiones dedicadas a las comunicaciones contaron con la presencia de múltiples expertos. Ambos formatos de intervención fueron todo un éxito. Las sesiones de mañana destacaron por la calidad de sus conferenciantes. Igualmente las comunicaciones fueron de sumo interés con gran éxito de audiencia en ambos eventos y con una excelente coordinación por parte de los coordinadores provenientes tanto del mundo militar como del campo académico.

La conferencia inaugural corrió a cargo de D. Marcelino Oreja Aguirre, ex Ministro de Asuntos exteriores, que nos ilustró sobre «El camino hacia una Estrategia global de Seguridad y Defensa de la Unión Europea: obstáculos y retos». Con una conferencia magistral y marcada por su amplia experiencia, fue capaz de desglosar de manera amena esos principales retos y desafíos.

La primera sesión que llevaba por título «La seguridad internacional: un marco de referencia general para la acción de la Unión Europea», estuvo a cargo de dos magníficos conferenciantes. D. Amador Enseñat y Berea, General de División, participó con la Conferencia: «La contribución de Naciones Unidas a la Seguridad Internacional: la evolución del concepto de Operaciones de Apoyo a la Paz». Posteriormente y cerrando la mañana, D. Charles Powell Solares, profesor de Historia Contemporánea de la Universidad San Pablo Ceu y Director del Real instituto Elca-

no trató de una forma excepcional «La estrategia de seguridad y defensa de EEUU: prioridades y nuevas formas de liderazgo».

En el segundo día de congreso, la sesión de las conferencias tuvo por título «La seguridad europea. Cooperación estratégica OTAN-UE». En esta sesión se contó con la presencia de expertos civiles y militares en esta área. Comenzó la misma, D. José Luis Urcelay Verdugo, almirante y representante Militar de España ante la OTAN y la Unión Europea con la magnífica conferencia que llevaba por título «Una alianza del Siglo XXI. Adaptación a los nuevos retos de seguridad». Seguidamente intervino D. Nicolás Pascual de la Parte, Embajador Representante de España en el Comité Político y de Seguridad de la Unión Europea, que nos ofreció una significativa conferencia sobre «La Política Común de Seguridad y Defensa: opciones políticas, capacidades militares y nuevos retos».

Finalmente, la mañana se cerró con un interesante y estimulante panel sobre «Estrategias europeas frente al terrorismo y al Ciberterrorismo». En el mismo participaron D. Antonio Esteban López. Coronel de Infantería. Unidad de Estudios del MADOC; D. Ángel Gómez de Ágreda. Teniente Coronel del Ejército del Aire. Área de Análisis Geopolítico de la División de Estudios de Seguridad y Defensa de SEGENPOL y D. Víctor Manuel García Sacristán. Coronel de la Guardia Civil. Centro de Operaciones de la Guardia Civil.

La última mañana de sesión transcurrió de manera intensa, interesante y con brillantes conferencias. Fue una sesión dedicada a la estrategia global de seguridad y defensa de la Unión Europea, con las siguientes conferencias. En primer lugar, «El conflicto de Ucrania: consecuencias para Europa», impartida por D. José Pardo de Santayana, del Instituto Español de Estudios Estratégicos (CESEDEN-Ministerio de Defensa). «Las amenazas a la seguridad europea: El flanco Sur y Sureste» de D. Carlos Echeverría Jesús. Profesor de Relaciones Internacionales de la UNED. Finalmente, esta última sesión se clausuró con la magnífica y minuciosa conferencia sobre Seguridad y defensa europeas: desafíos y prioridades, impartida por D. Pedro Serrano de Haro Soriano. Embajador y Vicesecretario general en el Servicio Europeo de Acción Exterior responsable de Política de Seguridad Común y Defensa (PSCD) y Respuesta a Crisis.

Las sesiones de la tarde, se organizaron en diez paneles cada uno coordinado por un especialista académico y militar experto.

Cinco paneles estuvieron a cargo de profesores de universidad de distintas disciplinas: economía, ciencia política, sociología e ingeniería. Igualmente otros cinco paneles fueron dirigidos por expertos militares de distinto rango. Estos bloques abarcaron distintas temáticas: amenazas y riesgos para la seguridad; terrorismo internacional; ciberseguridad y ciberdefensa; cultura de defensa; economía e industria de defensa; enseñanza, formación y conocimiento en las Fuerzas Armadas; Estrategia Regional Europea; estrategias y problemas nacionales y regionales de seguridad; liderazgo, valores y procesos; instrumentos técnicas y modelos para la acción militar.

Los coordinadores, los cuales organizaron unas muy dinámicas sesiones, fueron D. Marcos Gómez Casal de la Escuela Militar de Defensa NBQ (EMDNBQ) de la Escuela de Guerra del Ejército (EGE); Dª Aurelia Valiño catedrática de la Universidad Complutense de Madrid; D. Luis Álvarez de la Universidad, profesor titular en las Palmas de Gran Canaria; D. Diego Becerril, profesor titular de la Universidad de Granada; Dª Claudia Pérez, profesora titular de la Universidad de Zaragoza; D. Antonio Martínez de Baños de la Academia General Militar; D. José Antonio Herráiz, de la Dirección de Instrucción, Doctrina, Orgánica y Materiales del MADOC. Dirección de Instrucción, Doctrina, Orgánica y Materiales; D. Galo Cruz Cárdenas. Universidad de las Fuerzas Armadas ESPE, República del Ecuador; D. Adolfo Calatrava, profesor de la Universidad Carlos III; D. Juan José Valero de la Muela Analista de la Jefatura de Adiestramiento y Doctrina de logística, de la DIDOM en la ACLOG (Academia de Logística del ET).

De todos estos trabajos, son resultado los dos volúmenes que aquí se presentan. El total de capítulos que constituye esta obra pretende que los contenidos y los resultados que se generan, puedan suponer una actividad de interés para los profesionales de la seguridad, estudiantes de grado y posgrado y másteres que quieran dedicar sus esfuerzos y futuros estudios a las disciplinas de la seguridad y la defensa. La difusión que se efectúa de los trabajos constituye otro pilar de importancia para dar a conocer trabajos de calidad e investigaciones novedosas. Los trabajos que forman parte de esta obra, conforman una valiosa y diversa documentación en torno a las cuestiones más actuales de carácter general y específico de los estudios de seguridad y defensa de nuestro tiempo.

La obra se organiza en torno a dos volúmenes repartidos en diez bloques temáticos que han compuesto los bloques de las comunicaciones tratadas durante el Congreso. En todos y cada uno de ellos se abordan multitud de temas

El primer bloque, «Amenazas y Riesgos para la Seguridad», consta de cinco capítulos donde se exponen cuestiones tanto de carácter transversal, como regional o de estudios de caso. Así tenemos que se tratan temas como la proliferación nuclear, la radicalización islamista, la situación sociopolítica en un estudio de caso como es Afganistán después de la retirada de Estados Unidos en 2014, los cambios en la sociedad europea como consecuencia de la crisis de los refugiados; o los sistemas armamentísticos autónomos. Todos ellos configuran un bloque temático sumamente interesante y completo para el estudio y comprensión de las amenazas y riesgos contemporáneos.

El segundo bloque, sobre «Terrorismo Internacional», abarca una serie de capítulos, concretamente cuatro, principalmente de temas más generales o globales con un caso particular. El primero de ellos es sobre contraterrorismo y reorientación de las Fuerzas Armadas de misiones de seguridad interior y la nueva estrategia de seguridad para una nueva forma de conflicto en el siglo XXI. El segundo se centra en la cuestión del Daesh, tratando de aclarar conceptos como Islam y terrorismo. El tercero trata de establecer si existe un perfil del terrorista yihadista y por último, se aborda el caso de Siria, concretamente en la zona de Al Shams, donde su autora trata la cuestión de un conflicto dentro del conflicto, Daula versus Hizbullah.

El tercer bloque temático se adentra en los actuales temas de ciberseguridad y ciberdefensa. En total lo componen seis capítulos que abordan de forma muy comprehensiva los principales problemas que atañen estas cuestiones: desde las estrategias de ciberseguridad y ciberdefensa en la UE y de la seguridad nacional y sus retos para la estrategia de seguridad y defensa euroatlántica, hasta temas más específicos igualmente preocupantes. Con la ampliación del entorno de seguridad, el tema de la trata de seres humanos como un asunto de seguridad y el estudio de si existen instrumentos suficientes para la lucha contra el cybertrafficking. En cuarto lugar, la defensa de la privacidad en la era de la ciberseguridad. Le sigue un capítulo donde se analizan detalladamente la seguridad de aplicaciones en red mediante diseño por contrato

y ADA 2012. Y por último, el capítulo final de esta sección se centra en la formación en ciberdefensa.

La sección cuarta sobre cultura de defensa, trata tres temas diversos, pero necesarios para entender aspectos determinados sobre esta materia. Encontramos desde un tema más teórico, otro tema más dedicado al trabajo de campo y finalmente un tema más descriptivo y analítico. El bloque comienza con el estudio de la aproximación histórico jurídica al concepto de guerra justa en la edad contemporánea. Le sigue el tema sobre el diseño y la validación de un instrumento de recogida de información en archivos militares, concretamente centrado en los archivos militares de Ceuta y Melilla. Por último, diversos autores nos ilustran sobre la actividad reservista al servicio de la cultura de defensa y la seguridad nacional.

El quinto bloque temático, bajo el título «Economía e Industria de Defensa», destaca por la participación de la «Cátedra Paz Seguridad y Defensa», concretamente con cuatro trabajos que afrontan las siguientes cuestiones: la Estrategia de Seguridad Nacional y la percepción de la amenaza: la inestabilidad económica y financiera, esto es si la ciudadanía española y de otros lugares del mundo, en un contexto geográfico y temporal, sienten como amenaza para la seguridad nacional la inestabilidad económica. En segundo lugar, nos encontramos con el estudio que se adentra en la perspectiva económica de la participación española en las Operaciones de Mantenimiento de la Paz, después de más de veinticinco años participando en misiones en el exterior en las que se han invertido más de 10.000 millones de euros y han intervenido más de 100.000 soldados. Seguidamente, se presenta un trabajo sobre los modelos de financiación de la Defensa y por último se trabaja sobre un modelo de gestión del conocimiento económico basado en el marco input output, con caso de estudio aplicado al sector la Defensa en España.

El sexto bloque y último del primer volumen, «Enseñanza, formación y conocimiento de las FFAA», está compuesto igualmente por tres trabajos que abordan desde el proceso Bolonia en la educación de la oficialidad y los puntos esenciales para su adaptación al marco OTAN, hasta el estudio sobre la gestión del conocimiento en la Dirección de Investigación, Doctrina y Orgánica y Materiales (DIDOM), pasando por un proyecto que trata de la visión, implementación y explotación del motor de búsque-

da de contenidos en la red de Intranet de Defensa. Todos ellos, con un marcado carácter programático y práctico, nos ayudan a entender las cuestiones más actuales sobre procesos formativos y de enseñanza en las FFAA.

El segundo volumen está compuesto por cuatro bloques. El Bloque número siete aborda la línea referente a «Estrategias y problemas nacionales y regionales de seguridad». La temática planteada y los seis capítulos que aquí se presentan emprenden tanto de manera general como más específica, las diferentes problemáticas sobre las estrategias europeas. Tenemos cuatro capítulos que se centran en temas más geopolíticos y geoestratégicos: (i) La OTAN y la UE, su presencia en la geopolítica y la geoestrategia Antártica; (ii) Hacia un nuevo concepto geopolítico en Europa; (iii) Identidad europea y seguridad europea; (iv) La UE y los conflictos congelados en el antiguo espacio soviético. A continuación le siguen dos capítulos que tratan sobre temas más concretos como el servicio europeo de acción exterior y el control de datos de los pasajeros aéreos en la UE en la lucha antiterrorista.

En el bloque octavo, que lleva por título «Estrategias y problemas nacionales y regionales de seguridad», se dispone en torno a una serie de capítulos que estudian y analizan diferentes regiones y países del mundo: América Latina, Oriente Medio, los Países Bálticos, Ucrania, España, Brasil y Afganistán En cuanto al tema de América Latina, la línea de trabajo versa sobre los dilemas estratégicos en tiempos de reflexión. En segundo lugar, la seguridad regional en Oriente Medio abarca la cuestión de la pugna hegemónica entre Irán y Arabia Saudí. La cuestión de los países Bálticos se trata desde la perspectiva de la OTAN, analizando el factor geopolítico. Seguidamente tenemos el tema de Ucrania y su situación actual al haber alterado las relaciones entre Rusia y la UE. A continuación se exponen dos capítulos referentes a los problemas españoles: «Constantes en la política de seguridad y defensa de España y la versatilidad de la relación con la OTAN» y «La seguridad y la defensa nacional en el nuevo Código Penal Militar». También Brasil, como potencia regional de América Latina, se aborda de manera interesante, centrándose su autor en «Los nuevos retos de seguridad y defensa y sus impactos en las transformación de las FFAA en Brasil. Por último, este bloque se cierra haciendo un repaso a la experiencia y lecciones aprendidas en la Reforma del Sector de la Seguridad en Afganistán.

Seguidamente, el bloque noveno, «Liderazgo, valores y procesos» está constituido por seis capítulos que se centran en cuestiones tanto de aspectos psicológicos en el desarrollo de la carrera de las FFA, como en cuestiones de valores. A este respecto tenemos dos trabajos: (i) Valores y cualidades del militar según las reales ordenanzas para las FFAA; (ii) Valores y cualidades del militar según análisis de las estrategias de adaptación al duelo del personal de una unidad militar tras su participación en una misión internacional. También se abordan cuestiones más diversas como la influencia de las Operaciones en el exterior sobre el Ejército de Tierra Español, el liderazgo de los pilotos en combate y la inserción femenina de las FFAA brasileñas.

Finalmente, con el bloque de trabajo número X, con el título «Instrumentos, técnicas y modelos para la acción militar», nos adentramos en un conjunto de trabajos sumamente específico, muchos de ellos desarrollados por grupos de investigación consolidados. Concretamente estos son: (i) Criptoprocesador compacto para la seguridad en sistemas de monitorización inalámbrica; (ii) Atención, electroencefalograma y tareas militares; (iii) Sistema vestible de monitorización de señales biométricas; y (iv) Metodología para la caracterización de combustibles forestales mediante técnicas de teledirección y trabajo de campo. El resto de los temas, centrados tanto en cuestiones más técnicas como de seguridad en general, afrontan igualmente temas referentes a los instrumentos y modelos para la acción militar: (i) Filosofía Lean en una unidad logística del Ejército de Tierra; (ii) La evolución de las tecnologías y estrategias de guerra y protección de los civiles; (iii) Ciudades más seguras en la España globalizada y (iv) Clasificación rápida de puentes.

BLOQUE I:

AMENAZAS Y RIESGOS PARA LA SEGURIDAD

LA PROLIFERACION NUCLEAR: UNA REALIDAD

Marcos Gómez Casal
Escuela Militar de Defensa NBQ

Resumen

Desde la aparición del arma nuclear muchos Estados han tenido la pretensión de lograr dicha capacidad. Unos lo han conseguido y otros no. Es fundamental lograr evitar la proliferación nuclear, para ello existen herramientas de no proliferación. Para alcanzar el éxito en este ámbito político deben analizarse detenidamente las motivaciones que cada estado tiene para lograr la capacidad nuclear, para así poder abordar con amplio espectro esta problemática. Esto, junto con aprender de los errores cometidos en el pasado y una buena diplomacia internacional es la única manera de mantener la esperanza de evitar la proliferación.

Palabras claves

Proliferación nuclear, No Proliferación nuclear, Arma nuclear, Armas destrucción masiva, NBQ.

1. Introducción

Con las explosiones nucleares de Hiroshima y Nagasaki el 6 y el 9 de julio de 1945 respectivamente, el final de la Segunda Guerra Mundial (SGM) estaba próximo. Dichas explosiones mostraron al mundo como una cabeza nuclear era capaz de devastar una ciudad en escasos instantes, ocasionando daños materiales nunca antes imaginados, así como causar gran número de muertos, heridos y la aparición de algo no bien entendido más que por unos pocos científicos… una zona radiológicamente contaminada, que la hacía impracticable para ningún uso.

Las explosiones nucleares supusieron una propaganda de nación indestructible para los Estados Unidos, habían logrado

desarrollar un arma de «destrucción total». Esto supuso el júbilo generalizado no solo de los políticos y militares, sino de la población civil de las naciones aliadas. Oculto bajo ese sentimiento de no poder ser derrotados en un futuro, empezó a surgir entre los políticos y militares una preocupación, ya que los demás estados intentarían alcanzar la misma capacidad, si eso ocurriera la única solución era tener mayor capacidad nuclear que los adversarios.

En 1949 la URSS hizo su primer ensayo nuclear, iniciándose la «carrera armamentística nuclear». El pico máximo de cabezas nucleares de EEUU se alcanzó en 1967 (31,255), mientras que la URSS lo alcanzó en 1986 (aproximadamente 45.000)[1], muchas capaces de ser lanzadas, en un breve espacio de tiempo, sobre objetivos militares y civiles. J.F. Kennedy, en un discurso ante las Naciones Unidas (NNUU)[2] en 1961, indicó que las armas nucleares suponían un mayor peligro para la sociedad que el beneficio que representaban para la seguridad. Su homólogo ruso también era consciente que el lanzamiento de una cabeza nuclear podría suponer no sólo la total destrucción del adversario, sino también la propia (Destrucción Mutua Asegurada - MAD). Tal es así que esta teoría también es conocida como la «1+1=0». Este concepto proviene de las doctrinas de los años 50 de los EEUU, siendo el tema central del planeamiento de la defensa de EEUU durante unos 30 años. Esto fue así ya que si bien por un lado un incidente podría llevar a la destrucción propia, por otro lado se consideraba que esa era la mejor medida de disuasión del empleo de armas nucleares.

2. Conceptos básicos

Antes de desarrollar el contenido del documento se considera oportuno introducir una serie de conceptos básicos de tipo técnico, el trato que se le da a los mismos no es muy exhaustivo por no ser tal profusión específica necesaria en este documento, proporcionando por tanto una visión muy genérica de los mismos.

1. *Robert Norris, Hans M. Kristensen,* «Global nuclear weapons inventories, 1945–2010,» *Bulletin of the Atomic Scientists (July 1, 2010).*

2. Discurso del Presidente John F. Kennedy ante NNUU, puede verse en: *http://www.state.gov/p/io/potusunga/207241.htm*

—Uranio natural: Es el existente en la naturaleza, consta de tres isótopos radiactivos, el Uranio 238 (99,285%), el uranio 235 (0,71%) y el uranio 234 (0,005%).
—Material nuclear[3]: Se consideran son el uranio 233, uranio 235, plutonio 239, plutonio 241, o cualquier combinación de estos radionucleidos. Al no existir el uranio 233 en la naturaleza es más sencillo proceder a enriquecer el uranio natural en su isótopo 235. El uranio empleado para uso armamentístico está enriquecido en torno al 90% o superior.
—Enriquecimiento de Uranio: es un proceso por el cual el uranio natural es enriquecido en su isótopo 235, dependiendo del grado de enriquecimiento, su uso se destina a reactores nucleares de potencia (Centrales Nucleares), reactores de investigación, propulsión de submarinos nucleares o armamento nuclear. Varias han sido las técnicas de enriquecimiento, estando algunas de ellas en desuso por considerarse obsoletas debido, fundamentalmente, el alto consumo energético así como la poca eficiencia. Actualmente la técnica de enriquecimiento más extendida es la centrifugación, si bien en un futuro no muy lejano puede ser desplazada por el enriquecimiento por láser.
—Cabezas nucleares[4]: Dispositivo de ingeniería diseñado y ensamblado para generar una explosión nuclear. Difiere de un dispositivo nuclear improvisado (IND) en que éste último es un dispositivo fabricado fuera de una cadena de producción de cabezas nucleares. Relacionado con este concepto está el de vector de lanzamiento, que es aquel dispositivo que permite a una cabeza nuclear alcanzar el objetivo deseado.

Las cabezas nucleares pueden clasificarse, según el material fisible que emplean, en cabezas de uranio o de plutonio. Dependiendo del programa nuclear que haya elegido uno u otro país, están más enfocados en obtener el uranio enriquecido (Little boy, 6 de agosto de 1945, Hiroshima) o en obtener el plutonio (Fat man, 9 de agosto de 1945, Nagasaki). La diferencia es que si

3. Definido en: *http://www.nrc.gov/materials/sp-nucmaterials.html*

4. Concepto definido en *Department of Defense, Dictionary of Military and Associated Terms, Joint Publication (JP) 1-02 (2016).*

la cabeza nuclear es de plutonio, se necesita menos cantidad del mismo para tener la misma potencia que una cabeza de uranio. El conseguir es un proceso técnicamente más complejo que el enriquecimiento de uranio. Básicamente consiste en extraer el material combustible del interior de un reactor nuclear, una vez ha sido irradiado, debido al normal funcionamiento del mismo, y separar el plutonio existente en un porcentaje relativamente bajo del resto del material. Luego es necesario disponer de un reactor nuclear para obtener plutonio, pero no para enriquecer uranio.

Según un dispositivo de detonación, una cabeza nuclear puede ser de tipo cañón (Little boy) o de implosión (Fat man). En el primer caso se tienen dos masas del material nuclear (WGU) separadas una determinada distancia, una de ellas es proyectada hacia la otra para conseguir la detonación nuclear. En el segundo caso el material nuclear es rodeado externamente por un sistema complejo de explosivos que al iniciarse hacen que el volumen del material nuclear se compacte produciéndose así la detonación nuclear. Los dispositivos de tipo cañón son técnicamente mucho más sencillos que los de implosión. Las cabezas de Uranio pueden ser tanto de tipo cañón como de implosión, si bien las de plutonio solamente pueden ser de implosión.

Según el tipo de reacción nuclear, una detonación nuclear puede ser de fisión o de fusión. El primer caso consiste en que núcleos pesados (uranio y plutonio) se fragmentan en otros más ligeros cuando incide sobre ellos un neutrón, en cada fisión se generan, según el caso, 2 o 3 nuevos neutrones, que permiten, si el diseño de la cabeza es correcto, iniciar una reacción nuclear en cadena auto-sostenible. Los fragmentos de la fisión son núcleos radiactivos, lo que en este tipo de dispositivos se genera una zona donde se deposita el material radiactivo (lluvia radiactiva), su extensión depende del material nuclear, potencia del arma, altura de explosión y condiciones climatológicas y del terreno. En cuanto la fusión nuclear es la unión de dos núcleos ligeros para obtener uno más pesado acompañado de una emisión de neutrones, normalmente este nuevo núcleo no es radiactivo, si bien el flujo neutrónico generado es mucho más elevado que en una cabeza nuclear de fisión. La potencia de la detonación que se logra en la fusión nuclear es mucho más elevada que en la fisión. Un inconveniente de la fusión nuclear es que actualmente la única opción que existe para que se puede producir en una cabeza nuclear es

alcanzar una temperatura tal que solo puede ser alcanzada en una reacción de fisión, con lo que todas las cabezas nucleares de fusión necesitan un componente previo que sea de fusión, es lo que se conoce como bombas termonucleares, de hidrógeno o H. La zona afectada por lluvia radiactiva en una cabeza termonuclear es mucho menor que en el caso de una de fisión pura.

—Sistema de armas nucleares[5]: Conjunto de cabeza/s nuclear/es y los medios de lanzamiento, así como el equipo, instalaciones, personal y procedimientos que permiten al/las arma/s nuclear/es alcanzar el objetivo establecido.
—Proliferación nuclear[6]: Es la propagación de la tecnología nuclear, entendida como tal en cualquiera de sus ámbitos. Se considera que existen dos tipos de proliferación nuclear:
  - Proliferación horizontal: La relacionada con la aparición de nuevos estados (actualmente está internacionalmente admitido también agentes no estatales) con armamento nuclear.
  - Proliferación vertical: La relacionada no sólo con el desarrollo de un mayor número cabezas nucleares, sino también la «calidad» de las mismas, con mejores prestaciones y más potentes.

La proliferación nuclear no solo se aplica a cabezas nucleares, las cuales son la máxima expresión de la misma, sino que es un concepto muy amplio en el que se encuadran los sistemas de obtención de material nuclear, el enriquecimiento, los dispositivos necesarios para poder iniciar una detonación nuclear, instalaciones necesarias que afectan a cualquier etapa del proceso de desarrollo del armamento nuclear, ensayos necesarios de realizar durante el desarrollo de una cabeza nuclear, etc.

—No-Proliferación nuclear: Conjunto de tratados y medidas encaminadas a evitar la proliferación nuclear.
—Tratado de No-Proliferación nuclear (TNP): Según el TNP establece que hay dos categorías de estados, los que

5. *US Departament of Defense, Directive DoDD 3150.02 (May 12, 2016).*
6. *Benjamin Frankel, Opaque Nuclear Proliferation: Methodological and Policy Implications (London: Frank Cass and Company limited, 1991)*

habían realizado un ensayo nuclear antes de su entrega a la firma (1968), tendrían la consideración de Estados Nucleares (NWS) y los restantes serían Estados No Nucleares (NNWS). Básicamente el contenido del tratado en cuanto a su articulado es el siguiente:

- Artículo I: Los NWS se comprometen a no transferir tecnología de la industria nuclear y tecnología sobre armas nucleares ni asistir en el en el desarrollo de armas nucleares a terceros países.
- Artículo II: Los NNWS se comprometen a no intentar desarrollar armas nucleares.
- Artículo III: Los NNWS se comprometen a someterse al régimen de salvaguardias totales del OIEA, organismo dependiente de NNUU. Así mismo establece que todas las partes se comprometen a facilitar el intercambio más amplio posible (materiales e información científica y tecnológica), en aras de facilitar el acceso a los usos pacíficos de la energía nuclear a todos los NNWS.
- Artículo IV: Todos los estados tienen el derecho inalienable a desarrollar la energía nuclear para usos pacíficos.
- Artículo VI: Los NWS se comprometen a establecer negociaciones para la reducción de sus arsenales nucleares.
- Artículo X: Establece que cualquier estado, ejerciendo su derecho a la soberanía nacional, puede retirarse del tratado si considera que existen «eventos extraordinarios», que pongan en peligro los interese supremos del mismo.

De ellos se deduce que los tres pilares del TNP son:

- No Proliferación.
- Desarme nuclear.
- Derecho al uso pacífico de la energía nuclear.

El TNP no plantea que un NNWS alcance, dentro del ámbito del tratado, el estatus de NWS. Por contra los NWS pueden, bajo el «amparo» del TNP, seguir manteniendo su estatus durante todo el tiempo que quieran. Otro punto que origina fricciones es que los NNWS tienen que declarar todas las instalaciones relacionadas con el ámbito nuclear a la OIEA, mientras que los NWS solamente aquellas que no son de «interés para la seguridad nacional». Ade-

más los NNWS están sometidos a un estricto control por parte del organismo regulador a tal efecto (OIEA), mientas que los esfuerzos realizados por parte del NWS en reducción de armamento nuclear (artículo VI), no son considerados suficientes por muchos NNWS. De hecho por un amplio sector se considera un mero giño hacia la opinión pública de los NNWS. Independientemente de ello, se considera que el grado de influencia del artículo VI en la actitud de los NNWS no es significativa, mientras no cambien su estatus.

A pesar de que en 1995 se alcanzó el acuerdo por el cual se lograba la extensión permanente del TNP, siguiendo las reuniones de revisión cada cinco años, cada estado miembro puede retirarse del mismo aludiendo cuestiones de interés nacional supremo (artículo X), avisando con tres meses de antelación. Esto fue el caso de Corea del Norte, que tras salirse del TNP realizó su primer ensayo nuclear. Esto puede originar un precedente peligroso, ya que hay muchos con la «capacidad nuclear latente», pudiendo en poco tiempo alcanzar la capacidad nuclear. Esto resalta la importancia política de abordar las causas de la demanda política de las armas nucleares, además de enfocarse en los esfuerzos destinados a hacer seguros las reservas de materiales nucleares y en restringir el suministro de tecnología específica armamentística de los NWS a los NNWS. Pero no es tarea fácil dar con la solución a la no proliferación, ya que las políticas que se adoptan en la subsanación de un problema de proliferación actual o futuro, pueden exacerbar otros.

3. La proliferación nuclear

Con el poderío mostrado por EEUU con la detonación de las bombas nucleares de sobre Japón, La URSS focalizó todo su esfuerzo en alcanzar intentar superar militarmente a EEUU, lo que ocasionó que mucho antes de lo que preveían en EEUU, realizase en primer ensayo nuclear (1949) y tan solo nueve meses más tarde que EEUU (1952) detonase la primera cabeza termonuclear (bomba H o de hidrógeno). Reino Unido realizó su primer ensayo nuclear en 1952.

Ante esta situación y con varias naciones desarrollando sus propios programas nucleares, el Presidente de los EEUU Eisenhower, en discurso ante las NNUU el 8 de diciembre de 1953[7], en lo que

7. Puede verse en: *https://www.iaea.org/about/history/atoms-for-peace-speech.*

puede considerarse la primera actuación en revertir la proliferación nuclear, hizo un ofrecimiento en los siguientes términos:

—Acordar una reducción de los arsenales militares entre los estados que disponían de ellos.
—EEUU se comprometía, e instaba a las demás potencias, a poner esa capacidad de destrucción retrotraída de los arsenales militares, en manos de los científicos de todos los países, mediante un uso pacífico de la energía nuclear, proporcionando beneficio a la humanidad.
—Creación de un banco de material fisible, en el que los gobiernos involucrados realizasen aportaciones conjuntas de sus reservas de uranio natural y materiales fisibles a una Agencia Internacional, la Organización Internacional de la Energía Atómica (OIEA), dependiente de las NNUU, que sería responsable de la custodia, el almacenamiento y la protección del material contribuido.
—Además ofrecía los conocimientos de los científicos para diseminar el uso pacífico de la energía nuclear en cualquiera de sus posibles aplicaciones.

Estas ideas se conocen bajo en concepto de «Átomos para la Paz», un año más tarde EEUU propuso en las NNUU la «Conferencia para los Usos Pacíficos de la Energía Atómica» (1955), siendo posiblemente la mayor reunión de científicos de la historia, unos 25.000. Estando presidida por Homi Bhabha, «padre» del futuro programa nuclear de India y en un ambiente de euforia, se compartió información que hasta ese momento era secreta. EEUU desclasificó cantidades significativas de tecnología y datos, científicos franceses revelaron el proceso de extracción del plutonio…

Todo ello alteró la forma con la que el mundo trató la energía nuclear. Visto con retrospectiva se puede afirmar que facilitó la expansión global de las armas nucleares, acelerando el proceso de proliferación[8], ya que se difundió asistencia y tecnología nuclear científica e industrial y varios países se beneficiaron de obtener instalaciones nucleares, conocimiento en materia nuclear, materiales nucleares y agua pesada. Algunos países receptores, como

8. Leonard Weiss, «Atoms for Peace» *Bulletin of the Atomic Scientists 59,* no. 6 (November-December 2003), pp. 41-42.

India, Pakistán y posiblemente Israel, desviaron parte de los recursos y conocimiento recibido a fines militares.

Por el contrario Átomos para la Paz, fue la semilla de la creación de la OIEA, desarrollo del concepto de salvaguardias nucleares y posiblemente lo más importante, el establecer un modelo de no-proliferación nuclear.

Lo que no se puede negar es que las grandes potencias anhelaban alcanzar la capacidad nuclear, tratando de alcanzar el armamento con mayor poder de destrucción de la historia, lo que les proporcionaría un status de superioridad frente a aquellos que no la poseyesen. Esto les conferiría un mayor peso específico en la toma de decisiones internacionales, por lo que la proliferación horizontal seguía incrementando el número de estados con capacidad armamentística nuclear. Francia en 1960 y China en 1964 realizaron sus primeros ensayos nucleares. Pero no sólo se incrementaba la proliferación horizontal, sino que ésta se conjugó con una gran proliferación vertical, tanto con el incremento de las cabezas nucleares, como con las mejoras en los vectores de lanzamiento y la aparición de las bombas termonucleares, así en 1968 los NWS disponían de esta capacidad.

En este punto se redactó el TNP, que puede ser visto como una expresión negociada y refinada de «átomos para la Paz» y está considerado la piedra angular de la No Proliferación Nuclear.

Múltiples y en diferentes ámbitos, son las medidas adoptadas desde la aparición del arma nuclear para evitar e incluso reducir la proliferación nuclear. Pese a ello la respuesta a la proliferación no ha sido todo lo deseable y satisfactoria.

En estos casi 50 años de historia del TNP muchos estados que tenían programado o planeado desarrollar un programa nuclear, han renunciado al mismo, existiendo incluso uno (Sudáfrica) que habiendo desarrollado varias cabezas nucleares procedió a su total desmantelamiento. Pero existe otra cara de esta misma moneda y es la que muestra que de una u otra manera 4 nuevos estados han alcanzado la capacidad nuclear, siendo, actualmente, ocho son los estados que han logrado alcanzar la capacidad nuclear (EEUU, Rusia, Reino Unido, Francia, China, India, Pakistán y República Democrática de Corea del Norte – Corea del Norte en adelante). Entre ellos no está contabilizado Israel, del cual se tiene la certeza, aceptada en el ámbito internacional, que dispone de armamento nuclear, llegando a realizar un ensayo nuclear

(1970). Respecto a esto último existe un gran oscurantismo llegándose a la conclusión, tras el análisis de los datos en poder de EEUU, que dicho suceso es claramente atribuible a un ensayo de una cabeza nuclear de Israel. La política israelí en el ámbito del armamento nuclear es que ni confirma ni desmiente la tenencia de armamento nuclear.

Una de las derivadas de la actual situación es la preocupación internacional en relación a cómo evitar en el futuro la proliferación horizontal y analizar posibles medidas que hagan factible una reducción de los arsenales nucleares, con el fin último de lograr un mundo libre de armas nucleares. Este no es un concepto nuevo y han sido muchas voces, algunas de ellas con mucho poder, dentro de los estados con armamento nuclear, las que han indicado que se debe alcanzar un mundo libre de armas nucleares. Actualmente la realidad indica lo contrario, si bien es posible que existan menos armas nucleares en el mundo, poco o nada hace indicar que se reducirá el número de estados poseedores de las mismas. Actualmente es tema de debate la necesidad de modernización del armamento nuclear y de sus instalaciones. Si esto se materializase, haría poco creíble la posibilidad de lograr un mundo libre de armas nucleares en bastantes años.

3.1. *Motivaciones para lograr armamento nuclear*

La proliferación nuclear no puede entenderse sino se analiza la motivación que tienen los diferentes estados de ser potencias nucleares, entendiendo por tales aquellas que disponen de armamento nuclear. Una pregunta que nos puede abordar es la siguiente: Muchos estados han planeado un programa armamentístico nuclear, bastantes han llegado a iniciarlos y finalmente nueve lo han logrado, ¿el motivo de lograr disponer de armamento nuclear, ha sido el mismo en todos los casos? La primera idea que pueda venir a la mente para dar respuesta la pregunta es la de la seguridad. Pero la seguridad es un concepto intangible y por ello no es el mismo para todos. En caso que ese sea el motivo, ¿seguridad para qué o ante qué?, ¿se considera un estado mucho más seguro que otro por el mero hecho de disponer armamento nuclear, o esto mismo puede suponer una amenaza para potencias mucho más poderosas, con mucho mayor poder nuclear, conver-

tirse en un peligro y sentirse por ello «obligados» a neutralizar al «débil»? El mismo presidente Kennedy en 1961 se dio cuenta que una espada de Damocles nuclear colgaba sobre cada hombre, mujer y niño y podría ser activada en cualquier momento por accidente, error de cálculo o locura[9].

Muchas son las preguntas que pueden surgir en relación al asunto y la respuesta de la seguridad puede resultar insuficiente ya que influyen muchas variables en relación a la motivación, como puede ser la situación geopolítica, el tipo de gobierno, la historia y pretensiones territoriales, la política de alianzas y pactos, etc. La idea de la consideración de la seguridad nacional como causa de la proliferación es peligrosamente inadecuada debido a que los programas nucleares pueden servir para otros fines más locales y menos obvios.

Según la teoría neorrealista, los estados son parte de un sistema internacional anárquico, por lo que deben basarse en la auto-ayuda para proteger su soberanía y seguridad nacional[10]. Aludiendo cuestiones de seguridad nacional podría verse en la necesidad de disponer de armamento nuclear. Si lo hacen antes que los demás, su seguridad nacional será incuestionable y en caso que otros ya dispongan de ella buscaran dicha capacidad para contrarrestarla. De esto se desprenden dos posibles vías. La primera es que las principales potencias mundiales pueden pretender alcanzar la capacidad por sí mismas, ya que alcanzar dicha capacidad no está al alcance de todos los estados. La segunda es que estados que no puedan asumir un programa nuclear completo, busquen alianzas con potencias nucleares, para los que esta es su única opción, pero esta solución no le asegura que en caso de tener que emplearse armas nucleares por su/s aliado/s nuclear/es, éstas sean empleadas. Además lo que en un momento pueda suponer una alianza, años más tarde ésta puede desaparecer. De ello se desprende que esta solución puede ser válida en el corto o medio plazo, pudiéndose dar el caso que no funcione a largo plazo y en ese momento ese estado tenga la capacidad de desarrollar un programa nuclear, capacidad que años antes no tenía.

9. Citado en: *http://www.state.gov/p/io/potusunga/207241.htm*

10. Kenneth N. Walt., «The Origins of war in neorealist theory,» in *The origin and prevention of major wars*, eds. Robert I. Rotberg, Theodore K. Rabb, and Robert Gilpin (New York: Cambridge University Press, 1989) 39-52

No hay duda que si surge un estado nuclear los estados vecinos puedan sentir la necesidad de lograr la capacidad nuclear en señal de equiparación de status quo, con la finalidad de mantener su seguridad nacional. De ahí que, como indicó el exsecretario de estado americano George P. Shultz (1982-89), la proliferación llama a la proliferación[11]. De manera muy simplista, resulta muy sencillo entender que la proliferación nuclear actual ha sido producida, prácticamente en su totalidad, siguiendo un efecto dominó. Tras Hiroshima fue la URSS quien sentía su seguridad amenazada, tras ella, Reino Unido y Francia veían peligrar la suya al observar el crecimiento de la amenaza militar soviética y reducirse la credibilidad de que EEUU ofreciera garantías a sus aliados, toda vez que la URSS tendría capacidad suficiente como para amenazar con represalias a EEUU[12].

El caso chino se explica por la amenaza de empleo de armas nucleares por los EEUU en la guerra de Corea (1950-53), donde EEUU estaba considerando seriamente emplear armas nucleares en la guerra, debido al apoyo proporcionado por China en mayor media y Rusia en menor, al régimen de Corea del Norte[13]. La amenaza de emplear armas nucleares contra la seguridad nacional de China se vio, nada más acabar la guerra de corea, en la crisis de los estrechos de Taiwán[14] (1954-55 y 1958). Esto unido a poca confianza en el aliado nuclear soviético en los años 50, así como una creciente hostilidad entre China y la URSS en los años 60 condujo a China al desarrollo del arma nuclear[15] (1964).

India, que acababa de tener en 1962 una guerra con China, decidió lograr la capacidad nuclear, alcanzándola con un ensayo nuclear en 1974 (buda sonriente). Se habló del mismo como la explosión nuclear pacífica, haciendo ver que la finalidad no era conseguir amenazar a ningún estado, sino dar una respuesta

11. George P. Schultz, «Preventing the proliferation of nuclear weapons», 1984.

12. Margaret Gowing, *Britain and the atomic energy* (London: Macmillan, 1964).

13. Ver: http://historynewsnetwork.org/article/9245

14. Ver: https://history.state.gov/milestones/1953-1960/taiwan-strait-crises

15. Avery Goldstein, Robust and affordable security: Some lessons from the second-ranking powers during the cold war, Journal of strategic studies Vol. 15, núm. 4, (December 1992).

«pacífica» a la superioridad militar china. Alcanzado un arsenal nuclear moderado sin hacer más ensayos ni desplegar las cabezas nucleares.

El que India alcanzase tal capacidad suponía un ataque a la línea de flotación de Pakistán. Independizado de India en 1947 de India y con la había tenido conflictos armados (1947, 65, 71 y 89) decidió tener armamento nuclear a la mayor brevedad posible[16], debido a la superioridad india tanto en el plano convencional como en el nuclear. El esfuerzo paquistaní en lograrlo fue desmesurado. El padre del proyecto atómico paquistaní fue el primer ministro Zulfiqar Ali Bhutto, que indicó abiertamente que Pakistán tendría que desarrollar su propio arsenal, aunque para costearlo el país «tuviese que comer hierba»[17].

Así en 1998 realizó cinco pruebas nucleares. Con posterioridad a dichas pruebas, los conflictos entre ambos estados no cesaron, si bien en la mayoría de los casos se reducen a escaramuzas o ataques a puestos policiales o militares, fundamentalmente en la región de Cachemira. A modo de ejemplo, solo en 2013 se registraron violaciones del alto el fuego en la llamada «Línea de Control», en el 21% de los días[18]. Pero como por efecto boomerang, el que Pakistán haya adquirido la capacidad nuclear supone mucho más que una amenaza a la seguridad India. Esto es así porque China apoyó a Pakistán no sólo en el proyecto nuclear, sino en la fabricación propia de misiles balísticos y apoyo internacional en la cuestión de cachemira. Esto último indica a pensar que cualquier cuestión relacionada con Cachemira que no interese a China será vetada en el Consejo de Seguridad de las NNUU (CSNU), al ser China uno de sus cinco miembros permanentes. Por todo lo expuesto, en caso de conflicto no es descabellado pensar que India tenga que plantear un posible enfrentamiento bifronte.

El caso de Israel el alcanzar la capacidad nuclear le supone no solo cuestiones de seguridad nacional, sino de integridad territorial. Tras sus múltiples guerras previas al ensayo nuclear

16. Ziba Moshaver, Nuclear weapons proliferation in the Indian Subcontinent (Basingstoke, U.K.: Macmillan, 1991).

17. Eva Borrego, India y Pakistán: el dilema nuclear, ARI núm. 68/2004 Real Instituto Elcano, 14/04/2004

18. Ver: https://actualidad.rt.com/actualidad/181748-india-pakistan-guerra-armas-nucleares

(Independencia 1947-49, Sinaí 1956, Seis días 1967, Desgaste o Atrición 1968-70, Yom Kipur 1973), siendo un estado sin ningún aliado poderoso en la región y con varios estados en la región que están decididos, tarde o temprano, a «destruir a Israel», en caso que perdiese una guerra, podría suponer que el estado israelí fuera borrado del mapa. Esto se debe a que a diferencia del resto de los estados de la región, posee un territorio tan reducido que en caso de ocupación de un porcentaje importante del mismo, le podría suponer perder su centro de gravedad. Si bien en todos sus comunicados oficiales, los diferentes representantes hebreos indican por un lado que no van a ser los primeros en introducir el arma nuclear en la región[19], por otro lado aplican una política de ambigüedad por la que ni confirman ni desmienten disponer de armamento nuclear[20].

Finalmente Corea del Norte ha tenido puede considerarse un caso diferenciador del resto. Ha pasado de estar apoyado por China fundamentalmente y Rusia en menor media en la guerra de Corea frente a EEUU, a estar prácticamente aislado del resto del mundo, sino fuera por su único aliado (China), si bien es cierto que recientemente, a finales de 2015, Rusia y Corea del Norte firmaron un acuerdo sobre la prevención de actividades militares peligrosas, según el cual ambas partes se comprometerán a mostrar una mayor cautela para no permitir incidentes armados en las proximidades de la frontera. Se trata de un acuerdo estándar en la práctica internacional que suele firmarse entre dos países que mantienen unas relaciones de amistad para incrementar el nivel de confianza. Además China ha declarado que no se opone a este acuerdo.

Por un lado China se reserva el rechazo en relación a los lanzamientos de misiles que habitualmente suele realizar Corea del Norte en dirección a Japón, llegando en alguna ocasión a sobrevolar el territorio nipón. Tal es así que veta cualquier medida al respecto en el CSNU[21], aludiendo el representante permanente de China en las NNUU, Liu Jieyi «No se debe hacer nada que exacerbe la tensión en la península coreana (…) algunos factores

19. Citado en: http://www.nti.org/learn/countries/israel/nuclear/

20. Ver: http://www.nti.org/learn/countries/israel/nuclear/

21. Ver: http://www.hispantv.com/noticias/china/283838/bloquea-condena-consejo-seguridad-lanzamiento-misil-corea-norte

contribuyen a la tensión (…) Existe un verdadero riesgo. Creo que debemos trabajar de manera responsable».

Por otro lado tanto Rusia como China han rechazado las cuatro pruebas nucleares coreanas realizadas hasta la fecha, siendo la última de ellas realizada en enero de 2016. Con motivo de cada una de ellas, el CSNU ha impuesto fuertes sanciones al país que limitan de forma estricta sus transacciones internacionales y agudizan su aislamiento económico, lo que ha hundido al país en lo económico, con un gran problema energético y con hambrunas por las que mueres miles de personas cada año, el dato más destacado es el de 2005, donde se estiman que entre 250.000 y 3 millones de personas murieron de inanición[22].

Además la paciencia de su «único valedor» (China) parece estar agotándose con el régimen de Pyongyang, ya que el tono de las declaraciones de rechazo tras el último ensayo nuclear así lo atestiguan.

La posible motivación para lograr la capacidad nuclear podría ser la que ésta le proporcionaría la seguridad necesaria, al dotarse de capacidad de disuasión nuclear para su supervivencia como régimen. Evitando cualquier posible intervención exterior, tanto para derrocar al presidente e imprimir un giro de 180º en el actual gobierno, o vencer al estado actual. Esto se debe a las relaciones internacionales que mantienen, conformando uno de los países del «eje del mal[23]» por la exportación de tecnología de misiles a países como Pakistán, Irán, Libia y Siria.

3.2. *Contención nuclear*

En este apartado se expondrán casos de abandono de programas nucleares de varios estados de forma cronológica, algunos de ellos con programas nucleares más o menos avanzados y otros que han llegado a tener armamento nuclear. Pero con el gran poder de disuasión que ofrece el armamento nuclear, ¿por qué algunos estados han optado por abandonar sus programas e incluso que se procediera al desmantelamiento de las cabezas nucleares? La

22. Ver: «World Hunger Series 2006 Hunger and learning», UNICEF, 2006.

23. George W. Bush, «President Delivers State of the Union Address», The President's State of the Union Address, The United States Capitol,Washington D.C., January 29, 2002.

respuesta la puede ofrecer el propio concepto de la seguridad, ya que si se tiene la clara opinión por parte de los dirigentes de un estado que para mantener la integridad territorial y seguridad nacional no se precisa disponer de armamento nuclear, no habría motivo para alcanzarla o mantenerla, en caso que ya se hubiera logrado.

Sudáfrica, que es y ha sido la gran potencia del sur de África. Durante los años 60 y 70 se produjo una expansión importante de países afines a la URSS y eso empezó a preocupar al gobierno sudafricano que en aras de defender su seguridad nacional e incluso su soberanía, como indicó el Presidente sudafricano De Klerk en su discurso de adhesión al TNP[24], inició un programa nuclear en 1974, que finalizó con la fabricación de seis cabezas nucleares. Esta decisión se vio reforzada cuando a partir de 1975 se incrementó sustancialmente el número de tropas cubanas en Angola ya que Sudáfrica se encontraba en una situación de relativo aislamiento internacional y se tenía la percepción que no se podría confiar en el apoyo exterior en caso de ser atacada.

Para finales de los años ochenta, el riesgo de un ataque dirigido por países de la órbita de la URSS, se había desvanecido, esto originó que en 1991 Sudáfrica procediera a eliminar las cabezas nucleares, debida a la drástica reducción de las amenazas exteriores a la seguridad nacional

Los casos de Argentina y Brasil son muy similares. Ambos pretendían alcanzar la capacidad nuclear, bien para intentar se la potencia militar del sur del continente americano o bien por miedo a que el otro alcanzase la capacidad nuclear. Sea cual fuera el motivo, existe una herramienta dentro de la no proliferación nuclear que es el establecer, mediante un tratado internacional al que se adhieren los países interesados, una zona libre de armas nucleares (NWFZ). El Tratado de Tlatelolco[25], entregado a la firma en 1969, afecta a América Latina y el Caribe (toda américa salvo EEUU y Canadá), prohíbe fabricar, realizar ensayos, usar, producir o adquirir por cualquier medio armas nucleares, así como recibirlas, instalarlas, desplegarlas o que se encuentren de

24. Ver: http://digitalarchive.wilsoncenter.org/document/116789.pdf?v=903e41951aad5558d462aeade819f433

25. Ver: http://www.opanal.org/wp-content/uploads/2015/08/Tratado-de-Tlatelolco.pdf

cualquier otra forma en el de del territorio de América Latina y el Caribe. Además en su protocolo II, firmado por los 5 NWS, se hace abstener a los NWS a menoscabar el tratado. Así en 1990 Argentina y Brasil paralizaron totalmente sus programas nucleares con la firma y adhesión al tratado. Con ello se logró un reconocimiento entre ambos países de no tener una amenaza a la seguridad nacional de ambos.

A principios de los años noventa se produjo el desmembramiento de la extinta URSS, así entre 1990 y 1991 se independizaron tres repúblicas socialistas soviéticas en las que se encontraba armamento nuclear, era el caso de Ucrania, Kazajistán y Bielorrusia. El devolver este armamento a Rusia se trató por separado, siendo las negociaciones más sencillas en algún caso y más complejas en otro. Pero, ¿por qué accedieron a perder esa capacidad nuclear adquirida «de repente»?, entre otros factores nuevamente vuelve a aparecer la seguridad nacional. En esos momentos las tres exrepúblicas no percibían amenaza de Rusia, ya que la independencia había sido acordada y sin conflictos, por otra parte EEUU ofreció garantías de que no tenían que temer por no disponer del arsenal nuclear[26].

4. La no-proliferación nuclear

Entre sus medidas existe un vasto número de tratados y acuerdos multilaterales o bilaterales:

—Que directamente evitan que los estados puedan obtener armamento nuclear
—Que reducen los arsenales de las potencias nucleares.
—Que prohíben los ensayos nucleares.
—Que establecen zonas del mundo libres de armas nucleares.
—Que limitan los sistemas de defensa de misiles balísticos.

El TNP ya ha sido tratado con anterioridad, por lo que no se expondrá en este apartado.

26. Sherman W. Garnett, Ukraine´s decision to join the NPT , Arms control today, vol. 25, no. 1 (January 1995).

4.1. *Reducción de cabezas nucleares*

Este apartado se inició con las conversaciones para la Limitación de Armas Estratégicas (SALT) 1.969-72 entre EEUU y la URSS, en relación a la regulación de la carrera armamentística nuclear entre ambos. Tuvieron como máximas derivadas la firma del Tratado sobre Misiles Antibalísticos (tratado ABM) y del Acuerdo Provisional sobre Limitación de Armas Estratégicas Ofensivas, poniendo límite a la construcción de misiles intercontinentales (ICBM) y los lanzadores instalados en submarinos (SLBM).

La segunda ronda de negociaciones (SALT II), tuvieron lugar entre 1974-79, siendo el resultado final el Acuerdo de Vladivostok, que estableció por primera vez límites al número total de lanzaderas de misiles y bombarderos estratégicos. Finalmente no fue ratificado por el Senado de los EEUU, como medida de presión frente a la invasión soviética de Afganistán y de la crisis de los «euromisiles», en la cual la URSS comenzaba a desplegar en la Europa central y oriental misiles nucleares de alcance intermedio (hasta 5000 kilómetros), claramente dirigidos a intimidar a Europa occidental con una guerra limitada, ya que la URSS pensaba que EEUU se negarían a participar, por la amenaza de los misiles estratégicos soviéticos.

En 1.982 Ronald Reagan, opuesto a SALT II, lanzó su primera propuesta de un Tratado para la reducción de Armas Estratégicas (START) y que trataba de un profundo recorte (50%) del número de misiles ubicados en bases terrestres. La URSS, rompió las negociaciones a finales de 1.983, como protesta por el despliegue en Europa por parte de los EEUU de misiles de alcance intermedio. Se reanudaron las negociaciones entre el Reagan y Gorbachov (1985-87), con la firma del Tratado de Armas Nucleares de Alcance Intermedio (INF), que se establecía la destrucción de todos los misiles de ambos países con un alcance entre 500 y 5.000 km. Mediante un programa de verificación de 13 años de duración.

En 1.991 el George Bush firmó con Gorbachov el Tratado START I por el que se acordaba reducir el número de cabezas nucleares a un máximo de 6000. El Tratado START II (1993), firmado por Bush y Boris Yeltsin, suponía la eliminación de casi tres cuartas partes de las cabezas nucleares que todavía poseían EE.UU, Rusia, Ucrania, Bielorrusia y Kazajistán, así como la eliminación de todos los misiles de

Ante el estancamiento internacional en relación a la reducción de las cabezas nucleares de las dos grandes potencias nu-

cleares mundiales, el 8 de agosto de 2010 los presidentes Dimitri Medvedev y Barack Obama firmaron en Praga el Tratado de Reducción de Armas Estratégicas (Tratado Nuevo START). Éste reinició realmente las relaciones entre EEUU y Rusia. Al igual que los anteriores solamente se tratan las armas nucleares estratégicas. Se puede afirmar que fue el primer fruto ponderable, en la gestión de Obama, del relanzamiento de las relaciones entre Moscú y Washington. De acuerdo con el Tratado de Praga de 2010, la máxima cantidad de ojivas nucleares, por cada país, deberá ser de 1550. Y los portadores de misiles, 700. El documento entró en vigor en febrero de 2011 y tendrá una vigencia de diez años.

Al igual que la mayoría de los acuerdos soviéticos, y más tarde ruso-norteamericanos de control y reducción de arsenales nucleares, este «nuevo tratado de desarme nuclear» nació en medio de discusiones. El documento pasó todos los procedimientos de la ratificación, tanto en el Congreso de EEUU como en la Cámara de diputados de Rusia. El tratado tiene hasta el día de hoy sus partidarios y adversarios. Los que critican el Tratado Nuevo START olvidan, a menudo, una cuestión simple pero de suma importancia. Sin este Tratado, Moscú y Washington podrían haberse quedado sin un acuerdo básico de control de los armamentos nucleares estratégicos. En 2009 expiró la vigencia del START I. Moscú abandonó en 2002 el START II, después de que EEUU se negara oficialmente a respetar las cláusulas del Tratado soviético-norteamericano de Defensa Antimisiles de 1972. El significado más importante de este nuevo Tratado de Reducción de Armas Estratégicas consiste en que el documento consiga la adhesión de ambas partes al proceso de reducción de los armamentos nucleares.

4.2. *Tratados de zonas libres de armas nucleares*

En este apartado se han querido englobar un amplio grupo de tratados que establecen zonas libres de armas nucleares (NWFZ), así como otros que prohíben la existencia de ubicar armamento nuclear en el lecho marino o espacio exterior.

El Tratado de la Antártida (1959), finalizó con las controversias sobre la soberanía en el continente. Entre otros puntos, se acordó que la Antártica se utilizará exclusivamente para fines pacíficos, prohibiendo toda medida de carácter militar, bases, maniobras y ensayos de cualquier clase de armas. De igual modo

prohíbe cualquier tipo de explosión nuclear en la Antártida y la eliminación de residuos radiactivos.

El Tratado sobre principios de la exploración y utilización del espacio ultraterrestre (1967), establece la prohibición de colocar en órbita alrededor de la tierra objeto alguno portador de armas nucleares u otro tipo de armas de destrucción masiva, así como colocar dichas armas en el espacio ultra terrestre, en la luna o en los cuerpos celestes.

El Tratado sobre la prohibición de emplazar armas nucleares y otras armas de destrucción masiva (ADM) en los fondos marinos y oceánicos y su subsuelo (1971), persigue que, mediante la prohibición de emplazamientos de armas nucleares en los fondos marinos o su subsuelo, así como los ensayos nucleares en los mismos, reducir la tensión internacional en relación a la amenaza nuclear.

El Tratado de Tlatelolco (1969) prohíbe fabricar, realizar ensayos, usar, producir o adquirir por cualquier medio armas nucleares, así como recibirlas, instalarlas, desplegarlas o que se encuentren de cualquier otra forma en el de del territorio de América Latina y el Caribe. Es vinculante a todas las colonias de terceros países que se encuentres en Latinoamérica y el caribe, lo que representa que actualmente todo el continente americano, salvo EEUU y Canadá, es una NWFZ. Además en su protocolo II, firmado por los 5 NWS, se hace abstenerse a los mismos de menoscabar el tratado.

El Tratado de Rarotonga (1985), prohíbe el emplazamiento, la adquisición o el ensayo de artefactos explosivos nucleares y el vertimiento de desechos nucleares dentro de la zona. Los países no firmantes del tratado son Los Estados Federados de Micronesia, las Islas Marshall y Palau. Existen tres protocolos al tratado, que fueron firmados por los 5 NWS, a excepción del protocolo 1 por Rusia y China, que no tienen ningún territorio en la zona. Estos protocolos suponen:

1. No fabricar, desplegar o ensayar armas nucleares en la zona
2. No emplear armas nucleares contra las partes del tratado
3. No hacer ensayos en el interior de la zona

El Tratado de Bangkok (1985), ratificado por 10 estados (Brunei Darussalam, Camboya, Indonesia, Laos, Malasia, Myanmar, Filipinas, Singapur, Tailandia y Vietnam), prohíbe el desarro-

llo, fabricación, posesión, adquisición, emplazamiento o tener el control de armas nucleares en los territorios de los Estados partes. Se define «territorio» como la parte terrestre, las aguas jurisdiccionales, las aguas de los archipiélagos, el fondo marino, su subsuelo, así como la capa atmosférica y espacial de lo anteriormente definido. Existe un protocolo al tratado, por el que los 5 NWS se comprometen a respetar el Tratado y no contribuir a la violación del mismo por algún estado parte. Ninguno de los 5 NWS ha todavía firmado este protocolo.

Status de Mongolia libre de armas nucleares (1992), tras la salida de las tropas rusas de Mongolia, decidió dar un cambio a su status geopolítico y convertirse en un estado neutral.

Tratado de Semipalatinsk, también conocido como Tratado de Semei o de Asia Central. Es el tratado de este tipo más reciente (2006), firmado por Kazajistán, Kirguistán, Tayikistán, Turkmenistán y Uzbekistán, prohíbe a los estados parte fabricar, adquirir, ensayar o poseer armas nucleares. Existen protocolos al tratado por el que los NWS no favorecerán la violación del tratado.

Este tratado ha presentado reticencias en EEUU, UK y Francia, ya que EEUU objetó acerca de la posibilidad que Irán pudiera ser parte del tratado, además estos tres NWS eran recelosos que no se incluyera ninguna prohibición de tránsito de armas nucleares por la zona de los estados parte, sobre todo EEUU, que considera esta premisa fundamental, ya que en caso contrario podría favorecerse el movimiento de cabezas nucleares de Rusia a través de los países firmantes del tratado en dirección a terceros países. Finalmente todos los NWS, salvo EEUU ratificaron los protocolos.

El Tratado de Pelindaba, firmado en 1996 y en vigor desde 2009, prohíbe la investigación, desarrollo, almacenamiento, adquisición, ensayo, posesión, control o despliegue de dispositivos explosivos nucleares, así como la existencia de vertidos de residuos radiactivos en los territorios de las partes del tratado. El Tratado también prohíbe cualquier tipo de ataque contra instalaciones nucleares en la zona del tratado así como se les requiere los más altos estándares de protección física a los materiales nucleares, sus instalaciones y equipamiento, los cuales serán usados exclusivamente para usos pacíficos. El Tratado tiene 3 protocolos, los dos primeros instan a los NWS a no usar o amenazar con usar ningún tipo de dispositivo nuclear explosivo contra ningún estado parte ni realizar ensayos nucleares, ni a asistir o animar en

la realización de ensayos nucleares en la NWFZ. En el protocolo III se insta a los países con territorios en la zona, que respeten la misma, este caso es de aplicación a Francia y España, refiriéndose concretamente a Ceuta y Melilla. De los 5 NWS todos, salvo EEUU han ratificado el los protocolos al Tratado, si bien sí que lo firmó en 1996. España no ha firmado ni ratificado los protocolos.

4.3. *Tratados de prohibición de ensayos nucleares*

Fundamentalmente son dos los tratados en este ámbito, el Tratado de prohibición parcial de ensayos nucleares (1963), por el que se prohíben los ensayos nucleares, de cualquier tipo, en la atmósfera, en el espacio exterior y bajo el agua. Deja por tanto la posibilidad de poder realizar ensayos nucleares subterráneos.

Un total de 113 países, entre ellos todos los que poseen armamento nuclear excepto Pakistán, lo han ratificado. Actualmente lo han firmado, pero no ratificado, 17 estados (Argelia, Burkina Faso, Burundi, Camerún, Chile, Etiopía, Haití, Libia, Malí, Pakistán, Paraguay, Portugal, Somalia, Tanzania, Uruguay, Vietnam, Yemen).

Un paso más en este tipo de prohibiciones es el Tratado de prohibición total de ensayos nucleares (TPTEN) entregado a la firma en 1996, prohíbe la realización de cualquier tipo de ensayo nuclear, incluidos los subterráneos. Actualmente, de los 196 estados que existen, 183 lo han firmado, de los cuales 164 lo han ratificado. El Tratado entrará en vigor cuando 180 días después de que los 44 estados que se indican en el Anexo 2 del tratado lo hayan ratificado los 44 países que figuran en su anexo 2, que vienen siendo aquellos en los que hay alguna instalación nuclear, aunque sea para usos civiles, en su territorio, en la fecha de la redacción del mismo y por supuesto todos aquellos que poseen armamento nuclear. De todos ellos no han firmado el Tratado 3 estados: Corea del Norte, India, Pakistán. Además, hay 5 estados que lo hayan firmado pero no ratificado: China, Egipto, Irán, Israel y EEUU. De ello se desprende que de todos los países con armamento nuclear, sólo Francia, Reino Unido y Rusia lo han ratificado. Consecuencia de todo ello, el tratado no está en vigor. Como consecuencia de ello, al no estar en vigor, las prohibiciones en este ámbito son las que regula el Tratado de prohibición parcial de ensayos nucleares.

Conclusión

El arma nuclear es el arma de «destrucción total» que es, o puede ser codiciada tanto por estados como por actores no estatales. Esto hace necesario, para lograr una estabilidad mundial, que no se produzca una dispersión de este tipo de armas, procurando evitar la proliferación horizontal, así como reducir el número de cabezas existentes. Es necesario por tanto analizar los motivos por los que los NNWS pretenden alcanzar dicha capacidad y que la diplomacia trabaje en el sentido de hacer que esas motivaciones desaparezcan al dejar de existir las causas que las originan. Esto no es tarea sencilla y el intentar solventar un caso puede agravar otros e incluso, como consecuencia de ello, que se estados que no tenían planeado disponer de armamento nuclear se lo planteen de forma más o menos seria.

La proliferación y la no proliferación van de la mano y para evitar la primera hay que generar unas herramientas válidas y potentes de las segundas. El TNP tiene sus detractores fundamentalmente porque establece que hay dos categorías de estados, los que «pueden» y los que «no pueden» disponer de armamento nuclear, así como que los que no tienen la percepción de que los esfuerzos por parte de los NWS son escasos en cuanto al desarme nuclear de los mismos. No todos los países han firmado el TNP, lo que implica que los países no miembros están fuera del sistema regulador y de control, de esta manera tres estados han alcanzado la capacidad nuclear, para incredulidad de los NNWS, que ven como ellos cumplen con unas estrictas regulaciones mientras que aquellos que no, no sólo han podido desarrollar armas nucleares, sino que han quedado impunes por ello. Además el tratado permite «libremente» salirse del mismo, como hizo Corea del Norte y no tener herramienta alguna en caso que al poco tiempo se tenga la capacidad nuclear. Siendo la única herramienta, al menos vista hasta la fecha, posibles sanciones por parte de la ONU. Las sanciones de la ONU parecen haber dado resultado con Irán, pero no con Corea del Norte.

Una gran medida de no proliferación son las NWFZ. Tras la revisión del TNP en 2010 la administración americana propuso crear una NWFZ en oriente próximo, que afectase a países como Irán, Irak, Israel, Egipto, Arabia Saudí, los países del Golfo Pérsico… Fue vista con buenos ojos por la mayoría de los países afectado, pero tenía el gran inconveniente de que Israel debería

proceder a desmantelar su arsenal nuclear. Finalmente se desvaneció la ilusión y esa NWFZ no ha visto la luz.

Un punto importante es la entrada en vigor del TPTEN, lo que supondría que no se podrían realizarse ensayos nucleares de ningún tipo. Esto reduciría mucho, aunque no eliminaría, la posibilidad de proliferación horizontal y en un momento en la que varios NWS están planteándose mejoras en sus cabezas nucleares, podría frenar la proliferación vertical en este aspecto. Con EEUU como principal elemento bloqueante del mismo es difícil que países que no lo han firmado/ratificado todavía lo hagan hasta que aquel no lo ratifique.

Todo esto, salvo que se tenga el firme compromiso multilateral de aprender de los errores cometidos, analizar la génesis de la motivación para adquirir armamento nuclear y realizar una buena diplomacia internacional, da un futuro desalentador en materia de proliferación nuclear que hace plantearse si realmente se quiere lograr un mundo libre de armas nucleares, como propugnó Obama en su visita en recuerdo de los afectados por la explosión nuclear de Hiroshima[27].

Referencias Bibliográficas

Bernstein, Jeremy, Nuclear Weapons. What you need to know, New York, Cambridge University Press, 2008,312 págs.

Borrego, Eva, «India y Pakistán: el dilema nuclear», Real Instituto Elcano, ARI 68/2004, 14/04/2004.

Bunn, Matthew, Securing the bomb 2010. Securing all nuclear materials in four years, Cambridge (Massachusetts), Harvard University, 2010, 131 págs., disponible en https://dash.harvard.edu/bitstream/handle/1/29914176/Securing_The_Bomb_2010.pdf?sequence=1, [consultado el 23 de febrero de 2017]

Carus, W. Seth, Defining «Weapons of Mass Destruction», Washington D.C., National Defense University Press, 2012, 92 págs.

De Klerk, F.W, «Discurso del presidente de Sudáfrica a la comisión de desarme de las Naciones Unidas», Nueva York, 24 de marzo de 1993, disponible en http://digitalarchive.wilsoncenter.org/document/116789.pdf?v=903e41951aad5558d462aeade819f433, [consultado el 20 de febrero de 2017].

Delpech, Thérèse, Nuclear deterrence in the 21st Century, Santa Monica, Rand Pubn, 2012, 181 págs.

27. http://www.news.com.au/world/asia/barack-obama-calls-for-a-world-free-of-nuclear-weapons-during-hiroshima-visit/news-story/ec04ba31dc93bcb1d12fac61e4a1f57f

EISENHOWER, Dwight D., «Discurso del presidente de los Estados Unidos de América en la 470 reunión plenaria de la Asamblea General de Naciones Unidas», Nueva York, 8 de diciembre de 1953, disponible en https://www.iaea.org/about/history/atoms-for-peace-speech, [consultado el 20 de febrero de 2017].

FRANKEL, Benjamin, Opaque Nuclear Proliferation: Methodological and Policy Implications, London, Routledge, 1991, 201 págs.

FREEDMAN, Laurence, La evolución de la estrategia nuclear, Madrid, Ministerio de Defensa, 1992, 522 págs.

GARNETT, Sherman W., «Ukraine´s decision to join the NPT», Arms control today, vol. 25, no. 1 Jan/Feb 1995, disponible en https://armscontrolnow.org/2014/03/08/ukraine-russia-and-the-npt/ [consultado el 23 de febrero de 2017]

GOLDSTEIN, Avery, «Robust and affordable security: Some lessons from the second-ranking powers during the cold war», Journal of strategic studies, Vol. 15, 1992, no. 4, págs 475-527.

GOWING, Margaret, Britain and the atomic energy, 1939-1945, London, Palgrave Macmillan, 1964, 492 págs.

US Department of Defence, Joint Chiefs of Staff. JP 3-12. Doctrine for Joint Nuclear Operations, Washington, Department of Defence, 2005, disponible en http://www.realinstitutoelcano.org/wps/portal/!ut/p/a0/04_Sj9CPykssy0xPLMnMz0vMAfGjzOKNg318fEKcHX1NTZz9QgKNTA1MDCBAvyDbUREACkEYzA!!/?PC_Z7_3SLLLTCAM54CNTQ2BL50000000000000_WCM_CONTEXT=/wps/wcm/connect/elcano/elcano_es/zonas_es/ari+68-2004, [consultado el 23 de febrero de 2017].

KENNEDY, John F, «Discurso del presidente Kennedy ante la Asamblea General de las Naciones Unidas», Departamento de Estado de los Estados Unidos de América, Septiembre 25, 1961, disponible en http://www.state.gov/p/io/potusunga/207241.htm, [consultado el 20 de febrero de 2017].

NORRIS, Robert and Kristensen, Hans M., «Global nuclear weapons inventories, 1945–2010», Bulletin of the Atomic Scientists, Vol. 66, 2010, Issue 4, págs 77-83.

MOSHAVER, Ziba, Nuclear weapons proliferation in the Indian Subcontinent, Basingstoke, U.K, Palgrave Macmillan, 1991, 290 págs.

OBAMA, Barack, «Discurso del Presidente Obama en Praga», Casa Blanca, 2009, disponible en http://www.whitehouse.gov/the_press_office/Remarks-By-President-Barack-Obama-In-Prague-As-Delivered/, [consultado el 20 de febrero de 2017].

Oficina de Relaciones Exteriores y Coordinación de Políticas del OIEA, Verificación del cumplimiento de los compromisos en materia de no proliferación nuclear, Viena, 2008, disponible en https://www.iaea.org/sites/default/files/safeguards0408_sp.pdf, [consultado el 20 de febrero de 2017].

PODVIG, Pavel, Russian Strategic Nuclear Forces, Cambridge, The MIT Press, 2004, 716 págs.

ROTBERG, Robert I, Rabb, Theodore K. and Gilpin, Robert, The origin and prevention of major wars, New York, Cambridge University Press, 1989, 360 págs.

SAGAN, Scott D., «Why do States build nuclear weapons?: Three models in the search of a bomb», International Security, vol 21, no. 3, Winter 1996-1997, págs 54-86.

SCHULTZ, George P., Preventing the proliferation of nuclear weapons, Washington D.C., U.S. Dept. of State, Bureau of Public Affairs, Office of Public Communication, Editorial Division, 1984, 3 págs.

US Department of Defense, DoDD 3150.02, Washinton D.C., 24 de abril de 2013 (incorporado cambio 2 efectivo el 12 de mayo de 2016), disponible en http://www.dtic.mil/whs/directives/corres/pdf/315002p.pdf, [consultado el 23 de febrero de 2017].

WEISS, Leonard, «Atoms for Peace», Bulletin of the Atomic Scientists, vol 59, no. 6, 2003, págs 41-42.

Rojas, Francisco (1992), América Latina en la posguerra fría: nuevas oportunidades para la cooperación para la paz. Relaciones Internacionales, núm. 41, San José de Costa Rica, Universidad Nacional de Costa Rica.

Rojas Aravena, Francisco (2012). Seguridad Internacional, el espacio y posición de América Latina, Grupo de Trabajo núm. 03/2011, Madrid, Centro Superior de Estudios de la Defensa Nacional (CESEDEN), Instituto Español de Estudios Estratégicos.

Rumsfeld, D. (2001), Informe Quadrennial Defense Review y en la Estrategia de Seguridad. Secretaría de Defensa de los EE.UU.

Salas Elgart, Pedro Félix (1962), El Tratado Interamericano de Asistencia Recíproca de Río. Santiago de Chile, Ed. Jurídica de Chile.

Smith, S. (2005), The contested concept of security. United States, Lynne Rienner.

Varas, Augusto (1995). La seguridad hemisférica cooperativa de la post «Guerra Fría». Documento Área de Relaciones Internacionales y Militares, Chile, FLACSO.

Varas, Augusto & Caro, Isaac (ed.) (2000), Medidas de confianza mutua en América Latina. Santiago de Chile, FLACSO, *Stimson Center*, SER.

«EE. UU. implica a sus fuerzas armadas en la seguridad interior frente a ataques terroristas». El País. 1 de octubre de 2001. [Recurso electrónico] http://www.belt.es/noticias/2001/01_octubre/01_05/01_ejercito.htm. [Consulta: 17-04-2013].

RADICALIZACIÓN ISLAMISTA. UN ANÁLISIS CONCEPTUAL

José Manuel Rodríguez-González
Facultad de Psicología. Universidad de Sevilla

María del Pilar Ceballos-Becerril
Facultad de Psicología. Universidad de Sevilla

Pedro Álvarez Nieto
Academia de Artillería. Segovia

Pablo Rey García
Facultad de Comunicación. Universidad Pontificia de Salamanca

Resumen

Sin duda alguna a partir del 11S se extrajo del *Pythos* de Pandora un nuevo mal, tanto para Occidente como para Oriente. Si bien el terrorismo ha sido un fenómeno estrechamente unido a la Historia de la Humanidad, las condiciones y características que ha ido adoptando a lo largo de los años en su versión próxima a un Islam concebido de forma radical y violenta han supuesto un foco de interés e investigación por parte de profesionales de muy diversas ramas de la Ciencia, en especial su faceta asociada a la radicalización de los efectivos que llevan a cabo las acciones violentas.
En la presente comunicación se lleva a cabo un análisis conceptual de la Radicalización desde dos aproximaciones inicialmente dispares; aunque complementarias: la Psicología y la Ciencia Política, llegando a detectar los posibles vínculos teóricos y aplicados precisos.

Palabras claves

Radicalización, Yihadismo, Terrorismo, Violencia Ideológica.

1. Introducción

El terrorismo ha conseguido una de sus metas, ha logrado llamar nuestra atención e incrementar nuestro nivel de preo-

cupación. Aquella tradicional afirmación de que *Terrorismo no es gente muriendo, si no gente mirando*, alcanza pleno sentido en estos momentos. No se trata de alarmismo, es la simple realidad. Cada atentado protagonizado por organizaciones yihadistas violentas alcanza no sólo en los medios de comunicación sino también en las redes sociales un nivel de significación importante. Se ha desarrollado una sensibilidad marcada que se pone en marcha de manera instantánea ante acciones cometidas contra Occidente; pero cada vez más cuando dichas acciones ocurren en países asolados por conflictos generados por una concepción rigorista de la religión e impuesta por grupos de radicales.

Por todo ello, afirmar que el Terrorismo se ha convertido en un problema de especial impacto tanto en Occidente como en Oriente es un lugar común y no es algo novedoso a fecha de 2016. Mantener que las acciones terroristas son llevadas a cabo por hombres y mujeres que han desarrollado un nivel de implicación importante en estas diversas organizaciones violentas no es más que una realidad. La tendencia actual en la investigación en esta área se centra básicamente tanto en el proceso que tiene lugar para conseguir que una persona a la que se ha captado acabe siendo capaz de poner en marcha acciones agresivas y/o violentas como en la forma en la que se ha captado a esa persona. No obstante parece que pasa a un segundo plano el hecho de considerar *¿qué es la radicalización?* o mejor aún, *¿a quién llamamos radical?* De la misma forma que sucede con el concepto Terrorismo, las aproximaciones, matizaciones e incluso excepciones son muy usuales, hasta tal punto que a veces perdemos la orientación en nuestros análisis.

Es por ello que el objetivo del presente estudio no es otro que el de delimitar una serie de líneas, destacar directrices (en la medida de lo posible) y, por supuesto, detectar acuerdos y diferencias teóricas, siempre sin perder de vista el papel que juegan los medios de comunicación en todo ello.

2. ¿Definiendo un concepto o delimitando un área de trabajo?

En fechas recientes Reinares (2016) afirma que:

> apremia … repensar el concepto mismo de radicalización, para aclarar si las medidas que hay que adoptar ante dicho proceso se refieren únicamente a evitar que haya individuos implicados en

> actividades terroristas o supone también hacer frente a visiones rigoristas y extremistas del credo islámico, como las salafistas u otras similares, cuyas actuaciones provocan la segregación de colectividades enteras de musulmanes en el interior de las sociedades europeas, así como fracturas entre musulmanes y no musulmanes que explotan los terroristas.

La consecuencia de la afirmación anterior conlleva un hecho desestabilizador, ni las instituciones de la Unión Europea ni las correspondientes a cada uno de los países que la conforman, tienen (a fecha de hoy) claro cuál es el problema implícito en la Radicalización, es decir, su naturaleza y, por desgracia, los mecanismos para hacerle frente o para ponerle remedio a sus efectos negativos.

Hace escasos meses, el comunicado de la European Commission (2016: 3) acerca de la Radicalización Violenta insistía en que se trata de «un fenómeno complejo que exige un conocimiento profundo y una respuesta multifacética». La aceptación de esta realidad supone un destacable avance en la lucha contra la violencia y la rigidez ideológica.

Sin duda no podemos negar que las posturas violentas que nos ocupan no son nuevas en la Historia de la Humanidad; pero no es menos cierto que en fechas actuales han alcanzado unas manifestaciones impactantes, han supuesto unos daños personales muy significativos y se evidencia el uso de unos medios de comunicación que superan lo usual.

¿Cómo poder lograr la meta de definir un término multidimensional tanto en sus causas como en sus consecuencias?

Dependiendo de las fuentes a las que recurramos los intentos de definición de la radicalización son dispares. Es por ello que consideramos más interesante ocuparnos sobre los aspectos en los que se centran los estudios centrados en esta temática.

1. *Visión desde la sociología*

Desde el ámbito de la Sociología lo habitual es recurrir a las características sociodemográficas de radicales detenidos por las Fuerzas y Cuerpos de Seguridad del Estado para llevar a cabo una prospección que permita extraer características «*comunes*» de los/as llamados/as radicales. En este sentido una pequeña selección de los trabajos de Reinares (2012 y 2015) y Reinares y García-Cal-

vo (2013 y 2016) proporcionan un claro ejemplo de lo que planteamos. Siguiendo esta línea de trabajo, se trata de implementar una postdicción a partir de la cual extraer enseñanzas válidas a corto plazo ya que, en base a lo cambiante de la sociedad actual, las conclusiones que podamos alcanzar se encuentran limitadas. Baste un ejemplo en este sentido, a partir del atentado de Niza de julio del presente año se rescata un término del que ya se hablaba en 2015, las *Radicalizaciones Exprés* e incluso de *Yihadistas Exprés*, referidas a aquellos conversos que directamente se convierten no al Islam, si no al Yihadismo. Su mutación no tiene unas causas principales de orden religioso, se debe más a un discurso polarizado de «*buenos y malos, oprimidos y opresores*» y donde el converso considera que lleva a término acciones orientadas a una mejora del mundo, a una ruptura de la situación opresora de una civilización contra otra.

En definitiva, no se trata tanto de definir que es un/a *Radical* o la *Radicalización* como de desglosar las características propias de estos o estas.

No obstante es viable hallar posturas críticas como la mantenida por Moreras (2015) cuando concluye, como resultado de una revisión de hasta 25 definiciones de Radicalización, que se trata de un concepto «*infrateorizado*» por cuanto «*se presenta como un hecho dado por supuesto, como un estado al que se llega debido a una predisposición que muestran los musulmanes, y no como un proceso social condicionado por numerosos y aleatorios factores*». Posicionamientos como este último sirven de guía ante las nuevas decisiones a abordar en cuanto a investigación.

2. *Visión desde la ciencia política*

Dadas las características del tema y de esta rama de la Ciencia, es preciso un estudio más amplio.

En la actualidad se asocia el Radicalismo a las doctrinas políticas de tipo yihadista que se han empezado a extender por los años noventa del siglo pasado y perduran en la actualidad. En ellas juega un papel importantísimo la religión. De manera ineludible se trasponen los conceptos religiosos del Islam a la vida política, social, económica, etc.

De esta forma se hablaría de un ejercicio absoluto del poder (religioso, con un sustrato político) y donde la confrontación de

ideas o posiciones no tiene cabida. El propio acuñamiento del término *Estado Islámico* resulta significativo por sí mismo.

Evidentemente estas consideraciones nos llevan directamente a plantear ¿es el radicalismo un concepto nuevo en el mundo de la política, en su más amplio espectro? La realidad nos encamina a afirmar que nos hallamos ante una vieja escuela de detentación del poder y sobradamente conocida en este ámbito. Mellón y Parra (2015: 21) recuerdan en este sentido que se trata de un término asociado ya en los años 70 al ejercicio de la violencia (siempre con fines políticos) en los sistemas democráticos occidentales.

En la actualidad *DAESH* y Al Qaeda (entre otros grupos) dominan ciudades y pueblos sirios donde ya se transforma en realidad el sueño del último (Al Qaeda) de crear un Estado Islámico. En especial, en las provincias de Alepo, Idlib y Raqqa. El empleo de métodos sanguinarios contra los que consideran como *desviados* del Islam ha generado tanto miedo como una ola de indignación en la propia población local. En este sentido resulta difícil que ganen la simpatía de los habitantes, entre otras razones porque los sirios se sienten muy alejados de este tipo de orientaciones ideológicas, especialmente después de ver la evolución desde 2003 de la vecina Irak (Mesa García, 2014: 3).

Se hace preciso replantear posiciones. Si hace 2 años se optaba por menospreciar todo el fenómeno derivado del DAESH por considerarlo como un nuevo grupo cuyo fin era retrasar el reloj de la historia para volver a los tiempos coránicos del Profeta, la realidad ha resultado muy distinta por afectarnos de una forma manifiesta. Sus mensajes, organización, logística, grupos de choque, propaganda y acciones llegan a todos los rincones del mundo. De la misma forma que Al Qaeda supo aprovechar los beneficios de la globalización, esta otra organización ha sabido mejorar las potencialidades no manifiestas.

Baste una simple muestra, en la Unión Europea se estima que el número de ciudadanos radicalizados que pasan a engrosar el número de combatientes extranjeros de la Yihad está tomando dimensiones peligrosas y preocupantes. Francia, con al menos 1400, se sitúa a la cabeza, seguida de Alemania (550) y Reino Unido (500). En Bélgica, Austria y Holanda se localizan 300, 164 y 123 respectivamente. Nuestro país alcanza aproximadamente los 115 combatientes (Torres Roselló, 2015: 6).

Todo ello justifica el interés de las instituciones europeas. En 2005 la Unión Europea (Europena Union, 2005) aprobó la *Estrategia Europea Contraterrorista*, en la que el primer punto de las medidas preventivas era combatir la Radicalización y el reclutamiento de terroristas mediante la «identificación de instrumentos y métodos de propaganda empleados por los terroristas».

Esta postura se mantuvo e incluso se sistematizó años más tarde (European Union, 2011). La acción a través de los medios de comunicación y de los contenidos de internet se convirtió en algo esencial en aquel momento (vital en el presente). Mediante la participación de The European Network of Experts on Radicalisation (ENER), se comenzó a centrar el interés en las vías de acceso a la radicalización violenta y el consecuente reclutamiento, esto es: la propaganda yihadista violenta y el papel que internet juega en todo ello.

Se considera que el diseño y la implementación de las medidas de lucha contra la radicalización se deben iniciar tanto en las instituciones y organizaciones de carácter municipal como en las regionales y las estatales, es decir, medidas conjuntas y adaptadas a cada situación. Se entiende que los actores locales son los más adecuados para la detección y la prevención de la radicalización, ya sea a corto o a medio plazo (así lo considera incluso el Plan Estratégico Nacional de lucha contra la Radicalización Violenta, Ministerio del Interior, 2015). No obstante la aproximación política y la social vuelven a caer en el mismo error, por la ausencia de definición o de descripción del Radicalismo. Como indicábamos más arriba, se trata de un concepto infrateorizado y ello perjudica enormemente a la hora de la prevención. La realidad apoya esta afirmación, la Resolución de 25 de Noviembre de 2015 (European Union, 2015) del Parlamento Europeo reconoce, de forma implícita que la estrategia original ha fracasado, una de las causas, sin duda, puede ser la que apuntamos.

3. *Visión desde la psicología*

Desde el punto de vista de la Psicología, los estudios acerca del Terrorismo, los terroristas y la forma en la que se lleva a cabo la radicalización de estos adolecen de graves déficits desde su inicio, tanto fuera como dentro de nuestras fronteras.

Partiendo de estas premisas, cualquier línea de trabajo que en un momento determinado se quiera establecer no va a tener otro sentido que verificar toda una serie de hipótesis de partida

que a todas luces pueden resultar improcedentes y, a partir de las conclusiones, volver a establecer nueva directrices al respecto.

El aspecto positivo es que se han acabado abandonando los análisis orientados a la identificación de cuadros de orden psicopatológico en los identificados como radicales. Como ya recogía Horgan (2009) se trata de una línea de trabajo improductiva y no es viable el establecimiento de una covariación positiva entre ambas variables.

Sin duda se hace preciso replantearse los estudios y dirigir la atención hacia otros focos más pertinentes y la comprensión del Proceso de Radicalización resulta básica, tanto para la prevención como para posterior desrradicalización. En la mayoría de las ocasiones hallamos que las investigaciones desde la órbita de la Psicología se dirigen al análisis de las dimensiones de personalidad y variables psicosociales de los identificados como terroristas y/o sus simpatizantes. La intención que guía este proceder no es otra que la de establecer un/os perfile/s a través del/os cual/es alcanzar una pretendida detección precoz de riesgo. El excelente trabajo de Trujillo y Moyano (2013) redunda en esta línea.

Como podemos ver, la tendencia continúa, se mantiene el abandono del análisis del mismo concepto de Radicalización.

4. *Medios de Comunicación y Radicalización*

El auge del terrorismo conlleva un aumento de su repercusión en los medios de comunicación, y de las menciones de los radicales que son sus autores *¿Cómo se les trata, con qué adjetivos se les caracteriza, cuál es el rigor léxico y semántico que utiliza la prensa española?*

Hay una abundante literatura sobre el fenómeno terrorista y su relación con los medios de comunicación, especialmente en un país que desde hace años soporta la lacra de la banda ETA (Reinares, 1982; Chomsky, 1989; Veres, *sd*), pero no se debe olvidar que el terrorismo no siempre ha sido obra de fanáticos necesitados de publicidad. La publicidad (la visibilidad mediática) es la forma actual de conseguir repercusión, y Walzer considera al terrorismo como una suerte de guerra continuada por otros medios, incluso en oposición a Liddell Hart (que abominaba del terrorismo) la coloca entre las estrategias de acercamiento indirecto (Walzer, 2001: 269), y define su esencia por sus consecuencias y sus objetivos, más que por su amplificación mediática. El terrorismo busca aterrorizar inocentes mediante los hechos, no mediante su

conocimiento. Además no necesariamente es llevado a cabo por fanáticos radicales. El teórico de la guerra justa distingue: terrorismos de Estado, acciones terroristas ilegítimas pero morales, o ejércitos que utilizan el terrorismo como acelerador de la posible victoria, entre otras modalidades. Incluso segmenta la historia del terrorismo en base al respeto a un código político, que hace distinciones entre víctimas lícitas e ilícitas.

El terrorismo yihadista actual, estaría situado en el último peldaño, el más bárbaro, aunque tenga su lógica interna, la lógica radical. Muy acertadamente define Walzer al terrorismo salvaje como *la forma totalitaria de la guerra*, la que no distingue códigos morales ni políticos (2001:276). Ahí, en el extremo del concepto, es donde se encuentra el radical. Y por los condicionantes actuales a la hora de entender un terrorismo irrestricto en un mundo globalizado y comunicado, es rentable atemorizar mediante el simple conocimiento de la amenaza, refrendada por la visibilidad de su cumplimiento en momentos oportunos. Aparece, por tanto, en esta definición de terrorismo, los dos ejes de este ensayo: el radical y la presencia mediática.

En primer lugar, en el contexto de estudios de conflicto, el acervo común ha asociado la palabra *radical* al término islamista, dentro del campo semántico del terrorismo. Parece que no caben, por tanto, asociaciones de otro tipo (radicales de ámbito político o radicales nacionalistas, por citar sólo matices). Sin embargo también en el ámbito deportivo se encuentran menciones semejantes, referidas a grupos de *hooligans*: los famosos seguidores radicales. De esta manera, el uso reiterado ha consolidado ambas expresiones, *seguidores radicales* e *islamistas radicales*.

Sin embargo la prensa española tiene un registro mayor en el vocabulario y el adjetivo *radical* se sigue utilizando con normalidad para cualquier otro tipo de caracterización, sin llegar a formar una categoría autónoma. Por poner un ejemplo, en el diario *El Mundo*, *radical-radicalismo* proporciona una respuesta en el buscador histórico de casi 8000 resultados. Si se restringe la búsqueda a las informaciones referidas a terrorismo, son 897. En otras palabras, una de cada diez veces que aparece el adjetivo radical, se hace en un contexto informativo de islamismo, bien sea de terrorismo o bien de conflictos armados abiertos, como Siria o Líbano. No es un porcentaje desdeñable, pero no es en absoluto un monopolio léxico.

En el fondo, no debería preocupar cómo se les denomina a los actores, pues bien se les llame radicales, islamistas o asesinos, el problema son los hechos, no los adjetivos. Hasta cierto punto, aprovechando el debate abierto sobre uno de los últimos atentados, es irrelevante si el conductor del camión de Niza era un radical obnubilado, un intelectual convencido o un psicópata encubierto. Incluso, en último término, también sería poco importante si el hecho en sí fue una actuación consensuada con DAESH o si la organización islamista aprovechó el atentado para reclamarlo como propio. Cualquiera de estas hipótesis sigue abierta, y es carne de debate en medios de comunicación más o menos serios. Lo que sí centra esta investigación es el proceso de radicalización, y si los medios de comunicación prestan la adecuada atención a este aspecto, que sí es relevante.

Una visita a las hemerotecas de los principales medios arroja luz: los procesos de radicalización están presentes, pero no se tratan con profundidad. En lo que va de año de 2016, *El Mundo* ha publicado 47 informaciones sobre radicales en la sección de Internacional, y 13 en la de España. De esas 47 informaciones, 30 hacen referencia a terrorismo islámico, y otras 7 entre las de la sección «*España*». Lo preocupante es que sólo una de ellas hace una descripción del yihadista tipo en España (Negrete, 2016), las demás se preocupan de hechos noticiosos (detenciones de propagandistas o captadores yihadistas, fundamentalmente).

El País ha publicado casi 30.000 informaciones con la palabra radical en el año 2016, de las que 5478 tienen que ver con yihadismo. De nuevo es una cifra parecida (un 18%) a la del otro gran periódico de España: de cada 10 veces que aparece la palabra radical, dos se relaciona con terrorismo. Es relevante, en primer lugar, la mayor cantidad de informaciones, así como una mayor variedad de secciones, con especial relevancia a la de internacional. Debe notarse la vocación internacional que ha caracterizado a este medio desde su fundación, así como los acuerdos que tiene con otros medios para compartir informaciones.

Las informaciones tienen fuentes variadas, primarias (Ministerio del Interior, Policías y servicios de información) y declaraciones pertinentes. Un primer repaso da además un cierto número de informaciones no dependientes de hechos noticiosos, sino documentales o ampliativos.

En otros medios de comunicación, como televisiones o la radio, en la emisión en directo es difícil encontrar materiales que profundicen correctamente en el tema, por la propia naturaleza del medio, y se cae más a menudo en la necesidad de constreñirse a la información pasajera.

Sí existen, sin embargo, posibilidades de recuperación desde la web, de documentales de RTVE emitidos en los programas *En Portada* (*Hijos del Desarraigo* de Pilar Requena) *Informe Semanal* (*Aliados contra el Yihadismo*), *Teleobjetivo* (un programa de especial servicio público, entrado en las Fuerzas y Cuerpos de Seguridad del Estado) o *Documentos TV*, así como *podcast* de las diferentes emisoras de radio de la corporación pública.

En medios audiovisuales privados existen también formatos que permiten la profundización: *A Fondo, El Objetivo, Salvados, En Tierra Hostil, o Equipo de Investigación*, de Atresmedia o *En el punto de mira, Conexión Samanta,* o *Infiltrados,* de Mediaset; todos ellos, en algún momento han tratado el tema del terrorismo yihadista y la radicalización, si bien desde formatos parcos y ambiciosos en la medida en que lo son las cadenas que los emiten. Su utilidad informativa es pareja a la calidad técnica. Es meritorio el esfuerzo de sus productores y directores por realizar productos y tratar contenidos de elevada cantidad, pero hay que tener presente, a modo de símbolo, que Telecinco decidió sustituir el 31 de diciembre de 2010 el canal CNN+ por un canal llamado *Gran Hermano 24 Horas.*

Lo preocupante de esta semblanza es que en España existen fuentes de probada calidad, como el Real Instituto Elcano o el Instituto de Estudios Estratégicos, que son utilizadas como fuente primaria en muy contadas ocasiones, al menos con visibilidad en el producto noticioso final. Se suele preferir, por el carácter evanescente de las informaciones, utilizar como fuentes a las ONGDs, Fuerzas y Cuerpos de Seguridad implicados, o portavoces políticos. Si bien es cierto que estos productos documentales están a disposición del público en las *webs* de sendas instituciones, eso no inhibe a los medios de comunicación de su deber de utilizar las mejores fuentes.

Decía Marshall McLuhan que sin comunicación no habría terrorismo (McLuhan, 1978), y esto se puede ampliar al radicalismo, teniendo en cuenta que los medios de comunicación han ampliado el espectro de su propia naturaleza. La simbiosis que

se establecía entre los medios y el terrorismo (aquellos proporcionaban su fin último al terrorismo, expandir su terror al gran público, mientras que este nutría de contenido a los primeros) es ahora un medio de utilidad para el radicalismo. El radical establece, como se ha visto, una doble vía de uso con los medios. Por un lado es capaz de profundizar en su radicalización, en un proceso de consumo e instrucción personal. Por el otro, el radical es capaz de establecer un proceso de captación y amplificación de su mensaje. No se debe olvidar que los medios de comunicación permiten la segmentación de audiencias, incluyendo la total personalización de la web.

3. Captación y radicalización

Si hay un elemento común en el discurso actual que caracteriza a los nuevos terroristas es su desarraigo con el territorio en el que viven y con el de su procedencia. De un lado acaban por rechazar la cultura moderna europea, por cuanto Europa es la culpable de todos sus males y de la falta de integración en la que se encuentran; de otro lado añoran su tierra de procedencia, llegando al extremo de idealizarla, buscando explicaciones, si es preciso, paralelas a la realidad o recurriendo a versiones reduccionistas de la Historia. La no pertenencia plena, la no identificación acaba por generar un fenómeno de Aculturación.

En cuanto a aquellos que viven y se desenvuelven en los países del mundo árabe, hallamos que se trata de jóvenes musulmanes sin perspectivas de futuro (aunque esta afirmación sería excesivamente generalista), en situaciones de pobreza acentuada y en una sociedad en la que la corrupción, las desigualdades y las injusticias (avaladas en ocasiones por regímenes autoritarios) son lo habitual. Ante este panorama no es extraño que a través del discurso adecuado y manejando de manera pertinente la frustración de estas personas, adopten una postura radical y la Yihad se convierta en una salida a todos sus problemas, aunque ello implique el sacrificio de sus propias vidas.

Un elemento facilitador que ha potenciado todo este proceso, como es bien sabido, ha sido la globalización y la rapidez de transmisión de informaciones a través de internet y las redes sociales. Ya no hay que buscar a los *guías* de la radicalización en las mezquitas (de hecho anteriormente, de ocurrir los contactos de forma

presencial, estos acontecían en lugares de culto improvisados, no reglados), basta una pantalla de ordenador o una tablet. Precisamente a DAESH se le reconoce lo cuidadoso y sistematizado de su labor divulgadora/captadora. El/la adepto/a podrá encontrar perfectamente organizados vídeos e imágenes mediante las cuales se les adoctrina en las bondades del yihadismo, la necesidad del empleo de la violencia y mediante multitud de mensajes comienza su adoctrinamiento y/o o autoadoctrinamiento radical. El medio empleado, en sí, dificulta (que no impide) la detección por parte de los cuerpos de seguridad, adopta una modalidad particular, casi íntima y alejada de todo.

La soledad, la puerta del alejamiento de la realidad y el punto de partida para la construcción de otra realidad, a imagen y semejanza de las propias necesidades y fantasías. Otro mundo es posible, de hecho *otros* lo están construyendo, incluso a costa de sus vidas. No se trata de una utopía, es una realidad que se puede seguir en tiempo real como se va constituyendo, de hecho es un Estado, el Estado Islámico ¿La Violencia? No es más que un medio para conseguir un fin cuya trascendencia supera la individualidad. Ya tenemos sembrada la semilla, el tiempo y los contactos determinarán la calidad o la profundidad del compromiso (la Radicalización) del/a seguidor/a.

4. Intentos de conceptualización ¿una tarea eficaz?

«Contrario a la creencia popular, la radicalización dirigida al terrorismo no es producto de la pobreza, de lavados de cerebro, de inmadurez juvenil, ignorancia o falta de educación, desempleo, falta de responsabilidad social, criminalidad o inestabilidad mental. La movilización de los jóvenes hacia este fenómeno social se basa en la amistad y el parentesco.» (Sageman, 2008: 39).

> «Es el proceso a través del cual un individuo adopta, en mayor o menor grado, actitudes y creencias que justifican tanto utilitaria como moralmente el terrorismo inspirado en una versión salafista y a la vez belicosa del credo islámico» (García-Calvo y Reinares, 2013).

Desde la afirmación de Sageman (2008: 39) a la de García-Calvo y Reinares (2013), el salto conceptual es importante y muy marcado. Se han seleccionado estas de la misma forma que podrían haber sido otras, lo importante es poder captar de forma

breve la disparidad y diversidad de puntos de vista que existen a la hora de abordar esta tarea.

Posiblemente sea Moreras (2015) el que adopte una medida más efectiva desde el momento en el que opta por hacer una clasificación en base a los contenidos semánticos de un total de 27 propuestas de conceptualización. De esta manera cabe destacar las siguientes categorías:

—Radicalización como proceso lineal y, por tanto, con diferentes estadios.
—Radicalización como proceso, pero de carácter individual, que implica un cambio actitudinal y existencial vinculado a poblaciones jóvenes.
—Radicalización asociada a conductas violentas en un porcentaje significativo.
—Radicalización como reacción a una pérdida de confianza en los valores democráticos o como enfrentamiento a regímenes autoritarios.
—Radicalización asociada a creencias religiosas, bien compartidas por los radicales, bien como resultado de una conversión religiosa de tipo rigorista.
—Radicalización entendida como un sinónimo de extremismo.
—Radicalización como medio de alcanzar notoriedad en un contexto dado.

Tal y como se puede deducir de lo expuesto, ocurre lo mismo que con el concepto de Terrorismo, son tan variadas las aproximaciones y tan diversos los intereses (a veces condicionados por circunstancias coyunturales) que al final no es viable una directriz clara. Diferentes intereses acaban facilitando otras tantas líneas de trabajo e investigación, algunas de las cuales, al encontrarnos en el campo de las Ciencias Sociales, pueden resultar o resultan improductivas. El problema es que en esta ocasión estamos jugando y trabajando no sólo con nuestra seguridad, sino también con la de los otros.

8. Conclusiones

Son escasos los intentos de unificar criterios a la hora de definir o, por lo menos, delimitar un marco conceptual común alrededor del concepto de Radicalización. Los posicionamientos divergentes

no solo generan líneas de trabajo dispares, también programas de intervención con «*activos radicalizados*» que, al partir de visiones sesgadas, pueden facilitar unos resultados cuestionables.

En definitiva, no erraríamos si siguiendo a Sedgwick (2010: 479) afirmásemos que la Radicalización es «Todo aquello que sucede antes de que estalle la bomba», es decir, una multitud de variables cuya combinación operativa aún sigue sin ser descubierta.

9. Bibliografía

European Commisssion. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regiosn.Suporting the prevention of Radicalisation leading to violent extremism.* [en linea], [June, 2016], [2 de agosto de 2016], http://ec.europa.eu/dgs/education_culture/repository/education/library/publications/2016/communication-preventing-radicalisation_en.pdf acceso 2016

European Unión. *Counter-Terrorism Strategy.* [en línea], [2005], [1 de septiembre de 2016], http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV:l33275

European Unión. *EU Action Plan on combating terrorism.* [en linea], [11 de enero de 2011], [1 de septiembre de 2016] http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2015893%202010%20REV%201

European Union.Draft *Report. On prevention of radicalisation and recruitment of European citizens by terrorist organizations.* [en linea], [2015], [1 de septiembre de 2016], http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+COMPARL+PE-551.967+01+DOC+PDF+V0//EN&language=EN

García-Calvo, Carola y Fernando Reinares, <<Procesos de radicalización violenta y terrorismo yihadista en España: ¿cuándo? ¿dónde? ¿cómo?>> [en línea], [Documento de Trabajo 16/2013, noviembre 2013], [20 de julio de 2016], http://www.realinstitutoelcano.org/wps/portal/web/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/terrorismo+internacional/dt16-2013-reinares-gciacalvo-radicalizacion-terrorismo-yihadista-espana acceso 2016

Horgan, John, *Psicología del terrorismo*, Barcelona, Gedisa, 2009, 272 págs.

McLuhan, Marshall, *Il Tempo*, 19 de febrero de 1978. Citado por Noah Chomsky *La cultura del terrorismo.* Barcelona, Ediciones B, 1989, 332 págs.

Mellón, Joan Antón e Ignacio Parra, <<Concepto de Radicalización>>, en Mellón, Joan Antón (ed.), *Islamismo Yihadista: radicalización y contrarradicalización*, Valencia, Tirant Lo Blanch, 2015, 17-37, págs.17-37.

Mesa García, Beatriz, <<Siria, el «nuevo dorado yihadista>>, [en línea], [documento de opinión 15/2014 de 13 feb. 2014], [9 de septiembre de 2016] http://www.ieee.es/Galerias/fichero/docs_opinion/2014/DIEEEO15-2014_Siria_DoradoYihadista_B.Mesa.pdf

Ministerio del Interior, *Plan Estratégico Nacional de lucha contra la radicalización violenta*, [en línea], [2015], [19 de julio de 2015], http://www.interior.gob.

es/documents/10180/3066463/CM_mir_PEN-LCRV.pdf/b57166c1-aaaf-4c0d-84c7-b69bda6246f5%20

Moreras, Jordi, <<Políticas de prevención de la radicalización>> [en línea], [Afkar/Ideas 45/2015], [3 de agosto de 2016], http://www.politicaexterior.com/articulos/afkar-ideas/politicas-de-prevencion-de-la-radicalizacion/

Negrete, Jorge (2016) <<Perfil del yihadista en España: varón, casado, sin estudios universitarios y con escasa noción del Islam>>, *El Mundo*, 12 de julio de 2016.

Reinares, Fernando, *Terrorismo y sociedad democrática*, Madrid, Akal, 1982, 182 págs.

Reinares, Fernando, <<Geografía Mundial del Terrorismo>>, [en línea], [ARI 10/2012], [24 de julio de 2016], http://www.realinstitutoelcano.org/wps/portal/web/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/terrorismo+internacional/ari10-2012

Reinares, Fernando, <<Fábricas de terroristas>>, [en línea], [10/2015], [27 de julio de 2016],http://www.realinstitutoelcano.org/wps/portal/web/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/terrorismo+internacional/reinares-fabricas-de-terroristas

Reinares, Fernando, <<Prevenir la radicalización yihadista: un fracaso europeo>>, [en linea], [2016], [14 de agosto de 2016], http://www.blog.rielcano.org/prevenir-la-radicalizacion-yihadista-un-fracaso-europeo/

Reinares, Fernando y Carola García-Calvo, <<Los yihadistas en España: perfil sociodemográfico de condenados por actividades terroristas o muertos en acto de terrorismo suicida entre 1996 y 2012>> [en línea], [documento de trabajo 11/213], [2 de agosto de 2016] http://www.realinstitutoelcano.org/wps/portal/web/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/terrorismo+internacional/dt11-2013-reinares-garciacalvo-yihadistas-espana-perfil-sociodemografico-1996-2012

Reinares, Fernando y Carola García-Calvo, <<Yihadistas en España desde el 11M>>, *El País,* [en línea] [11 de marzo de 2016], [4 de agosto de 2016], http://www.realinstitutoelcano.org/wps/portal/web/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/terrorismo+internacional/reinares-garciacalvo-yihadistas-espana-11m

Sageman, Marc, <<The Next Generation of Terror, *Foreign Policy*>>, vol. 165, 2008, núm. 1, págs. 36-42.

Sedgwick, Mark, <<The concept of Radicalisation as a source of confusion>>, *Terrorism Political Violence*, vol. 22, 2010, núm. 4, págs. 479-494.

Torres Roselló, Jordí, *El auge del yihadismo en Occidente: Un producto de la Modernidad*, [en linea], [documento de opinión 103/2015, septiembre 2015], [9 de septiembre de 2016], http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO103-2015_Auge_Yihadismo_Occidente_JordiTorres.pdf

Trujillo, Humberto y Manuel Moyano, *Radicalización islamista y Terrorismo: Claves Psicosociales*, Granada, Universidad de Granada, 2013, 336 págs.

Veres, Luis, <<Prensa, poder y terrorismo>>*, Amnis. Revue de Civilisation Contemporaine de l'Université de Bretagnem Occidentale*, [en línea], [revista], sd, [1 de septiembre de 2016], http:///Users/administrador/Downloads/Dialnet-PrensaPoderYTerrorismo-2650541.pdf

Walzer, Michael, *Guerras justas e injustas. Un razonamiento moral con ejemplos históricos*, Barcelona, Paidós, 2001, 448 págs.

LA SITUACIÓN SOCIOPOLÍTICA DE AFGANISTÁN TRAS LA RETIRADA ESTADOUNIDENSE EN DICIEMBRE DE 2014

Ana Belén Perianes Bermúdez
Spanish Women in International Security

Resumen

Tras la recuperación de su plena soberanía nacional no tutelada a finales del año 2014, Afganistán se enfrenta a riesgos especialmente graves en lo que concierne a su seguridad y estabilidad, como la persistencia de los santuarios de la insurgencia en Pakistán; la corrupción generalizada; el intenso crecimiento de la violencia; la falta de capacidades de las fuerzas de seguridad afganas; el punto muerto en que se encuentran desde 2013 las conversaciones entre el Gobierno afgano y los talibanes así como el resurgimiento de los últimos y, la pobreza y vulneración de derechos humanos que sufre la población, especialmente las mujeres, niñas y niños. El gobieno afgano ha de afrontar la delicada situación que vive Afganistán con los objetivos de fondo de la búsqueda de la reconciliación nacional y una exitosa transición económica que permita la viabilidad de la transición política.

Palabras claves

Soberanía, reconciliación nacional, insurgencia, talibanes, estabilidad.

1. Introducción

Afganistán enfrenta en la actualidad graves riesgos y amenazas para su estabilidad, al tiempo que ocupa un lugar destacado entre las principales preocupaciones de la agenda de seguridad de la comunidad internacional.

La retirada de buena parte de las tropas internacionales de Afganistán en diciembre de 2014, año en que la violencia había crecido intensamente en el país, coincidió en el tiempo con el

resurgimiento de los talibanes aprovechando el vacío de poder y la aparición en territorio afgano del autoproclamado Estado Islámico que, unidos a los problemas estructurales que ya presentaba el país, dificultan enormemente conseguir seguridad y estabilidad.

Ante el enconamiento de la situación del conflicto afgano, las Fuerzas Nacionales de Seguridad Afganas encaran un profundo debilitamiento y deficiencias esenciales que obstaculizaban sus capacidades para proporcionar seguridad al país: insuficiente capacidad logística, altas tasas de deserción, elevada corrupción y analfabetismo entre sus filas.

La delicada situación securitaria que afronta Afganistán se ve muy significativamente afectada por la crisis política e institucional que afronta el país, con un gobierno de unidad nacional incapaz por el momento de trabajar con el objetivo de fondo de la búsqueda de la reconciliación nacional bajo un modelo de país que garantice la gobernanza política junto con la mejora de las condiciones de vida de las mujeres y niñas y que aglutine la diversidad étnica de una sociedad tribal que lleva décadas soportando las consecuencias de guerras, pobreza, corrupción estructural, intransigencia religiosa y narcotráfico.

Ante este escenario, el gobierno del presidente Ghani Ahmadzai deberá afrontar la inestabilidad que vive Afganistán.

2. Antecedentes

2.1. *La guerra contra Afganistán*

El 7 de octubre de 2001, transcurrido menos de un mes desde los atentados del 11 de septiembre en territorio norteamericano, la Administración Bush declaró la guerra a Afganistán alegando el principio de autodefensa de la Carta de Naciones Unidas. Con anterioridad, las autoridades estadounidenses habían demandado sin éxito al gobierno talibán la entrega de Osama Bin Laden, en su momento líder de al-Qaeda.

George W. Bush y su equipo presidencial reaccionaron ante los referidos ataques terroristas determinando las nuevas amenazas globales a partir del salafismo yihadista de al-Qaeda, fijándola como el enemigo mundial ayudado por regímenes como el talibán en Afganistán (Perianes, 2015:83).

De este modo, de acuerdo a los valores de excepcionalidad que los fundamentos ideológicos del movimiento neoconservador

estadounidense establecen para Estados Unidos de acuerdo a la misión singular y providencial que entienden que el país está llamado a llevar a cabo en el mundo y, que además, vertebran la política exterior de las Administraciones de George W. Bush, éste último inició durante su primer mandato (2001-2004) una guerra contra Afganistán para, según argumentaba, conseguir la capitulación incondicional del régimen rebelde que apoyaba a los militantes salafistas yihadistas de al-Qaeda.

A partir de las justificaciones esgrimidas por la Administración Bush, Estados Unidos se erigió como la nación elegida por Dios para combatir el mal que encarnaba el régimen talibán por apoyar a los militantes de al-Qaeda en base a su estatus moral diferenciado y a su responsabilidad nacional como nación elegida por mandato divino para extender la visión norteamericana de democracia (entiéndase democracia liberal) por el mundo para consolidar su liderazgo global (Perianes, 2015:84).

Sin embargo, Afganistán era un Estado soberano desde cuyo territorio se había ordenado la ejecución de los atentados, pero sin implicación como tal en los mismos y los bombardeos estadounidenses a Afganistán ocasionaron miles de víctimas mortales afganas.

La Alianza del Norte, encargada de llevar a cabo el avance terrestre cuando la resistencia de los talibanes estaba muy deteriorada por los bombardeos, estaba formada por una serie de señores de la guerra contrarios al régimen talibán desde el final de la guerra civil. Su principal dirigente, el tayiko Ahmed Sha Massud, fiel al derrocado presidente Burhanuddin Rabbani y asesinado tres días antes de los atentados del 11S, perdió la vida en un atentado atribuido a al-Qaeda (Segura, 2004: 137).

«Libertad Duradera», la operación militar contra Afganistán, combinaba los bombardeos masivos con la infiltración de líderes disidentes cuya misión era intentar sublevar a la población pastún, suministrar información a los servicios de inteligencia estadounidenses y dar apoyo al avance de las tropas de la Alianza del Norte. Entre estos líderes disidentes destacaban Abdul Haq, capturado y fusilado por los talibanes el 29 de octubre de 2001 y Hamid Karzai, futuro presidente del gobierno provisional de Afganistán.

A mediados de noviembre de 2001, el régimen talibán conservaba únicamente la ciudad de Qunduz en el norte, que sería ocupada el 24 de noviembre y Qandahar, que después de días de

negociaciones entre el nuevo jefe del gobierno afgano, Hamid Karzai y los jefes tribales pastunes, se entregaría el 7 de diciembre. Poco después, Karzai proclamó el fin del régimen talibán.

La administración Bush se valió de su guerra a Afganistán, el derrocamiento del régimen talibán y el establecimiento de un gobierno afín a sus intereses para poner un pie en Asia Central y extender así a largo plazo en esta región su área de influencia (Perianes, 2015:84).

La cesión de bases en Tayikistán y en Uzbekistán, así como la ocupación de Afganistán permitían a Washington comenzar a llenar el vacío de poder dejado en la región tras la desaparición de la URSS, constituyendo un objetivo geoestratégico de primer orden. El establecimiento de alianzas con países antes alineados con la URSS permitiría consolidar la presencia norteamericana en el mismo corazón de Asia Central y modificar la relación de fuerzas con China.

2.2. *El régimen talibán*

La dictadura teocrática de los talibanes se significaba como uno de los regímenes más déspotas y totalitarios del mundo, conculcaba sistemáticamente los derechos humanos y llevaba a cabo una profunda y gravísima exclusión de género. Los talibanes estudiaban en las escuelas coránicas financiadas por los saudíes y eran pastunes (el grupo étnico mayoritario de Afganistán, que supone el 45% de su población), afganos o paquistaníes, hijos o huérfanos de pastunes muyahidines. Apenas conocían a las mujeres y recibían una rígida educación religiosa muy próxima a la interpretación wahabí del islam. Después de 1992, estos estudiantes crearon el movimiento talibán y participaron en la guerra civil (Perianes, 2015:136).

Con el apoyo de Arabia Saudí y de Pakistán, los talibanes ocuparon Kabul en 1996 y Mazar-i-Sarif en 1998. En consecuencia, la Alianza del Norte, formada por grupos de muyahidines mayoritariamente no pastunes y liderada por el comandante Massud, quedó reducida a una estrecha franja en el norte del país, en las fronteras de Turkmenistán, Uzbekistán y Tayikistán. La victoria de los talibanes suponía que, a partir de entonces, gobernaría en Kabul un régimen islámico cercano al wahabismo y, por lo tanto, aliado de Arabia Saudí.

El Afganistán de los talibanes se había convertido en el refugio de Bin Laden y su organización salafista yihadista, al-Qaeda, cuando fueron expulsados de Sudán en 1997. Varios años antes, en 1989, Bin Laden había fundado en la frontera entre Afganistán y Pakistán al-Qaeda con los salafistas de tendencia wahabí que acudieron a luchar financiados por Arabia Saudí contra los soviéticos.

Cabría destacar que en la década de los años 80 varios miles de internacionalistas salafistas acudieron a Afganistán o a Pakistán desde Oriente Próximo, el norte de África, Asia Central y Extremo Oriente. Una parte de ellos lucharon en la guerra de Afganistán como resultado de una compleja operación organizada por los servicios secretos de inteligencia saudíes y paquistaníes con el apoyo de Estados Unidos (Perianes, 2015:138).

La mayoría de estos militantes volvieron a sus países, donde fundaron grupos radicales islámicos de carácter violento (Argelia) o tomaron parte en otras guerras (Bosnia, Kosovo, Chechenia) en nombre de la *yihad* en su acepción belicosa de guerra santa. Algunos miles de ellos se quedaron con Bin Laden en Afganistán o fueron a los principales países del mundo musulmán, a Europa y a América. También es la *yihad* entendida como guerra santa, pero sin objetivos nacionales. Es así como al-Qaeda se convirtió entonces en una organización de alcance mundial y enmarcándose en contra del régimen de los Saud en Arabia Saudí.

Bin Laden y al-Qaeda consideraban que Estados Unidos y sus aliados eran los responsables de la paupérrima situación global en la que estimaban la situación de los musulmanes. Además, estaban especialmente convencidos de que las tropas estadounidenses tenían que ser expulsadas de la tierra sagrada de Arabia Saudí (Segura, 2004:138), manifestándose en contra de la presencia de Occidente en ese territorio.

En base a esta postura, desde comienzos de los años noventa, llevaron a cabo diversos ataques terroristas contra intereses estadounidenses: el *World Trade Center* en 1993, con seis muertos; un campamento militar estadounidense en Arabia Saudí en 1995, con diecinueve muertos; las embajadas estadounidenses de Nairobi (Kenia) y Dar es Salam (Tanzania), con doscientos veinticuatro muertos y el barco militar estadounidense *USS Cole* en Adén (Yemen) en el 2000, con diecisiete muertos. Al-Qaeda maximizó el potencial de sus acciones utilizando territorios sin

Estado, como Afganistán, Somalia o Yemen y convirtiéndose en una red que puede llevar a cabo acciones terroristas en cualquier lugar del mundo.

El poder de Bin Laden se basaba en buena medida en sus recursos financieros, ya que formaba parte de una de las familias más acaudaladas de Arabia Saudí. Además, se beneficiaba de las donaciones de sus simpatizantes en todo el mundo islámico, de las armas estadounidenses heredadas de la guerra de Afganistán y la utilización de las nuevas tecnologías. La Declaración de Guerra contra los norteamericanos que ocupan la tierra de los Lugares Sagrados (La Meca y Medina) realizada por Bin Laden el 23 de agosto de 1996, se confirmó ya como una seria amenaza para Estados Unidos. En este contexto es donde comenzaron a incubarse los atentados del 11S (Segura, 2004: 139).

2.3. *Afganistán tras el fin del régimen talibán*

La Administración Bush y la coalición internacional que lideraba dieron por finalizada la guerra a los tres meses aproximadamente de su inicio, cuando la Alianza del Norte completó la ocupación del bastión talibán de Kandahar. El nuevo gobierno provisional de Afganistán, presidido por Hamid Karzai, un comandante de etnia pastún y próximo al exmonarca Zahir que había participado en el gobierno de los muyahidines antes de la llegada al poder de los talibanes y que era favorable a la consecución de los intereses de la Administración de George W. Bush en el país, fue proclamado principios de diciembre de 2001.

Respecto a la situación en la que quedó el país, la instauración de un gobierno provisional no mejoró significativamente la realidad en Afganistán. Las donaciones internacionales para la reconstrucción únicamente se han hecho efectivas en una parte mínima y el país sigue sumido en la miseria, el desorden y la destrucción heredados tras casi tres décadas de guerra. Además, los señores de la guerra seguían controlando territorios y contestaban la autoridad del entonces presidente Karzai, confinado en Kabul y rodeado de una guardia pretoriana norteamericana.

Una vez concluida la guerra, Estados Unidos no había conseguido varios de los principales objetivos que le habían llevado a la misma: ni eliminar ni neutralizar a las cúpulas del régimen talibán y de al-Qaeda (Perianes, 2015:88). En este sentido, éstas últimas

habían desaparecido en busca de unas condiciones óptimas de seguridad para organizar y desarrollar las labores de resistencia, dirigiéndose tanto al interior del país como a Pakistán.

En un paso hacia delante de la Administración Bush, aún casi coincidiendo en el tiempo con los combates en las montañas de Tora Bora, la misma convocó la conferencia internacional que diera paso al Acuerdo sobre las disposiciones provisionales en Afganistán hasta el restablecimiento de instituciones permanentes de gobierno o Acuerdo de Bonn el 5 de diciembre de 2001 (Vega, 2011: 366), que fijaba los objetivos estratégico-políticos de la siguiente fase, de reconstrucción y estabilización.

El Acuerdo de Bonn, establecido con dirigentes afganos «no del todo representativos» con la excepción, entre otros, de los talibanes, pretendía promover la reconciliación nacional, la paz duradera, la estabilidad y los derechos humanos en Afganistán, de la cual reconocía su independencia, soberanía nacional e integridad territorial. Y, para alcanzar dichos objetivos, solicitaba el apoyo de la comunidad internacional.

El Consejo de Seguridad de Naciones Unidas creó a partir de su Resolución 1386 de 20 de diciembre de 2001 la Fuerza Internacional de Asistencia a la Seguridad, en adelante ISAF, con el objetivo de apoyar a la Autoridad Provisional afgana en sus labores de mantenimiento de la seguridad en Kabul y sus alrededores.

Con ello, se buscaba establecer un perímetro de seguridad para que tanto ISAF como la Autoridad Provisional afgana pudiesen desarrollar sus misiones de un modo seguro para poder alcanzar los objetivos estratégico-políticos asumidos en el Acuerdo de Bonn (Vega, 2011: 366). Al tiempo, la Operación Libertad Duradera mantenía sus objetivos de acabar con las cúpulas de al-Qaeda y talibán, erradicar sus capacidades de lucha y acción y procurar el establecimiento de un nuevo régimen moldeable a los intereses estadounidenses.

Sin embargo, la comunidad internacional no fue sensible a un hecho tan esencial como son las especificidades de la sociedad afgana. Ésta última, estructurada como una población esencialmente rural, aislada y muy conservadora, precisaba unos ritmos de transformación y adaptación mucho más lentos en el tiempo de los que se le pretendía imponer desde el Acuerdo de Bonn, esto es, la construcción, sobre todo, de un nuevo Estado democrático lo más semejante posible al modelo occidental. Además, Afganis-

tán llevaba soportando 24 años de guerra civil ininterrumpidos y la guerra aún no había finalizado por completo.

A pesar del mantenimiento del presidente Karzai al frente de la autoridad afgana en Kabul con el apoyo implícito de la Administración estadounidense tras las diversas fases formales de construcción del nuevo Estado, el primero no logró la autoridad suficiente dentro del país. Y no podía ser de otra forma, ya que no se contó con la colaboración de los señores territoriales para las labores de pacificación y de restablecimiento de la paz que la comunidad internacional pretendía llevar a cabo y que, sin embargo, resultaban precisas para combatir a las insurgencias, talibanes o miembros de al-Qaeda que pudiesen subsistir en sus territorios. Así pues, Karzai se convirtió en un señor territorial más de Afganistán al disponer únicamente de autoridad en Kabul, su área de control (Perianes 2015:89).

3. Situación sociopolítica de Afganistán tras la retirada estadounidense en diciembre de 2014

Tras la retirada de la mayor parte de las tropas estadounidenses en diciembre de 2014, año en que la violencia había crecido intensamente en Afganistán (Misión de Asistencia de Naciones Unidas en Afganistán, 2015:1), el resurgimiento militar de los talibanes aprovechando el vacío de poder y la aparición en territorio afgano del autoproclamado Estado Islámico han contribuido a profundizar significativamente la ya inestable e insegura situación en la que se encontraba el país.

Ante este enconamiento de la situación de conflicto afgano, las Fuerzas Nacionales de Seguridad Afganas se enfrentan a deficiencias esenciales que obstaculizaban sus capacidades en materia de seguridad: insuficiente capacidad logística, altas tasas de deserción y elevada corrupción y analfabetismo entre sus filas.

Las elecciones presidenciales de Afganistán celebradas en primera vuelta el 5 de abril de 2014 y en segunda vuelta el 14 de junio del mismo año, con el entonces presidente Karzai inhabilitado para presentarse debido a las limitaciones constitucionales de optar a un tercer mandato presidencial (Berenguer, 2014:2), se subrayaron como uno de los acontecimientos sociopolíticos más relevantes para el país desde el derrocamiento de los talibanes en 2001. La legitimidad política en Afganistán no dependía

únicamente del proceso electoral, sino también del apoyo permanente de buena parte de la estructura social y tribal del país representada a través de las asambleas de los ancianos (Bárcenas, 2014: 125-126) y de la influencia y capacidad de movilizar el apoyo a los candidatos entre las élites locales.

El nuevo presidente surgido de las elecciones celebradas en la primavera de 2014, Ghani Ahmadzai, debía gobernar Afganistán en el marco de dos elementos esenciales para el futuro del país (Corral, 2014: 8):

1. Bajo la plena soberanía nacional. A finales de septiembre de 2014 el Consejero de Seguridad Nacional afgano, Hanif Atmar y, el Embajador de Estados Unidos James Cunnighan firmaron el Acuerdo Bilateral de Seguridad, que permitiría la presencia estadounidense en suelo afgano hasta el final de 2024 y más allá. Estados Unidos continuaría con la capacitación de los 350.000 componentes de las Fuerzas Armadas y de Seguridad Armadas afganas e implementando acciones antiterroristas contra los talibanes (Pérez, 2014:128).

   Mediante el Acuerdo Bilateral de Seguridad, el Gobierno afgano autorizaba la presencia de 9.800 soldados norteamericanos hasta finales de 2015 y la permanencia de la mitad hasta 2017, fecha a partir de la cual podría existir una fuerza residual de mil militares.

   Asimismo, a finales de septiembre de 2014 la OTAN firmaba el Acuerdo de Estatuto de Fuerzas (SOFA), que daba inicio a partir del 1 de enero de 2015 a la nueva misión «*Resolute Support*» con la presencia en Afganistán de unos 3.000 efectivos y la garantía de 4.000 millones de dólares para financiar y equipar a las fuerzas afganas (Pérez, 2014:128). *Resolute Support* no implica combate y se estructura como una misión de asistencia, entrenamiento y asesoramiento a las Fuerzas Armadas afganas (OTAN, 2014).
2. El presidente afgano también debía definir su relación con la insurgencia talibán, cada vez más violenta. Las opciones del nuevo presidente afgano podrían ir encaminadas a pactar una reconciliación con los talibanes que pudiera permitir a éstos reincorporarse y formar parte de las instituciones políticas y sociales mediante sus líderes. De otro

modo, podría luchar contra los talibanes hasta la victoria de una de las partes, opción más compleja debido a que las tropas afganas no presentan las condiciones idóneas de entrenamiento y de recursos para obtener la victoria en un conflicto que las tropas internacionales no habían sido capaces de lograr en 13 años (Corral, 2014: 9). Las fuerzas de seguridad afganas, tanto policías como militares, no se encuentran capacitadas para garantizar óptimamente la seguridad y estabilidad en todo el territorio nacional afgano debido a la amenaza que suscitan los talibanes.

Los últimos persiguen legitimar su papel como actor político y acrecentar su poder, especialmente en los siguientes ámbitos: justicia, asuntos religiosos, asuntos sociales y educación. En esta línea, buscan establecer su estricta y rigurosa concepción del sistema islámico, así como expandir su control territorial en el corto y medio plazo.

Las conversaciones de paz entre talibanes y gobierno afgano

En cuanto a las conversaciones entre el Gobierno afgano y los talibanes, el proceso de paz afgano entró en punto muerto en 2013. En febrero del mismo año, el viaje a Qatar del líder de un partido religioso paquistaní (Jamiat Ulema-e-Islam Fazl (JUI-F)) muy próximo a los talibanes y, especialmente influyente en las áreas pastunes fronterizas con Afganistán, desvelaba la disposición talibán a establecer su representación permanente en Doha. Esta visita para entrevistarse con los líderes del movimiento talibán fue interpretada como una labor de acuerdo con las autoridades paquistaníes para impulsar la vuelta a las negociaciones por parte de los talibanes.

La oficina de la representación permanente de los talibanes en Qatar se abrió en junio de 2013 para ser cerrada al mes siguiente (Vílchez, 2013:28). La utilización de emblemas como la bandera del Emirato Islámico de Afganistán por parte de los talibanes levantaron las protestas del Gobierno de Karzai. Por su parte, la presión estadounidense obligó a las autoridades qataríes a retirar la bandera. El malestar que esto produjo entre los talibanes les llevó a cerrar su oficina en Doha y a paralizar de nuevo las conversaciones.

Según lo que se evidenciaba de las conversaciones llevadas a cabo hasta ese momento, Estados Unidos habría exigido a los talibanes el abandono de la violencia, la persecución de sus objetivos por medios políticos, su reconocimiento de la Constitución afgana y su renuncia a ofrecer apoyo a al-Qaeda. Con ello, la Administración estadounidense de Obama pretendería alcanzar un régimen afgano relativamente estable tras la retirada de las tropas internacionales (Vílchez, 2013:26).

Como se explicará más adelante, tras la crisis de liderazgo surgida en el movimiento talibán tras el anuncio en julio de 2015 de la muerte del Mulá Omar, una vez designado como nuevo líder, el Mulá Mansour proclamó que las conversaciones de paz con el gobierno afgano se suspendían indefinidamente.

Retos sociales que afronta el gobierno afgano

El gobierno del presidente Ghani Ahmadzai afronta diversos retos: a) la altísima corrupción que afecta al país y que le sitúa en las peores posiciones de la escala de naciones más corruptas según Transparencia Internacional (Transparencia Internacional, 2016); b) la pobreza y el elevado desempleo; c) la lucha contra el ascendente cultivo y tráfico de opio y que resulta esencial para la economía de un porcentaje muy significativo de afganos, que dependen de estas plantas y que financia en buena medida las actividades de la insurgencia; d) la escasa capacidad de actuación del Gobierno afgano a nivel local (Laborie, 2013:2); e) la vulneración de los derechos humanos, sobre todo de mujeres, niñas y niños; f) la persistencia de los santuarios de la insurgencia en Pakistán y, g) seguir manteniendo la ayuda internacional que recibe el país para financiar el desarrollo del país y las fuerzas armadas (Corral, 2014: 9).

Esto último será preciso con el objetivo de fondo de la búsqueda de la reconciliación nacional bajo un modelo de país que garantice la gobernanza política junto con la mejora de las condiciones de vida de las mujeres y niñas y que aglutine la diversidad étnica de una sociedad tribal que lleva decenios presenciando las consecuencias de guerras, corrupción estructural, intransigencia religiosa y narcotráfico. Cabría recordar que los pastunes constituyen la etnia más relevante del país suponiendo el 42% de los afganos, seguidos principalmente por los tayikos con un

porcentaje del 27, de los zaharas con el 9 y los turkmenos con el 3% (Ruiz, 2014a: 53).

La estabilidad afgana dependerá también en gran medida de la transición económica que lleve a cabo el país, puesto que no será viable políticamente hasta que cuente con una estabilidad económica razonable (Bárcenas, 2014:126). Según el estudio económico y financiero «Perspectivas de la economía mundial» publicado en abril de 2016 por el Fondo Monetario Internacional (FMI, 2016:24), las perspectivas económicas y financieras para Afganistán han desmejorado considerablemente debido a la agudización de los conflictos y los riesgos a la seguridad.

Afganistán es un país pobre y cuenta con uno de los Índices de Desarrollo Humano más bajos del planeta (*United Nations Development Programme*, 2016). Su gobierno depende en gran medida de las donaciones extranjeras y, la retirada completa de las tropas (y otro tipo de personal como funcionarios, empresarios o cooperantes) occidentales se significaría como un hecho económicamente adverso para Afganistán debido, además de a su elevado nivel de demanda y consumo de bienes y servicios, a la disminución de ayuda internacional directa que conllevaría, ya que los donantes no contarían con las suficientes garantías de gestión y control de las ayudas que realiza la comunidad internacional.

El agravamiento de los niveles de violencia en el país tras el enconamiento de la insurgencia talibán durante el año 2015 ha producido un significativo incremento del número de afganos desplazados o que se ven en la necesidad de solicitar asilo y refugio en otros países.

La Oficina de Coordinación de Asuntos Humanitarios estima que durante el año 2016, se contabilizaría un millón de afganos entre los desplazados internos y los que saliesen de sus fronteras, incluyendo a los retornados de Irán y Pakistán, en busca de una vida mejor (United Nations Office for the Coordination of Humanitarian Affairs, 2016:3).

Además, la vulnerabilidad de la población afgana que se ve obligada a abandonar sus hogares por motivos de seguridad se veía agravada por la inminente llegada del invierno (Organización Internacional para las Migraciones, 2016).

El resurgimiento del poder talibán

El auge del avance talibán en Afganistán se basa fundamentalmente en el vacío de poder generado tras la retirada de las tropas occidentales a finales de 2014, la incapacidad del gobierno afgano para afrontar satisfactoriamente los riesgos y amenazas que encara el país, la escasa capacitación de las fuerzas de seguridad afganas y, especialmente, la voluntad del movimiento talibán de demostrar que aún conserva poder tras la muerte del Mulá Omar (Ariza, 2016: 3).

Tras el anuncio en julio de 2015 del fallecimiento del anterior, las opciones de entablar negociaciones de paz entre los talibanes y gobierno afgano se desvanecieron por completo. A pesar de sus avances militares, la publicación de que la muerte del Mulá Omar había tenido lugar dos años antes derivó en una profunda desunión entre los talibanes y una seria crisis de liderazgo. Los procesos de elección del nuevo líder de la organización han producido tensiones entre sus diversas facciones. En este sentido, el nombramiento del Mulá Akhtar Mohammad Mansour como nuevo líder de los talibanes fue muy cuestionado y, al tiempo, la facción disidente del grupo, autodenominada como «el Alto Consejo del Emirato Islámico de Afganistán», proclamó el liderazgo del Mulá Mohammad Rasool (Laborie, 2016:5).

A la par, mientras otros comandantes talibanes optaban por la neutralidad, Ayman al-Zawahiri (líder de al-Qaeda) apoyaba públicamente a Mansour solicitando a sus contrarios su reconocimiento como nuevo líder de la organización. Combatientes talibanes simpatizantes del conocido como Estado Islámico (y, por tanto, opuestos a al-Qaeda), se alineaban con Rasool (Laborie, 2016:6).

Esta pugna por el liderazgo talibán constituye un hecho novedoso entre sus miembros, puesto que ésta ha sido la primera vez que la rivalidad entre sus notables ha derivado en una lucha abierta por el poder.

Tras su designación como líder del movimiento talibán, el Mulá Mansour anunció que las conversaciones de paz con el gobierno afgano se suspendían indefinidamente (Ariza, 2016:4).

La toma por sorpresa por parte de los talibán de la ciudad de Kunduz (al norte del país y con una población aproximada de 270.000 habitantes), en septiembre de 2015 se constituyó como uno de los hitos más destacados de las conquistas territoriales que

han llevado a cabo los insurgentes desde el fin de la ISAF (Laborie, 2016:4).

Tres meses más tarde y, confirmando el deterioro de la seguridad que viene sufriendo Afganistán con los ataques puntuales de alto valor a instalaciones gubernamentales e internacionales implementados por los talibanes, se produjo el ataque al complejo de la Embajada española en Kabul el 11 de diciembre de 2015, en el que fallecieron dos policías nacionales españoles (Laborie, 2016:5).

Operación Omari

Los militantes talibanes están expandiendo con éxito su control territorial sobre varias regiones del país tras la implementación durante este verano de 2016 de su ofensiva militar, conocida como Operación Omari (Forrest, 2016).

Frente al envite talibán, la contraofensiva de las fuerzas armadas y de seguridad nacional afganas, denominada Operación Shafaq, repelió varias operaciones talibanes, como la que pretendían desarrollar para aislar la capital de la provincia de Helmand.

Sin embargo, las fuerzas armadas y de seguridad nacional afganas aún no se encuentran suficientemente preparadas y con los recursos necesarios para implementar operaciones en más de una región simultáneamente, a pesar de la asistencia que reciben por parte de la OTAN y Estados Unidos.

Las ofensivas talibanes continúan limitando al gobierno sus opciones de control del terreno, expandiendo de esta manera su presencia en áreas remotas sin control gubernamental en las que las redes extremistas como el conocido como Estado Islámico y al-Qaeda pueden reorganizarse, degradando al tiempo la ya de por si baja moral que presentan las fuerzas armadas y de seguridad afganas. De seguir la situación así, las organizaciones extremistas podrían reconstituir sus santuarios en espacios fuera de control del gobierno afgano (Forrest, 2016).

La Operación Shafaq no fue diseñada para llevar a cabo operaciones en más de una región al mismo tiempo y los militantes talibanes están explotando esa vulnerabilidad con el objetivo de debilitar a la primera y para mejorar sus condiciones mientras preparan acciones que les otorguen más control territorial.

El desarrollo de la ofensiva militar de los talibanes está obligando a las fuerzas armadas y de seguridad afganas a desplegar y

redistribuir con frecuencia sus limitados recursos, reduciendo así la capacidad del gobierno afgano de llegar a áreas remotas que puedan ser utilizadas por las redes extremistas para reconstituirse.

El profundo debilitamiento que están produciendo los militantes talibanes a las fuerzas armadas y de seguridad afganas podría ser capitalizado por los grupos extremistas para ejercer la violencia y crear sus santuarios al este del país. Por ejemplo, los combatientes del denominado Estado Islámico están usando sus santuarios en la provincia de Nangarhar para realizar ataques de gran calado en Kabul. Por su parte, la red Haqqani está ejecutando su propia ofensiva en su histórico feudo de Loya Patkia (Forrest, 2016).

En definitiva, la ofensiva de verano de 2016 implementada por el movimiento talibán está debilitando significativamente la capacidad de las fuerzas armadas y de seguridad afganas de securizar el país, mientras que el gobierno afgano encara una profunda crisis política y presenta las condiciones idóneas para sufrir un colapso inminentemente (Forrest, 2016).

El gobierno afgano de unidad nacional enfrenta múltiples crisis debido a su incapacidad para cumplir con los requerimientos del Acuerdo de reparto de poderes de 2014. En este sentido, resulta muy elevada la probabilidad de que el gobierno Ghani-Abdullah no pueda cumplir con el plazo límite fijado con fecha de septiembre de 2016 para abordar la creación constitucional de la *Loya Jirga*[1], tal como se estipulaba en el Acuerdo de 2014 o, por otra parte, promulgar reformas electorales antes de las elecciones previstas para octubre de 2016.

El incumplimiento de los referidos plazos por parte del gobierno de unidad nacional derivará previsiblemente en un grave enfrentamiento político de los partidos de la oposición contra el gobierno afgano, que podría concluir con el colapso del anterior.

1. Gran Asamblea en la que grupos étnicos, dirigentes tribales o regionales, figuras políticas, militares y religiosas, funcionarios del gobierno, etc. se reúnen para tomar decisiones sobre muchos tipos de asuntos, como los referidos a la política nacional, política exterior, declaraciones de guerra, consideraciones de nuevos proyectos, etc. Éstas se adoptan por consenso.

Presencia del autoproclamado Estado Islámico en Afganistán

Otro de los riesgos que amenaza la estabilidad afgana es la presencia en el país del autodenominado Estado Islámico. La rama asiática del anterior, «*Wilayat Khorasan*» (la provincia del Jorasán) se ha ido estableciendo progresivamente en el país desde la autoproclamación del Califato en territorio sirio e iraquí por parte del líder de la referida organización yihadista (Abu Bakr al Baghdadi). El conocido como Estado Islámico domina algunos distritos de Kunduz, Helmand, Faryab y otras provincias junto a la provincia pakistaní (Laborie, 2016:5).

La pugna por el control del territorio afgano está produciendo hostilidades entre los partidarios de los talibanes y los del autoproclamado Estado Islámico. No obstante, tras la fundación del anterior, éste auguraba recibir un mayor apoyo de las poblaciones pastunes asentadas a ambos lados de la frontera afgano-pakistaní, en especial tras la designación de Hafiz Khan como líder de «*Wilayat Khorasan*» en enero de 2015.

Buena parte de los líderes pastunes ofrecieron su apoyo a los talibanes y, la lucha por el poder territorial entre los anteriores y los milicianos del conocido como Estado Islámico se está incrementado en los últimos meses (Laborie, 2016:7). A este respecto, las divisiones internas presentes dentro del movimiento talibán podrían favorecer la extensión del autodenominado Estado Islámico en territorio afgano.

En esta línea, la pugna por el poder que mantienen en la actualidad al-Qaeda central y sus franquicias con el autodenominado Estado Islámico por la dirección del movimiento global de la yihad se plantea hasta el momento como un interrogante. El incremento de la hostilidad entre las dos organizaciones yihadistas podría derivar en un agravamiento de la inestabilidad en Afganistán con posibles repercusiones para la seguridad del país (Martín, 2016: 6-8).

La cuestión sin resolver que plantea la rivalidad entre al-Qaeda y el autoproclamado Estado Islámico ocupará parte de los retos que enfrentará la comunidad internacional en términos securitarios en el medio y largo plazo.

Los Haqqani

La red Haqqani, fundada por Jalaluddin Haqqani, un antiguo jefe guerrillero que ganó influencia en la lucha contra la presen-

cia soviética en Afganistán, se configura como otro de los actores armados no estatales que más han influido en los sucesivos conflictos que vienen asolando Afganistán desde 1970 (De la Corte y Hristova, 2016:1).

De ideología deobandi, los Haqqani se convirtieron desde los inicios de la guerra declarada por la Administración Bush a Afganistán (en octubre de 2001) en una de las principales facciones insurgentes en la lucha contra la presencia de tropas occidentales en el país y el nuevo gobierno (De la Corte y Hristova, 2016:4).

Mediante el ejercicio de la violencia y vinculada a los talibán, al-Qaeda y otros grupos extremistas y del crimen organizado, la red Haqqani ha venido persiguiendo: la expulsión del territorio afgano de las tropas de la coalición internacional; dificultar la gobernabilidad del país procurando la perpetuación de la inestabilidad e inseguridad extremas; ganar poder entre las fuerzas de oposición al nuevo gobierno afgano surgido tras la declaración de la guerra al país en 2001 y, dotar del mayor nivel de autonomía posible a la región de Loya-Patkia (su área de mayor influencia, situada en el sudeste de Afganistán) (De la Corte y Hristova, 2016:5).

La pérdida en combate de varios de los miembros más influyentes de la red junto a los ataques de drones estadounidenses han debilitado al grupo y, por tanto, la influencia de los Haqqani parece haberse disminuido en sus tradicionales feudos de poder (Patkia, Paktika y Khost) (De la Corte y Hristova, 2016:6). Sin embargo, tras la crisis abierta en el seno de la dirección talibán tras darse a conocer la muerte del Mulá Omar en julio de 2015 y analizada anteriormente, los Haqqani se integraron en la estructura talibán liderada por el Mulá Mansour (De la Corte y Hristova, 2016:16).

Al-Qaeda central

En cuanto a al-Qaeda, conserva una influencia secundaria en Afganistán a pesar de contar con campos de entrenamiento activos en el país. La hostilidad que mantiene con el autoproclamado Estado Islámico por el liderazgo global de la yihad y su distanciamiento con los talibanes le han marginado en la lucha por el poder afgano (Ariza, 2016:6).

Incremento de la violencia

El *Global Terrorism Index 2015. Measuring the impact of terrorism* (*Institute for Economics and Peace*, 2016: 11-12) sitúa a Afganistán como el segundo país del mundo que más violencia terrorista ha sufrido durante el año pasado con 1.591 incidentes, 4.505 víctimas mortales y 4.699 heridos, sólo por detrás de Irak. Los resultados del estudio demostraron que el terrorismo continuó su tendencia al alza en 2015 y que cinco países concentraron el 78% de las víctimas mortales: Iraq, Nigeria, Afganistán, Pakistán y Siria.

El número de ataques terroristas ha venido así creciendo durante los últimos años significativamente en Afganistán: en 2014 se produjeron un 38% más de atentados y un 45% más de fallecidos que en 2013.

Los talibanes se configuran como los responsables de la mayor parte de incidentes terroristas y víctimas mortales producidos en Afganistán, distinguiéndose como uno de los grupos terroristas más mortíferos del mundo. En este sentido, el movimiento talibán ejecutó el 75% de los ataques terroristas con sus correspondientes víctimas en 2012, 2013 y 2014 (*Institute for Economics and Peace*, 2016: 23).

La Misión de Asistencia de Naciones Unidas en Afganistán (UNAMA) documentó 1.601 víctimas mortales y 3.565 heridos en los incidentes terroristas implementados en el país durante el primer semestre de 2016 (UNAMA; 2016: 11).

El impacto negativo del conflicto afgano en mujeres y niñas continúa siendo además muy elevado puesto que siguen sufriendo restricciones en el acceso a la educación, a la salud, a la libertad de movimientos, la vulneración de sus derechos humanos y castigos de justicia paralela denominados como «crímenes morales» (UNAMA; 2016: 11).

Afganistán en la Cumbre de Varsovia de la OTAN

Los jefes de Estado y Gobierno de las naciones que contribuyeron a la misión *Resolute Support* en Afganistán reconocieron en la Cumbre de Varsovia celebrada por la OTAN el 8 y 9 de julio de 2016 que, a pesar de los avances producidos en el país, éste aún enfrenta profundos riesgos y amenazas vinculados a asuntos como la corrupción, el narcotráfico, el desempleo, la inseguridad o la falta de oportunidades.

En consecuencia, en el marco de la Cumbre de Varsovia, las autoridades concernidas acordaron la necesidad de seguir apoyando a Afganistán en materia de asistencia securitaria y financiera (NATO, 2016:2-3), confirmando el compromiso que mantienen los aliados y socios de la OTAN con el país tras la extensión de la misión *Resolute Support* más allá de 2016.

Entre los acuerdos adoptados de cara al objetivo de la estabilización afgana, se anunciaron contribuciones financieras para el período 2018-2020 para asuntos relacionados con el sostenimiento y capacitación de las fuerzas armadas y de seguridad afganas, el reforzamiento de la asociación política y de cooperación práctica a largo plazo entre la OTAN y Afganistán y el mantenimiento estadounidense de 8.400 efectivos, cifra notablemente superior a los 5.500 previstos en un inicio (Moliner, 2016:14).

Conclusiones

Afganistán centra en la actualidad una de las principales preocupaciones en materia de seguridad de la comunidad internacional debido a las graves implicaciones globales que derivan de la situación de conflicto que vive el país.

El gobierno afgano enfrenta uno de los peores recrudecimientos de la violencia de los últimos años en un momento muy delicado de inestabilidad política e institucional. La falta de unidad política y nacional perjudica en gran medida las opciones de lograr una vía de solución a factores como el debilitamiento de las fuerzas militares afganas, la lucha contra la elevadísima corrupción, los altos niveles de pobreza y desempleo, la vulneración de los derechos humanos, la inseguridad humana, el aprovechamiento por parte del movimiento talibán del vacío de poder surgido tras la retirada en diciembre de 2014 de las tropas estadounidenses, el paulatino debilitamiento gubernamental por falta de apoyos y recursos o, la aparición en la escena afgana del autodenominado Estado Islámico con el riesgo que plantea su presencia en el país, conectada más con su campaña de expansión internacional que con su capacidad real de implementar acciones militares al estilo de las que ha venido realizando en Siria e Irak.

La retirada de Afganistán de las tropas internacionales en diciembre de 2014 produjo un vacío de poder rápidamente aprovechado por los talibanes para expandir sus áreas de control e influencia por el país y volver a los mayores niveles de violencia

sufridos por el país. La decisión de retirar tropas de Afganistán en un momento en que el país no se encontraba estabilizado ni política, económica e institucionalmente viable se está manifestando como un grave error estratégico de cara a la estabilización de un Estado sumido en décadas de guerra y violencia.

Afganistán sigue precisando ayuda y cooperación internacional para afrontar los retos que encaran su seguridad y estabilidad. Además, Afganistán es un país pobre y la retirada completa de las tropas y civiles occidentales se significaría como un hecho económicamente adverso debido al elevado nivel de demanda y consumo de bienes y servicios de los anteriores y a la disminución de ayuda directa que conllevaría, puesto que los donantes no contarían con las suficientes garantías de gestión y control de las ayudas que ofrece la comunidad internacional.

Por otra parte, la extensión del autoproclamado Estado Islámico en territorio afgano, podría facilitar su resiliencia en el momento de declive que vive en territorio sirio e iraquí, susceptible de incrementar sus capacidades en la pugna que mantiene con al-Qaeda por el liderazgo de la yihad global.

Bibliografía

Ariza Cerezo, Cristina (2016), «Claves del resurgimiento talibán en Afganistán», Documento de Opinión 36/2016, Instituto Español de Estudios Estratégicos, http://www.ieee.es/publicaciones-new/documentos-de-opinion/2016/DIEEEO36-2016.html, Consultado el 04/09/2016.

Bárcenas Medina, Luis Andrés (2014), «El Afganistán que deja Karzai», Política Exterior, marzo/abril, 158.

Berenguer Hernández, Francisco José (2014), «Las elecciones en Afganistán I», Documento Informativo 8/2014, Instituto Español de Estudios Estratégicos, http://www.ieee.es/Galerias/fichero/docs_informativos/2014/DIEEEI08-2014_EleccionesAfganistan_FJBH.pdf. Consultado el 11/09/2016.

Corral Hernández, David (2014), «Elecciones en Afganistán, un paso determinante», Documento de Opinión 28/2014, Instituto Español de Estudios Estratégicos, http://www.ieee.es/Galerias/fichero/docs_opinion/2014/DIEEEO28-2014_EleccionesAfganistan_DavidCorral.pdf. Consultado el 20/09/2016.

De la Corte, Luis. ; Hristova, Hristina. (2016), «La red Haqqani y la evolución del yihadismo local y transnacional en la región Af-Pak», Documento de Investigación 07/2016. Instituto Español de Estudios Estratégicos, Región MENA y Asia Central hasta la región autónoma UIGUR china de Sinkiang, http://www.ieee.es/Galerias/fichero/docs_investig/2016/DIEEEINV07-2016_Red_HAQQANI_AF-PAK_DelaCorte-Hristova.pdf.

FMI (2016), «Perspectivas de la economía mundial», abril 2016, https://www.imf.org/external/spanish/pubs/ft/weo/2016/01/pdf/texts.pdf Consultado el 05/09/2016.

Forrest, Caitlin (2016), «Afghanistan partial threat assesment: August 28, 2016», Institute for the study of war, http://post.understandingwar.org/backgrounder/afghanistan-partial-threat-assessment-august-28-2016, Consultado el 05/09/2016.

Institute for Economics and Peace (2016), «Global Terrorism Index. Measuring the impact of terrorism», http://www.visionofhumanity.org/sites/default/files/2015%20Global%20Terrorism%20Index%20Report_1.pdf Consultado el 05/09/2016.

Laborie Iglesias, Mario (2013), «Informe sobre el progreso hacia la seguridad y la estabilidad en Afganistán (julio 2013)», Documento de Análisis 46/2013, Instituto Español de Estudios Estratégicos, http://www.ieee.es/Galerias/fichero/docs_analisis/2013/DIEEEA46-2013_InformeAfganistanJulio2013_MLI.pdf. Consultado el 10/09/2016.

Laborie Iglesias, Mario (2016), «Un año después de la ISAF», Documento de Opinión 07/2016, Instituto Español de Estudios Estratégicos, http://www.ieee.es/publicaciones-new/documentos-de-opinion/2016/DIEEEO07-2016.html, Consultado el 05/09/2016.

NATO (2016), «Warsaw Summit Declaration on Afghanistan», Issued on 9 July 2016 by the Heads of State and Government of Afghanistan and Allies and their Resolute Support Operational Partners, http://www.nato.int/cps/en/natohq/official_texts_133171.htm. Consultado el 08/08/2016.

Martín Serrano, Lucas (2016), «DAESH vs. al-Qaeda. La lucha por la supremacía a las puertas de Europa», Documento de Opinión 70/2016, Instituto Español de Estudios Estratégicos, http://www.ieee.es/Galerias/fichero/docs_opinion/2016/DIEEEO70-2016_Daesh-AlQaeda_LuchaSupremacia_L.MartinSerrano.pdf, Consultado el 28/08/2016.

Misión de Asistencia de Naciones Unidas en Afganistán (2015), «Informe Anual 2014. Protección de civiles en conflictos armados. Afganistán», http://www.ieee.es/Galerias/fichero/Varios/NNUU/UNAMA_AnnualReport_Afghanistan_2014.pdf Consultado el 10/09/2016.

Moliner González, Juan (2016), «La Cumbre de la OTAN en Varsovia», Documento de Opinión 79bis/2016. Instituto Español de Estudios Estratégicos, http://www.ieee.es/publicaciones-new/documentos-de-opinion/2016/DIEEEO79bis-2016.html, Consultado el 10/08/2016.

Organización Internacional para las Migraciones (2016), «La OIM advierte sobre posible crisis humanitaria: miles de afganos repatriados desde Pakistán», publicado el 09/09/2016, https://www.iom.int/es/news/la-oim-advierte-sobre-posible-crisis-humanitaria-miles-de-afganos-repatriados-desde-pakistan Consultado el 15/09/2016.

OTAN (2014), «*NATO-led Resolute Support Mission in Afghanistan*», http://www.nato.int/cps/en/natohq/topics_113694.htm. Consultado el 10/09/2016.

Pérez Moreno, Alberto (2014), «¿Una nueva etapa en Afganistán?», Revista del Ejército. Ministerio de Defensa, noviembre, 883.

Perianes Bermúdez, Ana Belén, Tesis doctoral «La política exterior de las Administraciones de George W. Bush (2001-2008): Consecuencias para la seguridad internacional». Instituto Universitario General Gutiérrez Mellado. Madrid. 2015. https://www.educacion.gob.es/teseo/mostrarSeleccion.do

Ruiz, Rosa (2014a), «Afganistán, el difícil vuelo del ave Fénix», *Revista Española de Defensa*, junio, 307.

Segura i Mas, Antoni (2004), *Señores y vasallos del siglo XXI*, Madrid, Alianza.

Setas Vílchez, Carlos (2013), «Las relaciones entre Afganistán y Paquistán y las negociaciones de paz con los talibanes afganos», Revista el Instituto Español de Estudios Estratégicos, http://www.ieee.es/Galerias/fichero/Revista_Digital/RevistaIEEE_Num_2_Espanol-Ingles.pdf. Consultado el 10/09/2016.

Transparencia Internacional (2016), «Índice de percepción de la corrupción 2015 de Transparencia Internacional», http://transparencia.org.es/wp-content/uploads/2016/01/tabla_sintetica_ipc-2015.pdf Consultado el 10/09/2016.

UNAMA (2016), «*Afghanistan midyear report 2016. Protection of civilians in armed conflicts*», https://unama.unmissions.org/sites/default/files/protection_of_civilians_in_armed_conflict_midyear_report_2016_final.pdf Consultado el 03/09/2016.

United Nations Development Programme (2016), «*Human Development Report 2015: Work for Human Development*», http://hdr.undp.org/en/countries/profiles/AFG Consultado el 03/09/2016.

United Nations Office for the Coordination of Humanitarian Affairs (2016), «Afghanistan flash appeal. One million people on the move. Covering Sep-Dec 2016», Publicado el 25/09/2016, https://docs.unocha.org/sites/dms/Afghanistan/afg_2016_flash_appeal.pdf Consultado el 28/09/2016.

Vega Fernández, Enrique (2011), «Los errores estratégicos de la primera guerra al terrorismo en Afganistán», Instituto Universitario General Gutiérrez Mellado (ed.), en *La seguridad y la defensa en el actual marco socio-económico: nuevas estrategias frente a nuevas amenazas*. Madrid.

CAMBIOS EN LA SOCIEDAD EUROPEA COMO CONSECUENCIA DE LA CRISIS DE LOS REFUGIADOS. ¿AMENAZA CULTURAL, AMENAZA TERRORISTA O POLÍTICA OPORTUNISTA?

José Antonio Cantón Restoy
Ministerio de Defensa

Resumen

A la actual crisis económica y financiera europea se le añaden el azote de la alarma social del terrorismo islamista y un aumento de refugiados sin precedentes en los últimos meses, haciendo que los valores de tolerancia, justicia y equidad de la sociedad del viejo continente se vean aún más desgastados. El presente trabajo tiene como objeto y desde un enfoque socio-cultural aportar distintos argumentos donde se explican que ni el éxodo masivo de exiliados son una amenaza cultural, ni son una inseguridad para Europa, quien pese a la brecha producida en la arena política del eje este-oeste, se sigue manteniendo como una y múltiple.

Palabras claves

Sociedad, integración cultural, seguridad, refugiados.

1. Introducción

En los últimos meses estamos asistiendo en Europa a una de las crisis más importantes de migración humana desde el fin de la Segunda Guerra Mundial. El número de desplazados y migrantes ha aumentado considerablemente de la Ribera Sur del Mediterráneo, Próximo Oriente y Oriente Medio hacia la Ribera Norte del Mediterráneo por motivos de conflictos bélicos y de los cambios acontecidos desde 2011.

Los desplazamientos humanos, cobran hoy día una especial relevancia, pues de los 7 mil millones de habitantes del planeta; 1,5 mil millones viven en Estados en conflicto o en situación de fragilidad, y esta cifra va en aumento[1].

1. Ver: *http://www.ilo.org/global/topics/labour-migration/policy-areas/crisis/lang--es/index.htm.*

Éste 'fenómeno' es una función de naturaleza social y como tal la sociedad europea puede cambiar el sentimiento de solidaridad, pues pese a que se comparte cierta uniformidad intelectual y moral, se ha desarrollado un sistema de normas y una distribución de roles más elaborados, es decir, se ha entrado en acción positiva en virtud de la solidaridad de apoyo y ayuda a los migrantes, pero por otro lado, el choque de intereses nuestro-vuestro es una de las causas que más polémica causa y puede originar una actitud negativa.

Pero, ¿por qué la crisis de los refugiados está suponiendo una relativa situación de colapso para alguno de los países de la UE? ¿qué debe hacer Europa? Este fenómeno presenta una serie de características; la de ser inesperado y por ello coarta la capacidad de reacción, es imprevisible, pues pasa de un escenario externo a otro interno, luego lógicamente es de relevancia para los objetivos públicos de la institución, tienen un origen ajeno a la comunicación y normalmente la información que tenemos al respecto es incompleta.

La UE tiene una serie de obligaciones para con las personas que acceden a ella solicitando protección por las circunstancias de guerra y violaciones flagrantes de los derechos humanos que se viven en sus países de origen. Ante esta situación los ciudadanos se preguntan ¿Cuáles son las obligaciones de los Estados europeos?

2. Texto de la comunicación

2.1. *Origen de la crisis. ¿Refugiados o migrantes?*

Centrándonos en la zona de estudio, los acontecimientos desencadenados en Siria, Yemen y otros países, así como las tragedias acaecidas sucesivamente, en particular en los mares Mediterráneo y de Andamán, evidencian la necesidad imperiosa de que se conceda atención con carácter urgente a las necesidades humanitarias, sociales y económicas de los migrantes y los refugiados.

Concretamente el 85% de las llegadas provienen de países de origen como Siria, Afganistán, Irak y Somalia de las cuales el 30% son mujeres y niños[2]. La Convención de Ginebra de 1951 sobre el Estatuto de los Refugiados acuerda que un refugiado es una

2. Ver: *http://www.acnur.org/t3/recursos/estadisticas/*.

persona que «debido a fundados temores de ser perseguida por motivos de raza, religión, nacionalidad, pertenencia a un determinado grupo social u opiniones políticas, se encuentre fuera del país de su nacionalidad y no pueda o, a causa de dichos temores, no quiera acogerse a la protección de su país; o que careciendo de nacionalidad y hallándose, a consecuencia de tales acontecimientos fuera del país donde antes tuviera su residencia habitual, no pueda o, a causa de dichos temores no quiera regresar a él».

Un refugiado tiene derecho de asilo en condiciones de seguridad. Sin embargo, la protección internacional incluye algo más que la propia seguridad física. Los refugiados deberían recibir al menos la ayuda básica y los mismos derechos que cualquier otro extranjero que sea residente legal. Así, los refugiados tienen derechos civiles básicos, incluyendo la libertad de pensamiento, de movimiento, y el derecho al respeto como persona. De igual forma, los derechos económicos y sociales se aplican a los refugiados al igual que a otros individuos: derecho a asistencia médica, derecho a trabajar para los adultos, y derecho a la escolarización para los niños[3].

Pero, ¿cómo se puede distinguir entre un refugiado y un migrante económico?; normalmente un migrante abandona su país voluntariamente en busca de una vida mejor. Para un refugiado, las condiciones económicas del país de asilo son menos importantes que su seguridad. En la práctica, la distinción puede ser en ocasiones, difícil de establecer, pero es fundamental saber que el migrante disfruta de la protección del gobierno de su país y el refugiado no.

Los atentados del 11s pusieron de manifiesto los sesgos que una acción terrorista podía ejercer sobre la conciencia social y su trato hacia los refugiados. Por eso son muchas las voces que dicen el riesgo que puede suponer la infiltración de terroristas en estas riadas humanas y el problema se agrava aún más cuando esta visión es proyectada por autoridades, de uno u otro nivel, que tienen la capacidad de iniciar políticas sin un objetivo claro o de aportar argumentos de dudosa validez a los sectores más reaccionarios.

Los diferentes estratos y grupos sociales que componen la sociedad responden de manera muy diferente ante este tipo de

3. Ver: *http://www.acnur.org/t3/a-quien-ayuda/refugiados/quien-es-un-refugiado/*.

acontecimientos negativos[4]. En particular, las distintas ideologías políticas determinarán la forma en que esa nueva información es procesada y evaluada. En definitiva, variables como la fortaleza previa que cada persona mantenga sobre sus creencias, la naturaleza, la magnitud y contexto de la noticia o la dimensión que adquiera su difusión por parte de los medios, determinarán el posible cambio o no de la opinión pública social. La información que recibe un estrato de la sociedad puede ir en contra de su opinión o actitud inicial generando un estado de ambivalencia[5].

2.2. *Normativa vigente. ¿Se está aplicando adecuadamente?*

Se oyen en las noticias términos poco conocidos para la mayoría como país de origen

Seguro', en el que la UE presume que no hay causas que den lugar a la necesidad de huída y consiguiente protección internacional y 'tercer país seguro' o país distinto del de legítima huida por el que el solicitante ha transitado antes de acceder a la UE sin pedir protección internacional habiendo podido hacerlo.

Por las noticias también nos enteramos de que algunos Estados miembro de la UE 'sellan sus fronteras' y nos surge la duda de si será éste un comportamiento trasgresor de las obligaciones jurídicas a las que los Estados están comprometidos en materia de Derechos Humanos y Derecho de los Refugiados.

Los medios de comunicación nos proporcionan información actualizada pero incompleta o al menos, dan por sabidos términos y obligaciones jurídicas que la mayoría no conoce bien[6]. No son pocas las tertulias en las que se oye preguntar a quiénes hay que proteger, qué derechos tienen, si estamos obligados a acogerles, de los Pactos Internacionales (PIDCP, PIDESC y sus respectivos proto-

4. Cohen, Jessica, «Efectos sociales del terrorismo. Crisis de refugiados y argumentaciones erróneas», *IEEE*. Documento de Opinión núm. 112 (2015), págs. 6-7.

5. Caro Jiménez, Mari Carmen, et al. «Las emociones y la resistencia al cambio de actitudes». *Revista Española de Investigación de Marketing ESIC* núm. 18, (2014), págs. 19-21.

6. La brújula. David del Cura. *ONDA CERO,* «¿Conseguirá Europa una solución para la crisis de los refugiados?», (2016). Ver: *http://www.ondacero.es/programas/la-brujula/audios-podcast/tertulia/la-tertulia-conseguira-europa-una-solucion-para-la-crisis-de-los-refugiados_2016031756eb33126584a847c6eaab8c.html.*

colos adicionales), en el ámbito europeo pueden citarse determinadas disposiciones del Convenio Europeo para la protección de los Derechos Humanos y de las Libertades Fundamentales (CEDH), cuyas obligaciones han sido cuidadosamente explicitadas por la jurisprudencia del Tribunal Europeo de Estrasburgo (TEDH)[7].

Sin olvidar por supuesto el Tratado de la Unión Europea, Tratado de Funcionamiento de la Unión Europea[8] y la Carta de Derechos Fundamentales de la UE (CDFUE)[9]. Podemos añadir además toda la normativa derivada de directivas, reglamentos y decisiones sobre el Sistema Europeo Común de Asilo (SECA).

Y por último en el marco específico nacional español tenemos la Ley 12/2009 de 30 de octubre, reguladora del derecho de asilo y de la protección subsidiaria, en la cual en su artículo 38, «Solicitudes de protección internacional en Embajadas y Consulados», nos dice en su segundo párrafo que «El Reglamento de desarrollo de esta Ley determinará expresamente las condiciones de acceso a las Embajadas y Consulados de los solicitantes, así como el procedimiento para evaluar las necesidades de traslado a España de los mismos»[10]. Después de casi siete años de vigencia de ésta Ley, no se ha aprobado el reglamento de desarrollo por lo que la disposición sobre solicitudes de protección presentadas en Embajadas no es clara. Por ejemplo, la solicitud de asilo en una Embajada extranjera difícilmente puede realizarse en el propio país de persecución pues dicho país no suele admitir que le sean imputables violaciones graves de los derechos humanos e impediría la salida del solicitante, además de poder represaliar al Estado Embajada. Por eso, en general, esta práctica se realiza en países intermedios de tránsito[11].

7. Ver: http://www.echr.coe.int/Pages/home.aspx?p=basictexts&c=-fra#n1359128122487_pointer.

8. Europa, Tratado de Funcionamiento de la Unión Europea, Diario Oficial de la Unión Europea, 30 de marzo de 2010, [Cap. 3, Art.214.1], pág. 143.

9. Europa, Carta de los Derechos Fundamentales de la Unión Europea, *Diario Oficial de la Unión Europea*, 30 de marzo de 2010, págs. 389-403.

10. España, Ley 12/2009, de 30 de octubre, «reguladora del derecho de asilo y de la protección subsidiaria», *Boletín Oficial del Estado*, 31 de octubre de 2009, núm. 263, págs. 90860-90884.

11. Tubella, Patricia, et al. «Reino Unido amenaza con detener a Assange en la embajada de Ecuador», *El País, Internacional*, (2012). Ver: *http://internacional.elpais.com/internacional/2012/08/15/actualidad/1345051978_623282.html.*

Lo que sí está claro es que los Estados que forman parte de la Convención de Ginebra no pueden devolver a la persona al país de persecución o riesgo para su vida e integridad, ni a otro país inseguro, ni tampoco excluirles de la protección que les otorga a la citada Convención, es por lo que las reglas de la UE prevén y autorizan la expedición de visados especiales para aquellos que necesiten protección humanitaria. Sin embargo, no parece que los Estados hagan mucho uso de esta posibilidad, lo que redunda en los viajes peligrosos y las pérdidas de vidas humanas; además hay quien entiende que el Código de Fronteras de Schengen[12] impide la entrada irregular de los solicitantes y con ello su protección y eso no es así como a continuación vamos a ver.

2.3. *Acuerdo Schengen*

Las encuestas muestran que Schengen y el euro son los dos elementos que la población europea considera los activos más valiosos producidos por la UE, los que despiertan más adhesión al proyecto comunitario[13(13)]. Cecilia Malmström, Comisaria de Interior de la Comisión Europea, afirmó en un comunicado de prensa que las cifras del informe y el resultado de la encuesta de opinión apoyan la opinión de la Comisión de que la Unión Europea necesita una política de migración sólida y coherente, que responda tanto a corto como a largo plazo a las necesidades. Precisamos una gestión eficaz de nuestras fronteras exteriores, con el fin de garantizar la libre circulación dentro de la UE, de aportar una auténtica protección a quienes la necesiten y, al mismo tiempo, de brindar canales para la migración legal y la movilidad. Pero Schengen está en peligro, en grave peligro de desaparición en lo que respecta a las fronteras terrestres. Los líderes europeos como Juncker, Hollande y Merkel no cesan de repetir que la desaparición de Schengen es una amenaza al mercado común y por lo tanto al euro.

12. *http://www.interior.gob.es/web/servicios-al-ciudadano/extranjeria/acuerdo-de-schengen.*

13. Europa, Comisión Europea, «un nuevo informe y una nueva encuesta ofrecen una imagen más precisa sobre el estado de la migración, el asilo y la libre circulación en la UE», *Comunicado de prensa*, Bruselas (2012), Ver: *http://europa.eu/rapid/press-release_IP-12-552_es.htm.*

Lo que sí es cierto, es que el cierre de fronteras se ha extendido y ha provocado un efecto dominó. El resultado del número de migrantes y refugiados que están llegando, ha hecho que hasta Suecia, se haya visto superada y cierre su frontera con Dinamarca, la cual ha cerrado la suya con Alemania y ésta a su vez está controlando los accesos por su frontera con Austria, ésta hace lo mismo respecto a Eslovenia, y a Francia, a raíz del estado de emergencia decretado tras el atentado de noviembre de 2015, reintroduciendo controles en todas sus fronteras terrestres y aéreas[14].

Mientras, la Comisión calculaba en enero de este año que el restablecimiento de los controles de fronteras interiores de Schengen había costado ya 3.000 millones de euros a la economía de la UE, sobre todo por el freno al comercio internacional por carretera[15].

2.4 *¿Amenaza cultural, amenaza terrorista o política oportunista?. ¿Intereses comunes?*

Como ya he mencionado, asistimos asombrados a la falta de reacción de gran parte de los Estados que no cumplen con lo acordado. Pero no es la primera vez que los estados miembros cierran fronteras[16], la propia legislación europea establece que en aquellos casos en los que así lo exija el orden público o la seguridad nacional se podrá hacer, pero siempre de forma temporal. La interrupción de la libertad de circulación de personas por motivos vinculados a la movilidad de personas se ha planteado en diversas ocasiones. Ha sido el cierre de fronteras entre Italia y Francia en 2011, ante el incremento de inmigrantes irregulares procedente del primer país, el ejemplo que más se asemeja a la crisis actual. Buena parte de las políticas complementarias que permiten la gestión de la movilidad dentro de la UE aún permanecen en manos nacionales y así no es posible construir un espacio común de libertad, seguridad y justicia mientras la gestión del asilo, el control

14. González Veiguela, Lino, «Asilo en Europa: los más generosos». *FRIDE*, (2013), Ver: *http://www.esglobal.org/asilo-en-europa-los-paises-mas-generosos/*.

15. González Enríquez, Carmen, «Schengen: un bien colectivo que nadie defiende», *Real Instituto Elcano*, Comentario Elcano núm. 6 (2016), págs. 2-3.

16. Ver: *http://www.rtve.es/noticias/20120419/paris-berlin-quieren-estados-controlen-fronteras-crisis/517198.shtml.*

de fronteras externas o la política de integración de inmigrantes continúe en manos y sin políticas y mecanismos comunes.

La división en la arena política europea está servida, unos argumentando solidaridad, otros posible pérdida de identidad étnica y otros por incapacidad económica; hay una parte de Europa que da la bienvenida a los que huyen de la guerra y otra que les prohíbe la entrada. Una Europa que argumenta que debe anteponerse la protección de los derechos humanos en esta crisis humanitaria[17] y otra que reclama proteger identidades nacionales y étnicas de lo que considera una amenaza a la civilización europea. Ambas Europas encuentran su máxima expresión por un lado en la alianza entre la Alemania de Merkel y la Comisión Juncker[18] y por el otro el Gobierno húngaro de Orbán, a la cabeza del grupo de Visegrado.

Alemania recibió los halagos de muchos cuando Angela Merkel expresó su voluntad de acoger hasta 800.000 refugiados y reformar los mecanismos con los que cuenta la Unión para hacer frente a la llegada de nuevas olas[19]. Pero con su política de fronteras abiertas permitió la llegada de cientos de miles de refugiados, hay que recordar que la UE no podía escudarse en la obsoleta convención de Dublín, que obliga a los refugiados a registrarse en el país de entrada antes de poder transitar a otros países europeos. Todo esto suscitó las críticas de los socios del V4[20], incluso países como España o Portugal estuvieron poco proclives, en el primer reparto de refugiados. Merkel encontró un aliado en la Comisión Juncker, a Tsipras, pero pronto suscitó controversias entre su opinión pública por la falta de capacidad

17. Romero, Manuel, «Cinco ONG exigen a Europa que antepongan los Derechos Humanos de los migrantes a la seguridad nacional», *LAVOZLIBRE*, Europa Press, Madrid (2015), Ver: *http://www.lavozlibre.com/noticias/ampliar/1143692/cinco-ong-exigen-a-europa-que-antepongan-los-derechos-humanos-de-los-migrantes-a-la-seguridad-nacional*.

18. Ayala de, Jose Enrique, «La Comisión Juncker: un nuevo comienzo para Europa», *Instituto Español de Estudios Estratégicos*, documento de Opinión núm. 126, (2014), págs. 10-11.

19. Ver: *http://www.europarl.europa.eu/atyourservice/es/displayFtu.html?ftuId=FTU_5.12.4.html*.

20. Carlos de Izquierdo, Javier, «La estrategia de seguridad energética de la Unión Europea y España», *Instituto Español de Estudios Estratégicos*, Documento de Opinión núm. 15, (2016), págs. 10-13.

de absorción en los centros de procesamiento de asilo y quejas de las autoridades locales.

Países además como Dinamarca, cuya política de asilo contaba entre las más generosas de Europa, se mostró de acuerdo a la tesis del Este, llegando a publicar propaganda oficial en periódicos del Líbano bajo el titular «No vengan a Dinamarca»[21].

Por otro lado, en el flanco este, países como Hungría o Polonia se replegaban en torno a sus identidades nacionales e incluso étnicas y religiosas para justificar una política restrictiva. Argumentaban que el Este de Europa ya hizo frente a un incesante flujo de refugiados durante la crisis de Ucrania, por lo que no podían permitirse acoger refugiados provenientes esta vez de la frontera Sur de Europa como Siria. Los líderes del grupo de Visegrado consideran que sus estados del bienestar e infraestructuras sociales no les permiten ejercer una solidaridad a la alemana.

La adopción de la repartición de cuotas de refugiados por mayoría cualificada en el Consejo de Justicia y Asuntos Exteriores de 22 de septiembre de 2015 con la abstención de los países de Visegrado marcó un hito de la división intraeuropea en la crisis[22]. Alemania llegó a sugerir una retirada de fondos de cohesión a aquellos que se negaran a ser solidarios con el drama humanitario de los refugiados. Los Jefes de Estado y de Gobierno lograron apaciguar las divisiones internas en el Consejo Europeo de 15 de octubre, donde la Unión fraguó un acuerdo de mínimos para hacer frente a la crisis de refugiados reforzando las fronteras de la Unión y prometiendo ayuda a países terceros para la contención de flujos e integración de los mismos[23]. No hubo en las conclusiones del Consejo señal alguna de que la Unión se pudiera encaminar hacia la adopción de una política común de asilo o el refuerzo de la actuación en los países de origen de la crisis.

Además todo esto con condiciones, los refugiados deben permanecer en el país que acepte su asilo. Si son sorprendidos

21. Ver: *http://internacional.elpais.com/internacional/2015/09/07/actualidad/1441648233_876039.html.*

22. Morillas, Pol, «Se ahonda la división entre Oeste y Este», *CIDOB*, (2016), págs.. 23-25. Ver: *file:///C:/Users/Jou/Downloads/23-26_POL%20MORILLAS_CAST.pdf.*

23. Suanzes, Pablo R., «La Unión Europea aprueba el reparto de 120.000 refugiados», *EL MUNDO*, Prensa Internacional, Bruselas, (2015), Ver: *http://www.elmundo.es/internacional/2015/09/22/5601771946163f77078b45aa.html.*

moviéndose a otros se les podría incluso pedir que abandonen la UE. Porque para compensar a los más reacios al asilo ha habido que endurecer el mensaje. Los inmigrantes económicos deben ser devueltos a su país de origen inmediatamente, porque no tienen derecho al asilo. Y a los que sí quieren enviarles el mensaje de que pueden perder las prestaciones sociales, e incluso el derecho a quedarse, si incumplen las normas.

Con la actuación de tacañería mediante el argumento de posible fomento de racismo y xenofobia y trabas económicas por parte de ciertos países europeos a la hora de la recepción de refugiados, lo que se ha puesto de manifiesto, es la ausencia de voluntad política y empatía por parte del Consejo Europeo, pues la UE con una población de más de 500 millones de personas, puede asumir el impacto cultural, social y económico que representa menos del 1% de su población con una mayor garantía de éxito que para Líbano que con 1,2 millones de refugiados y con 4 millones de personas representa el 27% de su población, Turquía con 2 millones sobre 75, o incluso Jordania con 700.000 refugiados sobre una población de 6 millones de personas[24].

En cuanto a posible amenaza terrorista, hay que tener en cuenta que el terrorismo yihadista parece atraer la atención de los europeos interesados por la política internacional más que otros temas, como la economía o los refugiados. Es percibida por la opinión pública en su conjunto como la mayor de cuantas amenazas procedentes del exterior pueden afectar a Europa. Concretamente en nuestro país, según los resultados de noviembre de 2015 del Barómetro del Real Instituto Elcano[25], 37ª oleada, el 52% de los seis de cada 10 residentes en España entrevistados declaró tener 'mucho' o 'bastante' interés por la política internacional, e hizo mención expresa al terrorismo yihadista entre sus asuntos de atención preferente.

Éste aspecto por desgracia queda reforzado cuando se comprueba que el atentado del 24 de mayo de 2014 en suelo belga,

24. Ferrero Turrión, Ruth, «Seguridad y derechos humanos, la crisis de los refugiados como crisis de valores de la UE», *Instituto Español de Estudios Estratégicos*, documento de Opinión núm. 3, (2016), págs. 5-7.

25. Ver: *http://realinstitutoelcano.org/wps/wcm/connect/943d0a804b644165add-8bfeeaa369edc/37BRIE_Informe_Enero2016.pdf?MOD=AJPERES&CACHEID=943d0a-804b644165add8bfeeaa369edc.*

en el museo judío de Bruselas con cuatro víctimas mortales, lo comete un francés de origen argelino combatiente retornado del conflicto sirio[26]. Pero la principal amenaza para las sociedades europeas aún sigue proviniendo de individuos radicalizados a nivel local. De hecho varios de los rasgos comunes de los combatientes retornados son: de 2.ª o 3.ª generación en un país occidental, viviendo entre dos culturas la originaria de la familia y la del país donde vive, decepcionado de Occidente y cuya motivación es más personal que política[27].

A nivel europeo y dentro de la Estrategia Contraterrorista (EC) de la UE[28], se ha puesto en marcha en enero de este año, el Centro Antiterrorista Europeo en La Haya. También siguen en vigor las bases de la respuesta de la UE al problema de los combatientes extranjeros establecidas por el Consejo de Justicia y Asuntos de interior de este mismo año[29].

Conclusión

Consciente del déficit de identidad que ha aflorado últimamente entre los ciudadanos europeos, Jean-Claud Juncker, insistió en octubre del pasado año, que en la Unión Europea tenía que generarse más unión y más Europa. Pero la construcción de Europa que moviliza diferentes comunidades, en un espacio de más de quinientos millones de habitantes y con diferentes procesos sociales, culturales y políticos, donde en un período de no muchos años se ha pasado de 15 a 28 estados miembros, ésta, se hace más compleja.

Pese a todo ello, en el reciente Eurobarómetro de primavera de 2014 se expresaba un sustancial incremento del sentimiento ciudadano europeo, siendo muy remarcado entre los ciudadanos pertenecientes a los países con la moneda euro. Por una parte

26. Mora Tebas, Juan Alberto, «Yihad 3.3: La amenaza de los [combatientes] retornados», *Instituto Español de Estudios Estratégicos*, Documento de Análisis núm. 46, (2016), págs. 10-13.

27. Naciones Unidas, Resolución 2178 (2014), de 24 de septiembre de 2014, *Consejo de Seguridad*, «para paliar los efectos de los retornados», págs. 1-9.

28. Ver: *https://www.agpd.es/portalwebAGPD/internacional/Europa/Cooperacion_Policial_Judicial/Sistema_de_Informacion_SCHENGEN/index-ides-idphp.php*.

29. Ver: *http://www.consilium.europa.eu/es/policies/fight-against-terrorism/foreign-fighters/*.

están los que opinan que se puede establecer una pertenencia múltiple en la formación de identidades y que se define por un espíritu comunitario intercultural de diversidad; y por otra parte, los ciudadanos que han empezado a creer que la UE más bien contribuye a ensanchar divisiones entre países con la propagación de viejos estereotipos, a reducir el bienestar a golpe de recortes, a desconfiar de un sistema político comunitario que en la mayoría de los casos no va acompañado de valores morales.

Puede ser que los valores de tolerancia y apertura se encuentren en retirada, puede ser que Europa sufra una verdadera crisis de identidad con la puesta en marcha de políticas nacionalistas oportunistas por parte de gobiernos como el polaco o el húngaro o con la mayor presencia de movimientos populistas en países de Centroeuropa; pero también hace ya más de medio siglo, Europa en una fase de reconstrucción social, económica y política acertó en la construcción de un continente donde existiera la paz, se fomentara la economía así como la defensa de los derechos humanos.

Las reflexiones de los europeos son fenómenos no sólo individuales, sino también sociales y colectivas, dependientes pues de las condiciones de nuestra existencia individual y social, por ende vinculado a la historia. El padre de la sociología, Augusto Comte, afirma que existe una correlación entre lo mental y lo social; que todo sistema que explique el pasado será dueño del porvenir. Aplicando la metáfora de Zygmunt Bauman, la sociedad europea está inmersa en la modernidad líquida, y también da cuenta de la precariedad de los vínculos humanos en una sociedad individualista y privatizada, marcada por el carácter transitorio y volátil de sus relaciones.

Quizás Europa no esté cumpliendo la función de educación universal. Las diferencias en el seno de la sociedad europea son históricas, es decir, radican en el tiempo y no como muchos discursos políticos e ideológicos pretenden hacernos creer en la etnia, la cultura o el espacio. Si algunos estados como Reino Unido argumentan como principal factor para votar a la salida de la UE el descontento con la escalada de inmigración, es dar la espalda a la dimensión histórica de la humanidad, la que realmente nos hace absolutamente semejantes. Si los países bálticos se sienten más seguros bajo el amparo protector de la OTAN que en las políticas de seguridad que la propia UE pueda poner en marcha, es

creer en la diversidad geográfica sin relacionarla con el tiempo y con la historia. Si los países que hoy en día son los antiguos vecinos frontera del Imperio Otomano europeo muestran su total rechazo a la política de refugiados europea, es cometer la falta más grave contra el hombre, olvidar que la humanidad se enseñe a sí misma.

> «[…] es cierto que las fronteras no existen. Existen, temporalmente. Pero al mismo tiempo que ellas, existe una fuerza de creación y de verdad que nos une a todos, en la humildad y el orgullo al mismo tiempo. Yo nunca lo he sentido mejor que leer sus palabras y por ello quiero manifestar mi gratitud y mi solidaridad».
>
> Carta de Albert Camus a Boris Pastenark, 9 de junio de 1959.

Referencias bibliográficas

Ayala de, Jose Enrique, «La Comisión Juncker: un nuevo comienzo para Europa», *Instituto Español de Estudios Estratégicos*, documento de Opinión núm. 126, (2014), págs. 10-11.

Carlos de Izquierdo, Javier, «La estrategia de seguridad energética de la Unión Europea y España», *Instituto Español de Estudios Estratégicos*, Documento de Opinión núm. 15, (2016), págs. 10-13.

Caro Jiménez, Mari Carmen, et al. «Las emociones y la resistencia al cambio de actitudes». *Revista Española de Investigación de Marketing ESIC* núm. 18, (2014), págs. 19-21.

Cohen, Jessica, «Efectos sociales del terrorismo. Crisis de refugiados y argumentaciones erróneas», *Instituto Español de Estudios Estratégicos,* Documento de Opinión núm. 112, (2015), págs. 6-7.

Europa, Comisión Europea, «un nuevo informe y una nueva encuesta ofrecen una imagen más precisa sobre el estado de la migración, el asilo y la libre circulación en la UE», *Comunicado de prensa*, Bruselas (2012), disponible en http://europa.eu/rapid/press-release_IP-12-552_es.htm. [consultado el 27 de agosto de 2016].

Ferrero Turrión, Ruth, «Seguridad y derechos humanos, la crisis de los refugiados como crisis de valores de la UE», *Instituto Español de Estudios Estratégicos*, documento de Opinión núm. 3, (2016), págs. 5-7.

González Enríquez, Carmen, «Schengen: un bien colectivo que nadie defiende», *Real Instituto Elcano*, Comentario Elcano núm. 6, (2016), págs. 2-3.

González Veiguela, Lino, «Asilo en Europa: los más generosos». *FRIDE*, (2013), disponible en http://www.esglobal.org/asilo-en-europa-los-paises-mas-generosos/. [consultado el 26 de agosto de 2016].

Mora Tebas, Juan Alberto, «Yihad 3.3: La amenaza de los [combatientes] retornados», *Instituto Español de Estudios Estratégicos*, Documento de Análisis núm. 46, (2016), págs. 10-13.

Morillas, Pol, «Se ahonda la división entre Oeste y Este», CIDOB, (2016), págs. 23-25, disponible en file:///C:/Users/Jou/Downloads/23-26_POL%20MORILLAS_CAST.pdf. [consultado el 7 de septiembre de 2016].

Naciones Unidas, Resolución 2178 (2014), de 24 de septiembre de 2014, *Consejo de Seguridad*, «para paliar los efectos de los retornados», págs. 1-9.

Romero, Manuel, «Cinco ONG exigen a Europa que antepongan los Derechos Humanos de los migrantes a la seguridad nacional», *LAVOZLIBRE*, Europa Press, Madrid (2015), disponible en http://www.lavozlibre.com/noticias/ampliar/1143692/cinco-ong-exigen-a-europa-que-antepongan-los-derechos-humanos-de-los-migrantes-a-la-seguridad-nacional, [consultado el 2 de septiembre de 2016].

Suanzes, Pablo R., «La Unión Europea aprueba el reparto de 120.000 refugiados», *EL MUNDO*, Prensa Internacional, Bruselas, (2015), disponible en http://www.elmundo.es/internacional/2015/09/22/5601771946163f77078b45aa.html, [consultado el 7 de septiembre de 2016].

Tubella, Patricia, et al. «Reino Unido amenaza con detener a Assange en la embajada de Ecuador», *El País, Internacional*, (2012), disponible en http://internacional.elpais.com/internacional/2012/08/15/actualidad/1345051978_623282.html. [consultado el 26 de agosto de 2016].

LOS SISTEMAS ARMAMENTÍSTICOS AUTÓNOMOS MILITARES[1]: UN DESAFÍO PARA LA COMUNIDAD INTERNACIONAL EN EL SENO DE LAS NACIONES UNIDAS (ONU)

Milton J. Meza Rivas
Universidad de Barcelona, España

Resumen

Ciertas tecnologías castrenses, que en el pasado formaban parte de los libros y las películas de ficción, ahora llegan a ser una auténtica realidad. Diversos sistemas de armamento militar están desarrollándose con funciones cada vez más autónomas, sometidas a niveles de control indirecto, pese a que su ambigüedad genere escenarios llenos de incertidumbres y riesgos. Por ello, dentro de la ONU, expertos a nivel mundial tienen la tarea de estudiar este tipo de tecnologías emergentes, abordando prospectivamente el I+D de los sistemas armamentísticos autónomos militares que, por las particularidades de su diseño, producen interés y preocupación a nivel global. Así, este documento plantea varias de las dificultades que hacen de estos sistemas un auténtico desafío a la hora de ser estudiados por la comunidad internacional en pleno.

Palabras claves

Armas, sistemas autónomos, inteligencia artificial, robots, ONU.

Introducción

Durante los últimos años hemos podido observar como la investigación, el desarrollo, la innovación y el uso de las altas

1. En inglés: «*fully autonomous weapon systems*». Otros términos han sido comúnmente usados para referirse a este tipo de tecnología avanzada. Por ejemplo, sistemas de armas autónomas letales («*lethal autonomous weapon systems —LAWS—*»), armas robóticas (*robot weapons*), armas letales autónomas («*lethal autonomous weapons —LAWs—*»), robots autónomos letales («*lethal autonomous robots —LARs—*») o sistemas autónomos (*autonomous systems*). No obstante, a los efectos de la presente comunicación todos podrán ser empleados de manera intercambiable sin que eso ello desdibuje el sentido del término usado en el título principal.

tecnologías emergentes representan sin lugar a dudas una fuente inagotable de escenarios complejos llenos de incertidumbres y altos niveles de riesgo, cuya aminoración y/o contención han podido en cierta manera alcanzarse mediante acuerdos y decisiones políticas, jurídicas, económicas, sociales y éticas globales llevadas a cabo por agentes tecnocientíficos[2].

Por ello el Derecho, junto a la política, se encuentra cada vez más inmerso en cuestiones marcadas de un componente científico (Esteve Pardo, 2009) basado en el carácter ambivalente de las tecnologías[3].

Desde este enfoque, el desarrollo y la innovación tecnológica representan una promesa de progreso para la sociedad en tanto que proporcionan potenciales beneficios a la colectividad. No obstante, en razón de su contenido, conllevan a un cúmulo de riesgos, peligros o amenazas globales que deben ser sopesados, prevenidos, controlados y/o corregidos por el poder constituido propio del orden jurídico, político, económico, social y cultural vigente a nivel internacional.

Perspectiva de la comunidad internacional dentro del sistema de las naciones unidas acerca del I+D militar.

Desde la época de la «macrociencia»[4] y hasta nuestros días, los gobiernos del mundo han dejado de asumir a los fines de la ciencia y la tecnología como valores últimos, y los perciben como

2. Todo proceso de investigación, desarrollo e innovación tecnocientífico es llevado a cabo por agentes plurales y diversos que poseen intereses igualmente variados, a saber, políticos, sociales, jurídicos, militares, económicos, etc. *Vid.* Echeverría, 2003.

3. A los efectos del presente artículo se usará de manera intercambiable los términos genéricos «tecnología», «sistema», «máquina» o «dispositivo» para referirse a cualquier producto final que resulte de un proceso de investigación, desarrollo e innovación tecnológica.

4. Situada entre la época de la segunda guerra mundial y hasta los inicios de los años 80, época en la que luego emergió la *tecnociencia,* una modalidad de actividad humana y social que poco a poco se fue consolidando sociológica e institucionalmente en el mundo y que no sólo modifica la ciencia: también transforma la actividad tecnológica, industrial y militar, gracias al desarrollo de un sistema nacional de ciencia y tecnología que trasciende los límites de las comunidades científicas… preexistentes. No obstante, resulta oportuno precisar que, pese a al surgimiento de la macrociencia y luego de la posterior tecnociencia, tanto la técnica artesanal, como la ciencia y la tecnología han seguido existiendo hasta nuestros días.

«*instrumentales*» (Echeverría, 2003), subordinados a unos objetivos estratégicos que varían dependiendo del contexto que se trate, y que son en definitiva los que dan sentido a toda financiación y realización de proyectos gubernamentales presentes y futuros[5].

Dichos objetivos encuentran dos justificaciones básicas: por un lado, el argumento del *spin-off*, una tesis de carácter económico según la cual las inversiones en el desarrollo y la innovación militar producen efectos beneficiosos aplicables a otras áreas de investigación, favoreciendo de esta manera no sólo el progreso científico-tecnológico *per se*, sino también el desarrollo industrial y el crecimiento económico (Rodríguez Alcázar, 2011: 71).

Con el pasar del tiempo este concepto fue superado, entre otras razones, por la existencia de las tecnologías de «*doble uso*», aquellas que implican la necesidad de seguir teniendo en cuenta las consecuencias socioeconómicas que trae consigo la inversión y el desarrollo en la investigación militar, pero que además replantean la forma en que deben ser analizados los efectos de todo aquello que haya sido creado a través del I+D militar[6].

Por otro lado, encontramos el argumento de *la seguridad y el poderío militar* según el cual políticos y expertos reconocen que la supremacía castrence de los Estados depende, en gran medida, de la superioridad tecnológica de sus ejércitos. Asimismo, de forma correlativa, asumen que la seguridad de las naciones será siempre mayor en tanto que sus fuerzas armadas adquieran avances tecnológicos de gran dimensión y un número suficiente de artefactos militares de alta tecnología (Rodríguez Alcázar, 2011: 74-75).

Ahora bien, bajo ambas premisas, los avances tecnológicos resultantes del I+D militar tienden a relacionarse entonces con

5. Tales proyectos podrían tratarse, entre otros, de la mejora de capacidades en acciones de defensa y ofensiva militar, de métodos para alcanzar la victoria en las guerras, optimizar la productividad de sectores industriales e incluso incrementar el prestigio militar, disminuir el riesgo país, alcanzar niveles «envidiables» de seguridad y estabilidad social, económica y geopolítica.

6. Hoy gran parte de la comunidad internacional considera que, como principio, los sistemas diseñados y fabricados originariamente con propósitos militares pueden en cierta medida ser usados, modificados o convertidos al servicio de funciones civiles (o viceversa), aún y cuando ello llegue a significar mayores riesgos de que se incremente la proliferación de este tipo de tecnología o que incluso planteen nuevos problemas relacionados con la responsabilidad y la rendición de cuenta en razón de su uso posterior.

niveles de riesgo que deben ser sopesados cuidadosamente por sus agentes tecnocientíficos, ello en pro de mantener la salvaguarda de la especie humana.

Casos como la creación del laboratorio de radiación del Instituto de Tecnología de Massachusetts[7], el proyecto del computador e integrador numérico electrónico[8] o incluso la creación de la bomba atómica[9] —por tan sólo referir a algunos ejemplos importantes de la historia— son una muestra fehaciente del gran impacto que puede traer consigo el engranaje del ingenio humano para dar respuesta a intereses militares, permitiendo por un lado el alcance de importantes avances en disciplinas científicas diversas, y por otro la asunción de nuevas tecnologías con atributos capaces de ser usados para la eliminación de ejércitos y ciudades enemigas, pese a que la dimensión de destrucción que posean supere los límites tolerables por la moral humana (Ortega García, 2011: 190-191).

La historia nos ha enseñado que los Estados están inclinados a comportarse siempre en proporción al poder que ostenten. Y el peligro aumenta aún más cuando de actores no estatales se trate.

La necesidad de poseer armas o tecnologías castrenses cada vez más novedosas responde a una premisa fundamental, esto es, mantener un estatus hegemónico del poder de defensa y ataque, o alcanzar un estándar en el uso de la fuerza a nivel global que, bajo

7. Fundado en 1940, el cual se especializó en el proyecto del radar y cuyo alcance científico logró trasladarse al ámbito militar, civil y el tecnológico.

8. ENIAC, por sus siglas en inglés: *Electronic Numerical Integrator And Computer*. Desarrollado por el Laboratorio de Investigación Balística de la de la Universidad de Pensilvania, que pretendió acelerar el cálculo y mejorar la precisión de las tablas de tiro de artillería y de bombardeo, y cuyo logro mayor fue la creación del primer ordenador multitareas de la historia. *Vid.* Mollen, 2016. *Vid.* Echeverría, 2003: 26; también *Vid.* Heppenheimer, T. A., «La fábrica del hombre», en Minsky, 1986: 43.

9. Producto del *proyecto Manhattan*, un programa intergubernamental basado en necesidades puramente militares y que marcó un hito en el desarrollo de la ciencia moderna, alcanzando avances importantes en el campo nuclear y radioactivo. Fue el proceso ultra-secreto de diseño y construcción de la bomba atómica, que contó con el apoyo de varios estados - Estados Unidos, con el apoyo del Reino Unido y Canadá principalmente- en razón de su gran valor estratégico, y cuyos primeros lanzamientos se dieron sobre Japón en 1945. Estuvo bajo la dirección de Robert Oppenheimer, quien tuvo a su disposición medios materiales y humanos de alto nivel.

el argumento de salvaguardar la paz y la seguridad, garantice que las armas del oponente sigan siendo siempre las más inútiles u obsoletas.

Por ello, autores como Röling[10] aciertan al considerar que la función más razonable del poder armamentístico de un país siempre será, en definitiva, disuadir al enemigo a que actúe en contra de la paz, y para ello deberá demostrar su capacidad de resistencia o retaliación ante eventuales ataques que pueda producir en su contra cualquier adversario. Ergo las armas, a pesar de que puedan ser consideradas inaceptables por muchos, siguen siendo indispensables para garantizar la seguridad militar estatal, ya que su existencia permite crear un ambiente generalizado en el que el imaginario colectivo se sienta libre de riesgo de amenaza en su contra por parte de sujetos que actúen al margen del Derecho Internacional Público.

Por todo ello, parte de la comunidad internacional entiende que el avance tecnológico en general, extensible por obviedad a la esfera militar, demanda en suma la formación de nuevas costumbres sociales. Ello no significa el sometimiento de la sociedad a la tecnología. En lo absoluto. Son las situaciones en las que interactúan las personas con las tecnologías las que tienen que evolucionar mediante los mismos procesos naturales por los que cambian las costumbres humanas (Minsky, 1986: 67).

Ahora bien, es innegable que los rituales tradicionalmente válidos en una sociedad no son lo suficientemente idóneos para evaluar y/o crear medios que permitan disminuir los niveles de desconcierto, confusión y riesgo en el uso de cierta tecnología militar potencialmente disruptiva. Nótese que los rituales propios de la interacción entre personas y máquinas pueden ser probablemente distintos a lo que estamos acostumbrados.

Por ello, algunos estudiosos de este tema hemos venido desarrollando, no sólo en nuestras academias sino también en foros internacionales[11] junto al resto de la comunidad internacional,

10. *Vid.* Röling, B. V. A., 1984: 183.

11. Reuniones informales de expertos sobre sistemas de armas autónomas letales, celebradas en el marco de la Convención sobre prohibiciones o restricciones del empleo de ciertas armas convencionales que puedan considerarse excesivamente nocivas o de efectos indiscriminados. Para más información véase: http://www.unog.ch/80256EE600585943/(httpPages)/8FA3C2562A60FF81C1257CE600393DF6?OpenDocument, fecha de la consulta 27.09.2016.

un análisis amplio que va en esa dirección, abordando los impactos jurídicos, políticos, sociales, éticos y morales que trae consigo el uso de altas tecnologías militares emergentes, especialmente cuando se relacionan con la investigación, el desarrollo y el despliegue de sistemas de armas letales con altos niveles de autonomía basada en programas de inteligencia artificial.

Antecedentes del debate de los sistemas de armas letales completamente autónomos en la ONU.

En noviembre de 2013, las Altas Partes Contratantes de la Convención sobre Ciertas Armas Convencionales (CCW, por sus siglas en inglés[12]) aprobaron bajo consenso debatir los aspectos relacionados con los sistemas de armas letales autónomos, por considerar que dicho organismo es el foro más apropiado para ello en razón de su mandado y experiencia. No obstante, la resolución advierte que este es un asunto multifactorial, de gran trascendencia global, por lo que su estudio puede y debe seguir realizándose bajo diferentes enfoques en el seno de otros organismos internacionales (Altas Partes Contratantes de la CCW, 2013).

Así, en mayo del 2014, y en abril del 2015 y 2016, se realizaron la primera, segunda y tercera reunión oficiosa de expertos sobre sistemas de armas autónomas letales en el marco de la CCW. Estos eventos congregaron varias representaciones diplomáticas de Estados partes, firmantes y observadores de la CCW, así como también agentes de distintas organizaciones internacionales, organizaciones no gubernamentales (ONG) e instituciones académicas.

En dichas reuniones se han generado reflexiones prospectivas y holísticas en torno a un programa de trabajo estructurado en cinco bloques temáticos: a) mapa o conceptual del término «*autonomía*»; b) hacia una definición de trabajo sobre los sistemas de armas letales autónomos; c) desafíos para el DIH en el contexto de las armas autónomas; d) cuestiones éticas y de derechos humanos; y e) aspectos sobre seguridad internacional.

12. No obstante, el nombre completo en español es «Convención sobre prohibiciones o restricciones del empleo de ciertas armas convencionales que puedan considerarse excesivamente nocivas o de efectos indiscriminados» del año 1980.

Los sistemas de armas autónomas letales (SAAL): ¿por qué son un desafío para la comunidad internacional?

Lo primero que debemos destacar al respecto es que hoy en día no hay unanimidad en torno a una definición de estos sistemas. Tan sólo existen intentos de conceptualizaciones por parte de gobiernos, organismos multilaterales, ONG e instituciones académicas.

Durante el desarrollo de los debates en la CCW, algunos expertos han venido planteando ciertas precisiones terminológicas que más allá de aclarar la cuestión tienden a producir confusiones semánticas. Declaraciones y documentos especializados a menudo demuestran el uso libre de palabras como «automático», «automatizado», «semiautónomo», «autónomo», «supervisado», «completamente autónomo» e «inteligente» para referirse a todo un espectro de dificultad y sofisticación propia de estos sistemas (Scharre, 2016: 11).

Ello ha llevado a que parte de la comunidad internacional incurra en falacias conceptuales que les impiden entender en qué medida el grado de complejidad de tales tecnologías es independiente de la tarea para el cual se empleen y del tipo de control humano que sobre ellas exista. Sea bajo uno u otro término, el punto estriba en cómo definir estos sistemas. Sin definición de trabajo, pareciera que el juego del debate está trancado.

Luego de las tres primeras reuniones de la CCW (2014, 2015 y 2016), la mayoría sólo ha podido reconocer de manera muy simplista que los SAAL, como sistema autónomo *per se*, es aquel que, una vez activado, realiza una tarea por sí solo (Scharre, 2016: 8). Sin embargo, algunos piensan que, en virtud de su capacidad funcional, dichos sistemas podrían llegar a tener distintos grados de sofisticación (automático, automatizado, autónomo o inteligente). Asimismo, dependiendo del tipo de control humano ejercido sobre las funciones críticas que le hubieren sido programadas («seleccionar» y «atacar» un objetivo), podrían ser clasificados como semiautónomos, de operación autónoma supervisada y completamente autónomos.

Ahora bien, independientemente de la clasificación que se trate, lo importante que se debe tener en cuenta desde un principio es lo siguiente: tal y como he expresado en artículos ante-

riores[13], los «*sistemas de armas autónomas*» es expresión de origen del inglés[14]. Su principal criterio definitorio viene dado por el adjetivo «*autonomous*», que según el diccionario de Oxford comprende todo aquello «*que se gobierna a sí mismo o es independiente*» (*self-governing* o *independent*). Por su parte, dentro la categoría de ciencia, tecnología, matemática y computación, lo define como un sistema abstracto o red física que es independiente de, o no está sujeta a, influencias o controles externos.

Así pues, varios expertos dentro de las reuniones de la CCW han planteado que los sistemas de armas letales autónomos son aquellos que pueden llevar a cabo una misión con intervención humana limitada o sin ella, siendo capaces de lograr su auto-propulsión, procesar la información obtenida de su entorno o incluso dar respuesta a este de manera independiente[15].

Según el Departamento de Defensa de los Estados Unidos de Norteamérica (EEUU), dicha tecnología incluye además aquellos sistemas de armas autónomas que son supervisados por humanos y que están diseñados para permitir que los operadores puedan anular su acción, aún y cuando tengan la habilidad de seleccionar y atacar objetivos sin intervención humana luego de su activación (Departamento de Defensa de EEUU, 2012).

Por su parte, el Reino Unido los define como un grupo especial de tecnologías emergentes cuyo nivel de operatividad es «*completamente autónomo*» (Gobierno del Reino Unido, 2016). Tales sistemas tendrían la capacidad de entender, interpretar y aplicar al más alto nivel el efecto global del uso de la fuerza, y para ello se deberían basar en la comprensión precisa de aquello que un

13. Artículo de opinión escrito por el autor de este trabajo, publicado bajo el número 85/2016, Instituto Español de Estudios Estratégicos (IEEE), Madrid, 18 de agosto de 2016, [en línea], disponible en http://www.ieee.es/Galerias/fichero/docs_opinion/2016/DIEEEO85-2016_SistemasArmas_ONU_MiltonMeza.pdf, fecha de la consulta 27.09.2016

14. *Lethal autonomous weapons systems.*

15. Sobre el atributo de letalidad, el Relator Especial Heyns considera que los «*sistemas de armas autónomas*» debe ser entendido como un término genérico, por lo que sólo se le podría adherir el adjetivo «*letal*» cuando su uso se limite a los conflictos armados. Sin embargo, advierte que con el tiempo será cada vez más común observar que este tipo de tecnología pueda ser utilizadas por las fuerzas y cuerpos de seguridad de los Estados, aunque la intención normalmente sea para evitar la muerte. *Vid.* Heyns, 2016.

comandante tenga la intención de hacer, y más aún de las razones que soportan dicho propósito.

Suiza sugiere una «definición de trabajo» en la que entiende que estos sistemas de armas serían capaces de llevar a cabo tareas bajo el gobierno del DIH, en reemplazo parcial o total de un humano en el uso de la fuerza, y muy particularmente durante el ciclo de determinación de un objetivo (Gobierno de Suiza, 2016). Reconoce que la «*autonomía*» debe ser entendida como un amplio espectro tecnológico (UNIDIR, 2014) que va desde las limitadas funciones autónomas de los sistemas ya existentes a aquellas que son propias de los sistemas autónomos del futuro cuyo nivel de sofisticación será mucho mayor.

Autoridades del gobierno canadiense apoyan esta perspectiva (Gobierno de Canadá, 2016). En su opinión resulta más útil pensar a la autonomía como un «*espectro*» ligado estrechamente a la tecnología y a las capacidades de un sistema, al entorno operativo y a la tarea elegida.

Francia, por su lado, precisa que las armas autónomas son un tipo de tecnología armamentística que podría ser capaz de moverse libremente, adaptarse a su ambiente y llevar a cabo la selección de objetivos y el lanzamiento de efectores letales bajo la autoridad total de la inteligencia artificial (Gobierno de Francia, 2016).

Instituciones como Human Rights Watch[16] consideran que un sistema de armas con capacidad para ejecutar funciones críticas de selección y de ataque contra objetivos y sin implicación humana, es una alta tecnología de total autonomía cuyo desarrollo contraviene las reglas básicas del DIH y del DIDH, por lo que deben ser prohibidas.

Al hilo de ello, el Comité Internacional de la Cruz Roja considera que estos sistemas son un tipo de arma que puede seleccionar (es decir, buscar para detectar, identificar, localizar y seleccionar) y atacar (usar la fuerza en contra, neutralizar, dañar o destruir) objetivos sin intervención humana (CICR, 2016). Ellos tendrían la habilidad de aprender y/o adaptar su funcionamiento en respuesta a las circunstancias cambiantes del entorno en el que se despliegan, por lo que su uso podría reflejar un cambio cualitativo de los paradigmas en la conducción de las hostilidades (CICR, 2011).

16. Vid. (Human Rights Watch, 2015).

Todas estas propuestas terminológicas son una pequeña muestra de la amplitud con la que la comunidad internacional está abordando los sistemas de armas autónomos letales en el seno de las Naciones Unidas. En ellas se recogen aspectos compartidos por unos y rechazados por otros, aunque de su contenido se rescatan algunos elementos importantes:

—Son un tipo de alta tecnología aún inexistente[17].
—Su desarrollo gira en torno al avance en la investigación de la inteligencia artificial.
—Para algunos expertos es improbable que lleguen a existir, y para otros sólo se necesitan años, y no décadas, para que puedan ser creados[18].
—Su diseño les permitiría seleccionar y atacar un objetivo estratégico en razón de la delegación de autoridad que le es haya sido dada por los humanos.
—La determinación de ese objetivo responderá sólo a los criterios pre-definidos por los humanos.
—Es un arma que después de activada ejecutará sus funciones sin implicación o intervención humana.
—Poseería una función de letalidad, por lo que sus zonas de despliegue serán aquellas en las que se desarrollen conflictos armados u hostilidades.
—Podrían adaptarse a entornos complejos sobre la base de la información que obtengan del ambiente que les rodea.
—Y sus reglas de conducta serían determinadas únicamente por el diseñador/programador humano, por lo que la máquina no tendría niveles de autoaprendizaje y auto-elaboración que les permita por sí mismas cambiar dicha circunstancia.

17. En la tercera (3.ª) reunión informal de expertos sobre los sistemas de armas letales autónomos de abril del 2016, las delegaciones de los países de Alemania, Costa Rica, España, Estados Unidos, Francia, Israel, Japón, Países Bajos, Reino Unido, Suiza y Turquía fueron tajantes en señalar que actualmente no existen este tipo de tecnología. Por su parte, España, Japón y Reino Unido agregaron además que no tienen planes en desarrollarlos. *Vid. infra* apartado 16 de este artículo.

18. Para más información véase «Future of Life Institute, Autonomous Weapons: an open letter from IA & robotics researches», 28 de julio de 2015, [en línea] disponible en: http://futureoflife.org/open-letter-autonomous-weapons/, fecha de la consulta 27.09.2016.

Conclusión

Anticipar cada una de las situaciones que obligan a los humanos a decidir cómo deben actuar con las máquinas es algo bastante complejo, y para muchos incluso imposible, por lo que *ad initio* nos resulta difícil alcanzar la total normativización de cada supuesto de hecho, dentro y fuera de los debates que se suscitan en la ONU.

Como he venido planteado en presentaciones anteriores[19], la falta de unanimidad internacional para acordar un concepto generalmente aceptado sobre este tipo de sistemas es consecuencia de una realidad previamente advertida: los elementos de la discusión responden a perspectivas meramente prospectivas basadas en hipótesis y cálculos de probabilidades acerca de armas que aún no existen. Su estudio ha levantado dudas y cuestionamientos sin responder que seguirán siendo parte de futuros debates internacionales.

Según los avances tecnológicos conocidos al día de hoy, un robot autónomo letal, por muy bien diseñado y programado que esté, probablemente no pueda cumplir a rajatabla con los principios básicos del DIH (especialmente el de distinción[20], proporcionalidad[21] y precaución), ya que en razón de las complejidades que involucra una misión militar es difícil que la máquina cuente con una base de datos suficiente que le permita evaluar todo el contexto, lo cual incrementa el riesgo de que se produzcan daños no previstos e indiscriminados en contra inocentes.

Por ende, cualquier iniciativa relacionada con la no proliferación y el desarme debe ser estudiada y analizada bajo un correcto juicio de ponderación de valores, en el que se aprecie los peligros externos que trae consigo renunciar al progreso, se comprenda y respete la salvaguarda del derecho internacional de los derechos humanos y el derecho internacional humanitario, en el que se

19. *Vid. supra* el apartado 13 de este trabajo.

20. *Vid.* Organización de las Naciones Unidas (ONU). Protocolo I adicional a los Convenios de Ginebra de 1949 (1977) relativo a la protección de las víctimas de los conflictos armados internacionales, art. 51 y 57, [en línea] disponible en: https://www.icrc.org/spa/resources/documents/misc/protocolo-i.htm#8, fecha de la consulta 27.09.2016.

21. *Ibid.* art. 51 5) b).

aborde la seguridad global como una prioridad sin generar desequilibrios de poder, pero sobre todo, donde no se resienta la capacidad futura de defensa militar de los Estados Nación (Ortega García, 2011: 190).

Es un panorama idóneo, deseable, aunque arduo de alcanzar en la realidad. No olvidemos: todos competimos unos con otros por los recursos del universo accesible[22]. Una mayor, más diversa y competente cultura tecnológica es la vía idónea para obtener beneficios y diagnosticar cualquier riesgo y enfrentarlo. De allí que resulte entendible la necesidad de inversión de los Estados en el I+D militar: si países como Estados Unidos, China, Reino Unido o Israel, por tan sólo nombrar algunos[23], detuvieran unilateralmente su gran desarrollo tecnológico, pronto sucumbirían al poder militar de otros Estados (o incluso de actores no estatales) o a los éxitos económicos de sus socios comerciales.

Esta amanera de entender el avance tecnológico como un medio para garantizar mayor seguridad y poderío militar a los Estados, es lo que ha permitido que ciertas tecnologías castrenses, que en el pasado formaban parte de los libros y las películas de ficción, ahora lleguen a ser una auténtica realidad[24]. Diversos sistemas de armamento militar se están desarrollando con funciones cada vez más autónomas, sometidas a niveles de control indirecto o «*apropiado*», pese a que su ambigüedad pueda generar escenarios complejos llenos de incertidumbres y riesgos a los que el Derecho y la política están llamados a solucionar.

Algunos ejemplos que ilustran dicha complejidad se hacen patente en los procesos de investigación, desarrollo e innovación de los sistemas de armas autónomas letales, un tipo de tecnolo-

22. Vid. Moravec, H., «Los vagabundos», en Minsky, 1986: 113.

23. Para más datos sobre qué países destinan sus recursos en gasto militar (incluyendo el I+D) *Vid.* SIPRI, *World military spending resumes upward course, says SIPRI*, 2016.

24. En el primer tercio del siglo XX, las máquinas con ciertas funciones automatizadas no eran comunes en los campos de batalla, y prácticamente inexistentes en las ciudades. Ahora, el despliegue de sistemas aéreos, terrestres o navales no tripulados (o controlados remotamente) usados como armas de seguimiento, vigilancia, control y ataque sí que son muy habituales. Para más datos acerca del uso de esta nueva tecnología militar, *Vid.* OTAN, 2016. También vid. Jonas, A., Mcann, E. y Thomas, M., 2015.

gía avanzada militar que aún no se ha creado[25], pero que por sus particularidades e intereses estratégicos ha venido siendo objeto de amplios debates en el mundo, y muy especialmente en el seno del Sistema de las Naciones Unidas.

Referencias bibliográficas

Libros

Echeverría, J., *La revolución tecnocientífica*, Madrid, Fondo de Cultura Económica de España, 1.ª edición, 2003, 282 págs.

Esteve Pardo, J., *El desconcierto del Leviatán. Política y derecho ante las incertidumbres de la ciencia*, Madrid, Marcial Pons, 1.ª edición, 2009, 211 págs.

Jonas, A., Mcann, E. y Thomas, M., Urban Geography: a Critical Introduction. Oxford (UK), editorial Wiley Blackwell, 2015, 192 págs.

Miller, A. y Feinrider, M. (eds.), *Nuclear weapons and law,* Connecticut, Greenwood Press, 1.ª edición, 1984, 592 págs.

Minsky, M. (ed.), *Robótica la última frontera de la alta tecnología,* Barcelona, Planeta, 1.ª edición, 1986, 263 págs.

Ortega García, J., *Capítulo Sexto: armas de tecnología avanzada*, Madrid, Instituto Español de Estudios Estratégicos (IEEE), cuaderno de estrategia Nº 153, 2011, 230 págs.

Rodríguez Alcázar, J., *Ética, tecnología y seguridad,* Bogotá, Corporación Universitaria Minuto de Dios, 1.ª edición, 2011, 160 págs.

Páginas web

http://www.unog.ch/80256EE600585943/(httpPages)/4F0DEF093B4860B-4C1257180004B1B30?OpenDocument, página web de la Convención sobre prohibiciones o restricciones del empleo de ciertas armas convencionales que puedan considerarse excesivamente nocivas o de efectos indiscriminados. Fecha de la consulta 27.09.2016.

Documentos en línea

Altas Partes Contratantes de la CCW, *informe final del período de sesiones de 2013*, [Ginebra], documento CCW/MSP/2013/10, 2013, 11 págs. [en línea] disponible en: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G13/646/36/PDF/G1364636.pdf?OpenElement, fecha de la consulta 31.05.2016

25. En la tercera (3.ª) reunión informal de expertos sobre sistemas de armas autónomas letales celebrada del 11 al 15 de abril de 2016 en la sede de las Naciones Unidas en Ginebra, las delegaciones de los países de Alemania, Costa Rica, España, Estados Unidos, Francia, Israel, Japón, Países Bajos, Reino Unido, Suiza y Turquía fueron enfáticas al señalar que actualmente no existen este tipo de sistemas. Para más información al respecto véase: http://www.unog.ch/80256EE600585943/(httpPages)/37D51189AC4FB6E1C1257F4D004CAFB2?OpenDocument, fecha de la consulta 27.09.2016.

Altas Partes Contratantes de la CCW, Report on the 2016 Informal Meeting of Experts on Lethal Autonomous Weapons Systems, [Ginebra], 2016, 15 págs. [en línea] disponible en: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G16/117/16/PDF/G1611716.pdf?OpenElement, fecha de la consulta 31.05.2016

Comité de la Cruz Roja Internacional (CICR), 31st International Conference of the Red Cross and Red Crescent: International humanitarian law and the challenges of contemporary armed conflicts, [Ginebra], 2011, 53 págs. [en línea], disponible en: https://app.icrc.org/e-briefing/new-tech-modern-battlefield/media/documents/4-international-humanitarian-law-and-the-challenges-of-contemporary-armed-conflicts.pdf, fecha de la consulta 27.09.2016.

CICR, *Views of the International Committee of the Red Cross on autonomous weapon system, [Ginebra], 2016, 8 págs. [en línea], disponible en:* http://www.unog.ch/80256EDD006B8954/(httpAssets)/B3834B2C62344053C1257F9400491826/$file/2016_LAWS+MX_CountryPaper_ICRC.pdf*, fecha de la consulta 27.09.2016.*

Departamento de Defensa de EEUU, Autonomy in Weapons Systems, [Washington], Directiva Nº 30009.09, 2012, 13 págs. [en línea], disponible en: http://www.dtic.mil/whs/directives/corres/pdf/300009p.pdf, fecha de la consulta 27.09.2016.

Gobierno de Canadá, Canadian Food for Thought Paper: Mapping Autonomy, [Ginebra], 2016, 4 págs., [en línea] disponible en: http://www.unog.ch/80256EDD006B8954/(httpAssets)/C3EFCE5F7BA8613BC1257F8500439B9F/$file/2016_LAWS+MX_CountryPaper+Canada+FFTP1.pdf, fecha de la consulta 27.09.2016.

Gobierno de Francia, Cartographie des developpements techniques, [Ginebra], 2016, 3 págs. [en línea] disponible en: http://www.unog.ch/80256EDD006B8954/(httpAssets)/FAC3FC270C9E918EC1257F8F003FF520/$file/2016_LAWSMX_CountryPaper_France+MappingofTechnicalDevelopments.pdf, fecha de la consulta 27.09.2016.

Gobierno de Suiza, A purpose-oriented working definition for autonomous weapons systems, [Ginebra], 2016, 5 págs. [en línea] disponible en: http://www.unog.ch/80256EDD006B8954/(httpAssets)/A204A142AD3E3E29C1257F9B004FB74B/$file/2016.04.12+LAWS+Definitions_as+read.pdf, fecha de la consulta 27.09.2016.

Gobierno del Reino Unido, Statement to the Informal Meeting of Experts on Lethal Autonomous Weapons Systems, [Ginebra], 2016, 6 págs. [en línea] disponible en: http://www.unog.ch/80256EDD006B8954/(httpAssets)/44E4700A0A8CED0EC1257F940053FE3B/$file/2016_LAWS+MX_Towardaworkingdefinition_Statements_United+Kindgom.pdf, fecha de la consulta 27.09.2016.

Heyns, Christof, *Autonomous Weapon Systems: Human rights and ethical issues*, [Ginebra], 2016, 12 págs. [en línea] disponible en: http://www.reachingcriticalwill.org/images/documents/Disarmament-fora/ccw/2016/meeting-experts-laws/statements/heyns.pdf, fecha de la consulta 27.09.2016

Human Rights Watch, *Mind the gap: the lack of accountability for killer robots*, [Ginebra], 2015, 44 págs. [en línea] disponible en: https://www.hrw.org/

sites/default/files/reports/arms0415_ForUpload_0.pdf, fecha de la consulta 27.09.2016.

Instituto de las Naciones Unidas para la Investigación del Desarme (UNIDIR), *Framing Discussions on the Weaponization of Increasingly Autonomous Technologies*, [Ginebra], 2014, 12 págs. [en línea], disponible en: http://www.unidir.org/files/publications/pdfs/framing-discussions-on-the-weaponization-of-increasingly-autonomous-technologies-en-606.pdf, fecha de la consulta 27.09.2016.

Meza Rivas, M., artículo de opinión número 85/2016, Madrid, IEEE, 2016. [en línea], disponible en http://www.ieee.es/Galerias/fichero/docs_opinion/2016/DIEEEO85-2016_SistemasArmas_ONU_MiltonMeza.pdf, fecha de la consulta 27.09.2016.

Mollen, W., *ENIAC: The Army-Sponsored Revolution*, [Washington], Laboratorio de Investigación de la Armada de los Estados Unidos de Norteamérica, 2016. [en línea]. Disponible en: http://www.arl.army.mil/www/default.cfm?page=514&url=http://ftp.arl.army.mil/~mike/comphist/96summary/, fecha de la consulta 27.09.2016.

Organización de las Naciones Unidas (ONU). Protocolo I adicional a los Convenios de Ginebra de 1949 (1977) relativo a la protección de las víctimas de los conflictos armados internacionales. [en línea] disponible en: https://www.icrc.org/spa/resources/documents/misc/protocolo-i.htm#8, fecha de la consulta 27.09.2016.

Organización del Tratado Atlántico Norte (OTAN), The Secretary General's Annual Report 2015, [Bruselas], 2016, 128 págs. [en línea], disponible en: http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_01/20160128_SG_AnnualReport_2015_en.pdf, fecha de la consulta 27.09.2016.

Scharre, P., *Autonomous Weapons and Operational Risk*, [Washington], Centro por una Nueva Seguridad Americana, 2016, 55 págs. [en línea], disponible en: https://s3.amazonaws.com/files.cnas.org/documents/CNAS_Autonomous-weapons-operational-risk.pdf, fecha de la consulta 27.09.2016.

The Stockholm International Peace Research Institute, *World military spending resumes upward course, says SIPRI*, [Estocolmo], 2016, 78 págs. [en línea], disponible en: https://www.sipri.org/media/press-release/2016/world-military-spending-resumes-upward-course-says-sipri, fecha de la consulta 27.09.2016.

BLOQUE II:

TERRORISMO INTERNACIONAL

CONTRATERRORISMO Y REORIENTACIÓN DE LAS FUERZAS ARMADAS EN MISIONES DE SEGURIDAD INTERIOR. NUEVA ESTRATEGIA DE SEGURIDAD PARA UNA NUEVA FORMA DE CONFLICTO EN EL SIGLO XXI

José Antonio Herráiz Reyes
Néstor Soiza Vázquez

Resumen

Consecuencia de la estrategia global impuesta por el Sistema de Seguridad Internacional, se aprecia una dificultad real para deslindar los conceptos de defensa y el de seguridad, generándose un solapamiento de los citados conceptos y procedimientos tanto los relativos a la defensa como los concernientes a la seguridad, que se podrían agudizar durante el siglo XXI si persiste la falta de voluntad política para su potenciación y modernización. Esta situación derivará en una pertinaz presencia de grupos terroristas fundamentalistas yihadistas de corte islamista y en otros casos en un incremento de grupos narcoterroristas vinculados al crimen organizado y al tráfico de drogas, todos estos fenómenos potenciados por la inhibición forzada del «Estado de Derecho», en países con carencias institucionales o afectados por la pertinaz crisis económica. Esta situación en un mundo global genera «per sé» una dificultad para la gobernabilidad democrática de los territorios, promoviendo un incremento de la violencia e incapacidad del «Estado de Derecho» para atender al conjunto de la sociedad.

Palabras clave

Contraterrorismo, Fuerzas Armadas, Seguridad Interior, Ciberdefensa.

1. El futuro una realidad prospectiva

Desde una perspectiva histórica, superada ya la década en la que se produjeron los atentados del 11-S, debemos aceptar que el pensamiento estratégico ha sufrido una transformación esencial, consecuencia de las tácticas, técnicas y procedimientos impuestos por el terrorismo transnacional. En un escenario geopolítico

convulso que sufre cambios fundamentales a causa, en parte, por las decisiones estratégicas consecuencia del atentado y de una profunda crisis económica que atenaza las economías del mundo desarrollado; nos presenta un espacio global con un ambiente geoestratégico, que siente cómo el centro de gravedad del poder mundial se desplaza hacia el continente asiático y que muestra cómo ese poder, se diluye en un escenario con más actores implicados para cada gestión de crisis, algunos de los cuales con gran influencia mediática que además se sitúan fuera del control y ámbito estatales (López, 2004: 208).

La seguridad y la defensa deben ser contempladas respetando y considerando el contexto, social, histórico, cultural y geopolítico. Esta consideración ha sido especialmente evidente en las últimas décadas del siglo XX donde las perspectivas tradicionales para entender la seguridad internacional están siendo cuestionadas tanto desde el ámbito académico como desde el político (Buzan, 1991). [Un texto más reciente que trata las diferentes perspectivas teóricas en cuanto a seguridad en (Smith, 2005)].

Este proceso de globalización ha forzado la modificación de los paradigmas con los que se diseñan las relaciones de poder en el marco internacional y sus incidencias en los espacios regional y nacional. Una de las trabas fundamentales está relacionada con la fragmentación del conocimiento y su necesidad de depurar, integrar y compilar la información disponible, para proporcionar una perspectiva integral del problema con capacidad real de incorporar el perfil multidimensional de estos fenómenos desde la requerida visión global.

En los asuntos que abordaremos en esta comunicación, especialmente haremos referencia al contexto de seguridad y defensa, con especial incidencia en aquellas tendencias internacionales y regionales que conducen hacia una óptima gestión de las crisis internacionales que hoy nos preocupan, proponiendo un control más eficiente y la desarticulación de los posibles conflictos, mediante una coordinada actuación multilateral expresada en tratados, acuerdos, compromisos, declaraciones y protocolos de actuación.

En este marco de referencia en la década de 1990 se consideraba que si:

> «…lo multilateral se impone como tendencia en la resolución de los conflictos, la cooperación tendrá el mayor espacio y los dividendos para la paz serán más profundos» (Rojas, 1992: 21-26).

Continuando con aquellas tendencias internacionales y regionales, después de las transformación experimentada en el sistema de seguridad internacional, resulta recomendable conservar algunos de los componentes del concepto de «seguridad cooperativa», principalmente sus fundamentos esenciales y los objetivos propuestos, que habían quedado truncados en su desarrollo por las políticas unilaterales durante la administración Bush y más recientemente por las acciones multilaterales aprobadas por los miembros de la OTAN, en los límites del derecho internacional que la citada organización se impuso desde su fundación (Rojas, 2012: 70).

Entre estos fundamentos esenciales encontramos el multilateralismo y la acción consensuada en el sistema internacional de seguridad, que aconsejan la redefinición del concepto a la vista de los nuevos tipos de conflicto emergentes a nivel global. Esta redefinición debe buscar su vinculación con una visión de futuro referida a los posibles escenarios estratégicos regionales en los cuales se podría ver involucrada la OTAN y la Unión Europea.

El concepto de la «seguridad cooperativa» no fue la creación de un analista internacional, de un estratega, politólogo o autoridad política. Este concepto se fue acuñando durante las últimas dos décadas, mediante un proceso de evolución del pensamiento estratégico en la medida que se iban asimilando los cambios que se producían en el contexto internacional. En cualquier caso con la finalización de la confrontación Este-Oeste y con la liberación de las interrelaciones económicas entre los estados, derivada de la adopción de la economía de libre mercado como política de intercambio a escala global, surgió la necesidad de redefinir el planteamiento estratégico tradicional en materias de seguridad, de manera que se definiese un nuevo modelo que permitiese conservar la paz que inicialmente presentaba la transformación del mundo bipolar en otro unipolar, unido a una generalizada reducción de los contingentes militares diseñados para una trasnochada guerra global (Hardy, 2003: 2).

Este concepto de seguridad cooperativa, ha sido definido como:

> «…un sistema de interacciones interestatales que, coordinando políticas gubernamentales, previene y contiene las amenazas a los intereses nacionales y evita que las percepciones que de éstas tienen los diversos Estados se transformen en tensiones, crisis o

abiertas confrontaciones» (Varas, 1995), (Pellicer, 1995: 25, 26), (Carter; Perry; Steinbruner, 1992).

Este mismo concepto plantea la búsqueda de fórmulas de consulta en vez de confrontación; seguridad y confianza, en lugar de disuasión; transparencia, en vez de ocultamiento; prevención, en vez de corrección e interdependencia en vez de unilateralismo (Evans, 1994: 7).

Esta «seguridad asociativa» o la «asociación para la seguridad», debe recuperar los elementos esenciales, el ADN de la seguridad cooperativa, para desarrollar un concepto eficiente que sea de utilidad, en el marco de una transición en las relaciones de poder globales que se prevé extendida en el tiempo y que tomará caminos en ocasiones divergentes para satisfacer las diferentes dimensiones (militar, política, económica, social y cultural) de la citada seguridad cooperativa. En ese sentido, un objetivo básico será configurar un concepto teórico que pueda facilitar la conducción del planeamiento estratégico conjunto de los países que nos importan para esta comunicación (Rojas, 2012: 70, 71).

Esta «seguridad cooperativa» se sustenta en la promoción y fortalecimiento de medidas de fomento de la confianza entre los estados que promuevan una mayor transparencia en sus relaciones, a través de la mediación de organismos internacionales como las Naciones Unidas, así como en la promoción de políticas generales necesarias para facilitar la prohibición del empleo de las armas de destrucción masiva (químicas y biológicas); la desmilitarización de los territorios mediante el almacenamiento del armamento convencional, procurando su uso exclusivo como recurso del derecho a la legítima defensa de cada estado y la participación en fuerzas multinacionales para el establecimiento, mantenimiento o consolidación de la paz (Dichera; Esteban, 1994) (Varas; Caro, 2000: 217) (Delamar; Rojas, 1998).

Una vez presentada la necesidad de esta «seguridad cooperativa», nos centraremos en los efectos que el atentado del 11-S provocó en las relaciones institucionales internacionales, que han establecido de *facto* una visión estratégica posicional, multilateral y legitimada, en la que no se admite desde el citado incidente la falta de atención o desinterés de la sociedad, siendo a la vez causa y consecuencia de la evolución del panorama estratégico. En este panorama tan concreto, la fortaleza fundamental del

terrorismo transnacional, es su capacidad de manifestarse como expresión del momento de la fragmentación que experimentan amplias regiones del planeta en el proceso de globalización. Si la fuerza del terrorismo internacional radica en su capacidad para representar en el terreno político-estratégico el momento de la fragmentación, la respuesta al mismo en el marco de la estrategia internacional será acentuar y consolidar el proceso de integración hasta absorber e imbricar a los sectores y regiones que se manifiesten en el momento de la fragmentación y marginación (Dichera; Esteban, 1994) (Varas; Caro, 2000: 217) (Delamar; Rojas, 1998).

De todo lo hasta aquí expuesto, podemos destacar que el objetivo estratégico de este tipo de acciones, no puede ser otro que invertir la situación de ingobernabilidad creciente del sistema de seguridad internacional, para lo cual la clave del éxito deberá ser la recuperación institucional de los estados en proceso de descomposición y su integración en el contexto de la seguridad mundial. De este objetivo estratégico se obtiene la necesidad de iniciar un camino en el proceso de globalización que incluya la dimensión política, pues aquellos estados que no logren controlar efectivamente sus espacios territoriales y marítimos, serán proclives a ofrecer ambientes propicios para el asentamiento de grupos fundamentalistas que servirán de cuna a otros terroristas. Por esta razón, la presencia de estos grupos en el territorio de un estado más que el resultado de una política deliberada, es la muestra de que el mismo ha iniciado su proceso de descomposición. De aquí la atención e interés que el mundo desarrollado y los socios de la OTAN, prestan a estos estados con dificultad para controlar su territorio, con graves carencias institucionales o financieras, pues los estados fallidos o con graves disfunciones institucionales no son solamente un problema humanitario, sino también problema de seguridad nacional para los EE.UU. y por extensión para el conjunto de la comunidad internacional, entre la que analizaremos la Comunidad Europea.

Considerados los apartados anteriores, podríamos concluir que, este modelo de estrategia de seguridad exige para garantizar la seguridad interna del mundo occidental, crear un sistema de seguridad global, que implique al conjunto de países de la comunidad internacional. Como referencia destacar que fruto de esta interacción internacional durante el conflicto iraquí, se modificaron los objetivos iniciales de la operación, que no buscaban

exclusivamente la derrota de las fuerzas militares del régimen de Sadam Hussein, sino la remoción del régimen político iraquí y el establecimiento en su lugar de un moderno sistema institucional, político, económico y financiero, tutelado por la comunidad internacional, lo que significaba implícitamente por los EE.UU.

2. Nueva estrategia de seguridad para otra forma de conflicto

La necesidad de una nueva estrategia de seguridad se originó como consecuencia derivada del atentado a las Torres Gemelas del 11 de septiembre de 2001, el cual impuso un diseño específico para librar un tipo de guerra totalmente diferente de las precedentes. Una de sus características diferenciadoras es la variedad de los grupos étnicos, sociales y políticos involucrados que la hacen diferente del patrón tradicional de la guerra clásica entre estados; este factor profundiza una tendencia que emergió durante la década de 1990 con la progresiva extinción de los conflictos inter-estatales y la intensificación de los intraestatales.

Este atentado, demostró que ni los Estados Unidos ni la OTAN, ni ningún otro país u organización, disponían de una estrategia eficaz para hacer frente a ese tipo de terrorismo internacional. Las estrategias son ideas, capacidades, planes y procedimientos para alcanzar objetivos (Elosúa; García, 1993: 11). Hasta ese momento, las ideas se basaban en la disuasión del final de la «Guerra Fría» y utilizaban básicamente capacidades militares concebidas para conflictos convencionales y nucleares. Nada de lo anterior es adecuado para hacer frente a organizaciones terrorista como *Al Qaeda*, *Daesh* o *Boko Haram*; con una estrategia global basada en la manipulación de ideologías yihadistas, capaz de coordinar y ejecutar grandes atentados, solo limitado por las capacidades disponibles y por los intereses de su estrategia global en cada momento.

Este tipo de violencia desplegada por estos grupos, no es posible en la actuación de otros actores, ya que estos se encuentran controlados por sus respectivos parlamentos o por dirigentes que necesitan del apoyo internacional para alcanzar sus objetivos. La violencia del grupo terrorista fundamentalista de corte religioso islamista es dispersa, fragmentada y está orientada contra el ciudadano, como infiel que no merece su respeto como enemigo y

no contra las fuerzas militares convencionales. El objetivo de estas acciones violentas no es la ocupación de un territorio, como se contemplaba en los conflictos armados anteriores, sino el asalto al poder político a través de la propagación del terror y el odio étnico-religioso. Los objetivos políticos de antaño ahora están ligados a unas acciones extremadamente violentas que sufre específicamente la población civil de forma deliberada, soslayando el criterio de daños colaterales que esgrimían los conflictos precedentes.

Estamos ante un terrorismo que busca causar gran número de víctimas inocentes con atentados que socaven la moral del enemigo y su capacidad de respuesta «democrática». Ante este grave panorama internacional, la mayoría de los gobiernos occidentales se vieron obligados a reconsiderar su política de seguridad nacional (Irigaray, 2013).

Pero cabría preguntarse cómo han evolucionado esas estrategias en el ámbito político y en el militar. Para centrar el asunto debemos señalar que los gobiernos en esas circunstancias tan comprometidas, rara vez están en condiciones de implementar nuevas estrategias que supongan un cambio radical con las precedentes, porque esta forma de actuar implica en la mayoría de los casos una ruptura con el pensamiento social de sus ciudadanos y con las estructuras establecidas, pero además, los recursos disponibles condicionan las estrategias y procedimientos que deberán emplear. Como síntesis de lo hasta aquí esbozado, estos gobiernos que sufren el ataque del terrorismo más despiadado, se ven abocados en la mayoría de los casos a desarrollar políticas nacionales continuistas o en el peor de los casos, sin rupturas traumáticas con el concepto estratégico nacional aprobado por sus respectivos parlamentos.

Un ejemplo de lo anterior los tenemos en el caso argentino, que hasta el año 2013 el Senado de este país no sancionó el proyecto de ley para formalizar un acuerdo argentino-iraní para crear la Comisión de la Verdad, que revise la investigación judicial sobre el atentado terrorista a la AMIA en 1994. Recordar que la justicia argentina acusa por ese ataque al grupo libanés *Hizbulá* y atribuye la coordinación del mismo a ocho altos cargos del gobierno iraní de la época (el actual ministro de Defensa y ex jefe de la fuerza *Al Quds*, Ahmah Vahidi, un ex presidente y seis ex funcionarios del mismo gobierno). Si se aprueba por ambos países, la citada

«Comisión de la Verdad» esta sería integrada por dos juristas de cada país y uno de otra nacionalidad, que analizarían la documentación presentada por la justicia argentina a la parte iraní (Irigaray, 2013).

Desde un primer momento, Israel no dudó en relacionar este atentado con el cometido el 11-S, de ahí que el embajador israelí en Buenos Aires, Danny Ayalon, consideró el atentado en Argentina como el inicio de una ola de atentados que culminaron en el magnicidio del 11-S (Entrevista a Danny Ayalon, Clarín, 17 de marzo de 2012).

Otro ejemplo lo tuvimos después de los atentados del 11-S, donde las nuevas políticas y sus estrategias derivadas tampoco fueron rupturistas, pero generaron una aceleración en los ajustes estratégicos. Estos se fundamentaron en la conmoción de la opinión pública estadounidense, que se mostró proclive a defenderse con todos los medios a su alcance; y eso confluyó con la doctrina Rumsfeld, que preconizaba operaciones rápidas y decisivas contra el régimen talibán para acabar con el santuario de *Al Qaeda* e incluso contra el régimen iraquí de Sadam Husein. El éxito inicial tras eliminar el régimen talibán en una semana, concedió gran reconocimiento al instrumento militar que gozó desde ese momento de un merecido protagonismo en la lucha contra el terrorismo, y así se reflejó en la Estrategia de Seguridad Nacional aprobada por el presidente Bush en septiembre de 2002, que propugnaba la guerra global contra el terrorismo (Departamento de Estado EE.UU., 2002: 2).

Muchos analistas contemporáneos estudian este fenómeno desde el prisma de la guerra asimétrica, pues en definitiva la estrategia principal diseñada por los grupos terroristas se apoya en acciones de naturaleza asimétrica (Castro, 2003) (Centro Superior de la Defensa, 2011). Como en toda acción que busca conquistar y consolidar un objetivo operacional viable, la estrategia operacional del conflicto asimétrico se fundamenta en reconocer y destruir el centro de gravedad del adversario, es decir, identificar su principal debilidad para contrarrestar su fortaleza. La esencia de este tipo de estrategia se basa en discernir en cada fortaleza una debilidad y en cada debilidad una fortaleza (Castro, 2003) (Centro Superior de la Defensa, 2011). Esta debilidad puede identificarse en algunos casos a través de un razonamiento de inteligencia táctica militar, en otros de inteligencia operacional

militar y en la mayoría de inteligencia estratégica de los respectivos gobiernos que puede presentarse en varias caras del mismo prisma, con características militares, políticas, económicas, sociológicas o psicológicas.

En este contexto, el grupo que atentó el 11-S, logró identificar y atacar el centro de gravedad que históricamente diferenció a los Estados Unidos del resto del mundo civilizado. Ese centro de gravedad que diferenciaba a los EE.UU en materia estratégica, era su sentido de aislamiento y seguridad, que le proporcionaba su posición en el continente americano rodeado por los dos grandes océanos y con vecinos actualmente poco o nada beligerantes, con excepción de la diminuta Cuba (Castro, 2003) (Centro Superior de la Defensa, 2011).

El territorio continental norteamericano desde su consolidación como estado independiente nunca sufrió una amenaza militar exterior, permaneciendo distanciado de los conflictos europeos del siglo XIX y XX por el océano o por la flota británica. A lo anterior hemos de añadir que sus vecinos (Méjico, Cuba) siempre fueron mucho más débiles en capacidad militar o aliados incondicionales como Canadá. Esta seguridad estratégica se consideraba garantizada por su tradicional aislamiento geoposicional, pero cuando se producen los atentados del 11-S con más de 3.000 víctimas en Nueva York, número que superan a las bajas norteamericanas en el ataque japonés contra *Pearl Harbour*. El 7 de diciembre de 1941, los norteamericanos sufrieron 3.400 bajas con 2.300 muertos. El ataque dañó seriamente el poder naval y aéreo norteamericano en el Pacífico. A esto se agrega una diferencia sustantiva: las bajas que se produjeron en 1941 era personal militar que se encontraba enfrentando una acción de guerra convencional en territorio insular estadounidense (Ocaña, 2003), en ese momento desapareció el concepto inmutable de seguridad del territorio continental norteamericano.

Para combatir en este tipo de conflicto asimétrico, la estrategia diseñada por la administración norteamericana y aprobada por su presidente George Bush en septiembre de 2002, está considerada por los analistas como la primera de Seguridad Nacional propiamente dicha, ya que contemplaba el empleo de todos los instrumentos del estado, tanto civil como militar (Ballesteros, 2013: 32). Se trataba de una estrategia proactiva, más partidaria del ataque que de la defensa, en la que: *«En el nuevo mundo en*

que hemos entrado, el único camino hacia la paz y la seguridad es el de la acción» (Departamento de Estado EE.UU., 2002: 2) llegando a asumir el empleo del ataque preventivo.

Una de las principales innovaciones de estas nuevas estrategias de seguridad nacional, es generar otras de nivel inferior y de carácter transversal, como la estrategia contraterrorista. En este sentido señalar que en la Cumbre de Praga de la OTAN, celebrada en noviembre de 2002, se aprobaron importantes cambios para adaptar las estructuras de fuerzas a la nueva amenaza y escasamente un mes después, los países aliados acordaron su Concepto Militar contra el terrorismo, aprobado en diciembre de 2002 (Fernández, 2006: 7). Conocido como documento MC-472, recoge la posibilidad del ataque preventivo fuera de área, pero ante las reticencias de numerosos países causadas por las diferentes ópticas y sensibilidades sobre este tema, el documento recoge dicha posibilidad pero lo deja a criterio de las naciones.

Esta nueva clase de conflicto expresa la interdependencia que caracteriza al mundo globalizado contemporáneo. El contrasentido inicial es que mientras que el terrorismo actúa aprovechando la lógica de la globalización, los gobiernos occidentales se han defendido aplicando la lógica donde predomina la racionalidad estatal, entre otras consideraciones la que sus parlamentos le autorizan. Estamos tratando con terroristas suicidas formados en las mejores escuelas de ingeniería del mundo occidental, capaces de pilotar aviones muy sofisticados como los Boeing 757 y de elaborar y planificar estrategias con continuidad en el tiempo (el plan del atentado del 11-S se diseñó durante más de dos años). Considerando estos antecedentes, hemos de considerar que la respuesta institucional que autoriza un Estado-Nacional, es insuficiente frente a este fenómeno de conflicto asimétrico que se infiltra en redes globales y que explota las debilidades institucionales de los países occidentales, para ejecutar sus acciones y alcanzar sus objetivos en el marco de su estrategia global.

Por su parte, los gobiernos de los países amenazados por el terrorismo islamista, conscientes de su debilidad estratégica frente a este tipo de terrorismo yihadista, han ido adaptando sus estrategias de defensa a estrategias de seguridad, en la que los estados aprovechan todo su potencial civil y militar para lograr ser eficaces ante la amenaza presentada. En marzo de 2008, Gran Bretaña sancionó su primera Estrategia de Seguridad Nacional y

en junio de ese año Francia hacía público su Libro Blanco de la Defensa y Seguridad Nacional. En marzo de 2009, el Gobierno británico, promulgó su Estrategia Británica contra el Terrorismo Internacional y el Gobierno español aprobó la Estrategia Española de Seguridad en junio de 2011 (Ballesteros, 2013: 32).

Por ello, la administración norteamericana ha rediseñado el concepto tradicional del conflicto, pues hasta hace unas décadas sólo se consideraban conflictos aquellos que involucraban a entidades territoriales definidas como estados. La amenaza yihadista ha forzado la redefinición de los conceptos y naturaleza de los contendientes en los conflictos del siglo XXI. Para ello, el gobierno estadounidense y los organismos de seguridad regionales (OTAN, TIAR[1]), han activado distintos mecanismos políticos y militares, para hacer frente a una amenaza asimétrica que se caracteriza por ser de carácter no estatal y extraterritorial. En este sentido, es significativo reseñar los términos de la declaración de guerra del congreso norteamericano, en la que por unanimidad se autoriza al ejecutivo de ese país a utilizar toda la fuerza necesaria y apropiada contra quienes utilicen el terror contra los intereses norteamericanos allí donde se encuentren estos amenazados (Piovesana, 2011: 20), (Fis, 2008). Esta es la primera vez en la historia moderna desde el comienzo de la era del absolutismo, que una declaración de guerra no se realiza contra una entidad estatal de tipo territorial, sino contra una organización transnacional no territorial, no estatal e incluso contra individuos específicos (Castro, 2003).

En este espacio de asistencia recíproca, los diecinueve estados miembros de la OTAN (en aquel momento), redefinieron el principio de asistencia recíproca contemplado en el artículo 5º del tratado de Washington de 1949 y lo consideraron suficiente para aprobar la respuesta necesaria ante cualquier acción del terrorismo yihadista. Lo mismo ocurrió con el Tratado Interamericano de Asistencia Recíproca (TIAR) en la aplicación de los artículos 2.º y 3.º del mismo. En estos se menciona expresamente que para convocar a la asistencia recíproca se debe estar frente al ataque de un país extra-hemisférico. Al igual que en el caso de la OTAN con el artículo 5.º, se ha reinterpretado los artículos 2.º y 3.º, en-

1. IAR (Tratado Interamericano de Asistencia Recíproca). Firmado en Río de Janeiro en 1947.

tendiendo que el concepto de estado territorial extra-hemisférico queda subsumido en la novedad histórica, que es el ataque del terrorismo transnacional (Castro, 2003).

El Tratado Interamericano de Asistencia Recíproca (TIAR), conocido por el Tratado de Río, es un pacto de defensa mutuo interamericano firmado el 2 de septiembre de 1947 en Río de Janeiro. El área geográfica de acción del tratado, comprende a América y 300 millas desde la costa, que incluye la región entre Alaska, Groenlandia, en el norte y en la zona ártica hasta las islas Aleutianas. En el sur las regiones antárticas y los islotes de San Pedro, San Pablo y la Isla de Trinidad (detallado en artículo 4 del Tratado). Según el artículo 3.1 en caso de (...) «un ataque armado por cualquier Estado contra un Estado Americano, será considerado como un ataque contra todos los Estados Americanos y en consecuencia, cada una de las Partes Contratantes se compromete a hacer frente al ataque en ejercicio del derecho inmanente de legítima defensa individual o colectiva que reconoce el Artículo 51 de la Carta de las Naciones Unidas». Es el primer tratado de su tipo después de la segunda guerra mundial. La firma del Tratado del Atlántico Norte se realizó en el año 1949. El TIAR no ha sido sancionado por la totalidad de los estados miembros de la Organización de Estados Americanos. En el TIAR, el Consejo Permanente de la OEA actúa como organismo de coordinación y mecanismo de consulta, aunque sólo participan en la votación las partes contratantes del TIAR. El Consejo es el encargado de evaluar si existen las condiciones para convocar una reunión de consulta de los integrantes del TIAR o la aplicación de las medidas correspondientes. La firma del TIAR fue una de las razones por las que Costa Rica disolvió su ejército en 1948, al considerar las previsiones del Tratado como garantía suficiente para asegurar su defensa nacional.

El TIAR ha sido invocado al menos una veintena de ocasiones durante las décadas de 1950 y de 1960 (Salas, 1962), especialmente durante el bloqueo a Cuba en 1962 y la guerra entre Honduras y El Salvador en 1969 (De Blas, 2000: 518) sin embargo nunca fue invocado durante las amenazas de la«Guerra Fría». La invocación en la época objeto de la investigación fue como consecuencia derivada del magnicidio del 11 de septiembre de 2001 (Griffiths, 2011: 23).

En el caso de la guerra de las Malvinas en 1982,se convocó por parte argentina a los países signatarios, pero los EE.UU. miembro del TIAR como de la OTAN, prefirió cumplir las obligaciones

derivadas de sus compromisos internacionales con sus aliados europeos de la OTAN, de la que el Reino Unido la otra parte en litigio era miembro, esta decisión se interpretó en Argentina como una traición de Estados Unidos (Klauer, 2005: 117).

Una de las razones presentada por los EE.UU., para no asumir en aquella ocasión los compromisos contraídos con el TIAR, fue que Argentina inició el conflicto armado para recuperar por la fuerza las islas Malvinas —territorio en litigio administrado por el Reino Unido—, por tanto no procedía su aplicación en este caso; similar fue la posición adoptada por chilenos y colombianos, que también adujeron el carácter defensivo del tratado acorde con su artículo 3.1. Como complementario de lo anterior, presentamos la resolución 502 del Consejo de Seguridad de las Naciones Unidas, que exigió la retirada de la fuerza ocupante argentina como condición para cualquier proceso de negociación. Esto no significó la retirada o suspensión temporal de los EE.UU. del TIAR al no presentarse un comunicado oficial ante la OEA de su renuncia como parte (Art. 25 del TIAR). Fue un no cumplimiento *de facto* de las obligaciones del tratado (García, 2013).

No obstante, la condición del tratado como instrumento de defensa multilateral para el continente americano quedó deslegitimado, razón por la que México renunció al tratado en 2002 (Bodemer, 2005: 66-68). El 5 de junio de 2012 los presidentes del ALBA anunciaron que los miembros de esta unión también se retiraban del Tratado (Prensa Latina, 2012).

Los países que conforman el TIAR son los expresados a continuación (incluye fecha de adhesión); Argentina (1947), Bolivia (1947 / Renunció al TIAR el 5 de junio de 2012), Brasil (1947), Chile (1947), Colombia (1947), Costa Rica (1947), Cuba (1947), EE. UU. (1947), El Salvador (1947), Guatemala (1947), Haití (1947), Honduras (1947), México (1947 / Renunció al TIAR el 6 de septiembre de 2002), Panamá (1947), Paraguay (1947), Perú (1947 / Denunció al tratado el 22 de enero de 1990 y retiró la denuncia el 16 de diciembre de 1991), República Dominicana (1947), Uruguay (1947), Venezuela (1947 / Renunció al TIAR el 5 de junio de 2012), Nicaragua (1948 / Renunció al TIAR el 5 de junio de 2012), Ecuador (1949 / Renunció al TIAR el 5 de junio de 2012), Trinidad y Tobago (1967), Bahamas (1982).

Después de la guerra de la Malvinas fueron muchas las voces que se alzaron contra la permanencia de Argentina dentro de este

Tratado, sin embargo tras el 11-S el tratado renació, pues se consideró aquel atentado como un ataque contra todos los estados del continente americano, no obstante, Estados Unidos nunca solicitó una colaboración tácita en el ataque al gobierno talibán en Afganistán, pero desde aquella hora, este se consagraba como instrumento contra el terrorismo internacional.

3. Sistema de seguridad global. Política exterior y de seguridad de los EE.UU.

La situación detallada en apartados anteriores y el magnicidio del 11-S, como parámetros determinantes, aconsejaron a la administración norteamericana modificar las prioridades de su política exterior, situando en primer plano la seguridad de su territorio, de sus intereses y de sus ciudadanos en cualquier punto del planeta. El sistema de poder estadounidense considerado como el conjunto armónico que integra su espacio político, el empresarial, los medios de comunicación social en su más amplio espectro, el sistema de conocimientos que aglutina como un todo a universidades y centros de investigación, indujeron a la opinión pública norteamericana a una conclusión necesaria para aquellos momentos de dolor y consternación nacional: la única estrategia que garantiza el mantenimiento de la seguridad interior de los Estados Unidos es la promoción institucional de un sistema de seguridad global, ya que un conflicto bélico convencional no se considera actualmente eficiente en cualquier circunstancia. De hecho, Estados Unidos ha destinado durante las dos últimas décadas a su seguridad interior, buena parte de sus efectivos militares, fuerzas que antes desplazaba a los más diversos escenarios internacionales, en este caso encontramos a los «marines» que se podrán desplegar en territorio norteamericano ante cualquier amenaza terrorista. No obstante, todo ello sin olvidar, que también será necesario mantener la presencia militar fuera de sus fronteras.

Sólo así la comunidad internacional puede aceptar la campaña militar en Afganistán, catalogada como respuesta inmediata al atentado del 11-S, aún siendo conscientes del desastre militar que supuso para la extinta Unión Soviética un conflicto a gran escala en el citado territorio. Para ser coherentes con su política exterior, tuvo que ampliar y adecuar sus objetivos estratégicos más allá de sus fronteras incluyendo en la nueva lucha contra el

terrorismo global aquellos países ajenos al sistema internacional, los denominados *rogue state* (estados parias), preferentemente aquellos que mostraran capacidades tecnológicas para desarrollar o que ya hubiesen desarrollado armas de destrucción masiva, sea nuclear, química o biológica. Los países identificados con la metáfora del «Eje del Mal», fueron Irak, Irán y Corea del Norte.

Esta modificación impuesta por las circunstancias en la concepción de la seguridad de los Estados Unidos es consecuencia directa de la presencia de nuevas perspectivas y flujos de interés en el plano estratégico, que referida al liderazgo estadounidense en el mundo occidental, condiciona las estrategias del conjunto de países aliados del denominado mundo libre.

¿Cuál será para nuestra comunicación el punto de partida de este nuevo diseño de las estrategias principales, consecuencia de los atentados terroristas del 11 de septiembre? Esencialmente los atentados del 11-S y la decisión de la administración norteamericana de organizar en el planeta un sistema de seguridad global, fueron consecuencia derivada del proceso de desestabilización de las estructuras político económica que mostró el mundo durante la década de 1990.

En este contexto diseñar una política exterior norteamericana para el continente en los albores del siglo XXI, irremisiblemente nos lleva a la consulta de documentos oficiales y contrastar opiniones y declaraciones de analistas e investigadores del asunto, en este caso con respecto a las prioridades de la política exterior de los EE.UU., Jeffrey E. Garten, sostenía que:

> «...en el futuro los EE.UU. ya no dependerán exclusivamente de Europa y Japón, sino también de diez países que ya no pueden ser considerados subdesarrollados, sino emergentes» (Blanch, 2000: 122).

Asimismo, también considera que:

> «...el gobierno norteamericano mantendrá su tendencia hacia Europa en asuntos geopolíticos y la relación con Latinoamérica continuará en manos de profesionales, que tendrán sus propias dificultades para captar la atención de los líderes políticos que son su jefes» (Blanch, 2000: 122).

Cómo síntesis de lo expuesto, podemos afirmar que EE.UU. no consideraba a corto plazo la situación de América Latina como

una de sus prioridades vitales inmediatas, según se desprende de la nueva política de Seguridad de los EE.UU (Castro, 2003) y que el asunto ALCA, quedaba incluido en un escenario económico supeditado a la evolución política de la crisis social que padecía el subcontinente.

4. La doctrina militar dual: nuevas tendencias contraterroristas

La doctrina militar dual tiene su origen en la denominada Doctrina Powell[2] (García, 2001: 21, 22), que analizaremos someramente desde su aplicación en un conflicto con presencia de fuerzas militares en oposición, como el caso de las guerras de la coalición internacional contra Irak y el caso de acciones contraterroristas contra el yihadismo islamista; para el primer caso apuntaremos que el secretario de estado norteamericano Collin Powell y la asesora de seguridad Condoleza Rice, declararon en los medios de comunicación social que el traspaso de poder a los iraquíes se realizaría dos o tres meses después de la caída del presidente Sadam Hussein (Reese; Wright, 2008: 156). Frente a esta declaración, el jefe de estado mayor del ejército norteamericano, general Shinseki, manifestó su preocupación por las dificultades que deberían superar:

> «Estamos hablando de controlar, una vez concluidas las hostilidades, un territorio geográficamente muy considerable, afectado por el tipo de tensiones étnicas que pueden conducir a otro tipo de problemas. Por tanto […] se requiere una presencia significativa de tropas sobre el terreno» (Ballesteros, 2013: 33).

Durante este mismo conflicto, el vicesecretario de defensa norteamericano Wolfowitz manifestó su opinión contraria a la expresada por el general Shinseki:

2. Esta doctrina propugna la utilización de la fuerza militar en forma aplastante con el fin de asegurar la victoria con un mínimo número de bajas. El concepto de Fuerza Decisiva, conocido como «Doctrina Powell», se puede estudiar en su diseño final en el NMSD de 1992 como una concepción entendida para operaciones militares a gran escala, sobre las conclusiones aprendidas de la Guerra del Golfo: véase Blackwell, James et al. The Gulf War: Military Lessons Learned. Interim Report of the CSIS Study Group on Lessons Learned from the Gulf War, Washington DC. 1991.

> «Resulta difícil concebir que vayan a necesitarse más fuerzas para proporcionar estabilidad al Irak posterior a Sadam, que las que se requerirían para librar la propia guerra» (Parker, 2010: 431).

Precisamente la estabilización y consolidación institucional de Irak fue el primer escenario de experimentación de las nuevas estrategias postconflicto de los EE.UU. El plan diseñado para la estabilización iraquí requirió modificar la estrategia prevista hasta dos veces en cuatro años: la primera, se denominó «Libertad para Irak» en marzo del año 2003, esta fue modificada en noviembre del año 2005, por otra denominada «Para la victoria de Irak» (Ballesteros, 2013: 33).

Ambas estrategias se caracterizaban por asumir los criterios de la «Doctrina Rumsfeld» y también ambas fracasaron en su propuesta de resolución final del conflicto. En enero de 2007, los órganos de planeamiento de EE.UU. necesitaban una nueva estrategia inspirada en los principios del manual de contrainsurgencia de las fuerzas armadas estadounidenses (FM 03-24). Esta nueva estrategia fue denominada «Un nuevo camino hacia delante», que proponía la transferencia de la seguridad a las autoridades locales en agosto de 2010. El criterio derivado de esta última estrategia se basaba en transferir lo más rápidamente posible y con garantías suficientes, la responsabilidad de la seguridad integral a las autoridades locales, aunque siempre contando con la premisa de seguir apoyando a estas autoridades con unas fuerzas armadas y policiales adecuadamente formadas y equipadas. Paralelamente a las premisas anteriores, se discriminaron los tipos de amenazas como *Al Qaeda* de otras con los que cabía la posibilidad de la negociación. El paradigma de este nuevo enfoque fue la «Estrategia de la Anaconda», ideada por el general David Petraus contra *Al Qaeda* en Irak, que tenía como objetivo principal asfixiar a la organización yihadista eliminando sus apoyos económicos, ideológicos y populares entre otros, al tiempo que se negociaba políticamente con la rama sunita no yihadista (Ballesteros, 2013: 33).

En estas últimas décadas del siglo XX e inicio del XXI, las estrategia militar ha evolucionado de los frentes continuos propios de los conflictos tradicionales (Iª y IIª guerras mundiales), capaces de controlar grandes extensiones de terreno a otro tipo de operaciones rápidas y decisivas. En este último tipo de operaciones se combina el movimiento y el fuego de todo tipo de armas

pesadas, con el envolvimiento vertical (utilizando aeronaves de gran maniobrabilidad) y las operaciones en profundidad (que golpean el corazón del despliegue enemigo), que daban paso a las operaciones basadas en efectos (EBAO).

El último paso de esta nueva estrategia consistía en asumir como deseable el concepto de aproximación integral (*Comprehensive Approach*), donde convergen la defensa, la diplomacia y el desarrollo como instrumentos clave necesarios para la estabilización de un territorio en conflicto. Sin duda, el máximo exponente de este nuevo enfoque o aproximación integral son los equipos de reconstrucción provincial actualmente desplegados en Afganistán (Ballesteros, 2013: 33).

Conviene resaltar que los errores estratégicos en el diseño de esta nueva política de defensa, han dificultado la resolución de los conflictos actuales y en gran medida, han complicado la lucha contra el terrorismo internacional. Entre otros factores, porque han consumido un gran esfuerzo militar, económico y político. El caso más evidente de fracaso en el diseño de la estrategia de seguridad nacional, lo tenemos en los atentados del 11-S que mostraron de forma fehaciente como la denominada «Doctrina Powell» (García, 2001: 21, 22), era inapropiada para luchar contra este terrorismo global. No podemos esperar una victoria militar clásica cuando una de las partes en litigio no muestra sus objetivos militares sobre el terreno, utiliza el concepto de la guerra global considerando el planeta como el campo de batalla y dispone de recursos económicos inagotables para reclutar a sus combatientes. No obstante, la «Doctrina Powell» no ha sido descartada, pues incluso en este nuevo espacio de batalla global, puede tener aplicación en los casos de conflictos en espacios geográficos concretos de tipo convencional.

Ante esta carencia doctrinal, para complementar la «Doctrina Powell», los órganos de planeamiento norteamericanos diseñaron una doctrina militar que debería aplicarse exclusivamente en aquellos escenarios donde resultase inapropiada la anterior. Esta doctrina complementaria ha sido publicada en el *Quadrennial Defense Review* o contemplada en la Estrategia de Seguridad Nacional, considerando en ella las premisas necesarias para atajar las acciones del terrorismo yihadista (Departamento de Estado EE.UU., 2002: 6).

El objetivo principal de esta nueva estrategia de seguridad, contemplado en ambos documentos oficiales se justifica en la des-

articulación de estos grupos terroristas, mediante el agotamiento de sus fuentes de financiación y recursos logísticos. Por extensión, uno de los objetivos secundarios pero fundamentales, son aquellos estados, algunos de ellos en descomposición, que facilitan la ocultación y protección de estos grupos. Dada la característica global de la amenaza, la doctrina norteamericana promueve la participación en su estrategia de la mayoría de la comunidad internacional mediante un apoyo logístico real y eficiente, una contribución de fuerzas especializadas en este tipo de combate y la necesaria cooperación en materia de inteligencia.

Esta nueva doctrina establece que el uso de la fuerza, cuando se trate de acciones contraterroristas, se realizará buscando la participación de la comunidad internacional, si no fuese posible esta presencia internacional, la acción contraterrorista se desencadenaría igualmente por las fuerzas armadas norteamericanas. Este criterio se especifica en el capítulo V de su estrategia de seguridad: *«Impedir que nuestros enemigos provistos de armas de destrucción en masa, sean una amenaza para nosotros, nuestros aliados y nuestros amigos»* (Departamento de Estado EE.UU., 2002: 6). En estas circunstancias específicas no se contempla el precepto de la disuasión ya que se trata de estados que, como en el caso de Irak, ya habían utilizado este tipo de armas en el pasado, durante la guerra contra Irán o en la represión contra los kurdos en el Kurdistán iraquí (Mora, 2001: 34).

Otro concepto que marcará un hito histórico en esta nueva estrategia de seguridad será la «legalidad» del uso de las armas de destrucción masiva que se justifica ante este nuevo tipo de enemigo y que contempla la propuesta del «ataque preventivo» (Rojas, 2004: 12), como contrapartida al ataque despiadado del terrorismo global. En este contexto, esta estrategia de seguridad señala que el mayor riesgo no se encuentra en actuar sino en no hacerlo. En este supuesto se enmarca el razonamiento principal de las operaciones militares que se plantearon contra Irak, en las sucesivas guerras del Golfo.

5. Reorientación de las Fuerzas Armadas a misiones de seguridad interior

La consecuencia derivada del ataque del 11-S fue un empleo creciente de las fuerzas armadas en misiones de seguridad interior., para ello los EE.UU. como hemos referido, había finalizado

en septiembre de 2001 una revisión de su política militar frente a las nuevas amenazas, incluida la terrorista.

> «Tenía previsto presentar ese informe ante el Congreso a principios de octubre de 2001, pero como consecuencia de los atentados modificó varios aspectos del informe original, añadiendo la creación del Mando Militar de Defensa Interior, que dependerá directamente de la Junta de Jefes del Pentágono y coordinará todas las operaciones antiterroristas de la armada, la fuerza aérea, el ejército y los marines de los EE.UU.» (Rumsfeld, 2001).

Desde aquel momento el cuerpo de marines constituyó una brigada antiterrorista, la más numerosa con esta especialidad de las fuerzas armadas norteamericanas con unas misiones específicas asignadas en la seguridad interior de los EE.UU., la citada unidad antiterrorista la integra un millar de marines adiestrados para este tipo de misiones y con capacidad de respuesta en 24h.

> «Las fuerzas armadas de Estados Unidos han asumido amplias funciones para salvaguardar la seguridad nacional, en una reestructuración diseñada por el Pentágono tras los atentados del 11 de septiembre, en la misma línea de actuación que la seguida durante los años de la guerra fría. La revisión de la política militar estadounidense, concluida a principios de septiembre con la elaboración del informe *Quadrennial Defense Review*, plantea los retos ante las nuevas amenazas, que incluyen la amenaza terrorista. Pero a este replanteamiento de la defensa se ha sumado, tras los atentados, la creación del Comando Militar de Defensa Interior» («EE. UU. implica a sus fuerzas armadas en la seguridad interior frente a ataques terroristas». *El País*. 1 de octubre de 2001).
>
> «Nuestra nación y sus fuerzas armadas se encuentran en una fase de transformación, después de una década de guerra, hacia un futuro que se presenta con un marco de seguridad paradójico. Mientras el mundo tiende en su conjunto hacia una mayor estabilidad, las tecnologías destructivas se encuentran disponibles para una mayor cantidad y variedad de adversarios. Como resultado, potencialmente, el mundo es más peligroso que nunca» (Dempsey, 2001: 3)[3].

3. *oncepto Capstone de Operaciones Conjuntas: Fuerza Conjunta 2020*. [recurso electrónico]. En www. globalsecurity.org/military/library/policy/dod/joint/ccjojf2020. Pdf. [Consulta: 16-05-2013].

En esta misma reorganización de las fuerzas armadas norteamericanas para atender este nuevo tipo de amenaza, la armada de este país dispuso buques lanza mísiles para la defensa antiaérea de su territorio que desplegó en aquellas zonas de mayor riesgo (tanto en las costas del Atlántico como en las del Pacífico). Asimismo la fuerza aérea desplegó varios escuadrones de aeronaves y personal auxiliar para complementar las misiones de vigilancia aérea de la guardia aérea nacional (Dempsey, 2001: 3). En el entorno europeo destacar la participación de las fuerzas armadas españolas en el control y vigilancia de la línea del ferrocarril de alta velocidad y centrales nucleares cuando la situación lo demandó. Despliegue de las fuerzas armadas francesas después de los atentados de París por las calles de la capital francesa o el de las fuerzas armadas belgas o británicas después de los últimos atentados yihadistas en suelo belga y británico.

Incluida en esta reorganización de la estructura defensiva nacional del sistema norteamericano se inició un proceso de renovación de los servicios de inteligencia, para garantizar su eficiencia contra el nuevo fenómeno terrorista mediante la especialización en la formación de los recursos humanos con capacidad para analizar el nuevo fenómeno y el entrenamiento de agentes con capacidad de infiltración y supervivencia en organizaciones de este tipo. Las medidas esbozadas están destinadas a equilibrar el predominio de la denominada «inteligencia tecnológica», que consistía básicamente en confiar exclusivamente en la obtención de información con los medios técnicos desplegados (satélites, electrónicos o geoposicionales de alerta temprana). Con las medidas propuestas para la obtención, compilación y explotación de información por analistas y especialistas en inteligencia, se reforzarán las capacidades necesarias para combatir eficazmente este fenómeno (Departamento de Estado EE.UU., 2002: 20, 21).

En este sentido, este nuevo tipo de conflicto será librado fundamentalmente por estructuras de inteligencia norteamericanas con el apoyo de sus aliados (OTAN, TIAR…) y en menor medida por otros estados integrados en los sistemas de seguridad internacional. Será una guerra muy diferente a las anteriores y según Collin Powell, consistirá primero en operaciones de inteligencia, segundo en operaciones policiales con grupos especializados antiterroristas y en última instancia, se planearan operaciones militares (Castro, 2003).

6. Terrorismo en la red y ciberdefensa

6.1. *Internet y su incidencia en el fenómeno terrorista*

Internet ha demostrado ser un medio de comunicación sumamente dinámico, que llega a un público cada vez mayor en todo el mundo. El desarrollo de tecnologías cada vez más sofisticadas ha creado una red con un alcance mundial y barreras al acceso relativamente bajas. La tecnología de Internet hace que resulte fácil para una persona comunicarse con relativo anonimato, rapidez y eficacia, a través de las fronteras, con un público prácticamente ilimitado. Los beneficios de la tecnología de Internet son numerosos, comenzando por la facilidad singular con que se comparten información e ideas, lo que está reconocido como derecho humano fundamental. Sin embargo, cabe reconocer que la misma tecnología que facilita dicha comunicación puede explotarse también con una finalidad terrorista. El uso de Internet con fines terroristas genera oportunidades y desafíos en la lucha contra el terrorismo.

Se suele utilizar Internet para promover actos de terrorismo y prestarles apoyo, este enfoque ha dado lugar a la clasificación de seis categorías que suelen solaparse, a saber: la propaganda (incluido el reclutamiento, la radicalización y la incitación al terrorismo); la financiación; el adiestramiento; la planificación (tanto por medio de comunicaciones secretas, como mediante la información de dominio público); la ejecución; y los ataques cibernéticos. A continuación analizamos cada una de estas categorías con mayor detalle.

6.1.1. *Propaganda*

Uno de los principales usos de Internet por los terroristas es la difusión de propaganda. Esta generalmente adopta la forma de comunicaciones de audio y video, que imparten formación ideológica o práctica, dan explicaciones y justificaciones o promueven actividades terroristas. El material puede consistir en mensajes, presentaciones, revistas, tratados, ficheros de video y audio virtuales, y en otras ocasiones juegos de video elaborados por organizaciones terroristas o simpatizantes.

a) Reclutamiento

Internet puede utilizarse no solo como medio para publicar mensajes y videos extremistas, sino también como una forma

de establecer relaciones con un auditorio más receptivo a su propaganda y solicitar su apoyo. El uso de barreras tecnológicas al acceso a las plataformas de reclutamiento, también aumenta la complejidad del rastreo de las actividades relacionadas con el terrorismo por los servicios de inteligencia y las fuerzas del orden.

b) Incitación

Mientras que la propaganda en sí, en general no está prohibida, muchos Estados consideran que el uso de propaganda por terroristas para incitar a cometer actos de terrorismo es ilegal. Internet ofrece material y oportunidades en abundancia para descargar, editar y distribuir contenido que podría considerarse una exaltación ilegal de los actos de terrorismo o una incitación a cometerlos.

Asimismo reseñar que el derecho a la libertad de expresión consagrado en las democracias del mundo occidental, también está vinculado a otros derechos importantes, incluidos los derechos a la libertad de pensamiento, de conciencia y de religión, creencia y opinión.

c) Radicalización

El reclutamiento, la radicalización y la incitación al terrorismo pueden considerarse como puntos a lo largo del camino del itinerario terrorista. En este caso la radicalización se refiere principalmente al proceso de adoctrinamiento que suele acompañar a la transformación de los «reclutas» en individuos decididos a actuar con violencia, inspirados por ideologías extremistas.

6.1.2. *Financiación*

Las organizaciones terroristas y sus partidarios también pueden usar Internet para financiar actos de terrorismo. El procedimiento que los terroristas utilizan Internet para recaudar fondos y recursos, se podría clasificar en cuatro categorías generales: la recaudación directa, el comercio electrónico, el empleo de los servicios de pago en línea y las contribuciones a organizaciones benéficas.

6.1.3. *Adiestramiento*

En los últimos años, las organizaciones terroristas han recurrido cada vez más a Internet como campamento de adiestramiento alternativo de terroristas. Hay una gama cada vez más amplia de medios de comunicación que proporcionan plataformas para la difusión de guías prácticas en forma de manuales en línea, ficheros de audio y video, materiales de información y asesoramiento. Estas plataformas de Internet también ofrecen instrucciones detalladas, a menudo en formato multimedia de fácil acceso y en varios idiomas, sobre temas tales como, el procedimiento de afiliarse a organizaciones terroristas, cómo fabricar explosivos, armas de fuego u otro tipo de artefactos o materiales peligrosos, así como directrices para el planeamiento y la ejecución de ataques terroristas. Estas plataformas actúan como campos virtuales para el entrenamiento del aspirante a terrorista. También se utilizan para compartir, entre otras cosas, métodos, técnicas o conocimientos operativos específicos con el objeto de perpetrar actos terroristas.

6.1.4. *Planificación*

La planificación de una acción terrorista implica la comunicación a distancia entre varias partes interesadas, un caso reciente lo tenemos en Francia, este nos ilustra cómo se pueden utilizar diferentes tecnologías propias de Internet para facilitar la preparación de actos terroristas, incluso facilitando extensas comunicaciones dentro de una misma organización o entre organizaciones que promueven el extremismo violento, sin que las fronteras interestatales supongan un obstáculo.

También se pueden tomar decisiones utilizando Internet para elegir el blanco potencial de un ataque y el medio más eficaz de alcanzar el propósito terrorista. Estas medidas preparatorias pueden ir, desde obtener instrucciones sobre los métodos recomendados de ataque, hasta la reunión de información de acceso público y de otra índole en relación con el objetivo propuesto. La capacidad de Internet para salvar distancias y cruzar fronteras, y el volumen de información a disposición del público en el ciberespacio, hacen de Internet un instrumento ideal para la planificación de actos terroristas.

a) Comunicaciones secretas preparatorias

La función más básica de Internet es facilitar la comunicación, en este sentido los terroristas son cada vez más expertos en la explotación de las tecnologías de las comunicaciones a fin de establecer contactos de manera anónima para la planificación de actos terroristas.

b) Información de dominio público

Las organizaciones y los particulares suelen publicar grandes volúmenes de información en Internet. En el caso de las organizaciones, esto puede ser resultado, en parte, del deseo de promover sus actividades y optimizar su interacción con el público. También se puede conseguir información confidencial, que pueden utilizar los terroristas con fines ilícitos, mediante los buscadores de Internet, que pueden catalogar y recuperar información insuficientemente protegida de millones de sitios web. Además, el acceso en línea a información logística detallada, como el acceso en tiempo real a imágenes de televisión de circuito cerrad, y aplicaciones como Google Earth, que están destinadas a ser utilizadas principalmente por particulares para fines legítimos, pueden ser usadas indebidamente por quienes intentan beneficiarse del libre acceso a las imágenes de satélites de alta resolución, mapas e información sobre territorios y edificios para el reconocimiento de posibles objetivos desde una terminal de computadora remota.

Especialmente en la era de los populares medios de comunicación de las redes sociales como *Facebook, Twitter, YouTube, Flickr* y plataformas de blogs, muchos usuarios publican por Internet, voluntaria o involuntariamente, una cantidad sin precedentes de información confidencial. Mientras que el propósito de quienes distribuyen la información puede ser proporcionar noticias o actualizaciones a su público con fines informativos o sociales, parte de esa información puede ser objeto de apropiación indebida y utilizada en provecho de actividades delictivas.

6.1.5. *Ejecución*

Algunos elementos de las categorías que se acaban de describir se pueden emplear en Internet para perpetrar actos terroristas, por ejemplo, las amenazas explícitas de violencia, incluso en

relación con el uso de armas, pueden difundirse por Internet para provocar ansiedad, miedo o pánico en una población o un sector de esta.

El uso de Internet para facilitar la ejecución de actos terroristas puede, entre otras cosas, ofrecer ventajas logísticas, reducir las probabilidades de detección y encubrir la identidad de los responsables. El acceso a Internet también puede facilitar la adquisición de los elementos necesarios para la ejecución del ataque. Los terroristas pueden adquirir cada uno de los componentes o servicios requeridos para perpetrar actos violentos mediante el comercio electrónico. La apropiación indebida de tarjetas de crédito u otras formas fraudulentas de pago electrónico pueden emplearse para financiar dichas compras.

6.1.6. *Ciberataques*

Un ciberataque generalmente se refiere a la explotación deliberada de redes informáticas como medio de gestar un ataque. Estos ataques suelen estar destinados a perturbar el funcionamiento normal de los blancos elegidos, como los sistemas de computadoras, servidores o la infraestructura subyacente, mediante el uso de técnicas de piratería informática, amenazas avanzadas y persistentes, virus informáticos, programas maliciosos, *phlooding* o cualquier otro medio de acceso no autorizado o malicioso. Los ciberataques pueden tener todas las características de un acto de terrorismo, incluido el deseo fundamental de infundir miedo en apoyo de objetivos políticos o sociales.

6.2. *Uso de internet para combatir las actividades terroristas*

Mientras que los grupos terroristas han ideado variadas formas de valerse de Internet para fines ilícitos, el uso de Internet también ofrece oportunidades de reunir inteligencia y desarrollar otro tipo de actividades para prevenir y combatir los actos de terrorismo, así como facilitar la obtención de pruebas para el enjuiciamiento de esos mismos actos. De las comunicaciones de los sitios web, salas de charla y otras comunicaciones de Internet se puede extraer un volumen importante de información sobre el funcionamiento, las actividades y, en ocasiones, los objetivos de las organizaciones terroristas. Además, el uso cada vez mayor de Internet con fines terroristas proporciona un aumento conco-

mitante de la disponibilidad de datos electrónicos que pueden reunirse y analizarse para combatir el terrorismo. Las fuerzas del orden, los servicios de inteligencia y otras autoridades están creando instrumentos cada vez más sofisticados para detectar, prevenir o disuadir, de manera proactiva, las actividades terroristas que se sirven de Internet. También se está expandiendo la utilización de los medios de investigación tradicionales, como los servicios de traducción especializados para la detección oportuna de posibles amenazas terroristas.

6.3. *Ciberdefensa y ciberseguridad*

La ciberseguridad es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedia, y la totalidad de la información transmitida y/o almacenada en el ciberentorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno.

Podemos identificar cuatro grandes grupos de ciberamenazas: ciberespionaje, ciberdelitos, ciberactivismo y ciberterrorismo. Para prevenir, mitigar y reaccionar frente a estas amenazas es preciso investigar esta nueva forma de interrelación social. Entender esta realidad implica un esfuerzo cognitivo e interpretativo que va más allá de los aspectos evidentes. Internet es el vehículo de una sociedad hiperconectada donde hemos modificado nuestros hábitos de vida, de relación y de desarrollo personal.

El cambio social que estamos experimentando permite estudiar, no sólo a los investigadores sociales, sino a profesionales de cualquier disciplina, identificar y vislumbrar modelos nuevos de integración y desintegración social. Pero también los modelos tradicionales de comportamiento adoptan estos nuevos vehículos para permanecer vivos en la sociedad. Sirva de ejemplo para este último caso la adopción por el crimen organizado del uso

intensivo de herramientas tecnológicas para expandir su acción a través de este nuevo medio. Medio que está categorizado como «el quinto espacio», adoptando y adaptando la terminología militar de los espacios a defender, a saber: tierra, mar, aire, espacio y ciberespacio.

Este Ciberespacio donde no hay regulación, ni límites geográficos genera un problema de interpretación de los conflictos según los paradigmas históricos. Las capacidades de defensa ante incidentes por parte del estado, están en jaque. Hemos de entender que las organizaciones burocráticas como el estado, tiene mecanismos de supervivencia frente a cambios de modelo, como podría decir Max Weber, y se encuentran «incómodas» frente a revoluciones como la que estamos experimentando. El estado ha de dar cumplida respuesta a una de las necesidades básicas de los ciudadanos, sean entidades físicas o jurídicas, y una de ellas es la seguridad, y estamos hablando de proporcionar a la ciudadanía una satisfacción a su «Percepción de Seguridad».

El concepto «Ciberseguridad» se ha integrado en nuestra vida diaria, la adopción de medidas frente a los riesgos inherentes a la exposición a las redes sociales de nuestros hijos, la vulneración de identidades en internet, la suplantación de éstas, el robo, la estafa, el ataque a la reputación, el ataque a infraestructuras críticas, el espionaje hace que los destinatarios de las ciberamenazas sean el global de la sociedad y se haya «democratizado» el destinatario, ya que a todos nos ha colocado el riesgo en plano de igualdad, siendo categorizados en función del interés del atacante .

Estados, empresas, universidades, ciudadanos en general estamos ante este radar. Para gestionar este tipo de riesgos es preciso una serie de elementos como la formación permanente, la concienciación de ciudadanos y del estado, el desarrollo de tecnologías fiables y generar un espacio de colaboración donde lo público y lo privado puedan desarrollar espacios que den cumplida respuesta a lo que es un objetivo común: la seguridad, un objetivo de todos.

España está desarrollando la Estrategia Española de Ciberseguridad, enmarcada en la Estrategia Nacional de Seguridad para España. El papel de las Fuerzas Armadas, frente a estas amenazas, muchas de ellas no recogidas en nuestro ordenamiento jurídico, hace que su formación y desarrollo de competencias en estas materias tenga una importancia fundamental. Se ha convertido en

imprescindible el entendimiento de estas necesidades como dice la Estrategia de Seguridad de Estados Unidos:

«La infraestructura digital es un recurso nacional estratégico y su protección una prioridad de seguridad nacional. Disuadiremos, prevendremos, detectaremos, nos defenderemos contra y nos recobraremos rápidamente de las ciberintrusiones y ataques: invirtiendo tanto en personal (campaña de concienciación sobre ciberseguridad) como en tecnología para mejorar la protección y aumentar la «resiliencia» de los sistemas y redes gubernamentales y empresariales. Reforzando la cooperación entre el sector privado y el Gobierno y a nivel internacional (normas, leyes, protección de datos, defensa de redes y respuesta a ciberataques)».

Las amenazas a la ciberseguridad representan uno de los retos más graves relacionados con la seguridad nacional, la seguridad pública y los retos a los que se enfrenta la nación. Nuestra vida diaria depende de la energía y de las redes eléctricas, pero adversarios potenciales podrían usar nuestras ciber-vulneralbilidades para interrumpir el suministro a escala masiva. Las amenazas a las que nos enfrentamos van desde hackers individuales a grupos de delincuencia organizada, desde redes terroristas a avanzados estados-nación.

Estamos asistiendo a conflictos entre estados distintos a los históricamente estudiados, donde la interconexión entre elementos en apariencia inconexos y las diferencias en el modelo de acción se han puesto de manifiesto. Términos como asimetría y globalización se ha convertido en elementos fundamentales para entender este tipo de fenómenos.

La soberanía nacional, considerada como la salvaguarda de la soberanía e integridad del territorio nacional y sus habitantes permitiendo el desarrollo de su libertad, de su actividad personal, económica y social que, a su vez, limita sustancialmente o evita, los efectos de riesgos internos y externos. Siguiendo estas líneas de actuación, la salvaguarda por parte del estado de estas libertades hace que se tengan que tomar todo tipo de medidas para hacer frente a esta situación, considerando que no es únicamente tarea del entorno público sino también del entorno privado, es decir, que para la salvaguarda de la seguridad del país hay que considerar que esta tarea es una tarea de todos.

Conclusiones

Permanencia y persistencia de conflictos interestatales de tipo tradicional vinculados a litigios fronterizos y otros de tipo coyuntural, relacionados con las materias primas y los recursos, potenciados en ambos casos por los débiles mecanismos regionales de prevención y alerta temprana, aunque también se contempla una permanencia de litigios internos con incidencia en países vecinos.

Permanencia y en algunos casos incremento del crimen organizado vinculado al tráfico de drogas y otros ilícitos transnacionales, potenciados por la inhibición forzada del «Estado de Derecho», en países con carencias institucionales o afectados por la pertinaz crisis económica, que dificultad para la gobernabilidad democrática de los territorios, generando un incremento de la violencia e incapacidad del «Estado de Derecho» para atender al conjunto de la sociedad.

Consecuencia de la estrategia global impuesta por el Sistema de Seguridad Internacional, una dificultad real para deslindar la defensa y la seguridad, generándose un solapamiento de los conceptos y procedimientos de defensa y seguridad, que se agudizarán por la falta de voluntad política para potenciarlas y modernizarlas.

En este siglo XXI la ciberdefensa se consolida como una de las mayores preocupaciones en los países desarrollados del mundo globalizado, por la posibilidad real de disponer en domicilios particulares de dispositivos conectados a la red susceptible de ser atacados . La mayor vulnerabilidad se materializa en el riesgo de usurpar los datos personales y de cualquier tipo de información sensible que estados o empresas trasnacionales en un mercado globalizado, deben custodiar como uno de sus principales activos.

Acrónimos y abreviaturas

A.

AMIA	Asociación Mutual Israelita Argentina.
ALCA	Asociación Libre Comercio de las Américas.
ALBA	Alianza Bolivariana para América.

C.

CESEDEN	Centro Superior de Estudios de la Defensa Nacional.

E.

EE.UU.	Estados Unidos de Norteamérica.
EBAO	Efects Based Approach to Operations.

O.

OEA	Organización de Estados Americanos.
OTAN	Organización del Tratado del Atlántico Norte.

T.

TIAR	Tratado Interamericano de Asistencia Recíproca.

Bibliografía

Ballesteros Martín, Miguel Ángel (abril de 2013), Evolución de las estrategias de seguridad y defensa en el siglo XXI. Revista Ejército núm. 865, Madrid, Centro Geográfico del Ejército.

Blanch, Antonio (2000), Luces y sombras de la globalización, Asociación Interdisciplinar José de Acosta, Madrid, Universidad Pontificia de Comillas.

Blackwell, James et al (1991), The Gulf War: Military Lessons Learned, Washignton DC, Interim Report of the CSIS Study Group on Lessons Learned from the Gulf War.

Bodemer, Klaus & Rojas Aravena, Francisco (2005). La seguridad en las Américas: nuevos y viejos desafíos, Iberoamericana.

Buzan, Barry (1991). People, States and Fear, Colorado, Lynne Rienner Publishers.

Castro, Jorge (2003), La nueva política de seguridad de los Estados Unidos: Hacia un sistema de seguridad global. Agenda Estratégica, Instituto de Planeamiento Estratégico, Buenos Aires, Conferencia en la Escuela de Guerra Naval el 13 de febrero de 2003 [recurso electrónico]. En http://www.agendaestrategica.com.ar/EstrategiaDetalles.asp? IdMaterial =450. [Consulta: 13-04-2013].

Carter, Ashton, B. & Perry, William J. & Steinbruner, John D. (1992), A new Concept of Cooperative Security. Washington, The Brookings Institution.

España. Ministerio de Defensa. Centro Superior de Estudios de la Defensa Nacional (2011). Adaptación de la fuerza conjunta a la guerra asimétrica, Madrid.

De Blas, Patricio (2000). Historia Común de Iberoamérica. Buenos Aires, EDAF.

De la Lamar & Rojas Aravena, Francisco J.(1998), El Nuevo Concepto de Seguridad Hemisférica Cooperativa. Colección P&SA, Santiago de Chile, FLACSO-Chile y W. Wilson Center.

Dempsey, Martin E. (10 de septiembre 2001), Capstone Concept for Joint Operations: Joint Force 2020. Washington, Reunión en la Junta de Jefes de Estado Mayor. [Recurso electrónico] http://www.cfr.org/defense-strategy/capstone-concept-joint-operations-joint-force-2020/p29212.

Estados Unidos. Departamento de Estado (17 de septiembre de 2002), Estrategia de Seguridad Nacional de los Estados Unidos de América. Washington, La Casa Blanca. [Recurso electrónico] http://merln.ndu.edu/whitepapers/USNSS-Spanish.pdf [Consulta: 17-04-2013].

Dichera, Antonio & Esteban, Carlos Daniel (1994), Criterios rectores para la formulación de medidas de confianza en un ámbito de seguridad cooperativa para el Cono sur, Chile, Flacso Stimson Center.

Elosúa, Mª Rosa & García, Emilio (1993). Estrategias para enseñar y aprender a pensar, Universidad Complutense de Madrid. Ed. Narcea.

Evans, Gareth (1994), Cooperative Security and Intrastate Confict. En Foreign Policy, núm. 96.

Fernández y Fernández, Miguel Ángel (2006), La OTAN y el terrorismo global. La estrategia de la Organización del Tratado del Atlántico Norte, Centro Superior de Estudios de la Defensa Nacional (CESEDEN), Documentos de Seguridad y Defensa núm. 4, Madrid, Ministerio de Defensa.

Fiss, Owen M. (2008), La guerra contra el terrorismo y el estado de derecho. Anuario de Derechos Humanos.

García, Diego S. (7 de marzo de 2013), La soberanía de las Islas Malvinas. Análisis IDEM, [Recurso electrónico] http://www.i-dem.org/?p=80667.

García Cantalapiedra, David (2001), El uso de las fuerzas armadas en la política exterior de EE.UU. y el futuro de la doctrina Weinberger-Powell tras el fin de la post-guerra fría: ¿el fin del síndrome Vietnam?, Conferencia Internacional: La seguridad europea en el siglo XXI, Granada, Universidad de Granada.

Garten, Jeffrey. En Blanch, Antonio (2000). Luces y sombras de la globalización, Madrid, Asociación Interdisciplinar José de Acosta, Universidad Pontificia de Comillas.

Griffiths, Spielman (2011). Teoría de la seguridad y defensa en el continente americano. Santiago de Chile, RIL Ed.

Hardy Videla, David A. (2003), «La seguridad cooperativa, un modelo de seguridad estratégica en evolución». Santiago de Chile, Revista de Marina.

Irigaray, Juan Ignacio (2013). «Avanza el acuerdo Argentina-Irán para esclarecer el atentado antisemita de 1994». El Mundo.es, Unidad Editorial Internet SL., Buenos Aires, 21 de febrero de 2013. [Recurso electrónico] http://www.elmundo.es/america/2013/02/22/argentina/1361498732.html [Consulta: 19-04-2013].

Klauer, Alfonso (2005), ¿Leyes de la historia? Tomo I, Juan Carlos Martínez Coll (ed.).

López Rodríguez, Buenaventura (2010). Panorama estratégico mundial 2010. Revista General de Marina, Madrid, En «Se desplaza el centro de gravedad de los asuntos internacionales». ABC, 29 de julio de 2004.
Mora, María (2001), «El Kurdistán iraquí». Nación Árabe, núm.51, Madrid, ICARIA.
Ocaña, Juan Carlos (2003). El ataque a Pearl Harbor. HistoriasigloXX. org, [Recurso electrónico] http://www.historiasiglo20.org/GLOS/pearlharbor.htm.
Parker, G. (2010), Historia de la Guerra, Madrid, Akal.
Pellicer, Olga (1995), La seguridad internacional en América Latina y el Caribe: El debate Contemporáneo. México DF, Universidad de las Naciones Unidas.
Piovesana, Enrico (2011), El Congreso de EEUU propone una «Guerra global permanente», National Defense Authorization Bill para el año 2012, sesión 1034, 16 de mayo de 2011, [Recurso electrónico] http://chemtrailsevilla.wordpress. com/2011/05/16/el-congreso-de-eeuu-propone-una-guerra-global-permanente/.
Prensa latina. «Ecuador se retirará del TIAR, anuncia Presidente Correa», 5 de junio de 2012.
Reese, Timothy R. & Wright, Donald P. (2008), Transición a la Nueva Campaña: El ejército de Estados Unidos en la Operación Libertad Iraquí, mayo 2003-enero 2005. MilitaryBookshop, Companyuk.
Rojas Aravena, Francisco (2004), Bajo la mirada del halcón: Estados Unidos-América Latina, post 11 de sep de 2001, Buenos Aires, Biblos.

DAESH O EL SECUESTRO Y DEFORMACIÓN DE UNA RELIGIÓN. ISLAM Y TERRORISMO: CONCEPTOS (DES)VINCULADOS

Manuel J. Gazapo Lapayese
International Security Observatory

Resumen

Los hechos acontecidos entre los atentados terroristas del 11-S en Nueva York y el 14-J en Niza han provocado que en Occidente se extienda la idea de que el islam es una religión vinculada a la violencia y al terrorismo. Sin embargo, no existe una relación de causalidad entre el islam y la violencia. Por un lado, diversos estudios internacionales demuestran que la comunidad musulmana rechaza el terrorismo de corte yihadista. Por otro lado, la realidad demuestra que Al Qaeda o Daesh han tergiversado y deformado el islam hasta poder utilizarlo como un catalizador a través del cual sacralizar su violencia y legitimar sus atentados. Todo ello hace necesario llevar a cabo un estudio multidimensional que permita desvincular ambos conceptos y construir una contranarrativa adecuada con la que hacer frente a la amenaza terrorista.

Palabras claves

Islam, Terrorismo, Desvincular, Tergiversación, Violencia.

1. En torno a la imantación del islam y el terrorismo

El terrorismo del siglo XXI pivota sobre el islam. Los atentados contra el World Trade Center de Nueva York hace ahora 15 años, los atentados en Riad en 2003, los atentados de Atocha en 2004, los atentados en el metro de Londres en 2005 o los atentados cometidos por Daesh en Francia, Bélgica y Estados Unidos en fechas más recientes, han provocado que en Occidente se extienda la idea de que el islam es una religión vinculada a la violencia y al terrorismo.

Sin embargo, tal y ha como se ha demostrado en numerosas ocasiones desde el Pew Research Center, una parte mayoritaria de

la sociedad musulmana condena las acciones cometidas por organizaciones terroristas yihadistas como Daesh, Al Qaeda o Boko Haram. Las estadísticas elaboradas por los investigadores Jacob Poushter o Michael Lipka muestran que la hipotética relación simbiótica entre los conceptos de islam y terrorismo es «ampliamente rechazada por la comunidad arabo-musulmana» (2015).

Ante semejante escenario, es necesario preguntarse qué factores hacen posible que la imantación de ambos conceptos sea tan intensa:

Un primer factor podría ser el impacto psicológico intrínseco a la ejecución de cualquier atentado terrorista o las exitosas estrategias de propaganda, captación y radicalización que ponen en práctica determinadas organizaciones terroristas yihadistas. Por ejemplo, Daesh hace que su mensaje se extienda por el ciberespacio como si de una metástasis cancerígena se tratara. La capacidad que tiene de expandir vía internet su interpretación bélica del islam hace que en las mentes de innumerables ciudadanos la religión musulmana se vincule casi sistemáticamente con el concepto de terror.

Un segundo factor podría ser el eco que producen y la atención que actualmente reciben los grupos yihadistas en la prensa internacional. Cuando se escucha en los medios de comunicación que un grupo terrorista «de corte islámico» ha matado a una decena de turistas en un mercado libanés, la gran mayoría de la opinión publica occidental no se para a reflexionar sobre la posibilidad de que esos asesinos hayan utilizado el islam como excusa para llevar a cabo una masacre. El lector o el televidente occidental obvia esa reflexión y asume como verdadero que ese grupo terrorista es un representante legítimo del verdadero islam. Si dicha situación se repite periódicamente, ese ciudadano occidental establecerá en su imaginario una relación directa entre islam y terrorismo. Y como no existe un único televidente o un único lector sino millones, la percepción de que islam y terrorismo son términos homólogos se acaba conformando como una verdad absoluta.

Un tercer factor podría ser la ausencia de una contranarrativa potente y cohesionada que emerja desde la propia comunidad musulmana. La incapacidad de desmontar el discurso de terror y violencia que exportan estos grupos yihadistas insufla incertidumbre en la opinión pública, que responde identificando in-

conscientemente a Osama Bin Laden o a Abu Bakr Al Baghdadi como los principales representantes del islam en el siglo XXI. En este sentido, si desde los años 80 el salafismo yihadista se ha ido expandiéndose sigilosa pero constantemente por Europa a través de determinadas mezquitas y centros culturales, no es difícil llegar a comprender que la única versión del islam que llegue a los oídos de la ciudadanía sea la que se encuentra más cercana a la violencia y al extremismo.

> Desde los años ochenta, el islam europeo ha estado representado fundamentalmente por la escuela salafista y la de los hermanos musulmanes. Esa base teológica clásica nunca se ha cuestionado. Los imanes aquí imitaban a los de Arabia Saudí, empeñados en aislar a los musulmanes del resto de la sociedad. Han ido imponiendo fatuas como las de que dar la mano a una mujer o decir a tu vecino feliz navidad es haram. Ese es el discurso que ha escuchado la juventud europea y para ellos eso es el islam. Empiezan a autoimponerse reglas que el islam no ordena porque creen que ese es el islam verdadero. Ese es el inicio de la radicalización y el movimiento yihadista se apoya en estas ideas. Los grupos radicales las instrumentalizan a favor de su causa. Todos los días veo chicos radicalizados que creen que solo hay una versión del islam […] La mayoría de los imanes no se enfrentan ni conocen la realidad social. Para empezar porque no son europeos y porque importan fatuas de otros países, a miles de kilómetros de distancia y con una realidad social totalmente diferente […] Sin una reforma jurídica, de interpretación de los textos, nos estamparemos contra un muro. Tenemos que evolucionar al ritmo del resto de la humanidad. En el islam hay muchas voces progresistas, pero están dispersas. (Carbajosa, 2016)

Ahora bien, más allá de los múltiples factores que pueden influir en la interpretación del islam como sinónimo de terrorismo, lo que quizás puede ayudarnos en mayor medida a comprender el porqué de esa imantación es el propio proceso por el que los yihadistas construyen su discurso.

2. En torno a la descontextualización: el paisaje literario y el paisaje histórico

Negar la existencia de aleyas de carácter beligerante en el Corán es un error, en tanto, implica obviar parte del complejo universo que conforma el islam. Del mismo modo, también es

un error interpretar el islam como una religión que tiene en la expansión de la violencia su fin último. El problema, por tanto, se encuentra en la forma en la que los terroristas hacen uso de esos fragmentos conflictivos:

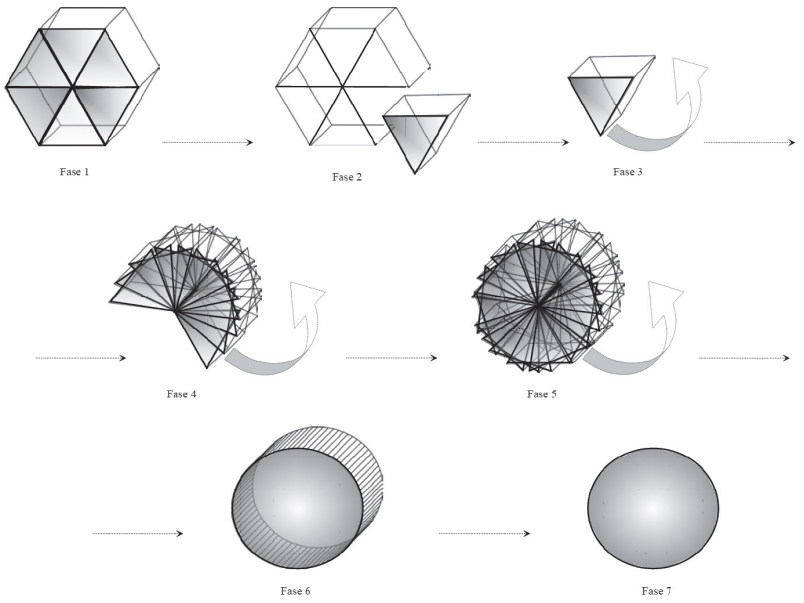
En primer lugar, los fragmentos violentos son descontextualizados de su *paisaje literario,* es decir, son extraídos y aislados del resto de texto. Los terroristas toman una aleya determinada y la aíslan de su paisaje literario inmediato, las aleyas inmediatamente anteriores y posteriores; y de su paisaje literario circunstancial, el Corán en su conjunto. Esto permite a los terroristas librarse de los condicionantes o limites que puedan existir en torno a una acción de combate y utilizarla en su beneficio, dándola el significado o dirección que más les interesa. Sin el paisaje literario inmediato y el circunstancial, las aleyas pierden su sentido y se tergiversa el mensaje original.

En segundo lugar, los fragmentos violentos son descontextualizados de su *paisaje histórico*, es decir, son aislados del momento o contexto histórico en el que el islam es revelado. Debe recordarse que el Corán fue escrito tras la muerte de Mahoma en el siglo VII en un momento histórico determinado que nada tiene que ver con el actual. En consecuencia, plantear la vida en pleno siglo XXI como un enfrentamiento entre fieles e infieles resulta anacrónico y poco funcional. No vivimos en la misma realidad histórica que en la que vivió Mahoma. Por lo tanto, muchas de las aleyas que se formularon en su momento ya no gozan de actualidad o vigencia si se interpretan de forma literal.

A pesar de ello, los terroristas obvian el paisaje histórico e interpretan esas aleyas como atemporales, lo que les permite emprender una guerra sin límites en el espacio-tiempo contra los infieles y los apóstatas. Precisamente, el efecto de anular el paisaje o contexto histórico es que en pleno siglo XXI los terroristas se sienten ya no solo legitimados sino obligados a combatir. Esto nos lleva a entender que cualquiera de los mensajes confusos y grises que puedan encontrarse en el libro sagrado del Corán son sometidos a este proceso de descontextualización por parte de los ideólogos terroristas con el fin de ser utilizados como justificación y legitimación sus actos. Se aprovechan de forma extraordinaria de los fragmentos violentos y de las ambigüedades que existen tanto en el Corán como en la Sunna. De este modo, el que existan contradicciones únicamente beneficia a aquellos interesados en utilizar el islam

como vehículo o motivo a través del cual justificar su violencia, como es el caso de los grupos terroristas de Al Qaeda o Daesh.

El resultado de todo ello es que el islam es raptado y desfigurado por parte de los terroristas, lo cual produce que éste se vincule forzosamente con la violencia. A continuación, se presenta un diagrama mediante el cual se explica cómo el terrorismo ha secuestrado, deformado y utilizando la religión islámica en su beneficio.



[Gráfico 1: Diagrama evolutivo de la distorsión. Fuente: elaboración propia, Manuel Gazapo]

2. Diagrama evolutivo de la distorsión

Primera fase: El diagrama se inicia con un poliedro polícromo que representa al islam en toda su riqueza, profundidad y complejidad. Dicho poliedro nos permite representar la religión musulmana como un crisol de conocimientos, aportaciones, mensajes y perspectivas. Cada porción de color representa una de las múltiples partes que conforman el islam. Concretamente, la porción gris representa la franja violenta o conflictiva intrínseca

al islam, es decir, todo aquellos mensajes bélicos y ambiguos de los que hemos hablando en apartados anteriores.

Segunda fase: Los terroristas buscan un pretexto a través del cual justificar sus proyectos, acciones y agresiones. Lo encuentran en el islam. Específicamente lo único que les interesa a los terroristas es la sección violenta, la cual, extraen y la apartan del resto. Puede observarse que todos los fragmentos que conformaban el cristal multifacético del islam pasan a estar en blanco. La única excepción es el ya citado fragmento de la violencia, representado en color gris. Los terroristas se desentienden de toda la diversidad de mensajes que componen el islam original y pasan a centrarse únicamente en su sección violenta. Esta se convierte en su objetivo de atención y pasa a ser extraída del conjunto. Se aísla.

Tercera y cuarta fase: Los terroristas hacen del fragmento violento su razón de ser y lo hacen girar buscando conformar una nueva totalidad. Buscan construir un nuevo prisma que gire únicamente en torno a aquellas aleyas y hadices que, tras haber sido meticulosamente descontextualizadas de su paisaje literario e histórico, legitiman la violencia.

Quinta fase: Los terroristas acaban por conformar un nuevo prisma que nada tiene que ver con el cuerpo geométrico originario. La esencia del nuevo cristal son los apartados más nebulosos y violentos de los textos originarios del islam, interpretados de forma literal y descontextualizada.

Sexta fase: Los terroristas continúan con su proceso de desfiguración del islam llegando a simplificar aún más su teoría. La profundidad de su planteamiento del mundo y la presencia de algún rasgo islámico en éste son, como apuntaba Faisal Devji, cada vez menores. No obstante, es en esta fase en la que acaban por construir y expandir su Yihad, alejada ya de toda realidad y entendida únicamente como sinónimo de violencia y de una guerra sin límites espacio-temporales.

Séptima fase: El ciclo finaliza con un circulo plano monocromo reflejo del estado actual del argumentario terrorista: una masa sin ninguna profundidad donde lo plural y lo diverso han desaparecido. La simplificación ha llevado a los terroristas a denominar *islam* a algo que nada tiene que ver con este, en tanto en cuanto, tampoco la porción violenta es respetada en su forma. La ausencia de toda dirección, motivación o justificación religiosa resuena y, únicamente, existe violencia y terror.

4. La necesidad de desvincular

El proceso de distorsión al que es sometido el islam por parte de los ideólogos terroristas no sólo les permite construirse una identidad y una legitimidad, sino que también hace que los ciudadanos occidentales reciban una versión deformada del islam y lo vinculen al terrorismo. Y eso, representa un gran riesgo para la estabilidad de nuestras sociedades y su futuro:

La mera posibilidad de que un reducto de la comunidad musulmana asentada en países occidentales sienta, a consecuencia de la estigmatización, que el Daesh defiende mejor sus intereses que un Estado de Derecho es un riesgo para nuestra seguridad, nuestros valores y nuestro futuro como sociedades democráticas. Desmontar el constructo que equipara islam y terrorismo es una misión de extrema urgencia ya que permitir que siga extendiéndose por Occidente no sólo representa una derrota para nuestros Estados de derecho, sino que también significa la apertura de una grieta que acelera el choque de civilizaciones que Daesh está buscado.

En este sentido, si atendemos a la idea de choque de civilizaciones, es necesario apuntar que este no tiene por qué materializarse en un conflicto tradicional donde dos potencias se enfrenten, sino en algo mucho más difuso e imperceptible en sus primeras fases. Un choque de civilizaciones en pleno siglo XXI puede ser simple y llanamente el resquebrajamiento del ideal de multiculturalidad europeo al ver en cada vecino musulmán un potencial terrorista. Es decir, no es necesario que haya una confrontación nuclear de por medio para que exista un choque de civilizaciones. Únicamente es necesario adentrarnos en un estado de psicosis por el cual veamos peligro en todo aquello que sea diferente a nosotros. Si dejamos que la imantación sistemática de los conceptos de islam y terrorismo cale en nuestros medios de comunicación y en nuestras sociedades, será inevitable ver en cada musulmán un potencial terrorista. Y eso, es algo que solo beneficia al Daesh, en tanto, este se nutre del desencanto que sufren los musulmanes que viven en países no islámicos.

Por lo tanto, si en un choque de civilizaciones ningún individuo está a salvo, desmontar el constructo que equipara islam y terrorismo no es únicamente beneficioso para el colectivo arabo-musulmán sino para toda la sociedad en su conjunto. El

proceso de desvinculación debe llevarse a cabo simultáneamente desde varios frentes:

4.1. *El terrorismo y el uso interesado de la religión*

Imaginemos a unos individuos aleatorios que buscan incrementar sus cotas de poder y se marcan como objetivo el establecimiento de su propio estado. Dichos individuos componen una organización terrorista denominada «NewState» y deciden iniciar una serie de atentados a lo largo de varios países europeos. Dichos terroristas, que tienen una fe ciega en su causa, son conscientes de que su búsqueda de mayores cotas de poder y la conformación de su nuevo estado no está respaldada por una filosofía o un argumentario suficientemente atractivo. No obstante, pasan a la acción. ¿Cuál sería el resultado obtenido? Posiblemente, el proyecto bélico no alcanzaría los objetivos planteados debido a que los atentados no estaban respaldados por una ideología suficientemente potente y magnética como para ganarse el apoyo de un colectivo social suficientemente numeroso o determinante. La poca aceptación obtenida por parte de la sociedad perjudicaría las tareas de reclutamiento de nuevos combatientes haciéndolas poco exitosas. La consecuencia de ello sería el abandono del proyecto y la posterior disolución de la organización.

La idea que subyace de este hipotético intento de construir un estado por parte de una organización terrorista poco «magnética» es que éstas necesitan de capital humano si desean alcanzar sus objetivos. Así, la razón de su más que probable corta existencia es la ausencia de una filosofía o una ideología suficientemente atractiva: si un argumentario correctamente fundamentado y estructurado, así como llamativo y sugerente es condición indispensable para conformar cualquier colectivo, lo es aún más si hablamos de la construcción de organizaciones terroristas. En éstas, la vida del combatiente pasa a estar en riesgo por lo que es preciso que los ideólogos y fundadores de las organizaciones terroristas construyan un ideario suficientemente sólido y atractivo como para dar seguridad a los combatientes en momentos de flaqueza y asegurar la captación y el reclutamiento de nuevos esbirros. Y es ahí donde la religión pasa a jugar un papel fundamental:

En primer lugar, las religiones, convenientemente alteradas y deformadas, aportan a los terroristas el fundamento ideológico

necesario en torno al que justificar y legitimar sus brutales agresiones. Utilizan el dogma de fe de las religiones como excusa para cometer asesinatos y matanzas atroces. La religión, adecuadamente desfigurada, pasa a ser utilizada como una pantalla a través de la cual los terroristas pueden atentar eludiendo cualquier responsabilidad.

En segundo lugar, las religiones entendidas como bolsas de gente, ofrecen a los terroristas un colosal sustrato de individuos sobre los que extender su propaganda y sus estrategias de radicalización, captación y reclutamiento. Herfried Münkler, reputado experto en teorías de la guerra, explica en sus obras que cuando se comete un atentado la organización terrorista tiene en mente dos destinatarios: «el agredido […] y el tercero» (2005: 134). El primer destinatario es obviamente el gobierno, población o individuo al que se está intentando dañar a través de un atentado terrorista o su amenaza. El segundo destinatario denominado como «el tercero al que se busca interesar» (2005: 137), serían todos aquellos ciudadanos susceptibles de poder apoyar la causa terrorista.

De este modo, el motivo religioso pasa a ser utilizado como vector de movilización. El que un grupo terrorista se «identifique» con una religión como el islam afirmando que busca defenderla y extenderla les garantizan un posible *tercero* muy amplio, es decir, un ingente número de potenciales nuevos combatientes y simpatizantes. Por lo tanto, si retomamos el ejemplo imaginario anteriormente propuesto podríamos plantear lo siguiente: si los ideólogos de «NewState» hubieran aderezado o insertado sus causas, motivaciones y objetivos dentro de un conducto religioso, es decir, hubieran afirmado que la construcción de su nuevo estado tenía como meta defender y extender los principios de una religión determinada, sus probabilidades de éxito hubieran sido posiblemente más altas. La prueba de ello la encontramos en Daesh, que tras alterar y deformar convenientemente el islam y maquillar sus atentados con una supuesta legitimidad religiosa, ha conseguido que sus acólitos y esbirros se multipliquen respecto a las cifras obtenidas por otros grupos terroristas contemporáneos.

La conclusión que puede extraerse de las ideas planteadas es que las religiones en general y el islam en particular no son sinónimo de terrorismo. Tal y como explica Magnus Ranstorp, mientras que las religiones no sean utilizadas por los extremistas

como su carburante o catalizador, éstas no generan terrorismo por sí solas.

4.2. *La incongruencia temática: el terrorismo yihadista aniquila musulmanes*

Otro de los puntos en donde puede observarse que no existe un islam terrorista son las propias prácticas de Al Qaeda y Daesh. Si estas organizaciones terroristas tienen por objetivo combatir a Occidente al identificarlo como principal responsable del declive del islam, las víctimas de sus atentados tendrían que ser exclusivamente población no musulmana. Más concretamente, si nos basamos en sus comunicados, sus víctimas deberían de ser occidentales estadounidenses, al ser los Estados Unidos de América su eterno enemigo. Sin embargo, la realidad es otra. La población musulmana ha sido y es el principal objetivo de los atentados cometidos por Al Qaeda en su momento y Daesh en la actualidad. La población musulmana que ha muerto a manos de grupos terroristas que dicen actuar en nombre del islam es colosalmente mayor que el número de muertos no musulmanes. Y es ahí donde algo falla, ¿Cómo puede ser posible que una organización que se proclama a sí misma como representante de la religión musulmana tenga como principales víctimas a sus propios fieles?

La respuesta se halla en la propia naturaleza del terrorismo anteriormente comentada: se trata de unos individuos con unos objetivos determinados -que nada tienen de religiosos- que se han servido del islam como mecanismo o canal a través del cual fortalecer y expandir su proyecto mesiánico y genocida. En el caso de Daesh, construir un nuevo Estado basado en la violencia.

La razón por la que aquellas organizaciones terroristas autodenominadas islámicas o yihadistas cometen atroces atentados contra la población musulmana se reduce a que para sus intereses es absolutamente necesario que no exista ningún musulmán que ponga en duda o contradiga su interpretación del islam. Ellos usan el adjetivo de islámico como una fachada que les permite sacralizar su violencia y así legitimar sus atentados. Por lo tanto, necesitan que su interpretación del islam, meticulosamente tergiversada y desfigurada, sea la única posible de cara a la comunidad internacional. Un dramático ejemplo de ello lo podemos encontrar en la tortura diaria que sufren las poblaciones de Irak y Siria desde la aparición de Daesh. Estos asesinos no respetan ni por asomo a los que se supone que son hermanos de fe y los ejecutan

sistemáticamente si consideran que apoyan a Occidente o no creen fervientemente en su causa. «A decir verdad, esos islamistas fanatizados han convertido en enemigos a cualquier persona o grupo que se oponga a su particular interpretación del islam, y entre sus oponentes siempre ha habido y sigue habiendo muchos musulmanes» (De la Corte & Jordán, 2007:21).

Abu Bakr, líder del Daesh, promete el paraíso a quienes den su vida por él y por el Estado que está intentando implantar mediante el terror en el espacio geográfico correspondiente a Irak y Siria. El problema está en que a Abu Bakr olvida que el Corán prohíbe terminantemente a los musulmanes matar a un hermano de fe. Consiguientemente, «por mucho que -los terroristas- apelen a Alá o a su profeta no pueden ser identificados con el islam […] Ni en puridad se les tendría que llamar yihadistas, ni considerar que su guerra es una Jihad» (Garriga, 2015: 38-48).

En definitiva, un grupo u organización terrorista que se autodenomina «islámico» y tiene como principales víctimas a poblaciones musulmanas, carece sistemáticamente de todo sentido y representatividad. Las constantes muertes de población musulmana demuestran no existe un islam terrorista.

4.3. *Experiencias históricas comparadas*

Existen ejemplos que manifiestan que las religiones siempre han tenido a lo largo de la historia el problema de acabar siendo utilizadas como justificación, coartada o excusa de actividades o proyectos cuestionables si se comparan con lo que el dogma religioso apuntaba originalmente. No hay más que acudir a los libros de historia para observar que las religiones del Libro han tenido escabrosos episodios de violencia.

Por un lado, el cristianismo**,** tal y como indica Walter Laqueur, fue utilizado en la época de las cruzadas y de la inquisición como excusa para cometer invasiones, saqueos, matanzas y torturas en masa. Se manipularon los textos bíblicos con el único fin de extraer versículos o fragmentos descontextualizados que legitimaran atrocidades encaminadas a alimentar las ansias de poder de unos pocos.

> Las arengas del papa Urbano y de otros príncipes de la Iglesia invitaban a los píos a ir a Tierra Santa para salvar los lugares sagrados de los sarracenos que los habían profanado y destruido […] No

> fue el papa el único personaje implicado en aquella incitación; también hay que contar con diversos sacerdotes demagogos, como Pedro de Amiens, un espécimen de fanático que reaparece la Edad Media hasta llegar a Savonarola, la Inquisición y la quema de brujas. (Laqueur, 2003: 35-36)

Por otro lado, en la actualidad, el islam está sufriendo la misma tortura, la misma tergiversación a la que el cristianismo se vio sometido en su momento. El islam está siendo utilizado por los terroristas como un canal o vector a través del cual cometer atentados en masa a lo largo y ancho de todo el planeta con el único objetivo de imponer un Estado, supuestamente islámico, que domine todo a través de la violencia y la radicalidad.

> El término yihad ha sido asiduamente empleado por grupos y Estados musulmanes para sacralizar el uso de la violencia, en muchos casos con fines políticos. Por consiguiente, no es extraño que algunos islamistas contemporáneos hayan recurrido a ese mismo concepto para dar apariencia de legitimidad religiosa a sus campañas terroristas. (De la corte y Jordán, 2007:41)

En ambos casos, independientemente del dogma religioso o del momento histórico, puede identificarse como han existido o existen hombres que se han valido de cultos religiosos para satisfacer sus intereses, acometer sus proyectos e incrementar sus beneficios. Eso pone en evidencia que las religiones, convenientemente desfiguradas, son utilizadas como pretexto para la realización de proyectos que al desnudo no encontrarían apoyo o simpatizantes. El problema de esa tergiversación es que se destruye el verdadero legado de la religión; tal y como afirma Chema Gil Garre, analista de terrorismo y seguridad internacional del International Security Observatory, «no hay mayor apostasía contra cualquiera de las religiones y, en particular el islam, que retorcer el texto sagrado para hacerle decir lo que en realidad no dice» (2016).

En definitiva, estas ideas ayudan a comprender que la idea de que el islam es sinónimo de terrorismo es incorrecta. «El islam es una religión de paz, otra cosa es, como ha ocurrido con el cristianismo y otras religiones, que se haya utilizado a dios como excusa para justificar la violencia y la guerra; pero nunca fue por motivos santos sino por motivos bastardos» (Gil: 2016). El perfil violento que a día de hoy la religión musulmana está adoptando en determinadas regiones del mundo no es algo que surja de los

propios textos sagrados sino de interpretaciones deliberadamente tergiversadas.

4.4. *Ausencia de lo humano*

Un gran conjunto de expertos entre los que se encuentran Luis de la Corte Ibáñez y Javier Jordán describen a los denominados yihadistas como «una minoría extraída de un conjunto total de 1.500 millones de musulmanes» (2007: 34). Debido a ello, tendemos a decir que son una porción muy reducida al par que muy activa dentro de la comunidad musulmana cuando en realidad no comulgan en absoluto con ninguna de las lecciones más puras que trascienden del Corán. Esas lecciones, como apuntan Faisal Devji o Tahar Ben Jelloun, no son otras que las mismas que se pueden extraer del cristianismo u otras religiones, es decir, el respeto al otro, la coexistencia, la dignidad, la justicia, la equidad, la tolerancia o el perdón.

De todas las contribuciones que condensan en su interior religiones como el islam o el cristianismo, las que verdaderamente aportan un valor añadido a la humanidad no son tanto las de carácter dogmático o divino (creer en la palabra revelada o en el juicio final) sino las de carácter más existencial (respeto o tolerancia). Y son justamente estas últimas las que ni por asomo respetan o proyectan los terroristas que dicen actuar en nombre del islam. Ningún terrorismo ya sea de extrema derecha, de extrema izquierda, yihadista o cristiano ortodoxo, cultiva estos valores y enseñanzas que se derivan de la esencia más pura de las religiones. Consiguientemente no es correcto dar por valido la imantación del islam con la violencia.

4.5. *Un mero ritual*

Si se analizan los textos de Faisal Devji se puede observar que uno de los argumentos que más defiende es que no puede existir un islam terrorista. Desde su perspectiva, los terroristas no solo aíslan las aleyas de su contexto literario e histórico como ya se ha explicado anteriormente, sino que llevan a cabo un radical proceso de simplificación de la liturgia musulmana más elemental hasta transformarla en un mero ritual en el cual encajar sus operaciones. Tanto Bin Laden en su momento, como Abu Bakr al-Baghdadi ahora, utilizan el islam como un vehículo robado a

través del cual expandir una ideología de odio y violencia. Para ello, prescinden de los «puntales básicos de la predicción musulmana tradicional» (Devji, 2007: 32) con lo que se aseguran una propagación universal de su mensaje.

> El tipo de proselitismo al que se refiere Bin Laden en sus reflexiones sobre los atentados del 11-S prescinde totalmente de preocupaciones pasadas de moda acerca de rituales y detalles doctrinales sobre la práctica islámica y la importancia de la formación lingüística y la correcta exégesis de los textos […] La ruptura explícita con algunas prácticas tradicionales del islam […] es una característica del Yihad global. (Devji, 2007: 32-33)

La supresión de esos elementos más tradicionales o, mejor dicho, más esenciales de la práctica religiosa responden por un lado al interés de agilizar los tiempos de adoctrinamiento e incorporación de nuevos simpatizantes y, por otro, al interés de ensanchar el perfil del potencial combatiente. Los ideólogos de las organizaciones terroristas como Daesh «minimizan o sencillamente eliminan todo hecho inconveniente» (Devji, 2007: 38) existente dentro del islam que pueda restarles nuevos adeptos.

> Esa despreocupación respecto a los detalles de la correcta práctica islámica ya se evidencia en sus comentarios iniciales, cuando Bin Laden dice que los autores de los atentados no pertenecían a ninguna tendencia conocida de la ley islámica […] Un movimiento global como el Yihad depende, para su supervivencia, de la erosión de las lealtades religiosas y políticas tradicionales. No en vano veíamos que, Al Qaeda, a semejanza de otros movimientos globales, cuenta con un abanico de miembros extraordinariamente diverso, pero sin culto ni ideología comunes y sin lazos de clase, etnicidad ni antecedentes personales, que sólo puede funcionar en red quebrantando e ignorando las formas obsoletas de fidelidad política y religiosa. (Devji, 2007: 32-39)

Ahora bien, lo que es verdaderamente llamativo es que a través de esas políticas de simplificación del islam los ideólogos yihadistas acaban por convertirse en aquello que pretenden combatir: «paradójicamente, la destrucción por parte de éste —Bin Laden— de las formas tradicionales de la autoridad islámica lo enlaza íntimamente con otros grupos que podría considerar inaceptables desde el punto de vista terrorista islámico» (Devji, 2007: 32).

En conclusión, al arrancar toda la profundidad intrínseca a la práctica musulmana lo que se acaba conformando es un mero ritual de adhesión a la guerra que no tiene nada islámico ni nada de religioso. Así, la expresión de *islam terrorista* o *terrorismo yihadista* es incorrecta en tanto en cuanto el adjetivo de *islámico* o *yihadista* que acompaña al concepto de terrorismo está vacío de contenido.

Conclusión

El contexto actual en el que nos encontramos sumergidos hace parecer real la idea de que el terrorismo del siglo XXI pivota sobre el islam. Ahora bien, tal y como se ha expuesto a lo largo del artículo, eso no significa que haya una relación de causalidad entre islam y violencia. Es decir, la comisión de atentados por parte de organizaciones terroristas en nombre del islam no debe hacernos entender la religión musulmana como un sinónimo de violencia y terror.

Como se ha explicado, los líderes terroristas utilizan el islam como un catalizador que les permite justificar sus acciones y agresiones y eludir responsabilidades. Para ello, deforman y descontextualizan la religión hasta límites insospechados. Por dicha razón, cuando se autodenominan «islámicos», en realidad, no están haciendo referencia a nada en concreto más allá que a ideas obsesivas basadas en la lucha genocida contra todo y contra todos los que no piensan como ellos.

Desvincular ambos conceptos es una condición *sine qua non* para garantizar el desarrollo pacífico de nuestras sociedades en el futuro. Evitar un choque de civilizaciones y prevenir la aparición de oleadas terroristas en un futuro depende en gran medida de nuestra capacidad de asimilar que las religiones en general y el islam en particular no son el problema, sino parte de la solución.

Bibliografía

Libros:

Ben Jelloun, Tahar (2015), *El Islam que da miedo,* Madrid, Alianza Editorial.

De la Corte, Luis & Jordán, Javier (2007), *La Yihad terrorista*, Madrid, Editorial Síntesis.

Devji, Faisal (2007), *Paisajes del Yihad. Militancia, moralidad, modernidad,* Barcelona, Ediciones Bellaterra.

Garriga, David (2015), *Yihad ¿Qué es?,* Barcelona, Ediciones Comanegra.
Laqueur, Walter (2003), *La guerra sin fin. El terrorismo en el siglo XXI*, Barcelona, Editorial Destino S.A.
Münkler, Herfried (2005), *Viejas y nuevas guerras. Asimetría y privatización de la violencia*, Madrid, Siglo XXI de España Editores.
Ranstorp, Magnus, «Al Qaeda en el ciberespacio: desafíos del terrorismo en la era de la información», en Reinares, Fernando & Elorza, Antonio (ed.), *El nuevo terrorismo islamista. Del 11-S al 11-M*, Madrid, Ediciones Temas de hoy, S.A., 2004, págs. 201-222.

Artículos de publicaciones en serie:

Gil, Chema, «El Jihad contra el Jihadismo. Nuevos elementos para la guerra», *Diario 16*, núm. 6 (2016), págs. 40-43.

Artículos e informes online:

Carbajosa, Ana. Si no reformamos el islam nos estamparemos contra un muro. *El País* [en línea] 28 de marzo de 2016 [citado 4 de octubre de 2016]. Disponible en Internet: <http://internacional.elpais.com/internacional/2016/03/28/actualidad/1459154249_420976.html>
Poushter, Jacob. In nations with significant Muslim populations, much disdain for ISIS. *Pew Research Center* [en línea] 17 de noviembre de 2015 [citado 4 de octubre de 2016]. Disponible en Internet: <http://www.pewresearch.org/fact-tank/2015/11/17/in-nations-with-significant-muslim-populations-much-disdain-for-isis/>

Gráficos:

[Gráfico 1: Diagrama evolutivo de la distorsión. Fuente: elaboración propia, Manuel Gazapo]

¿EXISTE UN PERFIL DEL TERRORISTA YIHADISTA?

Pablo Lobato de Enciso
Centro de Psicología. Enfermería del MAGEN en Sevilla

Resumen

El auge del autodenominado Estado Islámico en julio de 2014 ha renovado el interés por el fenómeno de radicalización en los jóvenes nacidos y criados en Europa que ya no sólo marchan a combatir en Irak o Siria, sino que atentan contra el territorio que les vio nacer. En un fenómeno que algunos investigadores definen como «ideología *fast food*». Realizamos una revisión no sistemática desde la Psicología de los estudios publicados desde el auge del Estado Islámico con el objetivo de analizar si existe un perfil psicológico del terrorista yihadista.

Palabras claves

Radicalismo, Terrorismo Yihadista, Psicología

1. Introducción

En los últimos años, Europa se ha visto sacudida por los golpes del terrorismo yihadista. Sólo, desde la proclamación del Califato por parte del autodenominado Estado Islámico, el terrorismo ha atacado el territorio europeo en varias ocasiones, generando centenares de pérdidas humanas. La actual crisis migratoria motivada por la situación política en países como Siria o Libia ha generado el recelo en la opinión pública europea por temor a nuevos atentados. Sin embargo, en la mayoría de los casos, quienes han perpetrado estas matanzas en Europa, no han sido personas criadas en entornos subdesarrollados, sino que han sido hombres y mujeres, si no nacidos, sí criados y educados en nuestras fronteras. Con pasaporte europeo.

El fenómeno que se inició el 7 de julio de 2005 en Londres, cuando un grupo de jóvenes nacidos y criados en Reino Unido se inmolaron en una serie de ataques coordinados, no fue un hecho aislado, al contrario fue el preludio de un nuevo reto al que han de hacer frente las fuerzas y cuerpos de seguridad del estado: la amenaza del terrorismo yihadista no proviene únicamente de fuera. En lo que se conoce como terrorismo *homegrown* (Cronne y Harrow 2011), o terrorismo autóctono (Reinares y García-Calvo 2013). Desde sujetos aislados, hasta células coordinadas el terrorismo yihadista ha atacado occidente de todos los modos posibles. Cuando ocurre el atentado, la sociedad demanda respuestas, ¿podemos predecirlo?, ¿podemos detectar a los terroristas antes de que realicen estas actividades? La detección precoz de estos individuos se supone fundamental como instrumento de lucha contra el terrorismo

Los objetivos de este trabajo son explorar aquellas cuestiones acerca del comportamiento terrorista que han sido investigadas en el ámbito de las ciencias del comportamiento, identificar los hallazgos más importantes, e intentar unificar y sintetizar estos observando los puntos en común y las discrepancias entre los autores, con el fin de trazar un posible perfil del terrorista yihadista que actúa en España.

2. El fenómeno de la radicalización en Europa

La amenaza de la radicalización islamista ha crecido en los últimos años. Los planes y ataques realizados en territorio europeo han tenido a la sociedad civil como objetivo prioritario aunque también se han producido contra símbolos nacionales y gubernamentales europeos. En la mayoría de los casos, quienes han ejecutado estas actividades han sido jóvenes ciudadanos nacidos y/ o criados en Europa.

Estas actividades no las han desarrollado únicamente en Europa. En los últimos años, muchos de estos jóvenes, han abandonado sus casas y hogares para luchar en países como Siria e Iraq (Bakker y de Bont 2016). Según un análisis (Neumann 2015) realizado por el *International Centre for the Study of Radicalization and Political Violence* (ICSR), Francia (con 1200 combatientes), Alemania (500-600) y el Reino Unido (500-600), son los países con mayor número de combatientes de esas nacionalidades en Iraq y Siria. Este mismo estudio también señala que proporcional-

mente, los países más afectados son Bélgica (40 personas por cada millón de habitantes, Dinamarca (27 personas por cada millón de habitantes) y Suiza (19 personas por cada millón de habitantes). Este mismo estudio señala que de España han salido entre 50 y 100 personas. (Neumann 2015) El estudio de Neumann (2015) señala que habrán muerto en combate entre el 5 y el 10% y retornarán a sus países de origen entre el 10-30% de los combatientes, muchos de ellos perfectamente instruidos y con capacidad de atentar contra su propio país.

2.1 *¿Por qué se radicalizan?*

En el año 2005, una comunicación de la Comisión de la Comunidad Europea al Parlamento Europeo y al Consejo sobre la captación de terroristas (Comisión de las Comunidades Europea 2005, 2), definía la radicalización violenta como «el fenómeno en virtud del cual las personas se adhieren a opiniones, puntos de vista e ideas que pueden conducirles a cometer actos terroristas».

No podemos señalar un único factor que podamos considerar esencial o determinante para que un individuo se radicalice. Parece necesaria una combinación de factores y pasos previos para que en un individuo se convierta en una persona dispuesta a cometer actos terroristas en los sean capaces de llevar a la muerte a otras personas e incluso a ellos mismos. Además, no en todos los sujetos, el radicalismo llega a sus últimas consecuencias, como señalan Rodríguez-González y Ceballos-Rodríguez (2014,4) *toda actitud llevada a un extremo propio a la irracionalidad o, por lo menos apartada de una lógica cartesiana imperante resulta ser una manifestación de radicalismo, una cosa es que éste se mantenga tan solo en el ámbito de la opinión y del gesto y otra muy diferente es que acabe llegando a la vez a la acción (violencia) y/o potenciando la manipulación de otros a la vez que se les dispone para la citada acción.*

La literatura científica trata de buscar explicación al por qué algunos jóvenes musulmanes europeos abrazan la radicalización. La mayoría de estudios se basan en muestras de población musulmana (Reinares 2006), (Trujillo, León, y otros 2010) (Gill, Horgan y Deckert 2014), conversos (van San 2015) o casos únicos (McCauley y Moskalenko 2014) y plantean hipótesis sobre las posibles causas de la radicalización de estos jóvenes. Una revisión de literatura nos sugiere la dificultad que existe para poder realizar una evaluación de los terroristas o presuntos terroristas,

ya sea por la dificultad de acceso a los terroristas detenidos, su más que probable falta de colaboración o la falta de estudios con sujetos control. Desgraciadamente, la mayoría de estos artículos no cumplen con los criterios empíricos convirtiéndose por tanto en textos especulativos (Victororoff 2005, 33).

Las razones de la radicalización las encontramos desde la perspectiva individual, pero también grupal. Generalmente, estos jóvenes son criados en barrios marginales de las capitales de provincia, emigrantes o hijos de emigrantes que llegaron a nuestro país en busca de una oportunidad, no siempre recompensada. En España, el fenómeno de la segunda y tercera generación es relativamente reciente a diferencia de lo que ocurre en países de nuestro entorno como Alemania, Francia y Reino Unido. Cada país tiene, por su propio pasado histórico un nicho diferente de población inmigrante. Así por ejemplo, en Reino Unido, la población de la antigua India Británica, lo que hoy lo conforman los estados de India, Paquistán y Bangladesh. En Alemania, existe una gran colonia originaria de Turquía y en Francia la población inmigrante es originaria, principalmente de Argelia, antiguo protectorado francés y los departamentos de ultramar.

2.2. *¿Cómo se radicalizan?*

Leiken (2004) establece dos tipos de acceso a estos grupos terroristas: por un lado los que define como *outsider*, es decir, personas que llegan a Occidente en principio por distintas causas, como disidentes políticos en busca de asilo, estudiantes universitario, antiguos muyahidines, o imanes. El otro grupo lo conformarían los *insiders* en el que se incluirían aquellos sujetos que pertenecen a la segunda o tercera generación de inmigrantes procedentes de países musulmanes y que por diferentes causas quedan estancados en barrios marginales en la periferia de ciudades europeas. A estos dos grupos, Taarnby (2005) añade un tercero, identificado por los conversos.

En los últimos años, tanto el número de los tres grupos ha aumentado considerablemente. A objetos de este artículo, nos centraremos prioritariamente en la figura de los *insiders*. Podemos hablar de estos jóvenes insiders como «sujetos diana», ya que por sus características son sujetos «*propensos a adoptar conductas extremas, que han nacido en los países receptores, han recibido una educación*

occidental y conocen a la perfección el sistema de valores y de relaciones imperantes». (Rodríguez-González y Ceballos- Rodríguez 2014, 6).

2.3. *Factores de presión*

Algunos estudios han vinculado el subdesarrollo y la pobreza como uno de los factores de riesgo principales hacia el extremismo religioso (Atwood 2003), aunque para la mayoría de autores, parece existir un consenso en que no hay una correlación entre el terrorismo y la pobreza (Cano 2009) (Reinares y García-Calvo 2013) (Sageman 2006), al igual que no existe una correlación de terrorismo con la salud mental (Corner y Gill 2015). No obstante, y aunque no lo expliquen por sí mismo, sí pueden considerarse como un factor de riesgo, ya que los entornos sensibles, guetificados y deprivados favorecen los climas de tensión multicultural, entornos que favorecen la radicalización. (Moyano y Trujillo 2014), (Trujillo y Moyano 2008).

Recientemente, un trabajo de los investigadores Moyano y Trujillo (2016) observa que en nuestro país existen varios indicadores que hacen pensar en la posibilidad de que se intensifiquen los incidentes críticos de violencia anclados en un conflicto de identidades culturales que pueden ser interpretadas en clave Islam-Occidente, aspecto que pueden aprovechar los grupos islamistas extremistas.

Así vemos que factores como el entorno, educación y cultura pueden contribuir a la proliferación de actividades radicalizadas, pero además hemos de tener en cuenta otros que también los favorecen como son los factores grupales. Así, el grupo o red terrorista, suele convertirse en el colectivo social de referencia, surgiendo una clara tendencia hacia la idealización de los miembros de éste, lo que propicia que surjan profundos lazos afectivos, lo que explicaría que surja primero la amistad entre los miembros del grupo, después la percepción de pertenencia y por último lugar la asimilación de la ideología imperante en éste. (Trujillo, Valenzuela, y otros 2006). Salir además de este círculo violento es muy difícil para personas que encuentran en él a amigos y familiares, generándose un intenso sentimiento de lealtad, facilitando la alienación de los jóvenes musulmanes. (Gill, Horgan y Deckert 2014).

2.4. *Factores de atracción*

Como refieren el Echeburúa y Corral (Echeburúa y de Corral 2004, 169) «*el fanatismo encuentra un caldo de cultivo adecuado en la inmadurez emocional de muchos adolescentes, que pueden resultar fácilmente manipulables*». Este periodo histórico, en el que prima la información rápida y poco contrastada, es el caldo de cultivo ideal para el pensamiento simplista y polarizado, fácilmente asumible sin necesidad de un proceso de digestión lento. En opinión de Haque, organizaciones como el Estado Islámico, favorece una ideología en la cual el mundo se divide en buenos y malos, y en el que el islam radical es la solución para todos los problemas de la humanidad, presentando de manera simple soluciones a grandes problemas. De este modo, la religión, como la etnia, la lengua y la cultura se convierten en factores de definición identitaria y distribuyen a la población según la lógica dentro-fuera, generando grupos. Que es lo primero que debe existir para que un conflicto sea posible. (Montesinos 2015).

En toda cultura, la religión puede jugar un papel central y, por lo tanto, generar efectos claros sobre distintos aspectos del comportamiento como lo pueden ser la forma en que se siguen las normas, patrones perceptivos, valores básicos, necesidades, motivaciones de logro, fórmulas de resolución de conflictos con otros colectivos sociales, etc. en el caso del yihadismo salafista hay una marcada intención de sesgar la hermenéutica coránica a favor de unos intereses políticos determinados, apelando a valores como hermandad, «*umma*» (comunidad musulmana) y lucha contra occidente, entre otros, utilizando el elemento unificador y de identificación de la cultura. (Trujillo, Valenzuela, y otros 2006, 292).

Si bien las redes sociales, juegan un papel fundamental como foco potencial de radicalización, el informe de Reinares y Calvo señala que solo un 18,4% de los detenidos en España se radicalizaron a través de manera *online*, situándose el *offline* diez puntos por encima. Siendo los entornos más proclives a la radicalización los domicilios privados, lugares de culto islámico y lugares al aire libre, así como los centros penitenciarios (Reinares y García-Calvo 2016).

3. El perfil del radicalismo en España

3.1. *Origen geográfico*

Según datos de la Unión de Comunidades Islámicas de España (Observatorio Andalusí 2016) residen en nuestro país 1.887.906 habitantes que profesan la religión musulmana, representando aproximadamente al 4% de la población total. Un crecimiento notable si tenemos en cuenta los datos que proporciona un reciente estudio (Berger 2016) basado en la encuesta realizada en 15 países por la *Pew Research Center* y que señala que en 2006, año en el que es realizada la encuesta, la población de origen musulmana en nuestro país reflejaba un 2% del total.

En cuanto a nacionalidad, el 41% han nacido o poseen la nacionalidad española, siendo extranjeros el 59% restantes, mayoritariamente marroquíes (el 40% de la población extranjera).

Esta población, no se distribuye de manera homogénea por todo el territorio, sino que está concentrada en algunos puntos del mismo, principalmente las ciudades autónomas de Ceuta y Melilla y las comunidades autónomas de Cataluña y Andalucía.

Estas comunidades y ciudades autónomas son un importante foco de radicalización, en especial en lugares que, por su contexto socioeconómico, cultural y demográfico se han convertido con el paso de los años, en guetos, barrios marginales, dentro de las propias ciudades.

3.2. *Edad*

El inicio del proceso de radicalización entre los detenidos en España por actividades relacionadas con actividades yihadistas radicaba en la horquilla de los 15-19 años de edad. Una media algo menor que la de otros estudios realizados con población reclusa europea (Bakker y de Bont 2016), pero que viene a demostrar que este rango de edad es una etapa evolutiva crítica en el que la percepción de apoyo social, los diferentes cambios sociales y la falta de oportunidades se convierte en factores de riesgo para la radicalización y posterior salto a las actividades terroristas.

3.3. *Sexo*

Mayoritariamente, el sexo de los detenidos por actividades relacionadas con el radicalismo y el terrorismo islámico en España

sigue siendo masculinúm. Sin embargo, el número de mujeres está creciendo rápidamente (Reinares y García-Calvo 2015). Convirtiéndose España, un lugar preferente para la captación y reclutamiento de mujeres. Además, las mujeres parecen estar adoptando un papel de mayor peso. Ya no se limitan al rol principal de concubinas y esposas, sino que participan de una manera proactiva en el terreno de la planificación y formación de potenciales terroristas.

3.4. *Espiritualidad*

La amplia mayoría de personas relacionadas con el terrorismo islamista en España (86,1%), son musulmanes de origen, el resto, de los casos se trata de conversiones. Sin embargo, los últimos informes que encontramos en España (Reinares y García- Calvo 2013) (Reinares y García-Calvo 2016), comparten los resultados de estudios internacionales (Bakker y de Bont 2016) en cuanto a la observación de los usos y costumbres del credo musulmán: presentan un elevado desconocimiento sobre su religión. En estudios internacionales, en los que se ha podido realizar un análisis individualizado de los yihadistas (Weggemans, Bakker y Grol 2014), destaca cómo en los meses previos a cometer actos de terrorismo, intensificaban la conducta religiosa, a través de las ropas, las continuas visitas a mezquitas o espacios de oración y estudios de textos y en el cumplimiento estricto de la observancia religiosa.

3.5. *Estrato socioeconómico y educativo*

Los últimos datos recopilados en España informa sobre el perfil sociodemográfico de los detenidos puestos a disposición judicial en España desde el año 2013 por actividades relacionadas con el Estado Islámico se caracterizan ante todo por ser hombres jóvenes, casados y con hijos, tanto españoles como marroquíes, en su mayoría con estudios secundarios y con tasa de desempleo similar a la de la población española en su conjunto. (Reinares y García-Calvo 2016). Estudios internacionales, están en consonancia con los datos que encontramos es España en cuanto a su estado civil. Entre los detenidos en Europa por actividades terroristas destacan los casados con hijos a pesar de la juventud. (Bakker y de Bont 2016) (Cano 2009). Sin embargo, el nivel educativo en España sí parece superior al de los países del entornúm.

4. La psicología en el estudio del terrorista

Desde la perspectiva psicológica, debemos entender la conducta terrorista como un fenómeno bio-psico-social, siendo el resultado de la interacción de un proceso social múltiple. En este sentido, el principal objetivo del terrorismo es transmitir un mensaje, no en una única vía, sino de manera que un grupo social trata de modificar la conducta de otros grupos a través de la violencia (De la Corte Ibáñez, y otros 2007) (Lawal 2002).

La Psicología social sugiere que las personas que exigen conductas terroristas son aquellas que además de estar inmersas en una cultura violenta, se encuentran en un tiempo de crisis que les convierte en más vulnerables para ser reclutados por las organizaciones terroristas vinculándolo a través de reglas ideológicas de tipo religioso, político o étnico, facilitando así el desarrollo de actitudes y creencias similares a la de sus pares (Trujillo, Valenzuela, y otros 2006).

Estos autores observan que la conducta terrorista es una justificación y legitimización de actos violentos con el fin de fortalecerse a ojos del grupo, reduciendo la disonancia cognitiva y las posibles dudas que sus actos pueden generar (Barrerto, Borja y López- López 2009) (Ramírez y Levi 2009) (Trujillo, Ramírez y Alonso 2009).

Sabucedo y colaboradores (2003), explica que una manera que tienen estos grupos de legitimar sus actos es atribuir al enemigo atributos muy negativos, haciéndole responsables de sus actos, siendo estos productos de una legítima defensa, deshumanizando al enemigo e incluso asociándolo con grupos nazis, fascistas o imperialistas (Sabucedo, Blanco y De la Corte 2003).

La necesidad de pertenencia al grupo fortalece a los nuevos miembros, convirtiéndose el grupo o red terrorista en el nuevo marco social de referencia, idealizando a los miembros de este, favoreciéndose así lazos afectivos y verdadera camaradería, que se traducirá en una percepción de pertenencia y posterior asimilación de la ideología imperante (Trujillo, Valenzuela, y otros 2006).

Como señalan estos autores, una visión social y estructural del terrorismo no explica completamente el fenómeno del terrorismo o incluso una aproximación de las posibles causas de naturaleza social que aumentan la probabilidad de que sucedan estas conductas violentas.

Desde el punto de vista biológico, algunos estudios con poblaciones violentas han mostrado que la agresividad es un descenso de la actividad serotoninérgica a la vez que aumenta la actividad dopaminérgica, lo que aparentemente tiene un origen genético (Gil- Verona, y otros 2002).

La conducta violenta en general puede estar asociada con la dificultad de aceptar normas sociales para la comprensión y resolución de conflictos, y además, tiene características hereditarias (temperamento) que afectan a la expresión de conductas agresivas de manera desproporcionada (López-López y Pineda 2011, 229).

Los sujetos que realizan actividades terroristas, no suelen caracterizarse por ser sujetos impulsivos, (de la Corte Ibáñez, y otros 2007) (Corner y Gill 2015) precisamente porque esa conducta podría ser un verdadero obstáculo para el desarrollo de esas actividades. Para McCarthy (2002), uno de los factores de riesgo que tienen la potencial conducta terrorista es que ellos mismos fueran víctimas de ataques de la misma naturaleza, especialmente en la adolescencia. De acuerdo con el autor, este es un momento crucial, en el que se unen la intensa búsqueda de sentido como factores biológicos (cambios hormonales, incremento de la adrenalina, intensidad de las emociones y sentimientos, etc.). De acuerdo con el aprendizaje que adquieren los sujetos jóvenes en el este proceso vital, toman parte hacia actitudes grupales (religiosos, étnicos, económicos, culturales etc.) y construyen sus propio sistema de estereotipos. Estos estereotipos son construidos a través de sus experiencias.

El problema de los estereotipos es cuando producen distorsión cognitiva, como es el atribuir características negativas a personas específicas y generalizarlas a un grupo entero con características similares.

Algunos autores señalan que entre las características de aquellos que abrazan la violencia como una forma de comunicación están las de la falta de cuidados hacia ellos o hacia otros, dificultades de empatía, mostrarse intolerantes hacia lo desconocido, rigidez cognitiva, falta de comprensión hacia el multiculturalismo y finalmente la deshumanización hacia los demás. (Wessells 2002) (McCauley, Psychological issues in the understanding terrorism and the response to terrorism 2002).

Dentro del rango de conductas con las que puede expresar un individuo su deseo de pertenencia al grupo, el vínculo con el

grupo juega un importante papel, el cual determina una cierta sensación de obligación y responsabilidad para con las actividades del grupo. Como explican Sabucedo y colaboradores (2003), las personas muestran su participación en un grupo activamente a través de su tiempo, dinero, habilidades, recursos o incluso dando su vida si fuera necesario.

5. Conclusión

El terrorismo es uno de los principales problemas a los que se enfrenta el mundo Occidente en general y Europa en particular, juegan un papel fundamental en la lucha contra este mal del siglo XXI.

Nuestro país no ha sido ajeno a la barbarie terrorista en las últimas décadas, si bien el fenómeno del terrorismo yihadista, parece abrirse con insistencia entre nosotros. La última década ha vivido amplio crecimiento de la sociedad musulmana en nuestro país, creciendo significativamente el número de personas nacidos y/o con nacionalidad española. Entre algunos jóvenes de segunda y tercera generación de los emigrantes, al igual que ocurre en otros países de nuestro entorno, se está detectando una vulnerabilidad hacia el radicalismo.

Buena parte de los estudios realizados sobre terrorismo yihadista han partido desde la ciencia política y la sociología, empleando una metodología subjetiva. Es necesario introducir líneas de investigación aplicando los principios científicos de investigación, con especial atención a los factores psicosociales determinantes en el reclutamiento y adoctrinamiento de terroristas para conseguir una mejor comprensión empírica de estos fenómenos.

A lo largo de este trabajo hemos explorado y analizado, desde la perspectiva de la Psicología, el fenómeno del terrorismo yihadista y su atracción por parte de estos jóvenes de segunda y tercera generación, estudiando las motivaciones y factores de presión y atracción que favorecen su inmersión en el mundo del radicalismo islámico. No podemos encontrar un perfil único de terrorista yihadista, puesto que las motivaciones, justificaciones, anhelos, expectativas y perfil de personalidad de cada individuo puede ser tan variado como las personas que integran estos grupos. Sin embargo, sí hemos podido señalar factores que precipitan esta

vulnerabilidad y a las que podemos mostrar especial atención con el objetivo de reducirlos.

Por parte de las autoridades es fundamental que se amplíen los presupuestos de lucha contra la radicalización, especialmente entre los jóvenes, creando programas en escuelas, centros penitenciarios y mezquitas.

Hay que implementar medidas a favor de la prevención educativa ante el desarrollo de posibles procesos psicosociales de radicalización islamista, especialmente en aquellos núcleos de población con más riesgo.

La Psicología es una ciencia imprescindible para el análisis, y comprensión de la conducta humana y como tal puede contribuir a desmontar la narrativa yihadista entre los jóvenes musulmanes, acercándoles a los valores propios de la sociedad occidental.

Agradecimientos

Este trabajo no habría sido posible sin la orientación, consejo y ayuda desinteresada del

Profesor Dr. José Manuel Rodríguez González.

También agradecer al Centro de Psicología del MAGEN en Sevilla, en especial al Comandante Psicólogo Diego Tomás Bascón Pachón su disposición, comprensión y apoyo para poder llevar a cabo este estudio.

Referencias bibliográficas

Atwood, J.B. «The Link between Poverty and Violent Conflict.» *New England Journal of Public Policy* 19, núm. 1 (2003): 159-165.

Bakker, E. and R. de Bont. «Belgian and Dutch Jihadist Foreign Fighters (2012-2015): Characteristics, Motivations, and Roles in the War in Syria and Iraq.» *Small Wars and Insurgencies* 27, núm. 5 (2016): 837-857.

Barrerto, I. H., Serrano, J Borja, and W López-López. «La legitimización como un proceso en ciencia política, medios de comunicación y construcción de culturas de paz.» *Universitas Psychologica* 8, núm. 3 (2009): 737-748.

Berger, L. «Local, National and Global Islam: Religious Guidance and European Muslim Public Opinion on Political Radicalism and Social Conservatism.» *West European Politics* 39, núm. 2 (2016): 205-228.

Cano, M.A. «Perfiles de autor del terrorismo islamista en Europa.» *Revista electrónica de ciencia penal y criminología*, núm. 11-7 (2009): 1-38.

Clark, R.P. «Patterns in the Lives of ETA Members.» *Studies in Conflict & Terrorism* 6, núm. 3 (1983): 423-454.

Comisión de las Comunidades Europea. «Afrontar los factores que contribuyen a la radicalización Violenta.» Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre la captación de terroristas., COM, Bruselas, 2005, 1-15.

Corner, E. and P. Gill. «A False Dichotomy? Mental Illness' and Lone-Actor Terrorism.»
Law and Human Behavior 39, núm. 1 (2015): 23-34.

Cronne, M. and M. Harrow. «Homegrown Terrorism in the West.» *Terrorism and*
Political Violence 23, núm. 4 (2011): 521-536.

De la Corte Ibáñez, L., A. Kruglanski, J. de Miguel, J. Sabucedo, and Díaz D. «Siete principios psicosociales para entender el terrrosimo.» *Psicothema* 19, núm. 3 (2007): 366- 374.

Echeburúa, E. and P. de Corral. «Raíces psicológicas del fanatismo político.» *Análisis y modificación de conducta.* 30, núm. 130 (2004): 161-176. 13.

Ferracuti, F. «A sociopsychiatric interpretation of terrorism. 129-140.» *The Annals of the American Academy of Political and Social Science*, 1982: 129-140.

Gill, P.J. Horgan, and P. Deckert. «Bombing alone: Tracing the motivations and antecedent behaviors of lone actor terrorists.» *Journal of forensic sciences* 59, núm. 2 (2014): 425-435.

Gil-Verona, J.A. et al. «Psicobiología de las conductas agresivas.» *Anales de Psicología* 18, núm. 2 (2002): 293-304.

Lawal, O. «Social-Psychological considerations in the emergence and growth of terrorism.» In *The psychology of terrorism*, by E Stout, 105-132. London: Praeguer, 2002.

Leiken, R. S. *Bearers of Global Jihad? Immigration and National Security After 9/11.*
Nixon Center, 2004.

López-López, W. and C .Pineda. «Terrorism: Two Complementary Approaches.» *Terapia Psicológica* 29, núm. 2 (2011): 225-231.

McCauley, C. «Psychological issues in the understanding terrorism and the response to terrorism.» In *The psychology of terrorism*, by E Stout, 131-156. London: Praeguer, 2002.

McCauley, C. and S. Moskalenko. «Toward a Profile of Lone Wolf Terrorists: What Moves an Individual from Radical Opinion to Radical Action.» *Terrorism and Political*
Violence 26, núm. 1 (2014): 69-85.

Montesinos, F.A. «Los componentes ideológicos del yihadismo.» *Cuadernos de estrategia* 173, núm. 3 (2015): 71-108.

Moyano, M. and H.M. Trujillo. «Intention of activism and radicalism among Muslim and Christian youth in a marginal neighborhood in a Spanish city.» *International Journal of Social Psychology*, 2014: 90-120.

Moyano, M. and M.H. Trujillo. «Incidentes críticos de violencia urbana vinculados al radicalismo islamista en España: simulación y análisis

de un escenario.» *Universitas Psychologica* 15, núm. 1 (enero-marzo 2016): 193-204.

Moyano, M. *Factores psicosociales contribuyentes a la radicalización islamista de jóvenes en España. Construcción de un instrumento de evaluación*. Granada: Universidad de Granada, 2011.

Neumann, P.R. «Foreign fighter total in Syria/Iraq now exceeds 20.000; surpasses Afghanistan conflict in the 1980s.» *International Centre for the Study of Radicalisation and Political Violence* 26 (2015).

Observatorio Andalusí. *Estudio demográfico de la población musulmana*. Madrid: UCIDE, 2016.

Post, J.M. and A George. *Leaders and their followers in a dangerous world: The psychology of political behavior*. Cornell University Press. 2004.

Ramírez, L, and S Levi. «Sentido común y conflicto: Impacto de las teorías legas sobre relaciones intergrupales.» *Universitas Psychologica* 9, núm. 2 (2009): 331-343.

Reinares, F. «Reinares, F. (2006). Towards a Social Characterization of Jihadist Terrorism in Spain Implications for Domestic Security and Action Abroad.» *ARI*, núm. 34 (marzo 2006): 1-8.

Reinares, F. and C. García- Calvo. *Los yihadistas en España: perfil sociodemográfico de condenados por actividades terroristas o muertos en acto de terrorismo suicida entre 1996 y 2012*. . Documento de Trabajo 3 (23) ,6., Madrid: Real Instituto Elcano, 2013.

Reinares, F. and C. García-Calvo. *El Estado Islámico en España*. Documento de trabajo, Madrid: Real Instituto Elcano, 2016.

Reinares, F. and C. García-Calvo. *Los yihadistas en España: perfil sociodemográfico de condenados por actividades terroristas o muertos en acto de terrorismo suicida entre 1996 y 2012*. Documento de Trabajo, 3 (23) ,6., Madrid: Real Instituto Elcano, 2013. Reinares, F, and C García-Calvo. *Terroristas, redes y organizaciones: facetas de la actual movilización yihadista en España*. Documento de trabajo, 17, Madrid: Real Instituto Elcano, 2015.

Rodríguez-González, J.M. and MP Ceballos-Rodríguez. «Aproximación psicológica al proceso de radicalización.» *I Congreso Internacional de Estudios Militares*. Granada, 2014. 1-16.

Sabucedo, J, A. Blanco, and L de la Corte. «Beliefs which legitimize political violence against the innocent.» *Psycothema* 15, núm. 4 (2003): 550-555.

Sageman, M. «The Psychology of Al Qaeda Terrorists the Evolution of the Global Salafi Jihad.» *Military psychology Clinical and operational applications*, 2006: 281- 294. Taarnby, M. «Recruitment of Islamist terrorists in Europe. Trends and perspectives.14

January, 2005, 42.» Research Report funded by the Danish Ministry of Justice. 2005, 1-57.

Trujillo Mendoza, H.M., C.C. Valenzuela, Moyano M., J. Gonzalez-Cabrera, and C. León. «De la Agresividad a la violencia terrorista.» *Psicología Conductual* 14, núm. 2 (2006): 289-303.

Trujillo, H.J. Ramírez, and F. Alonso. «Indicios de persuasión coercitiva en el adoctrinamiento de terroristas yihadistas: Hacia la radicalización violenta.» *Universitas Psychologica* 8, núm. 3 (2009): 721-736.

Trujillo, H.M. and M. Moyanúm. «El sistema educativo español en la prevención de la radicalización.» *Athena Intelligence Journal* 3 (2008): 75-83.

Trujillo, H.M., C León, D Sevilla, and J. González-Cabrera. «Riesgo de radicalización islamista en las mezquitas de una ciudad española.» *Psicología Conductual* 18, núm. 2 (2010): 423-440.

Trujillo, H.M., CC Valenzuela, Moyano M., J. Gonzalez-Cabrera, and C. León. «De la Agresividad a la violencia terrorista.» *Psicología Conductual* 14, núm. 2 (2006): 289-303.

Trujillo, H.M., F. Alonso, C. Jiménez-Ferrer, and Ramírez J.J. «Evidencias de manipulación psicológica coercitiva en terroristas islamistas.» *Athena Assessmentl*, marzo 2009: 1-15. van San, M. «Lost Souls Searching for Answers? Belgian and Dutch Converts Joining the Islamic State.» *Perspectives on Terrorism* 9, núm. 5 (October 2015): 47-56.

Victororoff, J. «The Mind of the Terrorist.» *Journal of conflict resolution* 49, núm. 1 (February 2005): 3-42.

Weggemans, D., E. Bakker, and P. Grol. «Who are they and why do they go: The Radicalization and Preparatory Process pf Dutch Jihadist Foreign Fighters.» *Perspectives on Terrorism* 8, núm. 4 (2014): 100-110.

Wessells, M. «Terrorism, social injustice, and peacebuilding.» In *The Psychology of Terrorism*, by E Stout, 57-73. London: Praeguer, 2002.

EL CONFLICTO DENTRO DEL CONFLICTO, DAULA VERSUS HIZBULLAH

Alejandra Hernampérez González

Resumen

Nos encontramos en la zona de Al Shams, en la Guerra de Siria, todos los ojos de occidente se ciernen sobre Dawla Al Islamiya y la población siria. No es lo único que está sucediendo. Estamos en lo que podría considerarse como un conflicto interno, según los Convenio de Ginebra de 1949, una «guerra civil» con diferentes bandos, pero internacionalizada.

No solo eso, dos grupos muy diferentes entre sí, uno de ellos, proveniente del Líbano, Hizbullah, contra Daula Al Islamí. No sólo diferentes por procedencia, sino también en lo que en religión se refiere. Un conflicto dentro de uno aún mayor. Sin olvidarme del contexto en el que se suceden todos los actos: refugiados y desplazados, las ayudas y apoyos que reciben cada grupo, la propaganda, los fundamentos religiosos… El apoyo exterior, el Líbano, Israel, Irán, Arabia Saudí...

Palabras clave:

Daesh, Hizbullah, califato, ideología religiosa, terrorismo.

0. Introducción

El Estado Islámico de Irak y Levante -ISIS- es una organización relativamente nueva, nacida tras la ocupación estadounidense de Irak en 2003. «Daesh» el acrónimo árabe que muchos árabes y extranjeros utilizamos para referirnos al ISIS. Nombre que detestan sus adeptos y, que suelen referirse a él como «*al Dawla al islamiya*».

Sus raíces ideológicas son mucho más antiguas y, se remontan a los primeros años del islam y a la generación de los primeros

musulmanes[1]. Los islamistas creen que la meta última de los verdaderos creyentes es establecer un Estado regido por las leyes de la sharía y gobernados por un califa[2]. El año 632, muerte de Mahoma, es el punto esencial de la ideología de Daesh. La idea del califato[3] ha sido un sueño sagrado que se ha ido transmitiendo de generación en generación entre los islamistas. Yihadistas célebres como Osama Bin Laden y Abu Musab al Zarqawi[4] albergaban ese mismo sueño. Desde un inicio, los yihadistas sirios han querido refundar un califato en Damasco (antigua capital de la dinastía de los Omeya[5]).

1. A comienzos del s.VII, Muhammad (571-632), que pertenecía a la tribu de los *Quraysh*, empezó a recibir revelaciones del arcángel Gabriel sobre la existencia de un único dios: Alá. Al principio la gente no creyó en el mensaje de Muhammad y, se produjo la Hégira o exilio en el año 622 que, marca el comienzo de la cronología árabe. En Medina, Muhammad organizó la primera comunidad de seguidores que se fueron multiplicando poco a poco. La nueva religión, Islam, comenzó a expandirse por toda Arabia hasta convertirse en el elemento unificador de todas las tribus dispersas que poblaban ese territorio. Los que se unieron a esta nueva fe, se les llamó musulmanes (creyentes).

2. Tanto suníes como chiíes coinciden en que un califa es un mandatario temporal del que se espera que gobierne «con justicia» dentro de los límites de la sharía. Los musulmanes suníes afirman que el linaje del califa debe remontarse directamente hasta la poderosa tribu de los *coraichitas* de La Meca o hasta cualquiera de sus subramas. Los musulmanes chiíes, creen que proceder de una familia notable de La Meca no basta para convertirse en califa. Los aspirantes potenciales han de descender, específicamente de *Ahl al Bayt* (familia del Profeta). Ello explica por qué Abu Bakr al Bagdadi insiste en usar dos apellidos cada vez que realiza una declaración o aparición pública: *Qurashi* y *al Hásani*.

3. Sistema político representado como un estado soberano de toda la fe musulmana, regido por una persona a la que se la denomina «Califa» bajo la ley islámica, sharía. También lo podemos definir como un sistema político único de la ideología del Islam que representa la unidad en referencia al líder de la *umma* o comunidad musulmana. Desde sus inicios, este fenómeno fue liderado por los discípulos de Muhammad, continuando el mismo sistema religioso que estableció el profeta, conociéndose como «*Califatos de Rashidun*». Cuando se habla de «califa» se hace referencia al sucesor de Mahoma significando que será el líder de la comunidad musulmana.

4. Ahmad Fadl al Nazal al Khalayleh, jordano (20 oct. 1966- 7 jun. 2006). Militante musulmán salafista, terrorista, que fue el líder de AQ en Irak. En 2005, declaró en una publicación la «guerra total» contra los chiitas en Irak.

5. El Califato Omeya fue el segundo de los cuatro principales califatos islámicos establecidos después de la muerte de Mahoma. La familia omeya, desde el miembro más antiguo, Ummayah Al-Akbar ibn ‘Abd Shams Banu ‘Abd Shams, nacido el 533 EC, había llegado primero al poder bajo el tercer califa, Uzmán (Uthman ibn

Se ven a sí mismos como una continuación de los poderosos líderes musulmanes, los sucesores del Profeta Muhammad: Abu Bakr al Sidiq, Omar ibn al Jabat, Utman ibn Afan y Ali ibn Abi Talid. Los primeros musulmanes, los cuatro verdaderos califas del islam sunní que, constituyeron el paradigma de la práctica islámica.

Los yihadistas salafistas[6] actuales afirman que quieren reformar el islam desde dentro, ayudando a liberar y purificar la fe de prácticas no islámicas. En la práctica, lo que pretenden es ver al mundo islámico regresar a su ética, sus virtudes y sus prácticas del prisma de la era primitiva musulmana, representada por los primeros califas.

Cuando el Daesh se apoderó de enormes proporciones de territorio en Siria e Irak durante el verano de 2014, muchos predijeron que se trataba de un fenómeno de corta duración que no tardaría en desaparecer. En 2016, este grupo terrorista ha afianzado su control sobre el territorio capturado, tras sobrevivir a una campaña de bombardeos masivos por parte de la Coalición Internacional desde septiembre de 2014 y, la aviación rusa desde septiembre de 2015. Ha instaurado su propio Gobierno, dotándolo de todos los atributos propios de un Estado.

Su califa, Abu Bakr al Bagdadi[7], ha recibido muestras de apoyo de grupos terroristas que actúan en diferentes zonas del mundo, como es el caso de Nigeria[8] y Egipto[9]. Además, su alcance ha

---

Affan) (r. 644-656), pero la dinastía Omeya fue fundada por Mu'awiya (Mu'awiya ibn Abi Sufyan), antiguo gobernador de Siria con Uzmán. Los Omeyas continuaron las conquistas musulmanas, incorporando el Cáucaso,Transoxiana, Sind, el Magreb y la península ibérica (Al-Andalus) en el mundo musulmán. En su mayor extensión, el Califato Omeya tenía unos 15.000.000 km², el imperio más grande que había visto el mundo hasta la fecha y el quinto más grande de los que han existido.

6. Afirman que quieren reformar el islam desde dentro, ayudando a liberar y purificar la fe de prácticas no islámicas. Pretenden ver al mundo islámico bajo el prisma de la era primitiva de los primeros musulmanes, representada en los primeros cuatro califas.

7. Nacido en Samarra, 28 de julio de 197. Es el autoproclamado califa de la banda terrorista Estado Islámico.Su nombre secular es Ibrahim Awwad Ibrahim Ali al-Badri al-Samarrai. El líder terrorista se autoproclamó nuevo califa de todos los musulmanes, exigiendo obediencia a los musulmanes de todo el mundo. Eligió el nombre de guerra Abu Bakr al-Siddiq, el primer califa del Islam, suegro de Mahoma, y a su vez el iniciador de la serie llamada de los califas ortodoxos.

8. En referencia al grupo terrorista Boko Haram.

9. En referencia al grupo terrorista Ansar Bayt Al Maqdis que actúa en la Península del Sinaí¨.

llegado hasta Europa, atentando en París en noviembre de 2015, en Bruselas en marzo de 2016 y en Niza en julio de 2016.

1. El conflicto sirio

El conflicto que se encuentra vivo en Siria comenzó el 6 de marzo de 2011. Ese día, un grupo de adolescentes fueron detenidos en Dara, sur de Siria, por dibujar en una pared un graffiti contra el régimen. Esta detención generó bastante molestar en la población que decidió realizar importantes manifestaciones en la ciudad, que fueron a su vez reprimidas por los Cuerpos y Fuerzas de Seguridad del Régimen. Se llegó abrir fuego contra los civiles, lo que provocó una serie de protestas que se fueron expandiendo por todo el país en cuestión de poco tiempo.

Aunque el régimen de Assad insiste en afirmar lo contrario, no parece que las protestas iniciales tuvieran una motivación ideológico-política, ni estuvieran planificadas. Lo que ha dado nombre a las llamadas «Primaveras árabes»[10], revueltas populares contra regímenes autocráticos y corruptos.

El primer incidente de rebelión armada se produjo en junio de 2011, en las proximidades de la frontera con Turquía[11]. Las movilizaciones se empiezan a extender por toda Siria, con una oposición armada. En julio de 2012, el Comité Internacional de la Cruz Roja (CICR) califica la situación en Siria como un conflicto armado interno[12], «guerra civil». Un conflicto que rápidamente se ramifica y que se internacionaliza.

Contra el régimen de Bashar al-Assad luchan numerosos grupos armados, todos con el objetivo común de derrocar al ré-

10. Blanc Altemir, A. «La comunidad internacional ante la llamada "primavera árabe"» en *Nosotros y el Islam*. 2012, pp. 46-84.

11. Civiles locales se hicieron con las armas de una comisaría de policía tras los disparos contra manifestantes de las fuerzas del régimen, parte de la unidad del ejército enviada a la zona deserta y, se une a los civiles armados en su lucha contra las fuerzas de seguridad.

12. Conflicto armados no internacionales, entre fuerzas gubernamentales y grupos armados no gubernamentales, o entre esos grupos únicamente. El derecho de los tratados de DIH también hace una distinción entre conflictos armados no internacionales en el sentido del artículo 3 común a los Convenios de Ginebra de 1949 y conflictos armadas no internacionales según la definición contenida en el artículo 1 del Protocolo adicional II.

gimen, pero no todos tienen de un proyecto político alternativo. Es necesario distinguirlos en dos grandes grupos:

—Los actores políticos, dentro y fuera de Siria, que se llaman «de la oposición». Al inicio hubo una unión en el *Consejo Nacional Sirio* (marzo 2011). Su falta de influencia sobre los grupos armados sobre el terreno y las luchas internas, forzaron a su sustitución (noviembre 2012) por el *Consejo Nacional de la Revolución Siria y las Fuerzas de Oposición*. Éste consejo es apoyado por el *Ejército Sirio Libre*.

—Los grupos yihadistas que se han ido convirtiendo en el elemento preponderante y, más peligroso para Occidente. Sólo mencionaré los grupos terroristas más significativos, que tienen entre sí una meta en común, la instauración en Siria de un Estado islámico:

- *Frente Al-Nusra* –Jabhat al Nusra- grupo afiliado a Al Qaeda (AQ). Creado en enero de 2012. Destaca el papel que tuvo su implantación en la práctica totalidad del territorio de Siria[13]
- *Estado islámico de Irak y Siria* nace en abril de 2013. Rompe con Al-Nusra y tiene un gran crecimiento. No se conoce el número total de sus integrantes, pero se cree que la mayoría de ellos son «Foreing Fighters». Actualmente, es el Estado Islámico (autoproclamado en el Ramadán de 2014) la organización que atrae en mayor medida a los radicales reclutados en los países europeos del Mediterráneo[14]
- A finales de 2013, alrededor de 50 grupos armados islamistas se reúnen y crean *Jaysh al Islam (el Ejército del Islam)*, con Zahram Allousch, ex comandante de Liwaa al Islam, que formaba parte del Ejército Sirio Libre, como líder.
- *Frente Islámico*, que desde noviembre de 2013, agrupa a varias organizaciones armadas rebeldes, entre las que destacan por su eficacia y fuerza en el combate Ahsrar-al-Saam, las brigadas Suqqor al-Sham y Liwaa al Tawheed.

13. Se encuentra presente y activo en 11 de las 13 regiones de Siria.

14. Reinares, F «Siria y la movilización yihadista en torno al Mediterráneo Occidental» Elcano 46/2014, de 7 de julio de 2014.

En los primeros meses del conflicto, se acordó una misión de investigación del Alto Comisionado de Derechos Humanos de las Naciones Unidas para determinar posibles violaciones cometidas y, también el Consejo de Derechos de Naciones Unidas pidió de manera expresa al Gobierno sirio el fin de los actos de violencia[15].

La resolución del Consejo de Seguridad 2043, de 21 de abril de 2012, autorizó al despliegue de la misión de observadores que debían verificar el cumplimiento de la «propuesta de los seis puntos» y del «cese de la violencia armada en todas sus formas por todas las partes». El primer mandato, daba 90 días para desarrollar la misión encomendada –UNSMIS[16]- debiendo vigilar el total cese de la violencia y los seis puntos de la resolución 2042; los cuales eras:

Colaboración con el enviado especial de las NNUU para el desarrollo de un proceso político que ampare las aspiraciones del pueblo sirio

1. Fin de los enfrentamientos y de la violencia en cualquiera de sus formas por ambas partes. Compromiso del Gobierno sirio de detener el avance de sus tropas y de la retirada de los efectivos en las cercanías de ciudades.
2. Facilitar la prestación de ayuda humanitaria en los lugares afectados por los combates.
3. Liberación de personas detenidas arbitrariamente o por el hecho de participar en actividades políticas pacíficas.
4. Libertad de circulación por el país a periodistas
5. Respeto a la libertad de asociación y al derecho de manifestación.

Los grupos yihadistas nacieron después del estallido de las hostilidades en Siria, sus raíces ideológicas se remontan a la rama siria de Hermanos Musulmanes. Si Mustafa al Sibai[17] fuer el padre

15. Resolución 19/22 del Consejo de Derechos Humanos, 23 de marzo de 2012.

16. El 16 de agosto de 2012 se acordó en el Consejo de Seguridad que el mandato de UNSMIS no sería prorrogado. El 24 de agosto los observadores internacionales ya no tenían que estar en territorio sirio porque el mandato había expirado.

17. Político sirio. Decano de la Facultad de Jurisprudencia Islámica y la Escuela de Derecho de la Universidad de Damasco. De 1945 a 1961 fue el líder del Frente Socialista Islámico, la rama siria de los Hermanos Musulmanes.

del islamismo político en Siria, Marwan Hadid[18] fue el padrino y fundador del yihadismo militante que hoy ejerce su influencia sobre miles de personas en el campo de batalla sirio.

A medida que el Frente al Nusra se expandía en los territorios controlados por los rebeldes, Abu Bakr al Bagdadi se sentía cada vez más indignado e incrédulo. El que había sido anteriormente su protegido, Abu Mohamed al Golani[19], le estaba dando un duro golpe al ver que no había seguido las instrucciones para crear el Estado Islámico de Irak y Levante, sino que había creado otro grupo terrorista que llegó a hacerse con grandes proporciones de tierra siria.

Al Bagdadi rechazó públicamente las directrices de AQ central, alegando que el mandato divino de ayudar a los hermanos en Siria debía prevalecer sobre cualquier otra consideración. Abu Mohammed al Adnani, portavoz del Daesh, lanzó un mensaje duro contra Al Zawahiri, en el que decía que la división de esfuerzos entre Siria e Irak propuesta por AQ central reconocía implícitamente la arbitrariedad de las fronteras, fruto de años de colonización. También cuestionó que hubiera tomado esa decisión sin consultarles, acusándole veladamente de tiranía[20]. Se abrió así una profunda brecha entre AQ central y el Daesh.

En mayo de 2013, incapaz de ocultar su frustación, Al Bagdadi se presentó en Alepo y empezó a reclutar personalmente a miembros de Al Nusra para integrarlos en el recién formado Daesh, tentándoles con duplicarles la paga. Al Golani pagaba a sus hom-

18. Nació en el seno de una familia rica de origen albano en 1934. Uno de sus hermanos era baasista, mientras que otro era comunista. Se unió a los Hermanos Musulmanes en su etapa universitaria; estudiaba agricultura industrial en la Universidad Ayn Shams de El Cairo. Sus seguidores le concedieron el título honorario de «jeque» cuando empezó a enseñar en la mezquita de Barudiya, a pesar de que nunca había sido oficialmente en la sharía. Nunca fue un *alim*.

19. Su nombre de guerra indica que desciende de una pequeña aldea situada en los ocupados Altos del Golán. Anunció la creación de Jabhat al Nusra mediante un mensaje de audio publicado en internet a principios de 2012. Nacido en 1979 en el este de Siria en el este de la ciudad petrolera de Deir ez Zor. Meses después de la muerte de Bin Laden, al Golani juró lealtad al líder de AQ, Ayman al Zawahiri. De ese modo, el Frente al Nusra se convirtió en la rama oficial de AQ en Siria.

20. Jordán, J «El Daesh». Cuaderno de Estrategia 173. *La internacional yihadista*. IEEE,

bres hasta 400$ mensuales; al Bagdadi aumentó el sueldo hasta 800$[21]. Eso animó a muchos a cambiar de bandera, también contribuyó que la popularidad Al Nusra había empezado a caer. Los enemigos de al Golani parecían aumentar con la misma rapidez con la que en otro tiempo había aumentado sus seguidores. Los activistas laicos acusaban a al Golani de «secuestrar la revolución pacífica».

Los altos mandos de AQ negaron toda relación con Daesh en febrero de 2013. El 16 de abril de 2014, al Bagdadi envió a al Golani un mensaje muy claro y contundente: asesinó a su máximo jefe en Idlib. Un mes más tarde, ambos grupos terroristas entraron en combate en la ciudad natal de al Golani, Deir ez Zor. En junio de 2014, la rama de al Nusra en la localidad siria de Bukamal juró fidelidad al Estado Islámico. El 13 de noviembre, el Daesh como al Nusra, anunció una tregua. Al Golani y al Bagdadi se reunieron y anunciaron el fin de las hostilidades y declararon que era la hora de unir fuerzas contra el régimen sirio y la Coalición Internacional[22].

El 29 de junio de 2014, Al Adnani anunció la restauración del califato en la persona de Abu Bakr al Bagdadi, y el 4 de julio hizo su primera aparición en la gran mezquita de Mosul[23] proclamando que bajo su guía la *umma* recobraría su «dignidad, poder y derechos».

El papel de la mujer en Daula al islamí

El 10% de la comunidad yihadista europea de Siria está constituido por mujeres de entre dieciocho y veinticinco años. El Gobierno sirio no dispone de la cifra oficial y, los yihadistas tampoco. Ambas partes parecen pensar que, dado a que no participan en las batallas, esas mujeres no merecen ser contadas, ni en muchos casos, analizados.

21. Moubayed, S. *Bajo la bandera del terror. Un viaje a las entrañas de Daesh.* Ed. Península Atalaya. Mayo 2016. p 114.

22. El 10 de septiembre de 2014 el presidente Obama anunció por cadena nacional y al mundo que Estados Unidos formará una coalición internacional para bombardear Siria e Irak.

23. La presentación de Al Bagdadi en la mezquita de Mosul tiene gran carga histórica, debido a que Mosul había sido una capital en tiempos del califato abasí; igual que lo fue Samarra, lugar de nacimiento de Al Bagdadi.

La Fundación Quilliam estima que 200 mujeres europeas se han trasladado a Siria desde el inicio de la guerra de 2011. Todas ellas se casaron con combatientes, bien del Daesh, bien del Frente al Nusra. Al menos setenta de ellas son francesas; 40 son alemanas; 60 británicas; 20 belgas y 35 holadensas[24]

Muchas de las mujeres que han partido hacia Siria revelan una comprensión escasa y superficial del conflicto sirio y del islam. De hecho, la mayoría de ellas lo ven sin matices: buenos contra malos; suníes contra chiíes; musulmanes contra cristianos. Algunas había oído hablar de los hechos de Hama de 1982, pero sólo por lo que les habían contados sus maridos a la llegada del país. Ninguna había tenido la menor relación ni con los Hermanos Musulmanes de Siria o AQ. Aunque habían memorizado ciertos versículos del Corán, en especial los que hacían referencia al velo y al papel de la mujer, demuestran un conocimiento deficiente del islam, su historia, su evolución y sus códigos de conducta.

Esa comprensión limitada de la religión es frecuente tanto entre las mujeres como entre los hombres europeos que acuden a Siria, lo que los convierte en blanco fácil para los reclutadores de Daesh, y en carne de primera línea de infantería una vez que se han unido a las filas de la organización.

Ninguna de las mujeres europeas que se han desplazado a Siria, saben leer el Corán en árabe. Todas se basan en traducciones inglesas, publicadas desde Arabia Saudí. Sin embargo, la mayor parte de lo que memorizan es en árabe. Las preparan para que repitan lo que oyen, palabra por palabra, y ellas articulan con dificultad los nombres, y después repiten las frases en público. La occidental más joven a unirse a Daula tenía apenas trece años[25] Daula se ha implicado tanto en el reclutamiento de mujeres extranjeras que ha abierto una «oficina de matrimonios» en la localidad de al Bab, cercana a la frontera con Turquía[26]. Ahí es donde las mujeres que llegan de occidente son registradas y donde las casan oficialmente con sus novios yihadistas. Se anotan sus perfiles y se describe a los yihadistas que buscan esposa –a las

24. Brenda Stoter «European Women convert, join IS» *Al Monitor,* 29 de octubre de 2014.

25. Sherwood, «Schoogirl jihadis: the female islamist leaving home to join Isis fighters», *Guardian.* 29 de septiembre 2014.

26. «ISIS fighters open «Marriage Bureau», *Al Arabiya,* 28 julio 2014.

parejas no les está permitido verse hasta que concluye la ceremonia del enlace. En el islam, la aprobación paterna es esencial en todo matrimonio. Se trata de una cuestión complicada que ha ralentizado el proceso, afirma Jennifer, la esposa estadounidense de un oficial de Daula, Zain al Abidin al Shami.

En algunos casos, el autoproclamado Estado Islámico nombra a un tutor, por lo general un anciano del lugar, para que «bendiga» el matrimonio. Algo válido en el islam, señala, algo que el propio autodenominado califa, al Bagdadi, ha casado a una de sus primas con un yihadista extranjero, y ha actuado en nombre de su difunto padre durante la ceremonia religiosa.

Estas mujeres gestionan día y noche, unas páginas de Facebook asociadas a Daesh, además de sus propias cuentas de Twitter e Instagram. Están en casi todas las redes sociales del Estado Islámico. Aunque Daula cuenta con unos canales oficiales, como son Hayat Center, la Fundación Itisam, Dabiq, éstos suele gestionarlo una generación de mayor edad, más focalizada con la burocracia y de la línea más rígida. El material que estas mujeres publican en las redes sociales, está bien preparado y resulta muy actual. Se dirige tanto a mujeres musulmanas como a cristianas de Europa. Casarse con un yihadista es una buena obra. Casar a un yihadista con una mujer no musulmana que se ha convertido al islam es aún mejor. A las mujeres europeas se las llama «hermanas», y se les dice que si se trasladan a Siria, su labor será casarse; no ser objetos sexuales de libre disposición para los yihadistas. A esas mujeres se las convence para que abandonen su vida anterior en Occidente, y se las convence no contándoles lo pecaminosa que es, sino más bien concentrándose en lo distinta y mejor que sería su nueva vida bajo el autoproclamado Estado Islámico. Las fotografías de bodas intentan potenciar la sensación de estar haciendo algo útil para la comunidad yihadista, y hablan del «honor» que representa ciar a hijos para que se conviertan en nuevos combatientes del islam.

Aqsa Mahmud —alias Um Layth— es la mujer de Daesh más conocida en las redes sociales. Se trasladó desde Glasgow hasta Siria en noviembre de 2013 y, actualmente escribe un blog todos los días para la organización yihadista. Con más de 2.000 seguidores en Twitter, empezó a escribir, en inglés, el «*Diario de un mujahirah*». En septiembre de 2014, hacía un llamamiento a otras europeas: «*a aquellas que aun sean capaces y puedan emprender el via-*

je…daos prisa en vuestra tierra… Ésta es una guerra contra el islam y ya se sabe que «se está con ellos o con nosotros». Así que escoged de bando»[27]

2. Daula Al Islamí Vs Hizbullah

A menudo, los conflictos armados no internacionales[28] pueden tener repercusiones internacionales que terminan involucrando a actores externos. Casi desde su inicio, la guerra en Siria se convirtió en un escenario en el que diversos actores estatales y no estatales, miden sus fuerzas e influencia. Países como Arabia Saudita, Qatar o Turquía, se han comprometido con el derrocamiento del gobierno del presidente Bashar al Assad y, han apoyado a diversos grupos rebeldes de orientación takfirí-yihadista.

Por otro lado, la República Islámica de Irán, con el que el gobierno sirio tiene una «antigua amistad», ha intervenido en el conflicto proporcionando apoyo logístico y militar al gobierno de Damasco. También nos encontramos con fuerzas no-estatales foráneas, como la organización chiita libanesa Hezbollah, que ha desempeñado un papel militar importante para el gobierno sirio. Sus vinculaciones con el llamado *Eje de la Resintencia* y otras milicias chiitas.

Al inicio de la Primavera Árabe en diciembre de 2010, Hezbollah expresó su simpatía por las protestas populares en países como Libia, Bahréin, Túnez y Egipto. En el caso de Siria, Hezbollah consideró que los manifestantes sirios tenían «demandas legítimas» que debían ser encauzadas a través del diálogo y sin el uso de la violencia.

Hezbollah busca preservar el llamado *Eje de la Resistencia* (*jabhat al muqawama)*, una alianza integrada por ellos, Irán, Siria, y Hamás, y a la que se vinculan también otros actores no estatales, como algunas milicias chiitas que operan en Siria e Irak. Éste Eje de la Resistencia ha articulado en los últimos años la oposición a las políticas de Israel, EEUU y sus aliados árabes en la región y, a partir del empoderamiento de grupos suníes radicales como

27. Um Layth, *Diary of a Muhajirah,* 3 de junio 2014.

28. artículo 3 común a los cuatro Convenios de Ginebra que dice así: el conflicto armado interno comprendería las acciones armadas en el interior de un Estado que dan lugar a hostilidades dirigidas contra un gobierno legal, que presentan un carácter colectivo y un mínimo de organización.

Daesh o el Frente al Nusra, el Eje también ha incluido al *takfirismo* como uno de sus enemigos.

Para Hezbollah, la intervención en el conflicto sirio es una expresión más de la «resistencia» contra Israel, así como una «guerra contra el terror» que tiene una transcendencia existencial. Para Hassan Nasrallah, la «nación islámica enfrente el peligro de una nueva Nakba, la del takfirismo estadounidense-sionista»: «la nueva Nakba es más peligrosa que la de 1948 o 1967 puesto que el pueblo palestino ha permanecido, y ha luchado siempre por sobrevivir y continúa existiendo. Sin embargo, la nueva Nakba amenaza no sólo la existencia y presencia del pueblo palestino sino también la del resto de pueblos y Estados de la región, como sucede en el caso de Siria, Jordania, Egipto, Irak, Yemen, Arabia Saudi, Pakistán y Afganistán. Países enteros están amenazados por la división, las guerras, la partición y la desaparición debido al takfirismo»[29].

La amenaza takfirí debe ser «derrotada a cualquier costo» según los líderes de Hezbollah. El Vicesecretario General, Sheik Naim Qasem, decía en febrero de 2015: «Vivimos un momento de lucha para liberar nuestros territorios ocupados (por el régimen de Israel). No pretendemos desencadenar una guerra, pero tampoco dejaremos que nos amenacen con ella… La resistencia es el único camino que lleva a la independencia y garantiza el futuro del Líbano. ¿Por qué la llamada coalición internacional está autorizada a luchar contra los takfiríes, y el Eje de la Resistencia lo tiene prohibido?»

Garantizar la supervivencia de Hezbollah, preservar los equilibrios políticos locales y su primacía en la política libanesa, así como su condición de cabeza de la «Resistencia» al Este del Mediterráneo, demanda una participación directa en el conflicto sirio, que no podía limitarse a una «solidaridad moral» con Damasco.

Más allá de las razones políticas y estratégicas, Hezbollah interviene en la guerra siria por razones religiosas, como son:

—Proteger los lugares santos del chiismo en Siria
—Protección de las poblaciones chiitas en las áreas fronterizas

29. Fernández. «Sayyed Nasralá: nuestra nación afronta una nueva Nakba» *Foreing Policy*. Julio 2015.

Según la organización *Shia Rights Watch*, los chiitas sirios son los más afectados desde el origen de las Primaveras Árabes, sometidos regularmente a asesinatos masivos, secuestros, desplazamientos forzosos y, la destrucción de sus lugares sagrados.

Tanto las amenazas a los chiitas sirios y a sus lugares santos, como a los que viven en aldeas situadas a un lado y otro de la frontera con Siria, han sido para Hezbollah una de las principales razones para intervenir en el conflicto armado. Se trata de un panchiismo[30] que tiene también combatientes voluntarios de otros países de la región, como son Irak, Pakistán y Afganistán.

La participación de Hezbollah en el conflicto sirio ha sido un proceso ascendente y marcado por la cautela. Hasta principios de 2012, la organización intentó evitar una participación directa, limitándose a brindar asesoramiento al gobierno sirio y, a dar protección a los santuarios chiitas como Sayyida Zaynab y a aldeas chiitas libanesas al este del Valle de Bekaa.

La situación empezó a cambiar en octubre de 2012, cuando se conoció la muerte de Ali Hussein Nassif, uno de los combatientes con más experiencia en las filas de Hezbollah. La cadena *Al-Manar* reconoció que Nassif había muerto en el marco de «actividades de yihad». Tras este anuncio, Hasan Nasrallah reconoció unos días después que miembros de la organización habían luchado contra los rebeldes sirios, pero puntualizó que «estaban actuando por su propia cuenta, no bajo la dirección del partido»[31].

Hacia principios de 2013, el perfil de Hezbollah en el conflicto armado empezó a cambiar significativamente, asumiendo un papel de actor involucrado junto al gobierno sirio. A mediados de 2013, la participación de Hezbollah constituía un factor decisivo en algunas de las victorias militares del régimen de Assad en el Valle de Bekaa y, específicamente en al Qusayr.

La victoria militar en Al Qusayr implicó un alto coste, pues sólo en la primera semana de la ofensiva Hezbollah perdió alrededor de cien combatientes. Esta batalla demostró que, en comparación con las tropas del gobierno sirio, e incluso con los rebeldes sirios, los

30. El panchiismo en Siria ha sido sólidamente apoyado tanto por Hezbollah como por Irán, a través de los Cuerpos de la Guardia Revolucionaria Islámica que, ha desempeñado un papel fundamental en el proceso de reclutamiento, entrenamiento y desplazamiento de combatientes chiitas hacia Siria.

31. Al Arabiya, *Hezbollah members bury fighters killed in Syria battle: report*. 2013.

combatientes de Hezbollah eran mucho más capaces de implementar tácticas sofisticadas. Lo que demuestra que la participación directa de Hezbollah en el conflicto armado suponía un valor añadido a las fuerzas del gobierno. Gran parte de las actividades militares de Hezbollah son concertadas en Damasco con el gobierno sirio.

Actualmente, Daesh sigue luchando en numerosos frentes: contra el ejército iraquí y las milicias chiíes en varias provincias iraquíes; contra los kurdos en el norte de Irak; contra varios grupos de la oposición; contra el ejército sirio en Deir ez Zor; y la organización Hezbollah.

La intervención actual de Hezbollah en Siria, en apoyo del régimen de Assad pone en entredicho el carácter o justificación como movimiento de resistencia. La implicación en la guerra de Siria, a partir de 2012 en Damasco, y en la región de al Qusayr a comienzos de 2013 ha generado importantes efectos, como los que nombro a continuación:

—El desarrollo de las capacidades de combate, de mando y control y de inteligencia de Hezbollah
—Éxitos en campo de batalla, que refuerzan capacidades y autoestima
—Un papel fundamental en el mantenimiento del régimen de Assad
—La pérdida de muchos de sus miembros, en una estimación superior a mil
—El ataque en bastiones de Hezbollah en Líbano, realizados por grupos suníes

Ante el incierto futuro de Assad, la organización política ha desplazado armamento y misiles, desde Siria hasta bases en el este del Líbano. La caída del régimen sirio sería trágica para Hezbollah.

No existen cifras aproximadas sobre el número de miembros de Hezbollah en Siria. Pero se habla de una presencia de 10.000 combatientes del grupo en Siria, cifra que no está confirmada pero que parecen excesivos, y posiblemente obedezca al propio objetivo de sobredimensionar sus capacidades. En cuanto a las pérdidas, Hezbollah ha podido perder alrededor de una quinta parte de los combatientes profesionales de la organización.

Hay que sumar un elevado número de voluntarios, y simpatizantes a lo largo de todo el mundo, y el empleo de las brigadas

libanesas de resistencia «*Saraya al Muqawamaal Lubnaniya*», entrenados militarmente y que, están siendo activados ante la amenaza procedente de Siria y para el propio Líbano, por parte de grupos terroristas como el Daesh y al Nusra.

En relación a la estructura operativa que Hezbollah ha desplegado en Siria, incluye medidas de espionaje técnico que emplean medios tecnológicos. También cuenta con brigadas encargadas de establecer hospitales de campaña móviles, cuyo número y extensión dependen de la batalla y las fuerzas implicadas en ella y, que incluyen médicos especialistas, cirujanos, anestesistas…

En consecuencia de la participación en el conflicto de Siria, Hezbollah añade las capacidades de infantería, misiles, unidades más grandes y, enfrentamientos en campo abierto en Siria, así como operaciones ofensivas en el entorno urbano. Han sido capaces de entrenar al ejército sirio con técnicas de guerrilla, mientras que también han ganado capacidades en mando y control, y coordinación en combate con otras fuerzas.

Batalla de Qalamoun

Los combates en Qalamoun[32] han sido, hasta el momento, uno de los escenarios de operaciones militares más importantes de la intervención de Hezbollah en Siria.

En agosto de 2014, las Fuerzas Armadas del Líbano fueron capaces de cortar muchas de las rutas de abastecimiento del Frente al Nusra en Arsal, pero eso no impidió que esa organización siguiera lanzando ataques contra las posiciones fronterizas. Con el ingreso de Daesh a Qalamoun a finales de 2014, abrió una confrontación entre el Frente al Nusra y Daula, que favoreció al gobierno sirio.

Entre mayo y junio de 2015, Hezbollah lanzó una ofensiva junto al Ejército Sirio Árabe contra el Frente al Nusra y otros grupos

32. Las montañas de Qalamoun son la porción nororiental de la Cordillera del Antilíbano, se extienden unos 80 km de norte a sur y tienen unos 40 km de ancho. La población de la zona está compuesta por diversas afiliaciones religiosas, incluyendo algunas aldeas cristianas. La zona alberga varias bases militares, algunas de las cuales llegaron a estar en mano de los rebeldes, posibilitándoles lanzar cohetes contra posiciones del gobierno sirio. El Ejército Libre Sirio, el Frente al Nusra y Daesh, han utilizado el área para establecer líneas de suministros y combatientes hacia y desde Arsal.

rebeldes. Se trató de una serie de ataques rápidos realizados por parte de la milicia chiita que, obligó a los rebeldes a abandonar gran capacidad de posiciones, dejando incluso abandonado el equipo de combate.

El 11 de mayo, el Ejército Sirio Árabe y Hezbollah tomaron la colina de Al Barouh, a las afuera de Al Juba, como otras cinco aldeas. Avances posteriores permitieron tomar Tallat Mussa, en el cruce fronterizo de Ras al Marra Arsal, y las colinas del oeste de Tal Tahljah.

En junio, Hezbollah se enfrentó por primera, vez en el campo de batalla, con Daula y, según *The Daily Star* perdió ocho combatientes y cuarenta y ocho militantes. El Secretario General de Hezbollah, afirmó un día después que el Ejército Sirio Árabe y Hezbollah tenían el control de la mayor parte de la cordillera. El 23 de junio, las brigadas del Ejército Sirio Árabe en coordinación con Hezbollah y las milicias sirias de las Fuerzas de Defensa Nacional, avanzaron a la zona de Jaroud Qarah, lanzando un ataque contra las posiciones de Daula.

Esta victoria ha sido ampliamente resaltada por Hezbollah. Para su Secretario General, Hassan Nasrallah, se trató de «un éxito militar sin precedentes», mientras que Sheik Naim Qasem lo definió como un «punto de inflexión en el conflicto con los grupos takfiríes», subrayando que la Resistencia está preparada para hacer frente a todos los desafíos.

La batalla de Qalamoun no tiene un carácter decisivo en el conflicto armado, pero indudablemente se ha tratado de un avance que denota las capacidades de combate de Hezbollah. Los comandantes de la organización planearon ciudadosamente la ofensiva y, previamente llegaron a cabo una minuciosa recopilación de información de inteligencia sobre el despliegue de los rebeldes, para lo cual recurrieron al uso de aviones no tripulados para poder obtener la mayor información posible.

Uno de los elementos que facilitó la victoria es que, el área de Qalamoun posibilitaba realizar un ataque con el estilo de «guerra de guerrillas» que Hezbollah ha empleado contra los israelíes en el Líbano y, de lo que tienen un gran conocimiento ofensivo.

Son este tipo de habilidades las que han empoderado a Hezbollah, pero también muestran cómo al Assad parece cada vez más dependiente de las capacidades militares de la organización; debido sobre todo a la escasez de recursos humanos y especialmente

de tropas de infantería eficaz. Ante esta debilidad del gobierno sirio para hacer frente por sí solo a los desafíos del conflicto armado, Hezbollah ha tenido que enviar cada vez más tropas, como cuerpos de élites como combatientes jóvenes.

La presencia militar de Hezbollah se concentra en los territorios situados en el Valle de Bekaa y las montañas de Qalamoun, en el área de al Qusayr, Al Zabadani y, ciertos santuarios chiitas en el corazón de Damasco, hay combatientes de Hezbollah que trabajan reforzando al gobierno sirio.

3. Cómo se posicionan los países de oriente medio en el conflicto

La actual rivalidad entre Arabia Saudita e Irán tiene un aspecto de intereses, pero la raíz del conflicto estriba en razones ideológicas de profundas raíces históricas, en la pugna entre sunnitas y chiitas.

Entender que la religión en el mundo musulmán juega un papel político importante mucho más que en Occidente, aún más entre Arabia Saudita e Irán, cuyos regímenes políticos basan su legitimidad en razones religiosas.

Ambos Estados se consideran mucho más que Estado-nación (en el sentido wetsfaliano), son ajenos a la cosmovisión política del islam y, ambos se consideran «más que un Estado» aspirando a ser la cabeza del Islam con vocación de dominio global.

La rivalidad hunde sus raíces en el cisma religioso que sufrió la *umma* casi desde su nacimiento –siglo VII-. Dentro del islam existen dos confesiones principales, el chiismo y el sunnismo. En su origen, la principal diferencia era estrictamente una cuestión sucesoria, entre los que defendían que el sucesor de Muhammad debía ser de la familia del Profeta y, consideran sucesor de Muhammad a Alí, su yerno (chiitas, seguidores de Ali) y, los que propugnaban el método tradicional árabe de elección entre los notables de la tribu (sunnitas de s*unna*, tradición). Dos facciones irreconciliables, enfrentadas en el campo de batalla.

Ambas confesiones comparten la creencia de que el poder es único y procede de Alá, todos los musulmanes forman una «comunidad de creyentes», *umma*, carentes de fronteras internas y que debe ser liderado por un único dirigente religioso-político, el Califa; éste debía ser árabe y pertenecer a la tribu *Quraish* –la de Muhammad.

Al Bagdadi se ha añadido el sobrenombre de «*al Quraish*», para indicar su dudosa pertenencia a la tribu *Quraish*. El carácter electivo original del califato permite a cualquier dirigente musulmán optar a este título, aunque es difícil que los árabes acepten como Califa a un musulmán no árabe[33].

Durante casi mil quinientos años, los chiitas han sido la parte desfavorecida del Islam, desarrollando una mentalidad que podríamos definir como «pueblo mártir» y de subordinación a los sunnitas.

Irán es indiscutiblemente la cabeza del chiismo, y por su posición geoestratégica como productor de petróleo y gas y, por su control del estrecho de Ormuz ejerce una influencia más que regional. Presenta un atractivo adicional debido a la «revolución islámica» que derrocó una dictadura apoyada por EEUU y, que además, ha resistido grandes presiones occidentales para derribarla. Es un Estado «revisionista» que considera que el orden mundial es injusto y se esfuerza en modificarlo según sus intereses.

La consideración de Irán como defensor de los «desfavorecido» que a nivel internacional se traduce en, la búsqueda de alianzas con Estados situados estratégicamente en áreas muy alejadas pero unidos con un enfrentamiento activo con EEUU (caso de Corea del Norte, Venezuela, Cuba o Nicaragua), alianzas que le dan una mayor proyección internacional.

Preservar los intereses del *Eje de la Resistencia* es también una cuestión de gran importancia estratégica para Irán. El apoyo de Hezbollah al gobierno sirio no puede considerarse al margen de las relaciones de apoyo y solidaridad que se triangulan entre los tres actores del Eje. Desde inicios de los ochenta, cuando Damasco decidió apoyar a la República Islámica de Irán en la guerra que había iniciado contra Sadam Hussein, Siria ha sido el principal apoyo árabe de Irán. Así lo expresaba en enero de 2012 Ali Akbar Velayati, asesor de Asuntos Exteriores del Líder Supremo de Irán, Ali Khamenei, «la cadena de la Resistencia contra Israel por parte de Irán, Siria, Hezbollah, el nuevo gobierno iraquí y Hamas, pasa a través de la vía siria. Siria es el anillo de oro de la cadena de la resistencia contra Israel»

Teniendo un gran protagonismo en política exterior, lo que implica a su relativo apoyo a Assad en Siria, Hizbulah en el Líba-

33. Para los sunnitas, los árabes son superiores al resto de los musulmanes, según la doctrina de la *kafaa*, impuesta por el califa Omar.

no, o a los rebeldes hutíes en Yemen. Sin embargo, Irán no es un país árabe, lo que dificulta que un iraní pueda ser líder del Islam.

Por su parte, Arabia Saudita, a través de sus ingresos por el petróleo le ha permitido financiar movimientos yihadistas en todo el mundo, proporcionándole una influencia muy importante en gran parte del mundo musulmán y entre las comunidades de inmigrantes musulmanes en Europa. Tiene en su territorio los dos lugares más santos de la religión islámica —La Meca y Medina—, la Casa de Saud, arrebató por la fuerza en 1926 estas dos ciudades a la casa real jordana[34]. Su legitimad para encabezar el islam sunnita se basa mucho más en la riqueza procedente del petróleo que en ninguna razón religiosa o histórica. Pese al apoyo de la dinastía saudí al «wahabismo».

Para los chiitas, la cuestión del Califato es un tema resuelto —el *Mahdi* oculto sigue siendo el Califa— y la existencia de una jerarquía eclesiástica reconocida le permite una fuerte unidad doctrinal que, por la unicidad del poder en el mundo islámico, se traduce en unidad de acción política. El mundo sunnita, sin embargo, se encuentra dividido en multitud de facciones, y con varios Estados optando como mejor o peor fortuna a encabezar el islam sunnita.

Conclusiones

La intervención de Hezbollah en el conflicto sirio ha supuesto un punto de inflexión en la historia de la organización. La organización chií decidió hacer frente a lo que considera como «una amenaza existencial» que pretende eliminar a todos los chiís y, por ende al *Eje de la Resistencia*. Un desafío imposible de evadir.

Desde el punto de vista militar, las ganancias parecen superar a las pérdidas. La intervención de Hezbollah ha sido vital para la derrota de diversos grupos rebeldes al este de la frontera con el Líbano.

Tras tres años de participación en la guerra de Siria, la organización libanesa mantiene una aureola de «invencibilidad». Por

34. Que había tenido el título de Protectora de las Ciudades Santas de Medina y La Meca desde el s.X y que, es generalmente reconocida en el mundo musulmán como descendiente del profeta Muhammad, por lo que cuenta con mayor legitimidad para reclamar el liderazgo del Islam

otro lado, la guerra siria ha permitido a Hezbollah perfeccionar habilidades de combate, lo cual representa un valor añadido, que representa de cara al conflicto que mantiene con Israel.

El mapa de quien controla cada zona de Siria actualmente está lleno de divisiones. El régimen de Asad -Ejército y milicias afines- tiene una gran parte del oeste del país, Damasco, Latakia, Tartús, casi toda la frontera con Líbano, una parte de Alepo, otra en el centro del país y en Deir Ezzor. La otra parte, se encuentra prácticamente bajo el dominio de Daesh. Pero gracias a la Coalición Internacional, Rusia y Hezbollah, Daesh está perdiendo terreno dominado. Controlan un trozo de Alepo, en el norte, una zona amplia de la provincia de Idlib, fronteriza con Turquía, un área cercana a Damasco y otra en Homs.

Los grupos rebeldes están presentes en la frontera entre Siria e Israel (Altos del Golán, territorio sirio ocupado por los israelíes desde 1967). Pero «casi toda la línea fronteriza con Israel está en manos del Frente al Nusra», señala el portavoz del Ejército israelí, Peter Lerner.

La franja norte, a lo largo de la frontera con Turquía y una parte de la iraquí, está en manos de las fuerzas kurdas, a excepción de unos tramos que controlan los rebeldes y el EI. Los yihadistas tienen una parte del este de Siria fronterizo con Irak, y zonas del norte, en Alepo, Al Raqa, As Shaddadah, áreas centrales y pequeñas partes en el sur.

Bibliografía

Achcar y Warschawski, *La guerra de los 33 días. Israel contra Hezbolá en el Líbano y sus consecuencias.* Icaria. 2006.

Benedetta Berti, *Hezbollah and Hamas. A comparative study.* Johns Hopkins. 2012.

Bucciarelli *Siria. La primavera marchita* A contraluz. 2015.

Corn, G., *Pensamiento y política en el mundo árabe. Contextos históricos y problemáticas, s. XIX-XXI* Bellaterra. 2015.

Cuaderno Estrategia 173, *La internacional Yihadista* IEEE. 2015.

Cuaderno Estrategia 174, *Economía y geopolítica en un mundo globalizado.* IEEE. 2015.

Documento Seguridad y Defensa 62 *Yihadismo en el mundo actual* IEEE. 2014.

Espinosa, J., *Siria, el país de las almas rotas* Debate. 2016.

Galiana Ros, M., *Yihadismo wahabita y sus raíces sionistas y talmúdicas* Ediciones Esparta.

Jordán, *Profetas del miedo. Aproximación al terrorismo islamista.* Universidad de Navarra. 2004.
Levitt, M., *Hezbollah: the global footprint of Lebanon´s Party of God* Georgetown University Press. 2013.
Martín, J., *Hizbulah. El brazo armado de Dios.* Ed. Catarata. 2006.
Martín, J., *Suníes y chiíes. Los dos brazos de Alá* Catarata. 2014.
Martín, J., *Estado Islámico. Geopolítica del Caos* Ed. Catarata. 2015.
Moubayed, S *Bajo la bandera del terror. Un viaje a las entrañas del Daesh* Península Atalaya 2016.
Mustafa, W., *La fiebre del levante. Historias reales de la Siria oculta* 2015.
Mutti, S., *El falseamiento del yihad y de la tradición islámica* Hipérbola Janus. 2016.
Napoleoni, *El Fénix islamista. El Estado Islámico y el rediseño de Medio Oriente.* Ed. Paidós. 2015.
Richard Norton, *Hezbollah: a short history.* Princeton. 2007.
Rogan, E., *Los árabes. Del imperio otomano a la actualidad* Crítica Barcelona. 2012.
Ortiz Moyano, *Yihad. Cómo el Estado Islámico ha conquistado internet y los medios de comunicación* Ed. 360º publicaciones 2016.
Power, B., *Hezbollah in Syria* Polonia 2015.
Power, B., *Hezbollah in Irak* Polonia 2015.
Qutb, S., *Milestones Islamic* Book Service 2002.
Yazbek, S., *A woman in the crossfire. Diaries of the Syrian revolution* Haus Publishing 2012.
Yazbek, S., *La frontera. Memorias de mi destrozada Siria* Stella Maris. 2015.

BLOQUE III:

CIBERSEGURIDAD Y CIBERDEFENSA

ESTRATEGIAS DE CIBERSEGURIDAD NACIONAL Y CIBERDEFENSA EN LA UE; RETOS PARA LA ESTRATEGIA DE SEGURIDAD Y DEFENSA EUROATLÁNTICA

Luis Álvarez Álvarez
Universidad de Las Palmas de Gran Canaria, ULPGC

Celso Perdomo González
Universidad de Las Palmas de Gran Canaria, ULPGC

Resumen

La Cumbre de Lisboa de 2010, incluyó la ciberdefensa en el Concepto Estratégico de la OTAN, se propició la Política de Ciberdefensa en 2011 y la creación de un Plan de Acción en 2012. En 2014 en la cumbre de Gales se aprobó un nuevo desarrollo de la Política de Ciberdefensa; ésta aclara que un ciberataque grave a un Estado miembro podría ser cubierto por el artículo 5 del Tratado. Recientemente la OTAN y la UE firmaron un acuerdo técnico para la cooperación en ciberseguridad. La Cumbre de Varsovia ha adoptado una serie de decisiones que cambiarán tanto las capacidades en ciberdefensa como la concepción estratégica de las mismas. La comunicación analiza los enfoques de ciberdefensa y ciberseguridad nacional de los países de la UE y sus implicaciones en el desarrollo de la estrategia de seguridad euroatlántica y de la propia UE.

Palabras claves

Ciberseguridad, Ciberdefensa, Estrategia de Seguridad y Defensa, Estrategia de Ciberseguridad.

1. Introducción

La ciberseguridad se identifica como el conjunto de tecnologías, procesos y servicios destinados a proteger los activos (físicos, lógicos, o de servicios) personales, empresariales y gubernamentales, que tengan soporte directo o indirecto en las Tecnologías de Información y Comunicaciones, TIC. Por otro lado, la ciber-

defensa forma parte del conjunto de las capacidades nacionales en el planeamiento y ejecución de operaciones militares en el ámbito de las TIC ya sean de soporte, propias o que afecten a la Seguridad Nacional.

En la Cumbre de Lisboa de 2010, la ciberdefensa se incluyó en el Concepto Estratégico de la OTAN, esto propició la actualización de la Política de Ciberdefensa en 2011 y la creación de un Plan de Acción en el 2012. En septiembre de 2014, un nuevo desarrollo de la Política de Ciberdefensa fue aprobado en la cumbre de Gales. La Política aclara que un ciberataque grave a un Estado miembro podría ser cubierto por el artículo 5 del Tratado del Atlántico Norte. El pasado 9 de febrero la OTAN y la Unión Europea (UE) a través de su equipo de Capacidad de Respuesta de Incidentes Informáticos (NCIRC) y su homólogo de la UE (CERT-EU) firmaron un acuerdo técnico para mejorar la cooperación en ciberseguridad[1]. Este acuerdo busca reforzar la cooperación contra ataques cibernéticos, es de destacar que los objetivos de capacidades de ciberdefensa se han integrado en el proceso de planificación de defensa de la OTAN; así, su centro de respuesta a incidentes cubre en la actualidad 41 estructuras físicas civiles y militares en Europa y Norteamérica.

La Cumbre de Varsovia celebrada los días 8 y 9 de julio de 2016 ha constatado que los ciberataques pueden ser tanto o más perjudiciales que un ataque convencional y en este sentido se adoptado planteamientos en el ámbito de la defensa que redefinen el espacio y las capacidades de confrontación.

La capacidad necesaria de coordinación, la homogenización de procedimientos de respuesta, así como una especificación de la gradación del ciberincidente constituyen el enfoque estratégico de la ciberdefensa. En la comunicación analizaremos los diferentes enfoques de ciberdefensa y ciberseguridad nacional de los países miembros de la UE para determinar los diferentes visiones e implicaciones en el desarrollo de la estrategia de seguridad euroatlántica y de la recién aprobada nueva estrategia de Seguridad de la UE «Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy».

1. NATO. «NATO and the European Union enhance cyber defence cooperation», 10 de febrero de 2016, acceso el 27 de julio de 2016, http://www.nato.int/cps/en/natohq/news_127836.htm

2. La nueva visión de la ciberdefensa de la Otan plasmada en la cumbre de Varsovia

La ciberdefensa es tratada por múltiples organismos de la OTAN. En primer lugar, cualquier respuesta de defensa colectiva de la OTAN ante un ataque cibernético estaría sujeta a una decisión del Consejo del Atlántico Norte (NAC, North Atlantic Council), que es el órgano supremo de la OTAN, integrado por los representantes de todos los Estados miembros y presidido por el Secretario General. El NAC decidiría por consenso.

El Comité de Defensa Cibernética (CDC, Cyber Defence Committee), antes de abril 2014 conocido como el Comité de Política y Planes de Defensa (Defensa Cibernética), es un órgano consultivo de alto nivel para la NAC en materia de defensa cibernética, mientras que también proporciona la asesoría a los aliados y el ejercicio de la gobernanza global de defensa cibernética interna de la OTAN.

El Consejo de Administración de Defensa Cibernética (CDMB, Cyber Defence Management Board) funciona bajo la supervisión de la División de Desafíos de Seguridad Emergentes, Emerging Security Challenges Division en el cuartel general de la OTAN. Se compone de representantes de las principales partes interesadas en la seguridad cibernética dentro de la OTAN, como el Mando Aliado de Operaciones (ACO), Mando Aliado de Transformación (ACT) y las agencias de la OTAN. El CDMB hace la planificación estratégica y la dirección ejecutiva de las redes de la OTAN. También supervisa Memorando de Entendimiento con los Estados miembros para facilitar el intercambio de información y coordinar la asistencia.

La Agencia de Comunicaciones e Información de la OTAN (NCIA, NATO Communications and Information Agency) fue creada el 1 de julio de 2012, de conformidad con el objetivo de la Declaración de la Cumbre de Lisboa, mediante la fusión de 7 agencias de la OTAN que se ocupan de las actividades de la CIS y actividades cibernéticas. La NCIA es el proveedor principal de la CEI NATO . La Capacidad de Respuesta a Ciberincidentes de la OTAN (NCIRC, NATO Computer Incident Response Capability) se incluye en el NCIA y es el organismo encargado de la protección técnica centralizada de activos cibernéticos OTAN. El NCIRC alcanzó plena capacidad operativa mayo 2014 .

El Centro Excelencia de Ciberdefensa Cooperativa de la OTAN (OTAN CCD COE, Cooperative Cyber Defence Centre of Excellence) es un centro de investigación y formación acreditado por la OTAN para la formación, la consulta, la experiencia adquirida, la investigación y el desarrollo en el campo de la seguridad cibernética Actualmente cuenta con 14 de las naciones patrocinadoras (Estados miembros de la OTAN) y un participante contribuyente (Austria). OTAN CCD COE está financiado y dirigido por las naciones patrocinadoras, pero los servicios también pueden ser solicitados a la OTAN a través de la ACT, a pesar de que no está incluido en la estructura organizativa de la OTAN.

Partiendo de la base de que la defensa colectiva es uno de los cometido esenciales de la OTAN, y atendiendo a que los ciberataques pueden ser tanto o más dañinos que un ataque tipo convencional, la Cumbre de Varsovia ha adoptado una serie de decisiones que cambiarán tanto las capacidades en ciberdefensa como el concepción estratégica de las mismas.

«Los ataques cibernéticos presentan un claro desafío a la seguridad de la Alianza y pueden ser tan perjudiciales para las sociedades modernas como un ataque convencional. Nos pusimos de acuerdo en Gales que la defensa cibernética es parte de la tarea principal de la OTAN en la defensa colectiva. Ahora, en Varsovia, reafirmamos el mandato de defensa de la OTAN y reconocemos el ciberespacio como un dominio de las operaciones en las que la OTAN debe defenderse tan eficazmente como lo hace en tierra, mar y aire. Esto mejorará la capacidad de la OTAN para proteger y llevar a cabo operaciones a través de estos dominios y mantener nuestra libertad de acción y decisión en todas las circunstancias. Continuamos con una intensificación de la política de la OTAN en la ciberdefensa y una mayor fortaleza de las capacidades de defensa cibernética, que se benefician de las últimas tecnologías de vanguardia[2]».

2. «We continue to implement NATO's Enhanced Policy on Cyber Defence and strengthen NATO's cyber defence capabilities, benefiting from the latest cutting edge technologies.»

NATO. «Warsaw Summit Communiqué». Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016, 9 de julio de 2016, acceso el 27 de julio de 2016, http://www.nato.int/cps/en/natohq/official_texts_133169.htm

Las decisiones en ciberdefensa en la cumbre de Varsovia se centran en:

—Se determina que el ciberespacio es un nuevo dominio de operaciones, conjuntamente con los dominios de tierra, mar y aire.
—La ciberedefensa se va a integrar en el planeamiento operativo de misiles y operaciones.
—Se mantiene la aplicación de la «Política Reforzada de Ciberdefensa de la OTAN» (NATO's Enhanced Policy on Cyber Defence) aprobada en Gales.
—Se hará un mayor esfuerzo en las políticas y capacidades nacionales de ciberdefensa a través del «Compromiso en Ciberdefensa» (Cyber Defence Pledge[3]) de los países aliadoas para mantener las capacidades operativas en relación con la rápida evolución de las ciberamenazas.
—Se va profundizar en la cooperación con la Unión Europea así como con la industria civil a través del acuerdo NATO Industry Cyber Partnership[4].

Tenemos que resaltar que estas nuevas decisiones en ciberdefensa difieren poco del planteamiento actual del Departamento de Defensa de Estados Unidos. La publicación de The Department of Defense Cyber Strategy (United States. Department of Defence, 2015) ha supuesto un cambio sustancial respecto a los planteamientos y visión de la ciberseguridad y su estricta relación con la ciberdefensa militar. Los objetivos estratégicos son:

1. Establecer y mantener fuerzas y capacidades operativas para dirigir operaciones en el ciberespacio.
2. Defender las redes de información del DoD, asegurar los datos del DoD y mitigar los riegos para las misiones del DoD.
3. Capacitación para defender los intereses vitales y estratégicos de EE.UU. de ciberataques destructivos, dañinos o de consecuencias significativas.

3. NATO. «Cyber Defence Pledge», 8 de julio de 2016, acceso el 27 de julio de 2016, http://www.nato.int/cps/en/natohq/official_texts_133177.htm

4. NATO Industry Cyber Partnership, acceso el 20 de julio de 2016, http://www.nicp.nato.int/

4. Mantener un plan y opciones en el ciberespacio para emplear esas opciones en controlar una intensificación de conflicto y mantener la supremacía.
5. Realizar y mantener alianzas con socios internacionales para disuadir las amenazas e incrementar la estabilidad y seguridad nacional.

Así mismo el documento expone que el Departamento de Defensa establecerá instrumentos para defender al país contra cualquier adversario «durante tiempo de paz, crisis o conflicto»; lo que claramente determina que el Pentágono ha desarrollado capacidades para ciberoperaciones que siguiendo sus manuales doctrinales incluyen estrategias diplomáticas, informacionales, militares, económicas y jurídicas. Resaltemos por último, que esta estrategia, no recibe la denominación de estrategia de ciberseguridad o ciberdefensa, si no que apuesta por el planteamiento de estrategia en el ciberespacio (ciberestrategia).

Por otro lado, el recientemente actualizado Manual de Leyes de la Guerra del EEUU (DoD Law of War Manual - June 2015, Updated May 2016, United States. Office of General Counsel) cita en cuanto a la aplicación de derecho específico de reglas de la guerra (de enfrentamiento) a las operaciones cibernéticas:

> «…las normas relativas a la realización de los ataques no dependen de qué tipo de arma se utiliza para llevar a cabo el ataque. Por lo tanto, las operaciones cibernéticas pueden estar sujetas a una variedad de las normas de la guerra en función la naturaleza de la operación cibernética. Por ejemplo, si las consecuencias físicas de un ataque cibernético constituyen el tipo de daño físico que pueda ser causado por un ataque convencional; el ataque cibernético estaría igualmente sujeto a las mismas reglas que se aplican a los ataques con bombas o misiles.»

2.1. *Relaciones OTAN-Rusia e implicaciones en la ciberdefensa*

En la cumbre de Varsovia se ha plasmado que desde el punto de vista de algunos países de la Alianza, Rusia es considerada un rival estratégico, y como tal se debe mantener una relación de diálogo con alternativas de disuasión ante sus actuaciones recientes, que van desde la anexión de Crimea, la presencia de tropas en Georgia y Moldavia, violación sistemática del espacio aéreo en el

Báltico, ejercicios militares en la frontera de Ucrania y ciberataques a la propia Ucrania y otros países aliados[5].

A modo de ejemplo, el 23 de diciembre del 2015, la red eléctrica de Ucrania sufrió un ciberataque que provoco la interrupción del suministro durante varias horas, el corte afectó a más de 600.000 hogares de la región de Ivano-Frankivsk. El ciberataque se habría realizado con el uso del troyano BlackEnergy[6] y mediante el uso simultáneo de técnicas de ingeniería social[7]. Se considera que esta es la primera vez en la historia que un ciberataque ha provocado un corte de suministro eléctrico. Los posteriores análisis determinaron que el ataque tenía origen en Rusia[8].

Pero los ciberataques a infraestructuras críticas no han sido solo las actuaciones que afectan a la ciberseguridad de los países aliados, la propia sede de la OTAN, la OSCE e incluso empresas y eventos de los sectores de defensa y aeroespacial han sufrido incursiones de ciberespionaje[9].

5. Robin Emmott y Sabine Siebold. «NATO agrees to reinforce eastern Poland, Baltic states against Russia», *Reuters,* 8 de Julio de 2016, acceso el 15 de Julio de 2016, http://www.reuters.com/article/us-nato-summit-idUSKCN0ZN2NL

6. F-Secure Labs. «BlackEnergy & Quedagh: The convergence of crimeware and APT attacks», 2014. https://www.f-secure.com/documents/996508/1030745/blackenergy_whitepaper.pdf

7. Dan Godin. «First known hacker-caused power outage signals troubling escalation», *Ars Technica,* 4 de enero de 2016, acceso el 15 de enero de 2016, http://arstechnica.com/security/2016/01/first-known-hacker-caused-power-outage-signals-troubling-escalation/

8. Kim Zetter. «Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid.» *Wired*, 3 de marzo de 2016, acceso el 2 de abril de 2016, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

9. In addition to targeting European security organizations and governments, it appears that APT28 is targeting attendees of European defense exhibitions. Some of the APT28- registered domains imitated those of defense events held in Europe, such as the Farnborough Airshow 2014, EuroNaval 2014, EUROSATORY 2014, and the Counter Terror Expo. In September 2014, APT28 registered a domain (smigrouponline.co[.]uk) that appeared to mimic that for the SMi Group, a company that plans events for the «Defence, Security, Energy, Utilities, Finance and Pharmaceutical sectors.» Among other events, the SMi Group is currently planning a military satellite communications event for November 2014.

FireEye. «APT28: A window into Russias´s Cyber Espionage Operations?», 2016, acceso el 7 de agosto de 2016, https://www2.fireeye.com/rs/fireye/images/rpt-apt28.pdf

Por otro lado Rusia utiliza la «guerra de información» en una lucha constante por ganar las narrativas ante la opinión pública tanto a nivel interno como en el ámbito internacional[10]. Esta estrategia de desinformación[11] continua se fundamenta en su doctrina militar de tal manera que la guerra de la información, desde el punto de vista ruso, se lleva a cabo en «*tiempo de paz*», en el *«preludio de una guerra»* y en *«tiempo de guerra»* en tres ámbitos: *«estratégico»* (el ámbito estatal afecta a diferentes ministerios y organismos, así como a operaciones en dos o más frentes), «*operativo»* (la escala de las operaciones de un frente, un ejército, un cuerpo) y «*táctico»* (la escala de operaciones de una unidad combinada o una subunidad) (Limno & Krysanov, 2003). Los *maskirovka* (métodos de engaño; camuflaje, y ocultación) (Ventre, 2009, p. 165) son un elemento constitutivo de la «guerra de información» en tiempo de paz[12]. Es un elemento basado en estratagemas que «controlan» al enemigo mediante la creación de una falsa impresión de la situación real y el estatus de fuerzas que se oponen al enemigo, y sobre el concepto, tiempo y naturaleza de sus operaciones, obligándole a actuar de una forma predecible que sea desfavorable para él mismo (Limno & Krysanov, 2003).

La actual Doctrina Militar de Rusia, firmada por el Presidente Puttin el 26 de diciembre de 2014, hace especiales referencias al peligro de actores no identificados utilizando la guerra de información y la subversión política, así como la fuerza, para desestabilizar y derrocar regímenes. La propia Rusia, al parecer, está en riesgo, y la juventud de Rusia es particularmente vulnerable a la

10. Neil MacFarQuhar. «A Powerful Russian Weapon: The Spread of False Stories». *The New York Times*, 28 de agosto de 2016, acceso el 1 de septiembre de 2016, http://www.nytimes.com/2016/08/29/world/europe/russia-sweden-disinformation.html?_r=0

11. Anne Applebaum y Edward Lucas. «The danger of Russian disinformation». *The Washington Post*, 6 de mayo de 2016, acceso el 17 de mayo de 2016, https://www.washingtonpost.com/opinions/the-danger-of-russian-disinformation/2016/05/06/b31d9718-12d5-11e6-8967-7ac733c56f12_story.html

12. Rafael M. Yusupov, Director del SPIIRAS (*St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences*), considera que las dos principales amenazas en el ciberespacio son el espionaje y la «distorsión de la información», y que estas ocurren en tiempo de paz. http://irc.ifmo.ru/en/88695/partner/413/St.Petersburg_Institute_for_Informatics_and_Automation_of_the_Russian_Academy_of_Sciences_%28SPIIRAS%29.htm

subversión. El Kremlin también teme el uso de sus adversarios de «fuerzas especiales y organizaciones extranjeras» en clara referencia a organizaciones no gubernamentales extranjeras que operan en territorio ruso[13].

Esta visión de Rusia sobre su entorno estratégico y de relaciones internacionales, hace que las actuales capacidades de ciberseguridad y ciberdefensa tanto de la UE como de la OTAN necesiten estar en continua mejora, redefiniendo las aptitudes de anticipación y de disuasión[14].

3. La ciberseguridad en «la estrategia global para la política exterior y de seguridad de la UE» (Shared vision, common action: a stronger Europe. A global strategy for the european union's foreign and security policy)

En febrero de 2013, la Comisión Europea, junto con la Representación de la Unión para Asuntos Exteriores y Política de Seguridad, publicó una estrategia de ciberseguridad acompañada de una propuesta de Directiva de la Comisión sobre la seguridad de las redes y de la información (European Commission. Digital Agenda for Europe, 2013). Se preveían una serie de medidas específicas para reforzar la resiliencia de los sistemas informáticos, reduciendo la delincuencia en la red y fortaleciendo la política de ciberseguridad y ciberdefensa internacional de la UE.

13. This doctrine differentiates between «dangers» and «threats:» the former designates concerns, the latter possible sparks for conflict. As in 2010, the NATO alliance, or, more accurately, its behavior and intentions, is classed as a danger, as are terrorism and violations of international agreements. But if many of the specifics are much the same, the tone of the overall document represents a shift, and a few of the individual changes are notable. This doctrine, in many ways something of a national security strategy document, is meant not only to describe Russian policy but also to send messages to friends, adversaries, and others. The challenge lies in understanding Russia's signals, as well as their repercussions.

Olga Oliker. «Russia's New Military Doctrine: Same as the Old Doctrine, Mostly», *The Washington Post*, 6 de enero de 2015, acceso el 17 de mayo de 2016, https://www.washingtonpost.com/blogs/monkey-cage/wp/2015/01/15/russias-new-military-doctrine-same-as-the-old-doctrine-mostly/

14. Silvia Martínez. «La guerra oculta de Rusia contra la UE», El Periódico, 2 de agosto de 2016, acceso el 8 de agosto de 2016, http://www.elperiodico.com/es/noticias/internacional/guerra-oculta-rusia-contra-5302960

La estrategia articula la visión de la UE sobre la ciberseguridad en torno a cinco prioridades:

—la ciberresiliencia;
—la reducción drástica de la delincuencia en la red;
—el desarrollo de una política de ciberdefensa y de las capacidades correspondientes en el ámbito de la Política Común de Seguridad y Defensa (PCSD);
—el desarrollo de los recursos industriales y tecnológicos necesarios en materia de ciberseguridad;
—el establecimiento de una política internacional coherente del ciberespacio en la Unión Europea y la promoción de los valores europeos esenciales.

Los responsables de la ciberseguridad en la UE son la Agencia Europea de Seguridad de las Redes y la Información (ENISA), el Centro Europeo contra el Cibercrimen (Europol/EC3) y la Agencia Europea de Defensa (AED), los cuerpos de seguridad y la Defensa, manteniendo una estrecha colaboración y respetando sus especificidades. La representación esquemática de estas responsabilidades se representa en la Figura 1.

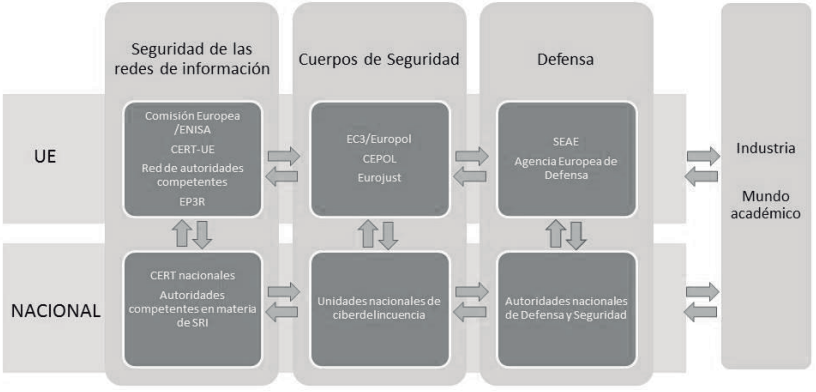


Figura 1: Esquema de los Órganos de los Estados Miembros y la Unión Europea en materia de Seguridad y Defensa

Fuente: Cuadro esquemático de los Órganos de los Estados Miembros y la Unión Europea en materia de Seguridad y Defensa. Imagen extraída 1 cuadro extraído de la Comunicación Conjunta al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones: Estrategia de ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro. Bruselas, 7.2.2013 JOIN (2013) 1 final.

Federica Mogherini, Alta Representante para asuntos exteriores y Política de Seguridad de la UE, presentó ante Consejo Europeo de junio de 2016 la «nueva estrategia de seguridad global de la UE» que ciertamente no aporta grandes novedades, y menos en una aproximación de más política común de defensa. Centrándonos en las referencias a la ciberseguridad, sí que la estrategia hace un recorrido por los conflictos híbridos, el terrorismo y las interrelaciones con la seguridad energética, y el control de infraestructuras críticas, y una referencia a la colaboración y el refuerzo de capacidades conjuntamente con la OTAN[15]; pero tan sólo se menciona en un párrafo dedicado a la ciberseguridad que:

> La UE aumentará su enfoque en la seguridad cibernética, el equipamiento para la ciberseguridad, cooperando con los estados miembros a mantener un ciberespacio abierto, libre y seguro.

Así mismo se hace una apuesta por la capacidad de resiliencia de sistemas, apuesta por la investigación y desarrollo en la materia, la certificación de productos y servicios y la colaboración con la industria civil.

Como iniciativa en este sentido el pasado 5 de julio, la Comisión Europea lanzó la primera asociación europea público-privada para la ciberseguridad. La UE destinará 450 millones de euros en esta iniciativa en el marco del programa *Horizon 2020. La respuesta de los operadores del mercado* en el marco de la Organización Europea de Ciberseguridad *(European Cyber Security Organisation*-ECSO)[16],

15. «la UE seguirá profundizando el vínculo transatlántico y nuestra asociación con la OTAN, al mismo tiempo que nos conectaremos con nuevos actores y exploraremos nuevos formatos para promover nuestra Estrategia. La UE invertirá en instituciones regionales, y en cooperación dentro de las regiones y entre regiones. E impulsaremos reformas de gobernanza global que puedan hacer frente a los desafíos de este siglo». Federica Mogherini. «Una estrategia para unir Europa». *El País,* 6 de julio de 2016, acceso el 2 de agosto de 2016, http://elpais.com/elpais/2016/07/16/opinion/1468701804_322725.html

16.ECSO represents an industry-led contractual counterpart to the European Commission for the implementation of the Cyber Security contractual Public-Private Partnership (cPPP). ECSO members include a wide variety of stakeholders such as large companies, SMEs and Start-ups, research centres, universities, clusters and association as well as European Member State's local, regional and national administrations, countries part of the European Economic Area (EEA) and the European Free Trade Association (EFTA) and H2020 associated countries. http://www.ecs-org.eu/

presumiblemente invertirán una cantidad cercana a los 1800 millones de euros.

Por último y como citamos anteriormente, el acuerdo técnico de colaboración en ciberseguridad firmado por la UE con la OTAN incluye la participación de la Unión en el ciberejercicio anual organizado por la Alianza[17].

4. Tendencias en la definición de estrategias de ciberseguridad y ciberdefensa en la UE y la OTAN

Para un análisis comparativo en las estrategias de ciberseguridad y su conceptualización de la ciberedefensa, estudiamos todos los países que han realizado o están actualizando estrategias de ciberseguridad y/o ciberdefensa, para determinar las tendencias y características más relevantes. Así mismo en los casos en los que existen referencias a otros documentos, como libros blancos o estrategias de seguridad nacional con apartados vinculados a ciberseguridad, ciberdefensa o seguridad de la información hemos resaltado sus interrelaciones y ejes principales; de igual manera se ha analizado la estrategia de Ciberseguridad de la UE[18] y las especificidades en ciberseguridad y ciberdefensa de la propia OTAN. El análisis comparativo se centra fundamentalmente en las siguientes características:

—La consideración de la ciberseguridad como un asunto vinculado a la Seguridad Nacional o la Defensa Nacional. En este sentido también hemos estudiado si cada país (en su caso organización) posee Estrategia de Seguridad Nacional y su correlación con el planteamiento de las políticas y estrategias de ciberseguridad.

—Existencia o no de estructuras institucionales diferenciadas, con roles y responsabilidades claramente definidos en el ámbito civil, policial y militar.

17. SHAPE Public Affairs Office. «Experts put to the test during NATO's largest annual cyber defence exercise», 20 de noviembre de 2015, acceso el 22 de julio de 2016, https://www.shape.nato.int/cyber-exercise-challenges-defense.

18. European Commission. Digital Agenda for Europe. «EU Cybersecurity plan to protect open internet and online freedom and opportunity - Cyber Security strategy and Proposal for a Directive», 7 de febrero de 2013, acceso el 8 de agosto de 2016, https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security

—Existencia de una estructura específica con un organismo o sistema definido dedicado a la protección de Infraestructuras Críticas.
—Existencia de un esquema de coordinación de seguridad nacional.
—Existencia de protocolos de coordinación con otras organizaciones de seguridad y/o defensa internacionales para la cooperación en materia de ciberseguridad y /o ciberdefensa.
—Existencia de programas o doctrinas de ciberdefensa nacionales.
—Existencia de un mando militar de ciberdefensa o estructura similar.
—Existencia de programa presupuestario específico en el ámbito de la ciberseguridad y/o la ciberdefensa.
—Existencia de programas de coordinación transversales e interdepartamentales de políticas y presupuestos de ciberseguridad, ciberdefensa e I+D+i asociados.
—Vinculación con los servicios de Inteligencia, civil y/o militar.
—Existencia de Equipo de Respuesta ante Emergencias Informáticas (CERT, del Computer Emergency Response Team, o Computer Security Incident Response Team, CSIRT), y vinculación y colaboración con organismos internacionales de ciberseguridad.
—Existencia de acuerdos formales internacionales de colaboración en materia de ciberdefensa.
—Existencia de programas de formación y estructura formal de capacitación para la ciberseguridad y/o la ciberdefensa.
—Existencia de protocolos I+D+i para el desarrollo de capacidades vinculadas a la ciberseguridad y/o la ciberdefensa con organismos de investigación, públicos y privados.
—Existencia de línea estratégica vinculada a las «operaciones de información» o en su caso existencia de una política definida como estrategia de información.
—Existencia de una Comunidad de Inteligencia en materia de ciberseguridad y ciberdefensa.

Estas características analizadas para los países que poseen estrategias de ciberseguridad, ciberdefensa o referencias en otros documentos a la seguridad nacional y el ciberespacio se exponen en la Tabla 1.

Estrategias y Programas de Ciberseguridad (CS) y/o Ciberdefensa Nacionales (CD)											
País	Fecha	Seguridad Nacional o Defensa Nacional.	Estructuras diferenciadas civiles, mil., policiales.	Estructura de Seguridad de IC.	Esquema de coordinación de Seguridad Nacional.	Programas de CD mil. Mando CD.	Coordinación interdepartamental y transversal de políticas y presupuestos de I+D+i, CS y CD.	Vinculación Servicios de Inteligencia. civ. – mil.	Programas específicos de formación en CS /CD.	Estrategia de Información o Política de Información diferenciada.	Programa de I+D+i de capacidades en CD militar.
Países OTAN											
Albania	SN 2014 CS 2014	✓		✓		✓		✓			
Bélgica	CS 2012 / 2014	✓	✓	✓	✓	✓	✓	✓	✓		
Bulgaria	SN 2010	✓	✓	✓		✓		✓			
Canadá	CS 2010 / 2013	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Croacia	CS 2015	✓	✓	✓		✓		✓			
República Checa	SN 2011 / 2015 CS 2014 / 2015	✓	✓	✓	✓	✓		✓	✓		✓
Dinamarca	SN 2012 CS 2014	✓	✓	✓	✓	✓	✓	✓	✓		
Estonia	SN 2010 CS 2014	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Francia	CS 2015 SN 2013	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Alemania	SN 2016 CS 2011 / 2015	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Hungría	SN 2012 CS 2013	✓	✓	✓		✓		✓	✓		✓
Islandia	CS 2014	✓	✓	✓	✓	✓		✓	✓		

Estrategias y Programas de Ciberseguridad (CS) y/o Ciberdefensa Nacionales (CD)											
País	Fecha	Seguridad Nacional o Defensa Nacional.	Estructuras diferenciadas civiles, mil., policiales.	Estructura de Seguridad de IC.	Esquema de coordinación de Seguridad Nacional.	Programas de CD mil. Mando CD.	Coordinación interdepartamental y transversal de políticas y presupuestos de I+D+i, CS y CD.	Vinculación Servicios de Inteligencia. civ. – mil.	Programas específicos de formación en CS /CD.	Estrategia de Información o Política de Información diferenciada.	Programa de I+D+i de capacidades en CD militar.
Países OTAN											
Italia	SN 2015 CS 2013	✓	✓	✓	✓	✓	✓	✓	✓		
Letonia	CS 2010 / 2014	✓	✓	✓	✓	✓	✓	✓	✓		
Lituania	CS 2011 / 2014	✓	✓	✓		✓		✓	✓		
Luxemburgo	CS 2015	✓	✓	✓	✓	✓		✓	✓		
Países Bajos	SN 2011 / 2013 CS 2012 / 2013	✓	✓	✓	v	✓	✓	✓	✓		
Noruega	CS 2012	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Polonia	SN 2014 CS 2013	✓	✓	✓	✓	✓	✓	✓	✓		✓
Rumanía	CS 2013	✓	✓	✓		✓		✓	✓		
Eslovaquia	SN 2013 CS 2015	✓	✓	✓	✓	✓		✓	✓		
Eslovenia	CS 2016	✓	✓	✓			✓	✓	✓		
España	CS / SN 2013	✓	✓	✓	✓	✓	✓	✓	✓		✓
Turquía	CS 2013	✓	✓	✓	✓	✓		✓			✓

Estrategias y Programas de Ciberseguridad (CS) y/o Ciberdefensa Nacionales (CD)											
País	Fecha	Seguridad Nacional o Defensa Nacional.	Estructuras diferenciadas civiles, mil., policiales.	Estructura de Seguridad de IC.	Esquema de coordinación de Seguridad Nacional.	Programas de CD mil. Mando CD.	Coordinación interdepartamental y transversal de políticas y presupuestos de I+D+i, CS y CD.	Vinculación Servicios de Inteligencia. civ. – mil.	Programas específicos de formación en CS /CD.	Estrategia de Información o Política de Información diferenciada.	Programa de I+D+i de capacidades en CD militar.
Países OTAN											
Reino Unido	SN 2010 CS 2011	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
EEUU	SN 2015 CS 2015	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Europa: Países NO OTAN (ISAF)											
Austria	CS 2011 / 2013	✓	✓	✓	✓	✓	✓	✓	✓		
Bosnia Herzegovina	SN 2010	✓	✓	✓				✓			
Chipre	CS 2013	✓	✓	✓				✓			
Finlandia	SN 2010 CS 2013	✓	✓	✓	✓	✓	✓	✓	✓		
Georgia	CS 2012	✓				✓		✓			
Irlanda	CS 2015	✓	✓	✓	✓	✓	✓	✓			
Unión Europea											
Unión Europea	CS 2013	✓	✓	✓	✓	✓	✓	✓	✓		✓

CS: Ciberseguridad, CD: Ciberdefensa, SN: Seguridad Nacional con referencias a la ciberseguridad y/o ciberdefensa
ISAF: International Security Assistance Force
Tabla 1: Análisis comparativo de las estrategias y programas de ciberseguridad y/o ciberdefensa nacionales
Fuente: Elaboración propia

Del estudio de los documentos, determinamos que en la inmensa mayoría se hace referencia a la seguridad de infraestructuras críticas, la seguridad económica o financiera vinculándolas con la ciberseguridad, en un enfoque de Seguridad Nacional[19]. En la Tabla 2 esquematizamos los aspectos comunes de las estrategias de ciberseguridad, relacionando las políticas o ejes comunes en las estrategias con sus objetivos e indicadores de actividad propuestos

Eje o Política de la Estrategia	Objetivos e indicador de la actividad
Consideración de la Ciberseguridad como un asunto de Defensa Nacional.	Resulta prioritaria la formulación de políticas globales e integradas, que impliquen a todas las áreas gubernamentales vinculadas, designando la autoridad responsable de su coordinación.
Estructura institucional formal.	Creación y fortalecimiento de las organizaciones con responsabilidades en materia de ciberseguridad, definiendo y delimitando sus funciones y roles y asignando los recursos precisos: presupuestarios y humanos.
Desarrollo de capacidades.	Necesidad de determinar nuevas estrategias para la ciberseguridad, que deben centrarse en el desarrollo y fomento de estructuras formativas, de investigación, desarrollo y certificación de capacidades.
Dependencia especial de la Comunidad de Inteligencia.	Tendencia significativa en la mayoría de los países para que las agencias de inteligencia o las unidades de inteligencia militar puedan, ganar influencia en la orientación general de la ciberseguridad.
Protección de infraestructuras críticas.	Desarrollo o mejora de los esfuerzos para proteger los sistemas TIC de Infraestructuras Críticas, lo que implica la identificación y categorización de estas infraestructuras y la designación de una autoridad nacional de seguridad.
Coordinación público-privada.	Incremento de las medidas para coordinar los esfuerzos del sector privado en materia de ciberseguridad con los planes estatales de ciberseguridad y ciberdefensa.
Cooperación Internacional.	Coordinación y cooperación de la mayoría de los países para establecer posiciones y prácticas de colaboración en materia de ciberseguridad.

Tabla 2: Aspectos comunes de las estrategias de ciberseguridad, ciberdefensa y seguridad nacional
Fuente: Adaptada de CCN-CERT, 2013 y ENISA, 2014

19. The term 'national cyber security' is increasingly used in policy discussions, but hardly ever defined. In this, it is very similar to the wider subject of cyber security itself – where common interpretations and implied meanings are much more frequent than universally accepted and legally-binding definitions. In cyber security, as a rule, the individual national context will define the specific definitions, which in turn will define the specific approaches – there are very few fixed points in cyber security.

Melissa E. Hathaway y Alexander Klimburg, «NATO Cooperative Cyber Defence Centre of Excellence. Comparison of 'National' and 'Cyber' Security; National (Cyber) Security Strategies in Selected OECD Countries». En National Cyber Security Framework Manual. Editado por Alexander Klimburg. (Tallin: NATO CCD COE Publication, 2012), 20-29 http://www.ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf

Todas las estrategias de seguridad nacional o las estrategias de ciberseguridad a las que hacen referencia éstas, mantienen las siguientes características comunes:

—Consideración de la Ciberseguridad como un asunto de Defensa Nacional, esto se hace patente en los 22 estados miembros de la UE que a su vez lo son de la OTAN.
—Establecimiento de estructura institucional que facilite la coordinación, la anticipación, la mitigación y la resiliencia de los sistemas y TIC.
—Identificación de la necesidad de desarrollar capacidades y conocimientos; atendiendo a que sólo considerando la posibilidad de obtener capacidades ofensivas se atienden las necesidades defensivas y de prevención.
—Protección de las infraestructuras críticas, habida cuenta de que la seguridad física y económica del Estado pasa por la invulnerabilidad de sus sistemas asociados.
—Coordinación para el establecimiento de medidas de prevención, seguridad y resiliencia entre los ámbitos público y privado sobre la base de que la gestión de muchos de los procesos y servicios fundamentales de cualquier economía se sustenta en la colaboración público-privada.
—Los intereses comunes de muchos países para establecer posiciones y prácticas de cooperación en materia de ciberseguridad, determinará nuevos marcos normativos, así como una mayor colaboración entre los CERT, la implicación de la ITU y la ONU. En este sentido el desarrollo del derecho internacional de los ciberconflictos se plantea como una de las políticas de urgente regulación.
—Tendencia significativa en la mayoría de los países para que las agencias de inteligencia o las unidades de inteligencia militar puedan, de facto, ganar influencia en la orientación general de la ciberseguridad. De igual manera la coordinación de la «comunidad de inteligencia» con el ámbito académico e investigador público y privado se considera la única ventaja competitiva para la mejora de las capacidades asociadas a la seguridad y la defensa.

Conclusiones

Las principales políticas estratégicas de ciberseguridad y ciberdefensa de cada uno de los estados miembros de la UE, así como la de la propia Unión identificando semejanzas y diferencias entre los planteamientos, tienden a reflejar las variaciones en la madurez de cada nación, su capacidad tecnológica, sus estructuras institucionales y su influencia estratégica en el esquema de poderes y relaciones internacionales.

Las capacidades necesarias, y la homogenización de procedimientos de respuesta, así como la especificación de la gradación del ciberincidente constituyen el pilar estratégico de la ciberdefensa.

La visión de las amenazas a la ciberseguridad de los aliados, y su planeamiento estratégico para afrontarlas o mitigarlas es más explícita en los países del Este de Europa.

Se infiere que la necesidad de una estrategia específica de ciberdefensa, entroncada en la política de seguridad y de defensa de la UE, y ésta además imbricada en la estrategia de ciberseguridad. Por otro lado, y bajo nuestra visión debe estar vinculada al acuerdo UE-OTAN en materia de ciberseguridad.

Referencias bibliográficas

Applebaum, Anne y Edward Lucas. 2016 «The danger of Russian disinformation». *The Washington Post*, 6 de mayo. Acceso el 17 de mayo de 2016, https://www.washingtonpost.com/opinions/the-danger-of-russian-disinformation/2016/05/06/b31d9718-12d5-11e6-8967-7ac733c56f12_story.html

Centro Criptológico Nacional. 2013. «Guía de Seguridad de las TIC. (CCN-STIC 820).

Guía de Protección contra Denegación de Servicio.» Acceso el 8 de agosto de 2016. https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/820/820-Proteccion_contra_DoS-jun13.pdf

Comisión Europea. 2013. Comunicación conjunta al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Estrategia de ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro. http://register.consilium.europa.eu/doc/srv?f=ST+6225+2013+INIT&l=es

Emmott, Robin y Sabine Siebold. 2016. «NATO agrees to reinforce eastern Poland, Baltic states against Russia». Reuters, 8 de Julio. Acceso el 15 de Julio de 2016, http://www.reuters.com/article/us-nato-summit-idUSKCN0ZN2NL

ENISA. 2014. «An evaluation Framework for National Cyber Security Strategies». Acceso el 8 de agosto de 2016, https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/an-evaluation-framework-for-cyber-security-strategies-1/an-evaluation-framework-for-cyber-security-strategies/at_download/fullReport

European Commission. Digital Agenda for Europe. 2013. «EU Cybersecurity plan to protect open internet and online freedom and opportunity - Cyber Security strategy and Proposal for a Directive.» Acceso el 8 de agosto de 2016, http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security

F-Secure Labs. 2014 «BlackEnergy & Quedagh: The convergence of crimeware and APT attacks.» Acceso el 13 de agosto de 2016. https://www.f-secure.com/documents/996508/1030745/blackenergy_whitepaper.pdf

FireEye. 2016. «APT28: A window into Russias´s Cyber Espionage Operations?.» Acceso el 7 de agosto de 2016. https://www2.fireeye.com/rs/fireye/images/rpt-apt28.pdf

Godin, Dan. 2016. «First known hacker-caused power outage signals troubling escalation», *Ars Technica,* 4 de enero. Acceso el 15 de enero de 2016, http://arstechnica.com/security/2016/01/first-known-hacker-caused-power-outage-signals-troubling-escalation/

Hathaway, Melissa E. y Alexander Klimburg. 2012. «NATO Cooperative Cyber Defence Centre of Excellence. Comparison of 'National' and 'Cyber' Security; National (Cyber) Security Strategies in Selected OECD Countries.» En *National Cyber Security Framework Manual.* Editado por Alexander Klimburg, NATO CCD COE Publication. Tallin

http://www.ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf

MacFarQuhar, Neil. 2016 «A Powerful Russian Weapon: The Spread of False Stories». *The New York Times*, 28 de agosto. Acceso el 1 de septiembre de 2016, http://www.nytimes.com/2016/08/29/world/europe/russia-sweden-disinformation.html?_r=0

Martínez, Silvia. 2016. «La guerra oculta de Rusia contra la UE». *El Periódico*, 2 de agosto. Acceso el 8 de agosto de 2016, http://www.elperiodico.com/es/noticias/internacional/guerra-oculta-rusia-contra-5302960

Mogherini, Federica. 2016. «Una estrategia para unir Europa». *El País*, 6 de julio. Acceso el 7 de julio. http://elpais.com/elpais/2016/07/16/opinion/1468701804_322725.html

NATO. 2016. «Cyber Defence Pledge». 8 de julio. Acceso el 27 de julio de 2016, http://www.nato.int/cps/en/natohq/official_texts_133177.htm

NATO. 2016. «NATO and the European Union enhance cyber defence cooperation». 10 de julio. Accceso el 27 de julio de 2016, http://www.nato.int/cps/en/natohq/news_127836.htm

NATO. 2016. «Warsaw Summit Communiqué». 9 de Julio. Acceso el 27 de julio de 2016, http://www.nato.int/cps/en/natohq/official_texts_133169.htm

NATO Industry Cyber Partnership, acceso el 20 de Julio de 2016, http://www.nicp.nato.int/

Oliker, Olga. 2016. «Russia's New Military Doctrine: Same as the Old Doctrine, Mostly». *The Washington Post*, 6 de enero. Acceso el 17 de mayo de 2016, https://www.washingtonpost.com/blogs/monkey-cage/wp/2015/01/15/russias-new-military-doctrine-same-as-the-old-doctrine-mostly/

Perdomo, Celso. 2016. «Operaciones de información y ciberdefensa; conceptualizaciones en las estrategias de seguridad nacional». Universidad de Las Palmas de Gran Canaria.

SHAPE Public Affairs Office. 2015. «Experts put to the test during NATO's largest annual cyber defence exercise». 20 de noviembre. Acceso el 22 de Julio de 2016, https://www.shape.nato.int/cyber-exercise-challenges-defense

United States. Department of Defence. 2015. *The Department of Defence Cyber Strategy*. http://www.dtic.mil/doctrine/doctrine/other/dod_cyber_2015.pdf

United States. Office of General Counsel. 2015. *Department of Defence Law of War Manual*. Actualizado Mayo 2016. http://www.defense.gov/Portals/1/Documents/DoD_Law_of_War_Manual-June_2015_Updated_May_2016.pdf

Zetter, Kim. 2016. «Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid.» *Wired*, 3 de marzo. Acceso el 2 de abril de 2016, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

Estrategias de Seguridad Nacional y Estrategias de Ciberseguridad

Albania. 2014. *National Security Strategy*. http://www.mod.gov.al/images/PDF/strategjia_sigurise_kombetare_republikes_se_shqiperise.pdf

Albania. Ministerio de Defensa. 2014. *Cyber Security Strategy. http://www.mod.gov.al/images/PDF/Strategjia_per_Mbrojtjen_Kibernetike.pdf*

Austria. (2012). *National ICT Security Strategy Austria.* Recuperado de http://www.oesterreich.gv.at/DocView.axd?CobId=48411

Austria. Federal Chancellery of the Republic of Austria. (2013). *Austrian Cyber Security Strategy.* Recuperado de https://www.bka.gv.at/site/3327/Default.aspx

Belgium. (2012). *Cyber Security Strategy. Securing Cyberspace.* Recuperado de https://www.b-ccentre.be/wp-content/uploads/2013/03/cybersecustra_fr.pdf

Belgium. Defence. Strategy department. (2014). *Cyber Security Strategy for Defence.* Recuperado de https://ccdcoe.org/sites/default/files/strategy/Belgian%20Defence%20Cyber%20Security%20Strategy.pdf

Bosnia Herzegovina. Ministry of Security. (2010). *Bosnia and Herzegovina Strategy for Prevention and Fight Against Terrorism.* Recuperado de http://www.msb.gov.ba/dokumenti/BiH%20Strategy%20for%20Prevention%20anf%20Fight%20against%20Terrorism.doc

Bulgaria. 2010. *White Paper on Defence and the Armed Forces of the Republic of Bulgaria.* http://www.md.government.bg/en/doc/misc/20101130_WP_EN.pdf

Canada. Govenment of Canada. (2013). *Action Plan 2010-2015 for Canada's Cyber Security Strategy.* Recuperado de http://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/ctn-pln-cbr-scrt/ctn-pln-cbr-scrt-eng.pdf

Canada. Government of Canada. (2010). *Canada's Cyber Security Strategy. For a Stronger and More Prosperous Canada.* Recuperado de http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf

Comisión Europea. (2013). Comunicación conjunta al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Estrategia de ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro. Recuperado de http://register.consilium.europa.eu/doc/srv?f=ST+6225+2013+INIT&l=es

Croacia. 2015. *The National Cyber Security Strategy of the Republic of Croatia.* http://www.uvns.hr/UserDocsImages/en/dokumenti/Croatian%20National%20Cyber%20Security%20Strategy%20(2015).pdf

Cyprus. Office of the Commissioner of Electronic Communicatons Postal Regulation. (2013). *Cybersecurity Strategy of the Republic of Cyprus.* Recuperado de https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategy-cyprus/at_download/file

Czech Republic. (2014). *Act on Cyber Security.* Recuperado de http://www.govcert.cz/download/nodeid-591/

Czech Republic. Ministry of Defence. (2011). *White Paper on Defence.* Recuperado de http://www.mocr.army.cz/scripts/file.php?id=98276&-down=yes

Czech Republic. Ministry of Foreign Affairs of the Czech Republic. (2015). *Security Strategy of the Czech Republic 2015.* Recuperado de http://www.army.cz/images/id_8001_9000/8503/15_02_Security_Strategy_2015.pdf

Czech Republic. National Security Authority: National Cyber Security Centre. (2015). *National Cyber Security Strategy of the Czech Republic for the period Recuperado de 2015 to 2020.* Recuperado de https://ccdcoe.org/sites/default/files/strategy/CZE_NCSS_en.pdf

Denmark. Centre for Cyber Security. (2015). *The Danish Cyber and Information Security Strategy* Recuperado de http://www.fmn.dk/eng/news/Documents/Danish-Cyber-and-Information-Security-Strategy-EN-vers.PDF.

Denmark. Ministry of Defence. (2012). *Danish Defence Agreement 2013-2017*. Recuperado de http://www.fmn.dk/eng/allabout/Documents/TheDanishDefenceAgrement2013-2017english-version.pdf

Denmark. Ministry of Defence. (2014). *National Strategy for Cyber and Information Security*. Recuperado de http://www.fmn.dk/nyheder/Documents/National-strategi-for-cyber-og-informationssikkerhed.pdf

España. Departamento de Seguridad Nacional. (2013). *Estrategia de ciberseguridad nacional = National cyber security strategy*. Madrid: Departamento de Seguridad Nacional. Recuperado de http://www.lamoncloa.gob.es/documents/20131332estrategiadeciberseguridadx.pdf

España. Departamento de Seguridad Nacional. (2013). *Estrategia de seguridad nacional : un proyecto compartido*. Madrid: Departamento de Seguridad Nacional. Recuperado de http://www.lamoncloa.gob.es/documents/seguridad_1406connavegacionfinalaccesiblebpdf.pdf

Estonia. Ministry of Defence. (2010). *National Defence Strategy*. Recuperado de http://www.kaitseministeerium.ee/sites/default/files/elfinder/article_files/national_defence_strategy.pdf

Estonia. Ministry of Defence. (2010). *National Security Concept of Estonia*. Recuperado de http://www.kaitseministeerium.ee/sites/default/files/elfinder/article_files/national_security_concept_of_estonia_0.pdf

Estonia. Ministry of Economic Affairs Communication. (2014). *Cyber Security Strategy 2014 - 2017*. Recuperado de https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf

Finland. Ministry of Defence. (2010). *Security Strategy for Society*. Recuperado de http://www.yhteiskunnanturvallisuus.fi/en/materials/doc_download/26-security-strategy-for-society

Finland. Ministry of Defence. (2013). *Finland's Cyber Security Strategy - Background Dossier*. Recuperado de http://www.yhteiskunnanturvallisuus.fi/en/materials/doc_download/48-finlandas-cyber-security-strategy-background-dossier

Finland. Secretariat of the Security and Defence Committee. (2013). *Finland´s Cyber Security Strategy*. Recuperado de http://www.yhteiskunnanturvallisuus.fi/en/materials/doc_download/40-finlandas-cyber-security-strategy

France. Agence nationale de la sécurité des systèmes d'information. (2011). *Information systems defence and security. France's strategy*. Recuperado de http://www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_Information_system_defence_and_security_-_France_s_strategy.pdf

France. Ministère de la Défense. (2013). *White Paper: Defence and National Security*. París: Ministère de la Défense Recuperado de http://www.defense.gouv.fr/content/download/215253/2394121/file/White%20paper%20on%20defense%20%202013.pdf

France. 2015. *French National Digital Security Strategy* http://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf

Georgia. *Cyber Security Strategy of Georgia 2012-2015*. Recuperado de http://www.dea.gov.ge/uploads/National%20Cyber%20Security%20Strategy%20of%20Georgia_ENG.pdf

Germany. Federal Ministry of the Interior. (2011). *Cyber Security Strategy for Germany*. Recuperado de https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CyberSecurity/Cyber_Security_Strategy_for_Germany.pdf?__blob=publicationFile

Germany. Gesetzentwurf der Bundesregierung. (2015). *IT Security Act = Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)*. Recuperado de http://www.bmi.bund.de/SharedDocs/Downloads/DE/Nachrichten/Kurzmeldungen/entwurf-it-sicherheitsgesetz.pdf?__blob=publicationFile.

Germany. The Federal Goverment. 2016. *White Paper 2016 on German Security Policy and the Future of the Bundeswehr*. https://www.bundeswehr.de/resource/resource/MzEzNTM4MmUzMzMyMmUzMTM1MzMyZTM2MzIzMDMwMzAzMDMwMzAzMDY5NzE3MzM1Njc2NDYyMzMyMDIwMjAyMDIw/2016%20White%20Paper.pdf

Hungary. (2013). *Act on the Electronic Information Security of Central and Local Government Agencies*. Recuperado de http://www.nbf.hu/anyagok/Act%20L%20of%202013%20on%20the%20Electronic%20Information%20Security%20of%20Central%20and%20Local%20Government%20Agencies.docx

Hungary. (2013). *Government Decision No. 1139 /2013 (21 March) on the National Cyber Security Strategy of Hungary,*. Recuperado de http://www.nbf.hu/anyagok/Government%20Decision%20No%201139_2013%20on%20the%20National%20Cyber%20Security%20Strategy%20of%20Hungary.docx

Hungary. Ministry of Foreign Affairs of Hungary. (2012). *Hungary's National Security Strategy*. Recuperado de http://2010-2014.kormany.hu/download/4/32/b0000/National%20Security%20Strategy.pdf

Ireland. (2015). *Ireland's National Cyber Security Strategy 2015-2017*. Recuperado de https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/NCSS_IE.pdf

Islandia. Ministry of the Interior. 2014 *National Cyber Security Strategy 2015-2026*. https://eng.innanrikisraduneyti.is/media/frettir-2015/Icelandic_National_Cyber_Security_Summary_loka.pdf

Italy. (2013). *Decree on National Cyber Security. GU n.66 del 19-3-2013*. Recuperado de http://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2013-03-19&atto.codiceRedazionale=13A02504&elenco30giorni=true

Italy. Presidency of the Council of Ministers. (2013). *National Plan for Cyber Security*. Recuperado de http://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/piano-nazionale-cyber.pdf

Italy. Presidency of the Council of Ministers. (2013). *National Strategic Framework for the Security of Cyberspace.* Recuperado de http://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-strategic-framework-for-cyberspace-security.pdf

Italia. Ministry of defense. 2015. *White Paper for international security and defence.* http://www.difesa.it/Primo_Piano/Documents/2015/07_Luglio/White%20book.pdf

Latvia. (2010). *Law on the Security of Information Technologies.* Recuperado de http://www.vvc.gov.lv/export/sites/default/docs/LRTA/Likumi/Law_On_the_Security_of_Information_Technologies.doc

Latvia. (2014). *Latvian cyber security strategy for the period 2014 to 2018.* Recuperado de https://ccdcoe.org/sites/default/files/strategy/LVA_CSS_2014-2018.pdf

Lithuania. Goverment of the Republic of Lithyania. (2011). *Programme for the Development of Electronic Information Security for 2011–2019.* Recuperado de http://www.ird.lt/doc/teises_aktai_en/EIS(KS)PP_796_2011-06-29_EN_PATAIS.pdf

Lithuania. Parliament of the Republic of Lithuania. (2014). *Cybersecurity Act.* Recuperado de https://ccdcoe.org/sites/default/files/strategy/LTU_CSAct_lt.pdf

Luxembourg. Ministère d'État. (2015). *National strategy on cyber security.* Recuperado de https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/Luxembourg_Cyber_Security_strategy.pdf

Luxembourg. Ministère d'État. (2011). *National Strategy on Cyber Security.* Recuperado de http://www.gouvernement.lu/3966881/2011-strategie-cybersecurite.pdf

Netherlands. (2011). *National counterterrorism strategy 2011 - 2015.* Recuperado de https://english.nctv.nl/Images/nationale-ct-strategie-2011-2015-uk_tcm92-369807.pdf

Netherlands. Ministry of Defence. (2012). *The Defence Cyber Strategy.* Recuperado de https://ccdcoe.org/sites/default/files/strategy/NDL-Cyber_StrategyEng.pdf

Netherlands. Ministry of Foreign Affairs. (2013). *International Security Strategy: A Secure Netherlands in a Secure World.* Recuperado de https://www.bbn.gov.pl/ftp/dok/07/NDL_International_Security_Strategy_2013.pdf

Netherlands. National Coordinator for Security Counterterrorism. (2013). *National Cyber Security Strategy 2: Recuperado de Awareness to Capability.* Recuperado de http://english.nctv.nl/images/national-cyber-security-strategy-2_tcm92-520278.pdf

New Zealand. New Zealand Government. (2011). *New Zealand's cyber security strategy.* Recuperado de http://www.dpmc.govt.nz/sites/all/files/publications/nz-cyber-security-strategy-june-2011_0.pdf

Norway. (2012). *Cyber Security Strategy for Norway. Action Plan.* Recuperado de https://www.regjeringen.no/globalassets/upload/FAD/Vedlegg/IKT-politikk/Handlingsplan_nasjonal_strategi_informasjonssikkerhet.pdf

Norway. Norwegian Ministries. (2012). *Cyber Security Strategy for Norway.* Recuperado de https://www.regjeringen.no/globalassets/upload/FAD/Vedlegg/IKT-politikk/Cyber_Security_Strategy_Norway.pdf

Poland. 2014. *National Security Strategy of the Republic of Poland.* http://en.bbn.gov.pl/download/3/1314/NSSRP.pdf

Poland. Ministry of Administration Digitisation Internal Security Agency. (2013). *Cyberspace Protection Policy of the Republic of Poland.* Recuperado de http://www.cert.gov.pl/download/3/162/PolitykaOchronyCyberprzestrzeniRP148x210wersjaang.pdf

Romania. Government of Romania. (2013). *Romania's Cyber Security Strategy and the National Action Plan on Implementation of the National Cyber Security.* Recuperado de https://www.cert-ro.eu/files/doc/StrategiaDeSecuritateCiberneticaARomaniei.pdf

Slovakia. 2015. *Cyber Security Concept of the Slovak Republic for 2015 – 2020.* https://ccdcoe.org/sites/default/files/strategy/SVK_NCSS.pdf

Slovakia. Ministry of Defence of the Slovak Republic. (2013). *White Paper on Defence of the Slovak Republic.* Recuperado de http://www.mosr.sk/data/WP2013.pdf

Slovenia. 2016. *Cyber Security Strategy of the Republic of Slovenia.* http://www.mizs.gov.si/fileadmin/mizs.gov.si/pageuploads/Informacijska_druzba/pdf/Cyber_Security_Strategy_Slovenia.pdf

Switzerland. Federal Department of Defence Civil Protection Sport. (2012). *National Strategy for Switzerland's Protection Against Cyber Risks.* Recuperado de http://www.isb.admin.ch/themen/strategien/01583/index.html?lang=en&download=NHzLpZeg7t,lnp6I0NTU042l2Z6ln1ad1IZn4Z2qZpnO2Yuq2Z6gpJCEeX9,fGym162epYbg2c_JjKbNoKSn6A--&t=.pdf

Turkey. Ministry of Transport Maritime Affairs Communications. (2013). *National Cyber Security Strategy and 2013-2014 Action Plan.* Recuperado de https://ccdcoe.org/sites/default/files/strategy/TUR_CyberSecurityEng.pdf

United Kingdom. UK Cabinet Office. (2010). *A Strong Britain in an Age of Uncertainty: The National Security Strategy.* Recuperado de https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf

United Kingdom. UK Cabinet Office. (2011). *The UK Cyber Security Strategy. Protecting and promoting the UK in a digital world.* Recuperado de https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf

United States. (2011). *Department of defense strategy for operating in Cyberspace.* Recuperado de http://archive.defense.gov/news/d20110714cyber.pdf

United States. Department of Defence. (2015). *The Department of Defence Cyber Strategy*. Recuperado de http://www.dtic.mil/doctrine/doctrine/other/dod_cyber_2015.pdf

United States. Executive Office of the President. (2011). *International strategy for cyberspace : prosperity, security, and openness in a networked world*. Washington, D.C. Recuperado de https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

United States. National Institute of Standards Technology. (2014). *Framework for Improving Critical Infrastructure Cybersecurity*. Recuperado de http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf

United States. Office of the Press Secretary. (2013). *Executive Order - Improving Critical Infrastructure Cybersecurity*. Recuperado de https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

United States. The White House. (2003). *The National Strategy to Secure Cyberspace*. Recuperado de https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf

United States. The White House. (2006). *The National Security Strategy*. Washington, DC. Recuperado de http://georgewbush-whitehouse.archives.gov/nsc/nss/2006/

United States. The White House. (2009). *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*. Recuperado de https://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

United States. The White House. (2010). *National Security Strategy*. Washington, DC. Recuperado de https://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf

United States. The White House. (2015). *National Security Strategy*. Washington, DC. Recuperado de https://ccdcoe.org/sites/default/files/strategy/USA_NSS2015.pdf

United States. The White House. (2002). *The National Security Strategy*. Washington, DC. Recuperado de http://georgewbush-whitehouse.archives.gov/nsc/nss/2002/index.html

LA SEGURIDAD DE LA INFORMACIÓN Y SUS IMPLICACIONES EN EL DESARROLLO DE LAS ESTRATEGIAS DE SEGURIDAD NACIONAL Y DE CIBERSEGURIDAD EN EL ENTORNO EUROATLÁNTICO

Celso Perdomo González
Universidad de Las Palmas de Gran Canaria, ULPGC

Resumen

Los incidentes relacionados con filtraciones y/o difusión de información como WikiLeaks, Snowden, y recientemente «los papeles de Panamá», denotan como la difusión de información de carácter sensible puede, y de hecho afecta a la seguridad de los países. Por otro lado, los diferentes roles de los *social media*, las redes sociales digitales, y su conexión con los *mass media*, en el sentido de coproducción de información y comunicación social, pueden ser utilizados en la consecución de objetivos más allá de los estrictamente informacionales. La comunicación interrelaciona este nuevo contexto, en el que la información es el vector de acción tanto de las vulnerabilidades como de las acciones defensivas y preventivas de la seguridad, analizando las implicaciones en desarrollo de las estrategias de ciberseguridad y de seguridad nacional en la UE y en el ámbito de la OTAN.

Palabras claves

Seguridad de la Información, Ciberseguridad, Ciberdefensa, Estrategia de Seguridad Nacional, Estrategia de Ciberseguridad.

1. Introducción

La aproximación al concepto de seguridad de la información se imbrica en el entorno de la ciberseguridad, y la ciberdefensa; éste ha ido evolucionando en un «ecosistema» cada vez más complejo, dinámico e interrelacionado donde los diferentes roles de los *social media*, las redes sociales digitales, y su conexión con los *mass media*, en el sentido de coproducción de información y comunicación social, pueden ser utilizados en la consecución de objetivos más allá de los estrictamente informacionales.

Así pues, los incidentes de seguridad de la información, trascienden el ámbito tecnológico y de comunicación social y pueden llegar a desestabilizar el marco económico-financiero.

Debemos resaltar la diferencia de lo que se conoce como seguridad de la información frente al aseguramiento de la información. La seguridad de la información (Information Security, INFOSEC) y el aseguramiento de la información (Information Assurance, IA) aunque en cierta medida tienen puntos de encuentro, el aseguramiento de la información se ha centrado tradicionalmente en un enfoque de tecnología. Las operaciones diarias de las aplicaciones de seguridad e infraestructura tales como cortafuegos, sistemas de prevención de intrusiones, la lucha contra la piratería informática, etc.

Aseguramiento de la Información (IA, *Information Assurance*) se compone de medidas que protegen y defienden a la información y los sistemas de información garantizando la disponibilidad, integridad, autenticación, confidencialidad y no repudio. Esto incluye el suministro para la restauración de los sistemas de información mediante la incorporación capacidades como la protección, detección y reacción (NATO Allied Joint Publication 3.10, 2009).

2. El peligro de la desinformación masiva

El informe de Riesgos Mundiales del *World Economic Forum* (2012) incluye una descripción y un análisis de los datos asociados a 50 riesgos mundiales repartidos en cinco categorías: económica, medioambiental, geopolítica, social y tecnológica. Entre los riesgos tecnológicos, los considerados como de mayor probabilidad e impacto son: ciberataques, fallo de los sistemas críticos e incidentes masivos de fraude o robo de datos.

Es de resaltar lo que el informe define como «el lado oscuro de la conectividad» muestra la parte del mapa de riesgos mundiales relacionados con la ciberdelincuencia y la alteración de sistemas. Este tipo de riesgos podrían intensificar las preocupaciones tradicionales en materia de seguridad, como la resolución diplomática de los conflictos y el terrorismo. Además la potencial inoperatividad de cualquiera de las llamadas «infraestructuras críticas» se considera como el centro de gravedad de las amenazas de naturaleza tecnológica, señalando igualmente que, aunque

el riesgo de que la probabilidad de que una sola vulnerabilidad pudiera provocar la caída en cascada de otras infraestructuras críticas (o las redes que las sustentan) es relativamente baja, tendría, no obstante, un altísimo impacto.

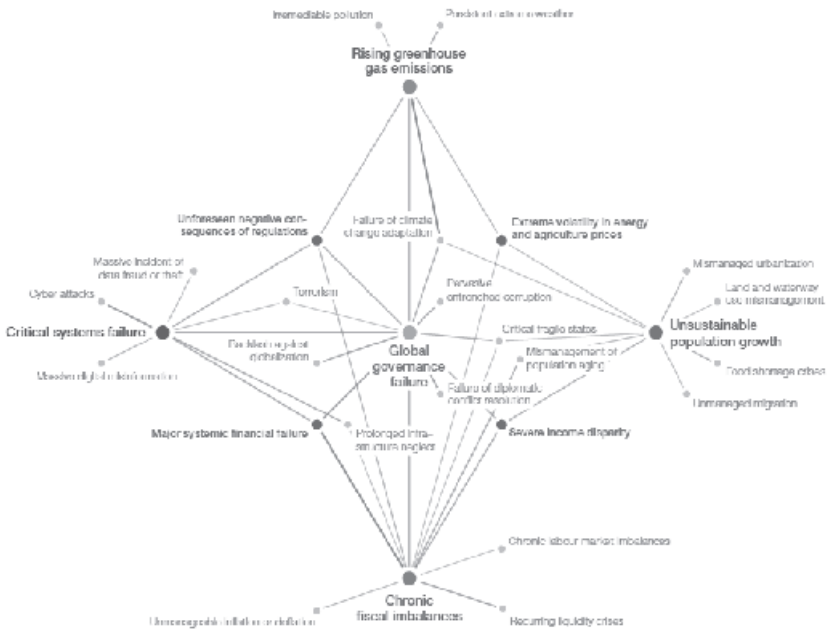


Figura 1: Mapa de riesgos globales 2012
Fuente: Informe de Riesgos Mundiales del World Economic Forum, 2012

En su desenlace final la sucesión de hechos podría claramente minar la gobernabilidad global. La Figura 1 representa el «mapa de riesgos globales».

La versión del informe de Riesgos Mundiales del *World Economic Forum* (2013), alerta sobre el citado grupo de riesgos interrelacionados y lo define como «Incendio digital incontrolado en un mundo hiperconectado» refiriéndolo al riesgo producido por la desinformación masiva que se extendiese vía Internet; así cita como introducción el histórico incidente provocado por Orson Welles en 1938 cuando miles de estadounidenses confundieron la adaptación radiofónica de la novela de H.G. Wells «La guerra de los mundos» con un comunicado de prensa oficial y cundió el pánico, al creer que su país había sido invadido por marcianos.

El Informe *Global Risks* 2014, con una perspectiva de diez años, evalúa 31 riesgos de naturaleza mundial que podrían causar impactos negativos importantes en industrias y países. Los riesgos como en los anteriores informes se agrupan en cinco categorías —económica, medioambiental, geopolítica, social y tecnológica— y se miden tanto en términos de sus probabilidades de concreción, como en su impacto potencial. Con una alta probabilidad aparece de nuevo los ataques cibernéticos y con un mayor impacto potencial una interrupción crítica de la infraestructura de la información, que constituye un riesgo tecnológico. Textualmente se expone:

> La creciente dependencia de Internet para realizar tareas esenciales y la expansión masiva de dispositivos conectados a Internet hacen que el riesgo de una falla sistémica —a una escala capaz de desintegrar sistemas o incluso sociedades— sea mayor que nunca. Las recientes revelaciones sobre vigilancia gubernamental han disminuido el deseo de la comunidad internacional de cooperar a fin de construir modelos de gobernanza destinados a resolver esta debilidad del sistema. El efecto podría ser una balcanización de Internet, o el denominado «apocalipsis cibernético», en el que los piratas informáticos gozan de una superioridad abrumadora y en el que se han generalizado las interrupciones masivas».

En 2015 la actualización del informe determina que:

> «el año 2015 se distingue claramente del pasado por el incremento de los riesgos tecnológicos, en particular los ataques cibernéticos, y las nuevas realidades económicas, lo que nos recuerda que las tensiones geopolíticas se presentan en un mundo muy diferente al que existía antes. La información se expande en un instante por todo el mundo y las nuevas tecnologías han incrementado la influencia de nuevos actores y nuevas maneras de hacer la guerra».

El informe de 2016 se expone en relación a este tema que los delitos cibernéticos tienen un coste para economía mundial en torno a los 445.000 millones de dólares. Por otro lado se cita como tendencia global emergente el aumento de la ciberdependencia y como riesgo económico a escala global los ciberataques.

A modo de ejemplo, en abril de 2013, el Syrian Electronic Army, SEA, logró hackear la cuenta de Twitter de la agencia Associated Press para mostrar brevemente un mensaje informando de que el presidente Barack Obama había sido herido en dos explosiones de la Casa Blanca. En cuestión de segundos 136.000

millones de dólares se perdieron en los mercados bursátiles a pesar de que se restauró en pocos minutos la normalidad emitiéndose un comunicado oficial[1]. En la Figura 2 podemos apreciar el tweet y su repercusión en el mercado de valores.

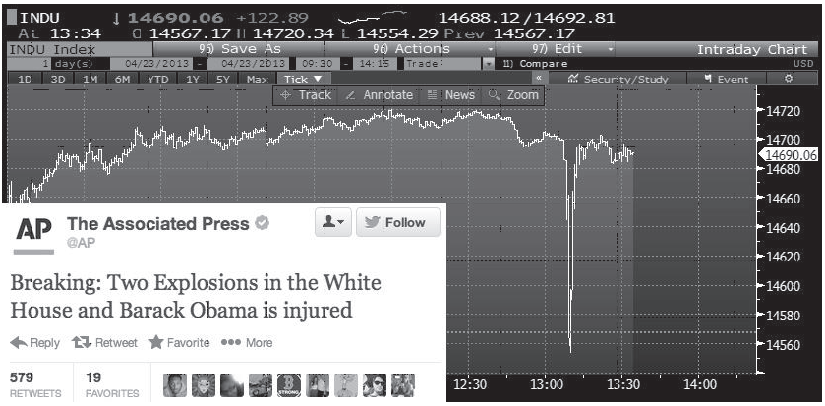


Figura 2: Ataque a la cuenta Twitter de Associated Press

Fuente: The Washington Post, 23-4-2014 Syrian hackers claim AP hack that tipped stock market by $136 billion. Is it terrorism? https://www.washingtonpost.com/news/worldviews/wp/2013/04/23/syrian-hackers-claim-ap-hack-that-tipped-stock-market-by-136-billion-is-it-terrorism/

Por lo tanto la desinformación masiva, como el uso de información como vector de desestabilización y de conflicto, constituye de facto un riesgo y amenaza a la seguridad.

1. At 1:07 p.m. on Tuesday, when the official Twitter account of the Associated Press sent a tweet to its nearly 2 million followers that warned, «Breaking: Two Explosions in the White House and Barack Obama is injured,» some of the people who momentarily panicked were apparently on or near the trading floor of the New York Stock Exchange.

At 1:08, the Dow began a perilous but short-lived nosedive. It dropped about 150 points, from 14697.15 to 14548.58, before stabilizing at 1:10 p.m., when news that the tweet had been erroneous began to spread. By 1:13 p.m., the level had returned to 14690. During those three minutes, the «fake tweet erased $136 billion in equity market value,» according to Bloomberg News' Nikolaj Gammeltoft.

Max Fisher. «Syrian hackers claim AP hack that tipped stock market by $136 billion. Is it terrorism?», *The Washington Post*, 23 de abril de 2013, https://www.washingtonpost.com/news/worldviews/wp/2013/04/23/syrian-hackers-claim-ap-hack-that-tipped-stock-market-by-136-billion-is-it-terrorism/

3. Especificidades del concepto de seguridad de información en el programa de ciberseguridad de Rusia

Una vez hemos realizado la aproximación conceptual a la desinformación y uso, nos centraremos en la estrategia de desinformación que practica Rusia, puesto que su evolución ha sido cada vez más beligerante frente a los intereses de la UE y sus aliados.

En 1996 se crea en la «Duma» el *Duma Subcommitte for Information Security* (Carr, 2011), sus objetivos era tratar de fijar políticas sobre la seguridad de la información y defensa en materia de ciberguerra. En el año 2000 hacen pública su «Doctrina de Seguridad de la Información» y en paralelo el sector tecnológico ruso, conjuntamente con las universidades y centros de investigación comienzan el desarrollo de un programa de ciberguerra.

La estrategia rusa reconoce que la guerra de información requiere medidas ofensivas y defensivas. Así la creación de «bombas lógicas» o «armas software» forman parte importante del programa; la lista de armas incluye virus (que causen la pérdida de datos), gusanos espías, troyanos, y accesos a infraestructuras críticas de forma remota. La planificación de este tipo de programas requiere tanto del esfuerzo académico, empresarial como militar y se apoyan en la capacidad organizativa y experiencia de los servicios secretos como la FAPSI (FAGSI, *Federal Agency for Government Communications and Information*) o el FSB (Servicio Federal de Seguridad) (National Security CyberSpace Institute, 2010)[2].

La capacidad defensiva se ha determinado mediante una serie de directivas sobre uso y explotación de sistemas operativos susceptibles de ser usados por el ejército ruso; ejemplo de ello fue la directiva de marzo de 2000 ordenando a las empresas rusas

2. Analysts say that multiple countries, in addition to China, have cyber capabilities, including friendly nations such as the United Kingdom or Israel, as well as less friendly nations including North Korea and Russia. Alan Paller, director of research at the SANS Institute, says that 100 countries have cyber espionage capabilities and that the Google incident represents the tip of the iceberg. Admittedly, espionage is routinely accepted and nations such as China and Russia, as well as the United States, are reportedly bolstering their cyber espionage capabilities. War over an espionage attempt is unlikely. The fact is, many nations have cyber espionage capabilities, and there is a need to better secure systems and networks accordingly. http://www.nsci-va.org/WhitePapers/2010-02-CyberEspionage-Is%20the%20US%20Getting%20More%20Than%20It's%20Giving-final.pdf

proporcionar medidas de seguridad específicas en los sistemas operativos UNIX y Windows si estos eran utilizados por algún sistema del ejército ruso.

El programa de ciberdefensa ruso también describe elementos tácticos y operativos de un ciberataque, en similitud con las estrategias del PLA de China, se determinan todos los sistemas de información del enemigo, denegando acceso a información, se especifica que la circulación de moneda y el sistema bancario debe ser interrumpido y la población sometida a operaciones psicológicas, incluyendo contra propaganda y desinformación sistemática. Es quizás esta la principal diferencia con las estrategias China o EEUU, el peso determinante del factor psicológico (Kramer, Starr, & Wentz, 2009) sobre la población de un supuesto enemigo[3].

La doctrina militar de 2010 analiza la seguridad de la información en un contexto militar y permite interpretar la ciberguerra como un acto de guerra. La doctrina reconoce «el compromiso de Rusia de utilizar instrumentos políticos, diplomáticos, legales, económicos, informativos y militares para proteger los intereses nacionales de Rusia y de sus aliados».

Según la doctrina, la ciberguerra puede impedir conflictos, sobre todo para identificar amenazas e influenciar la opinión pública y estatal. La primera amenaza militar externa de la lista es «la intensificación de la situación político-militar (relaciones internacionales) y la creación de condiciones para el uso de fuerzas militares». Para evitar este conflicto hay que «utilizar tecnologías modernas y

3. No Russian definitions of IW and IO utilize the term *cyber*, although several discuss informationization. In general, Russian military theorists view information-related topics in two categories: information-technical and information-psychological. Russia does not separate information-related topics into the same kinds of categories that the United States and China do, such as psychological operations, computer network operations, operations security, deception, and the like.

The technical aspect is of greatest interest in most countries, but the psychological aspect is the area of most attention in Russia.

…/…

In October 2005, Konstantin Nikolskiy defined the principal object and meaning of IW to consist of «a disorganization of the structure of society and distortion of public consciousness, as a result of which society loses moral-psychological and scientific-technological potential and thereby is deprived of the capability to wage armed warfare.» He defined information threats as «ideological-religious», scientific-technological, and emotional-psychological.» He argued for viewing the world as an aggregate of specific properties of systems.

de la información para evaluar y predecir el desarrollo de las situaciones político-militares a nivel regional y global, así como el estado de las relaciones bilaterales en la esfera política-militar». Internamente, la doctrina identifica como una amenaza importante «el trastorno de las autoridades estatales, de las instalaciones militares y estatales y de la infraestructura de la información de la Federación Rusa». El artículo 12 de la doctrina identifica las características del conflicto militar moderno, incluida «la integración del ejército y las capacidades no-militares y el papel en la ciberguerra» (literalmente «conflicto de información»). El artículo 13 describe la ciberguerra, definiéndola como una «intervención temprana para conseguir objetivos políticos sin el uso de las fuerzas militares», y después de utilizar la fuerza, el objetivo es «generar una reacción favorable en la comunidad mundial en el caso de acción militar» (President of the Russian Federation, 2010).

El enfoque ruso de la guerra de información (*Information Warfare,* IW) y su visión de lo que debería estar incluido en este concepto, no es el mismo que el de Occidente. La guerra de la información, desde el punto de vista ruso, se lleva a cabo en «*tiempo de paz*», en el *«preludio de una guerra»* y en *«tiempo de guerra»* (Limno & Krysanov, 2003).

La nueva Doctrina Militar de Rusia, firmada por el Presidente Putin el 26 de diciembre de 2014, hace especiales referencias al peligro de actores no identificados utilizando la guerra de información y la subversión política, para desestabilizar y derrocar regímenes. Según su planteamiento Rusia, está en riesgo, y la juventud de Rusia es vulnerable a la subversión[4].

El 8 de mayo de 2015, la Federación Rusa y la República Popular de China firmaron un acuerdo bilateral de cooperación

4. This doctrine differentiates between «dangers» and «threats:» the former designates concerns, the latter possible sparks for conflict. As in 2010, the NATO alliance, or, more accurately, its behavior and intentions, is classed as a danger, as are terrorism and violations of international agreements. But if many of the specifics are much the same, the tone of the overall document represents a shift, and a few of the individual changes are notable. This doctrine, in many ways something of a national security strategy document, is meant not only to describe Russian policy but also to send messages to friends, adversaries, and others. The challenge lies in understanding Russia's signals, as well as their repercussions.

Olga Oliker. «Russia's New Military Doctrine: Same as the Old Doctrine, Mostly», enero 2015, http://www.rand.org/blog/2015/01/russias-new-military-doctrine-same-as-the-old-doctrine.html

en el campo de la seguridad de la información internacional[5]. El tratado, que algunos han llamado un «pacto de no agresión» por el ciberespacio, detalla las medidas de cooperación que ambos gobiernos se comprometen a llevar a cabo, incluido el intercambio de información y una mayor cooperación científica y académica. Con este acuerdo, Rusia y China continúan avanzando en su visión de la «seguridad de la información», una visión de los problemas de seguridad en el ciberespacio que es marcadamente diferente de los enfoques occidentales de «ciberseguridad». Entre los aspectos a resaltar en nuestro análisis, destacamos que el pacto también define las amenazas informáticas como la transmisión de información que podría poner en peligro a los «sistemas sociales políticos y socio-económicos, y el ambiente espiritual, moral y cultural de los Estados.»

Como hemos podido comprobar, el concepto operaciones de información, es el que se centra en sus visiones conceptuales de ciberseguridad y ciberdefensa planteadas por China y Rusia.

Este planteamiento acerca de la seguridad de la información y de la «guerra de información» trasciende al ámbito de Rusia y China, y se extiende en el entorno de influencia internacional, así en la resolución del Informe del Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional de Naciones Unidas de julio de 2015[6] China, la Federación de Rusia, Kazajstán,

5. Already in 2009 Russia and China signed an agreement on cooperation in the field of international information security in the framework of the Shanghai Cooperation Organization. Later, in 2011 both countries submitted a proposal for an international code of conduct for information security to the United Nations. Although the proposal failed to garner sufficient support in the relevant Committee of the General Assembly, Russia and China redoubled their efforts. An updated version of the code of conduct is currently circulating in the UN in time for this fall's General Assembly session. All these initiatives sought to advance Russia's and China's views on a variety of cybersecurity issues while shoring up their positions in international discussions. This year's bilateral agreement is no exception in this regard. The Next Level For Russia-China Cyberspace Cooperation? http://blogs.cfr.org/cyber/2015/08/20/the-next-level-for-russia-china-cyberspace-cooperation/

6. United Nations General Assembly, A/70/174, «Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security,» July 22, 2015 http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174&referer=/english/&Lang=S

Kirguistán, Tayikistán y Uzbekistán, aportaron al informe final la petición de un código internacional de conducta para la seguridad de la información[7].

En este contexto, Ventre (2009) sostiene que muchos enfrentamientos a través de redes informáticas e Internet son el resultado de situaciones políticas de entorno tensas, y propone un modelo que se muestra en la Figura 3.

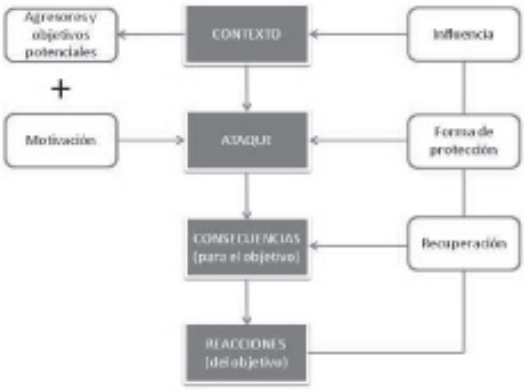


Figura 3: Ciclo de escalada del conflicto en la guerra de información (Information warfare cycle)

Fuente: Adaptado de Information warfare de Ventre, 2009, ISTE, London, UK.

Si bien el citado modelo fue desarrollado específicamente para el caso de ciberataques por motivos políticos, se puede utilizar para modelar cualquier incidente en el que se ha producido un evento catalogado en el ámbito de la guerra de información (*Information Warfare*, IW). Es evidente que determinados contextos internacionales entre países adversarios y con motivaciones potenciales para la escalada del conflicto, pueden dar lugar a un ataque IW. Esto tiene consecuencias para el objetivo, que reaccionará intentando recuperar sus sistemas y al mismo tiempo protegerse

7. «No utilizar tecnologías de la información y las comunicaciones ni redes de la información y las comunicaciones para interferir en los asuntos internos de otros Estados o socavar su estabilidad política, económica y social».

Propuesta de China, la Federación de Rusia, Kazajstán, Kirguistán, Tayikistán y Uzbekistán de un código internacional de conducta para la seguridad de la información (véase A/69/723) http://www.un.org/ga/search/view_doc.asp?symbol=A/69/723&referer=/english/&Lang=S

de los ataques actuales y futuros. Cualquier reacción del objetivo, y cualquier represalia o respuesta, se traducirá en el contexto general viéndose nuevamente influenciado por esta nueva situación.

La configuración de la estrategia de desinformación y propaganda de Rusia contra occidente se ha desarrollado de manera muy activa en los últimos años. Esta estrategia se centra específicamente con acciones de en medios de comunicación y redes sociales que buscan desprestigiar y generar inestabilidad política en toda Europa y específicamente en la UE[8].

Esta situación llevó al Parlamento Europeo[9] a aprobar una resolución en junio de 2015 en la que se instaba al Servicio Europeo de Acción Exterior al seguimiento y análisis de las estrategias de propaganda de la Federación Rusa:

Reitera su llamamiento en favor del refuerzo de las capacidades de análisis y de seguimiento de la propaganda de Rusia, especialmente en lengua rusa, a fin de poder identificar y responder con rapidez y de manera adecuada a la información intencionadamente sesgada que se difunde en varias lenguas de la UE; pide a la Comisión que ponga a disposición sin demora financiación adecuada para proyectos concretos destinados a hacer frente a la propaganda y desinformación rusa en la UE y fuera de ella, que facilite información objetiva al público en general en los países de la Asociación Oriental y que desarrolle los instrumentos adecuados de comunicación estratégica; acoge positivamente, a este respecto, las conclusiones del Consejo Europeo del 20 de marzo de 2015 sobre un plan de acción para luchar contra campañas de desinformación[10]; pide a

8. Neil MacFarquart. «A Powerful Russian Weapon: The Spread of False Stories», *The New York Times*, 28 de Agosto de 2016, http://www.nytimes.com/2016/08/29/world/europe/russia-sweden-disinformation.html?_r=0

9. European Parliament resolution of 10 June 2015 on the state of EU-Russia relations (2015/2001(INI)) http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2015-0225+0+DOC+XML+V0//EN

10. Bruselas, 20 de marzo de 2015 (OR. en) EUCO 11/15, Reunión del Consejo Europeo (19 y 20 de marzo de 2015). Conclusiones «El Consejo Europeo ha destacado la necesidad de contrarrestar las actuales campañas de desinformación de Rusia y ha invitado a la alta representante a que, en cooperación con los Estados miembros y las instituciones de la UE, prepare antes de junio un plan de acción sobre comunicación estratégica. La creación de un equipo de comunicación constituye una primera medida en ese sentido». http://eeas.europa.eu/euvsdisinfo/docs/disinformation_review_25-07-2016_eng.pdf

la Comisión y a los Estados miembros que desarrollen asimismo un mecanismo coordinado para la transparencia y la recogida, seguimiento e información en materia de asistencia financiera, política o técnica prestada por Rusia a partidos políticos y otras organizaciones dentro de la UE, con el fin de evaluar su participación e influencia en la vida política y en la opinión pública en la UE y sus vecinos del Este[11], y que adopten las medidas adecuadas.

En cualquier caso estas actuaciones no se han visto reflejadas ni la «La Estrategia Global para la Política Exterior y de Seguridad de la UE» como la estrategia de ciberseguridad europea no especifican como amenaza o riesgo potencial, y por lo tanto no determinan estrategias para minimizarlas.

4. Difusión de información sensible: Wikileaks, incidente Snowden, «Panamapapers»... suma y sigue

La difusión de información sensible, sin las debidas cautelas, puede ser más perjudicial que la manipulación, bloqueo o desinformación masiva.

4.1 *Wikileaks*

En 2010 conocemos el «escándalo Wikileaks», desencadenado por la publicación de miles de mensajes clasificados del Departamento de Estado de Estados Unidos. El 28 de noviembre de 2010, WikiLeaks filtra a la prensa internacional (The Guardian, The New York Times, Le Monde, El País y al semanario Der Spiegel) una colección de 251.187 cables o comunicaciones entre el Departamento de Estado estadounidense con sus embajadas por todo el mundo (denominados en inglés United States diplomatic

11. La reclamación Mogherini insistía en «hacer una comunicación proactiva de las políticas de la Unión Europea, corregir la desinformación cuando aparezca y apoyar el desarrollo de más medios independientes de la región». Sus objetivos son tres: comunicar directamente en los países del partenariado Este —Moldavia, Bielorrusia, Georgia o Azerbaijan entre otros— sobre el trabajo que desarrolla la UE, apoyar a los medios de comunicación independientes en la región y responder a la campaña de desinformación rusa.

Silvia Martínez. «La guerra oculta de Rusia contra la UE», *El Periódico*, 2 de agosto de 2016, http://www.elperiodico.com/es/noticias/internacional/guerra-oculta-rusia-contra-5302960

cables leak, Cablegate o Secret US Embassy Cables). El número y procedencia de los cables filtrados se detalla en la Figura 4.

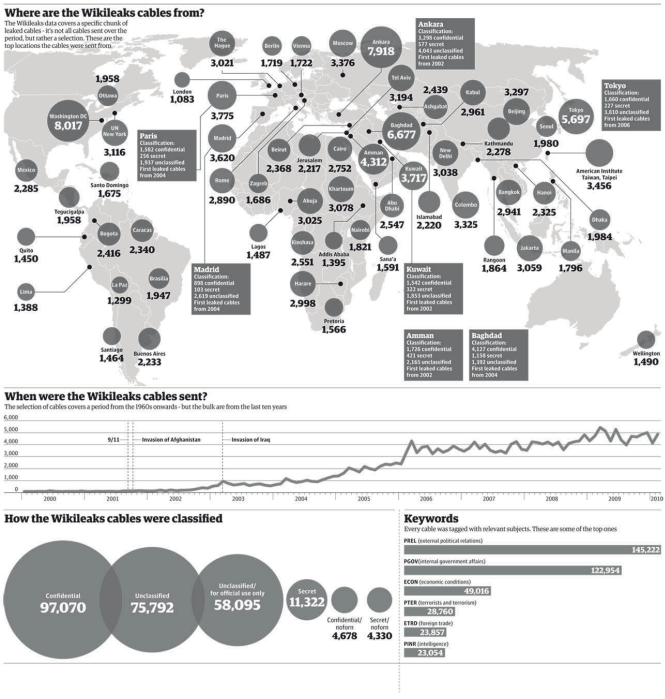


Figura 4: Procedencia de los cables filtrados por WikiLeaks

Fuente: WikiLeaks embassy cables: download the key data and see how it breaks down, The Guardian 3-12-2010 http://www.theguardian.com/news/datablog/2010/nov/29/wikileaks-cables-data

El hecho pone de manifiesto la dificultad de las organizaciones para defenderse frente a amenazas internas, así como la irreversibilidad de la filtración de la información (European Union Agency for Network and Information Security, 2010). La cronología del incidente se detalla en la Tabla 1.

Fecha	Hechos y repercusiones
5 de abril de 2010	Se publica un video en el que se ve cómo soldados estadounidenses matan al reportero de Reuters Namir Noor Eldeen, a su ayudante y a nueve personas más.
25 de julio de 2010	Los periódicos The Guardian, The New York Times y Der Spiegel hacen públicos un conjunto de unos 92.000 documentos sobre la Guerra de Afganistán entre los años 2004 y 2009, los cuales les llegaron a través de WikiLeaks.
22 de octubre de 2010	WikiLeaks publica 391.831 documentos filtrados desde el Departamento de Defensa de los Estados Unidos sobre la Guerra de Irak entre el 1 de enero de 2004 y el 31 de diciembre de 2009. Estos documentos se publicaron además en The Guardian, The New York Times, Le Monde, Der Spiegel, El País, Al Jazeera y el Bureau of Investigative Journalism.
28 de noviembre de 2010	WikiLeaks filtra a la prensa internacional (The Guardian, The New York Times, Le Monde, El País y al semanario Der Spiegel) una colección de 251.187 cables o comunicaciones entre el Departamento de Estado estadounidense con sus embajadas por todo el mundo (el incidente se denominada en inglés United States diplomatic cables leak, Cablegate o Secret US Embassy Cables).
30 de noviembre de 2010	WikiLeaks opta por mover su información a servidores de Amazon de computación en nube, ya que había recibido un ataque de denegación de servicio.
1 de diciembre de 2010	Amazon, ante la presión del gobierno de Estados Unidos, deja de albergar Wikileaks. China bloquea los hiperenlaces a wikileaks.

2 de diciembre de 2010	El proveedor EveryDNS rescinde el contrato con Wikileaks y corta su acceso. El partido pirata suizo ofrece alojamiento a Wikileaks con la nueva dirección wikileaks.ch y varias direcciones IP de acceso directo.
3 de diciembre de 2010	Se aprueba en Estados Unidos una reforma de ley conocida como el Acta SHIELD (Securing Human Intelligence and Enforcing Lawful Dissemination), una modificación del Acta de espionaje que prohíbe la publicación de información clasificada o comunicaciones internacionales de inteligencia.
4 de diciembre de 2010	PayPal cancela la cuenta que tenía con WikiLeaks, a través de la cual la organización obtenía financiación en forma de donaciones, aduciendo una supuesta violación de las políticas de uso en referencia a que no están permitidas «actividades que defiendan, promuevan, faciliten o induzcan a otros a participar en actividades ilegales». En una reacción al bloqueo de la dirección central, simpatizantes de WikiLeaks crearon más de mil espejos de la web de WikiLeaks.
6 de diciembre de 2010	Tanto MasterCard como PostFinance Swiss Postal bloquean la posibilidad de donaciones o pagos a WikiLeaks a través de sus sistemas de pago.
6 de diciembre de 2010	Anonymous lanza Operation Payback en defensa de WikiLeaks.
7 de diciembre de 2010	Es detenido en Inglaterra Julian Assange, fundador y director de WikiLeaks, siguiendo una orden de detención europea emitida por Suecia a raíz de una acusación de violación por parte de dos mujeres suecas. Ese mismo día Visa retira la capacidad de hacer donaciones o pagos a WikiLeaks.

9 de diciembre de 2010	Twitter cancela la cuenta de uno de los grupos de apoyo a WikiLeaks, Anonymous y después Facebook elimina la página de Operation Payback (Operación venganza) de ataques DDoS en defensa de WikiLeaks.
10 de diciembre de 2010	Anonymous decide modificar su estrategia de ataque a quienes participaban en el bloqueo a WikiLeaks, menos ataques DDoS y más divulgación de las filtraciones de WikiLeaks.

Tabla 1: Cronología de los incidentes vinculados a WikiLeaks
Fuente: Adaptado de El País. Las revelaciones de Wikileaks http://elpais.com/tag/c/91871e200f2c2bf8987c3cdbd09d178a y Wikileaks https://wikileaks.org/index.es.html

En España las filtraciones de Wikileaks tuvieron una elevada repercusión mediática. Los 3.620 cables diplomáticos publicados tratan de las relaciones de España con Irán, Cuba, Francia, Siria y Afganistán y versan sobre temas específicos como la política exterior, asuntos de interior, participación en conflictos internacionales, condiciones económicas y terrorismo. Además se realizan valoraciones sobre políticos en activo[12].

En el desarrollo de estos eventos se pueden distinguir tres aspectos a analizar con relevancia respecto a la seguridad de la información:

—La filtración de documentos con información sensible de los sistemas del Departamento de Estado de los Estados Unidos, realizada presuntamente por un usuario interno. El hecho pone de manifiesto la dificultad de las organizacio-

12. «Chacon is young and came to her position earlier this year with little experience in defense matters, but it would be a serious mistake to underestimate her or fail to respond substantively to her interest in this issue. She is a savvy politician and close to President Zapatero. It is rumored that Zapatero plans not to run again in 2012 and that he wants Chacon to be his successor. Whether or not that is true, Chacon is a power player here, and we can be sure that her interest in seeing the U.S. make the ADC a treaty is more than a whim»…/… Cable en el que la Ministra de Defensa Carmen Chacón pide elevar el Convenio de Cooperación de Defensa a Tratado. El País, 7 de diciembre de 2016, http://elpais.com/elpais/2010/12/07/actualidad/1291713447_850215.html

nes para defenderse frente a amenazas internas, así como la irreversibilidad de la filtración de información[13].

—El cese de los servicios de nombres de dominio (DNS) y de servicios de nube (*cloud*) relacionados con el sitio web de Wikileaks. Aunque formalmente se justificó este cese por violaciones de los términos en los acuerdos de servicio, se pone de manifiesto la debilidad de estos servicios frente a diferencias políticas y legales. Se pone en entredicho la neutralidad de los proveedores de servicio ante presiones políticas.

—Ciberataques realizados tanto a favor como en contra de Wikileaks. Supuestamente un hacker llamado Jester organizó un ataque de denegación de servicio (DoS) contra el sitio web de WikiLeaks. Posteriormente, en su apoyo, el grupo Anonymous distribuyó la herramienta «*Low Orbit Ion Cannon*» (LOIC) para lanzar ataques de denegación de servicio distribuido (DDoS) contra Visa, Paypal y sitios gubernamentales.

Desde el punto de vista de la seguridad TIC, estos incidentes ponen de manifiesto las siguientes cuestiones:

—No es necesaria una gran infraestructura para realizar un ataque satisfactorio: el número de ordenadores utilizados en los ataques fue relativamente pequeño (centenares). Algunos artículos de prensa reflejaban un número seis veces superior al real, lo que es indicativo de lo poco fiable que es la información sobre *botnets*.

—La robustez de algunos servicios ante estos ataques ha demostrado la resistencia de arquitecturas de nube ante ataques de denegación de servicio.

—La utilidad LOIC permite a terceras partes ejecutar comandos remotamente. Aparte de las posibles implicaciones legales, los usuarios ceden, al instalarla, el control sobre sus ordenadores a terceras partes potencialmente no confiables.

13. Prof. Helmbrecht, ENISA's Executive Director notes: «The freedom the internet allows in moving between jurisdictions and technologies makes cyber security an asymmetric challenge. But our economy and our governments are heavily reliant on functioning and resilient systems. Therefore it is a challenge which must be met through global co-operation to strengthen all aspects of cyber security.» http://www.enisa.europa.eu/media/news-items/enisa-statement-on-wikileaks-events

—Reacción legal ante este tipo de incidente como las modificaciones a la Directiva de la Unión Europea sobre Cibercrimen (*EU cybercrime directive*), introducida en 2010 por la Comisión Europea.

Las últimas filtraciones se vinculan al Consorcio de Periodistas de Investigación (ICIJ)[14], que difundió el 21 de septiembre de 2016 los datos de una filtración con referencias de más de 175.000 sociedades opacas u «offshore» en las Bahamas a nombre de diversas personas físicas y jurídicas. Esta nueva filtración se produce después de la relativa a los «Papeles de Panamá» publicados en abril de 2016, que consta de 1,3 millones de documentos de compañías, fondos, sociedades y fundaciones registradas en Panamá entre 1990 y 2016.

4.2. *El incidente Snowden*

El 5 de junio de 2013, el diario británico «The Guardian» revela la existencia de una orden judicial que permite a la NSA, *National Security Agency*, acceder durante tres meses al registro de todas las llamadas telefónicas efectuadas por los clientes del operador estadounidense Verizon. Al día siguiente los diarios «The Washington Post» y «The Guardian» informan de que la NSA y el FBI han solicitado a nueve gigantes de Internet, entre ellos Microsoft, Yahoo!, Google y Facebook, acceder a sus servidores para vigilar e interceptar comunicaciones de internautas extranjeros fuera de Estados Unidos (Greenwald, 2013). Este programa, hasta entonces secreto, denominado Prism**,** forma parte de una ley aprobada en 2007, bajo el mandato de George W. Bush, y renovada en diciembre de 2012. En un principio las compañías afectadas negaron que hubieran autorizado a los servicios de espionaje entrar en sus servidores, posteriormente hemos conocido la necesaria colaboración entre las compañías y diferentes agencias de seguridad[15]. La Figura 5

14. International Consortium of Investigative Journalists https://www.icij.org/

15. NSA Prism program slides.

Prism, according to the Snowden documents, is the biggest single contributor to the NSA's intelligence reports. As a 'downstream' program, it collects data from Google, Facebook, Apple and others. http://www.theguardian.com/world/interactive/2013/nov/01/prism-slides-nsa-document

forma parte de la presentación de Prism, filtrada por Snowden y disponible en la página de *The Guardian*[16].

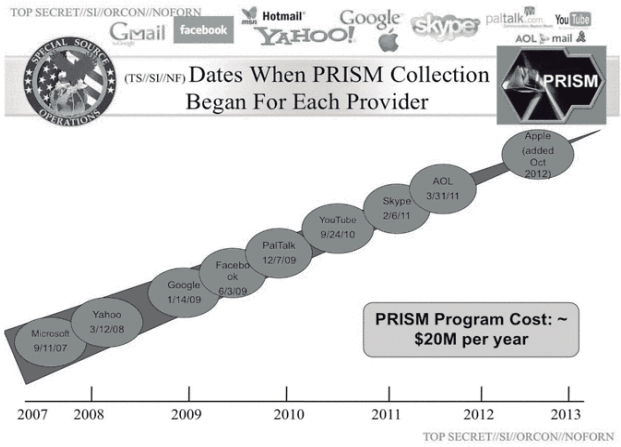


Figura 5: Programa PRISM de vigilancia masiva de la NSA
Fuente: The Guardian. The NSA files, http://www.theguardian.com/us-news/the-nsa-files

El 13 de mayo de 2014, Glenn Greenwald, el periodista y confidente de Edward Snowden, presentó su libro «*No place to hide*». Entre los nuevos datos aportados Greenwald destacan los relativos al modo en que la NSA opera a la hora de interceptar dispositivos de comunicaciones como *routers* y *switches* antes de que lleguen a sus compradores, con el objeto de insertar chips y/o firmwares (códigos de reconocimiento y acceso) que permitan monitorizar las transferencias de datos que se realizan a través de estos dispositivos. La colaboración del sector de empresas de TIC y proveedores de servicios de Internet con la NSA se ha expuesto en profundidad en el epígrafe 4.5 Ciberespionaje de estado vs ciberespionaje económico: inteligencia y seguridad económica.

No podemos dejar de mencionar la interrelación existente entre las capacidades de análisis masivo de datos, las herramientas tecnológicas vinculadas al *big data* y la privacidad y derecho a la intimidad del ciudadano. La connivencia de las grandes empresas

16. The NSA Files, Edward Snowden's surveillance revelations explained, The Guardian, 2013 Guardian US interactive team and Ewen MacAskill http://www.theguardian.com/us-news/the-nsa-files

de tecnologías de la información de Estados Unidos con la Agencia Nacional de Seguridad y la CIA, puestas en conocimiento de la opinión pública por las filtraciones del citado caso Snowden alientan a la identificación del binomio *big data / big brother*[17]. La práctica del hacking es generalizada y entendida como un derecho propio; según un documento de la NSA, sus capacidades han conseguido infectar al menos cincuenta mil ordenadores con un malware llamado «Quantum Insertion» (Greenwald, 2014). La Figura 6 muestra los lugares donde se han realizado esta clase de operaciones y el número de inserciones satisfactorias.

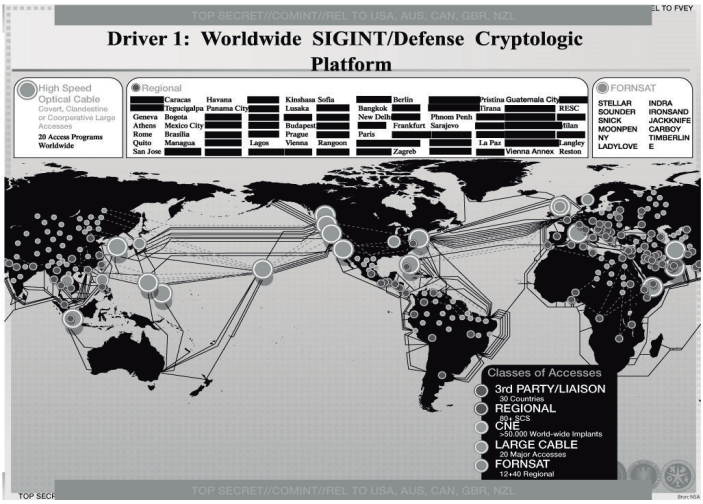


Figura 6: Sigmint Mundial. Plataforma Criptológica de Defensa. Quantum Insertion, NSA

Fuente: Snowden: sin lugar donde esconderse, Greenwald (2014), S.A. Ediciones B, https://edwardsnowden.com/es/2013/11/23/worldwide-sigintdefense-cryptologic-platform/

17. Big data technologies will be transformative in every sphere of life. The knowledge discovery they make possible raises considerable questions about how our framework for privacy protection applies in a big data ecosystem. Big data also raises other concerns. A significant finding of this report is that big data analytics have the potential to eclipse longstanding civil rights protections in how personal information is used in housing, credit, employment, health, education, and the marketplace. Americans' relationship with data should expand, not diminish, their opportunities and potential.

The Big Data and Privacy Review. The White House. «Big data: seizing opportunities, preserving values». Executive Office of the President. May 2014 https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf

La NSA también ha actuado en connivencia con otros gobiernos para crear su sistema de vigilancia global (Boeke & Eijkman, 2015). En líneas generales, la NSA mantiene tres categorías de relación: la primera es el grupo de los Cinco Ojos (EE.UU., Gran Bretaña, Canadá, Australia y Nueva Zelanda, llamada FVEY, *five eyes*); EE.UU. espía con esos países pero casi nunca en ellos, salvo que sea solicitado por esos países; en el segundo nivel hay países con los que la NSA trabaja para llevar a cabo proyectos específicos de vigilancia aunque también los espía de forma exhaustiva; el tercer grupo se compone de países en los que EE.UU. espía habitualmente y con los que casi nunca coopera (Greenwald, 2014).

En este sentido debemos resaltar las implicaciones que para el planeamiento de la seguridad y la defensa en Europa puede suponer el llamado «Brexit», ya que de un lado ha fortalecido el establecimiento del eje franco-alemán en materia de defensa[18], y de otro podría provocar un replanteamiento de las políticas de seguridad y defensa en el ámbito de UE y de la OTAN por parte de los países nórdicos[19].

La cronología del caso Snowden, las siguientes filtraciones y sus implicaciones en las relaciones bilaterales de muchos países con Estados Unidos se han visto afectadas y desconocemos el impacto social y económico que el desarrollo de los acontecimientos nos puede deparar. Las últimas informaciones relativas a las capacidades y procedimientos de la NSA, lo vinculan con el llamado «Equation Group», que a su vez parece haber sido *hackeado* por el autodenominado «ShadowBrokers», lo cual ha destapado manuales de uso de código malicioso utilizado en operaciones de espionaje[20].

18. El renacido eje franco-alemán, al menos en materia de defensa, propone una mayor integración en esa área, políticas comunes de integración y derecho de asilo e incluso medidas para impulsar el crecimiento económico, en un documento de nueve páginas titulado con la pompa habitual: Una Europa fuerte en un mundo de incertidumbres.

Claudi Perez. «Londres torpedea las propuestas para mejorar la defensa común en la UE». *El País*, 27 de septiembre de 2016, http://internacional.elpais.com/internacional/2016/09/27/actualidad/1474973291_744722.html

19. Tobias Etzold y Christian Opitz. «Nordic Europe after the Brexit Vote», SWP Comments 42, Septiembre 2016, http://www.swp-berlin.org/fileadmin/contents/products/comments/2016C42_etz_opt.pdf

20. The Intercept, «The NSA Leak Is Real, Snowden Documents Confirm» https://theintercept.com/2016/08/19/the-nsa-was-hacked-snowden-documents-confirm/

Las filtraciones del caso Snowden relativas a la colaboración de Facebook con la NSA, provocaron previa denuncia de un ciudadano austriaco ante el Tribunal de Justicia de la Unión Europea[21] la redefinición del acuerdo de compartición de datos entre empresas de EEUU, estableciendo el llamado Escudo de la privacidad UE-EEUU, que de facto representa más protección para los flujos de datos transatlánticos[22].

Para un análisis en profundidad de todas y cada una de las informaciones que vamos conociendo debemos tener en consideración todos los actores implicados y sus reacciones conforme vamos conociendo hechos, evidencias y pruebas. El seguimiento exhaustivo de las informaciones de The Guardian[23], The Washington Post[24], The Intercept[25], Electronic Frontier Founda-

21. El Tribunal de Justicia declara inválida la Decisión de la Comisión que declaró que Estados Unidos garantiza un nivel de protección adecuado de los datos personales transferidos http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117es.pdf

22. Comisión Europea, «La Comisión Europea pone en marcha el Escudo de la privacidad UE-EE.UU.: más protección para los flujos de datos transatlánticos». La Oficina del Director de Inteligencia Nacional explica además que la recopilación en bloque de datos solo podrá utilizarse en condiciones específicas predeterminadas y tiene que ser lo más concreta y precisa posible. Detalla las salvaguardias existentes para la utilización de los datos en esas circunstancias excepcionales. El secretario de Estado estadounidense ha establecido un mecanismo de recurso en el ámbito de la inteligencia nacional para los europeos a través de la figura del Defensor del Pueblo dentro del Departamento de Estado. http://europa.eu/rapid/press-release_IP-16-2461_es.htm

23. The Guardian. The NSA files. http://www.theguardian.com/world/the-nsa-files

24. The Washington Post. National Security, NSA secrets. http://www.washingtonpost.com/world/national-security/nsa-secrets/

25. The Intercept es una revista electrónica creada por Glenn Greenwald, Laura Poitras, y Jeremy Scahill. Lanzada en febrero de 2014 por la organización First Look Media, está financiada por Pierre Omidyar, fundador de ebay. The Intercept persigue dos objetivos. A corto plazo, la revista servirá como una plataforma para informar sobre los documentos publicados por Edward Snowden, y a largo plazo «producir un periodismo valiente, de confrontación a través de una amplia gama de temas: abuso, corrupción financiera o política, o violación de las libertades civiles». El sitio ofrece a sus «fuentes» una función anónima y segura similar a los archivos de WikiLeaks basada en una solución de código abierto SecureDrop gestionada por Freedom of the Press Foundation. https://firstlook.org/theintercept/

tion[26], la NSA y la propia Administración Obama, nos podría ir clarificando la perspectiva y el análisis estratégico de estos hechos.

Respecto a las filtraciones podemos establecer las siguientes conclusiones:

—Los ciudadanos independientes, la sociedad civil, que de otra manera no podría participar con capacidad de actuación y participación en conflictos internacionales, comienzan a tener un nuevo rol en el ciberespacio.

—Las motivaciones van desde el activismo político o social, el espionaje industrial y económico, el espionaje de estado, la ciberdelincuencia hasta el ciberincidente patrocinado por un estado.

—La reacción de la población en general, en el mundo occidental, ante las filtraciones de la NSA y WikiLeaks, ha sido relativamente leve; esto se debe a las diferencias intrínsecas de los puntos de vista diferenciados de quienes conocen el ciberespacio en comparación con aquellas que anteponen sus opiniones en el dominio físico. Caso diferente representan las filtraciones relativas al Consorcio de Periodistas de Investigación puesto que son relativas a personajes públicos y empresarios con transacciones en paraísos fiscales.

Conclusiones

La inexistencia de una estrategia específica de información asociada a la estrategia de ciberseguridad o de seguridad europea permite la injerencia desinformativa por parte de terceros países, fundamentalmente Rusia.

La información es el vector de acción tanto de las vulnerabilidades como de las acciones defensivas y preventivas de la seguridad, así pues sus implicaciones en el desarrollo de las estrategias de ciberseguridad y de seguridad nacional debe considerarse como prioritaria.

26. Electronic Frontier Foundation es la principal organización sin fines de lucro para la defensa de las libertades civiles en el mundo digital. Fundada en 1990, la EFF está implicada principalmente en la privacidad del usuario en internet, la libertad de expresión, y la innovación a través de litigios de impacto, análisis de políticas, el activismo de base, y el desarrollo tecnológico. «Timeline of NSA Domestic Spying». https://www.eff.org/nsa-spying/timeline

Las capacidades de control de interceptación de datos son deficitarias en el ámbito de la UE, y a en ocasiones colisionan con los intereses y capacidades de EEUU.

El llamado «Brexit» puede afectar a la política de coordinación europea en materia de ciberseguridad máxime por las especiales relaciones de Gran Bretaña con EEUU en la interceptación de datos y comunicaciones relacionados con la seguridad y la defensa.

Referencias bibliográficas

Bendiek, Annegret. «Due diligence in cyberspace: guidelines for international and European cyber policy and cybersecurity policy», SWP, mayo de 2016. [Consulta: 17 de junio de 2016]. Disponible en http://www.swp-berlin.org/fileadmin/contents/products/research_papers/2016RP07_bdk.pdf

Boeke, Sergei y Quirine AM Eijkman. «7 State surveillance in cyberspace». In Jarvis, Lee, Stuart MacDonald y Thomas M. Chen (Eds.), Terrorism Online: Politics, Law and Technology: Routledge. 2015.

Carr, Jeffrey. *Inside cyber warfare: Mapping the cyber underworld,* «O'Reilly Media, Inc.», 2011.

El País. Las revelaciones de Wikileaks. [Consulta: 20 de julio de 2016]. Disponible en http://elpais.com/tag/c/91871e200f2c2bf8987c3cdbd09d178a

ENISA. *Big Data Threat Landscape and Good Practice Guide*. 2016. [Consulta: 7 de julio de 2016]. Disponible en https://www.enisa.europa.eu/publications/bigdata-threat-landscape/at_download/fullReport

ENISA y Marinos, Louis. *ENISA Threat Taxonomy - A tool for structuring threat information*. 2016. [Consulta: 5 de julio de 2016]. Disponible en https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/etl2015/enisa-threat-taxonomy-a-tool-for-structuring-threat-information/at_download/file

Etzold, Tobias; Opitz, Christian. «Nordic Europe after the Brexit Vote», SWP Comments 42, Septiembre 2016. [Consulta: 20 de septiembre de 2016]. Disponible en http://www.swp-berlin.org/fileadmin/contents/products/comments/2016C42_etz_opt.pdf

European Union Agency for Network and Information Security. 2010. «ENISA statement on Wikileaks events». [Consulta: 7 de septiembre de 2016]. Disponible en http://www.enisa.europa.eu/media/news-items/enisa-statement-on-wikileaks-events

Greenwald, Glenn. *No place to hide: Edward Snowden, the NSA, and the US surveillance state*. Macmillan. 2014.

Greenwald, Glenn; MacAskill, Ewen. 2013. «NSA Prism program taps in to user data of Apple, Google and others». *The Guardian*, 7 de junio. [Consulta: 25 de Agosto de 2016]. Disponible en http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

Kramer, Franklin D., Starr, Stuart H. y. Wentz, Larry K. *Cyberpower and national security* (1st ed.). Washington, D.C.: National Defense University Press: Potomac Books. 2009.

Korzak, Elaine. «The Next Level For Russia-China Cyberspace Cooperation?», Council on Foreign Relations, 20 de gosto 2015. [Consulta: 3 de agosto de 2016]. Disponible en http://blogs.cfr.org/cyber/2015/08/20/the-next-level-for-russia-china-cyberspace-cooperation/

Limno, A. N. y Krysanov, M. F. «Information warfare and camouflage, concealment and deception». Military Thought, 12(2), 2003. [Consulta: 28 de julio de 2016]. Disponible en http://ics-www.leeds.ac.uk/papers/vp01.cfm?outfit=pmt&folder=66&paper=1257

MacFarQuhar, Neil. 2016 «A Powerful Russian Weapon: The Spread of False Stories». *The New York Times*, 28 de agosto. [Consulta: 1 de septiembre 2016]. Disponible en http://www.nytimes.com/2016/08/29/world/europe/russia-sweden-disinformation.html?_r=0

Martínez, Silvia. 2016. «La guerra oculta de Rusia contra la UE». El Periódico, 2 de agosto. [Consulta: 8 de agosto 2016]. Disponible en http://www.elperiodico.com/es/noticias/internacional/guerra-oculta-rusia-contra-5302960

National Security CyberSpace Institute «Cyber Espionage: Is the United States getting more than its giving?», 2010. [Consulta: 21 de junio de 2016]. Disponible en http://www.nsci-va.org/WhitePapers/2010-02-CyberEspionage-Is%20the%20US%20Getting%20More%20Than%20It's%20Giving-final.pdf

NATO. *Allied Joint Publication 3.10. Allied Joint Doctrine for Information Operations*, 2009 [Consulta: 19 de agosto de 2016]. Disponible en https://info.publicintelligence.net/NATO-IO.pdf

Oliker, Olga. 2016. «Russia's New Military Doctrine: Same as the Old Doctrine, Mostly». *The Washington Post*, 6 de enero. [Consulta: 17 de mayo de 2016]. Disponible en https://www.washingtonpost.com/blogs/monkey-cage/wp/2015/01/15/russias-new-military-doctrine-same-as-the-old-doctrine-mostly/

Perdomo, Celso. 2016. «Operaciones de información y ciberdefensa; conceptualizaciones en las estrategias de seguridad nacional». Director: Luis Álvarez Álvarez. Universidad de Las Palmas de Gran Canaria.

Perez, Claudi. 2016 «Londres torpedea las propuestas para mejorar la defensa común en la UE». *El País*, 27 de septiembre. [Consulta: 27 de septiembre de 2016]. Disponible en http://internacional.elpais.com/internacional/2016/09/27/actualidad/1474973291_744722.html

Russia. *The military doctrine of the Russian Federation.* Approved by Russian Federation by presidential edict, February 5. 2010. [Consulta: 27 de agosto 2016]. Disponible en http://carnegieendowment.org/files/2010russia_military_doctrine.pdf

The Guardian. «The NSA files». [Consulta: 8 de septiembre de 2016]. Disponible en http://www.theguardian.com/us-news/the-nsa-filesv

Ventre, Daniel, *Information Warfare*. London: ISTE, 2009
Wikileaks. 2016, [Consulta: 1 de septiembre 2016]. Disponible en https://wikileaks.org/index.es.html
World Economic Forum. «Global Risks 2012», 2012. [Consulta: 17 de agosto de 2016]. Disponible en 2016 http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2012.pdf
World Economic Forum. «Global Risks 2013». 2013. [Consulta: 17 de agosto de 2016]. Disponible en 2016 http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2013.pdf
World Economic Forum. «Global Risks 2014», 2014. [Consulta: 17 de agosto de 2016]. Disponible en 2016 http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2014.pdf
World Economic Forum. «Global Risks 2015», 2015. [Consulta: 17 de agosto de 2016]. Disponible en 2016 http://www3.weforum.org/docs/WEF_Global_Risks_2015_Report15.pdf
World Economic Forum. «Global Risks 2016», 2016 [Consulta: 17 de agosto de 2016]. Disponible en 2016 http://www3.weforum.org/docs/Media/TheGlobalRisksReport2016.pdf

TRATA DE SERES HUMANOS COMO UN ASUNTO DE SEGURIDAD. ¿EXISTEN INSTRUMENTOS SUFICIENTES PARA LA LUCHA CONTRA EL CYBERTRAFFICKING?

Ana Belén Valverde Cano
Doctoranda en Derecho Penal por la Universidad de Granada

José Antonio Castillo Parrilla
Doctorando en Derecho Civil por la Universidad de Granada

Resumen

Con la ampliación del concepto de seguridad, la trata de seres humanos ha pasado a ser considerada en los últimos tiempos como un asunto que afecta a la seguridad de los Estados. Tanto la Estrategia de la Unión Europea para la erradicación de la trata de seres humanos 2012-2016 como diversas iniciativas del Consejo de Europa, han destacado el incremento de las posibilidades de captar víctimas a través de la Red, debido a las facilidades que proporcionan las Tecnologías de la Información y la Comunicación.
Las principales normas internacionales en la materia, el Protocolo de las Naciones Unidas para prevenir, reprimir y sancionar la trata de personas y en el marco europeo el Convenio del Consejo de Europa sobre la lucha contra la trata de seres humanos, han establecido unas intensas obligaciones de prevención del delito y de cooperación entre los Estados. Por otra parte, la Sentencia del TEDH de 7 de enero de 2010 (Caso *Rantsev v. Chipre y Rusia*) extendió las obligaciones del artículo 4 del Convenio Europeo de Derechos Humanos a la trata, estableciendo unos estándares muy altos de protección de las víctimas y persecución del delito en aquellos ámbitos en los que pueda florecer especialmente, como es, por ejemplo, Internet.
A lo largo de estas páginas nos preguntamos si gozan los Estados, y particularmente España, de instrumentos suficientes para cumplir con estas obligaciones de cooperación y de lucha contra la modalidad de trata en la que las TIC desempeñan un papel importante, sea como método o como instrumento para facilitar la comisión del tipo (*cybertrafficking*).

Palabras clave

Trata de seres humanos, Ciberdelincuencia, TEDH, *Cybertrafficking*.

1. Introducción: la trata de seres humanos y la incidencia de internet como fenómeno social en el favorecimiento de la comisión de delitos

En Derecho Internacional Público, la definición aceptada de trata de personas es la que se encuentra en el Protocolo de las Naciones Unidas para Prevenir, Reprimir y Sancionar la Trata de Personas, Especialmente Mujeres y Niños (Protocolo de Palermo)[1], que complementa la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, del año 2000. Este Protocolo (junto con las notas interpretativas de los *travaux prèparatoires*[2]), puede considerarse como el único instrumento universal que aborda todos los aspectos de la trata de personas[3], y su definición es la que también recoge el Convenio del Consejo de Europa sobre la lucha contra la trata de seres humanos de 2005 (Convenio de Varsovia)[4], para el ámbito regional europeo.

Por otra parte, según el artículo 3 del Protocolo de Palermo, «por trata de personas se entenderá la captación, el transporte, el traslado, la acogida o la recepción de personas, recurriendo a la amenaza o al uso de la fuerza u otras formas de coacción, al rapto, al fraude, al engaño, al abuso de poder o de una situación de vulnerabilidad o a la concesión o recepción de pagos o beneficios para obtener el consentimiento de una persona que tenga autoridad sobre otra, con fines de explotación. Esa explotación

1. En línea, consultado por última vez el 30 de septiembre de 2016. Disponible en: http://www.ohchr.org/Documents/ProfessionalInterest/ProtocolTraffickingInPersons_sp.pdf

2. A/55/383/Add.1

3. J. Allain., *The Law and Slavery. Prohibiting Human Exploitation* (Boston, Brill Nijhoff, 2015), 266-267; A. Gallagher, *The International Law of Human Trafficking* (Nueva York, Cambridge University Press, 2010), 74; S. Scarpa, *Trafficking in Human Beings: modern slavery* (Oxford, Oxford University Press, 2008), 15; O. Patterson, «Trafficking, Gender and Slavery», *The Legal Understanding of Slavery: From the Historical to the Contemporary* (Oxford, Oxford University Press, 2012), 172.

4. En línea, consultado por última vez el 30 de septiembre de 2016. Disponible en:http://www.accem.es/ficheros/documentos/pdf_trata/Convenio_Consejo_de_Europa.pdf

incluirá, como mínimo, la explotación de la prostitución ajena u otras formas de explotación sexual, los trabajos o servicios forzados, la esclavitud o las prácticas análogas a la esclavitud, la servidumbre o la extracción de órganos». Por ende, distinguimos tres elementos: acción (captación[5], transporte, traslado, acogida o recepción), medios comisivos (que pueden ser violentos, fraudulentos o abusivos[6]) y finalidad de explotación.

La Estrategia de la Unión Europea para la erradicación de la trata de seres humanos (2012-2016)[7] señala la creciente importancia de Internet y el uso de las nuevas tecnologías en la trata de seres humanos. Esta nueva dimensión, planteada anteriormente en el marco del Consejo de Europa a través de diversas iniciativas[8], destaca el incremento de las posibilidades de captar víctimas mediante la Red, ya que ofrece oportunidades de empleo (en su mayoría atractivos puestos de trabajo en el extranjero como modelos, bailarinas, artistas de cabaret, etc.) que son accesibles a través de simples motores de búsqueda o ventanas emergentes, foros de diálogo (chats) y correo *spam*. Además, las redes sociales son cada vez más utilizadas como herramientas de captación.

5. La Oficina de Naciones Unidas contra la Droga y el Delito (UNODC) identifica Internet como uno de los medios de publicidad a través de los cuales captar posibles víctimas de trata. *Cfr.*: NACIONES UNIDAS, UNODC, *Manual para la lucha contra la trata de personas*, Publicación de las Naciones Unidas, Nueva York, 2007, p. 88. (En línea, consultado por última vez el 30 de septiembre de 2016). Disponible en: https://www.unodc.org/pdf/Trafficking_toolkit_Spanish.pdf.

6. E. Pérez Alonso, *Tráfico de personas e inmigración clandestina. (Un estudio sociológico, Internacional y Jurídico-Penal)* (Valencia, Tirant lo Blanch, 2008), 178.

7. Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. *Estrategia de la UE para la erradicación de la trata de seres humanos (2012-2016)*. COM/2012/0286 final. (En línea, consultado por última vez el 30 de septiembre de 2016). Disponible en: http://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX%3A52012DC0286

8. Entre ellas destaca el proyecto financiado por el gobierno de Mónaco denominado «*Misuse of the Internet fortherecruitment of victims of trafficking in human beings*» (2005/DG2/VC/405),con el objetivo de ayudar a los Estados Miembro a implementar unas apropiadas medidas legales, administrativas y técnicas, así como una concienciación más efectiva. *Vid.*, SYKIOTOU, A., *Trafficking in human beings: internet recruitment*, Council of Europe, 2007, pp. 7-8. (En línea, consultado por última vez el 30 de septiembre de 2016). Disponible en: https://ec.europa.eu/anti-trafficking/sites/antitrafficking/files/trafficking_in_human_beings_internet_recruitment_1.pdf

No es que el auge de las nuevas tecnologías, en particular Internet, haya dado lugar a nuevas formas de trata de personas (la ciber-trata o el *cybertrafficking*), sino que más bien las nuevas tecnologías han dado a la modalidad tradicional de trata una nueva dimensión[9]. En otras palabras, el *cybertrafficking* o la captación de víctimas de trata de seres humanos vía Internet no es una novedosa forma de trata, sino una nueva modalidad que ha contribuido al aumento del fenómeno. Como indica un Informe del Consejo de Europa de 2003 sobre pornografía infantil (una de las finalidades de la trata): «Muchos de los que coleccionaron pornografía infantil no hubieran comenzado la actividad, o por lo menos no hasta el punto en el que lo hicieron, si no fuera por las nuevas tecnologías de la información disponibles. Esta tecnología no genera por sí misma el interés o la actividad, pero juega un rol muy importante facilitándola» (p. 37). Y es que Internet, como fenómeno social, favorece el incremento de delitos de pornografía infantil debido a 1. que ofrece grandes posibilidades en relación con la distribución global de los contenidos pornográficos (por ejemplo, a través de redes P2P) y a que los consumidores de dichos contenidos se sienten amparados por la menor visibilidad que les garantiza la red pese a que, paradójicamente, su huella digital permitirá a las autoridades descubrir y probar las conductas que realizan con una mayor facilidad[10]. Así, webs aparentemente inocuas que están abiertas a todos los usuarios, pueden ser muy peligrosas, especialmente para menores o adolescentes, y convertirse en centros de captación de personas para su subsiguiente explotación.

Internet es una herramienta extraordinariamente eficiente en manos de criminales, especialmente aquellos que pertenecen a bandas organizadas, y permite optimizar los beneficios económicos, abaratando los costes de la captación por las características propias del cibercrimen (más barato, más rápido, con gran capacidad de producir efectos a distancia sin necesidad del traslado

9. Ibid, p. 18.

10. COUNCIL OF EUROPE, *Cybercrime training for judges: Training manual (draft)*, Project on Cybercrime, Council of Europe, 2009, p. 44. (En línea, consultado por última vez el 30 de septiembre de 2016). Disponible en: https://www.coe.int/t/dghl/cooperation/lisbonnetwork/meetings/Bureau/TrainingManualJudges_en.pdf

del delincuente, es más fácil ocultar las pruebas, etc.[11]11), por lo que ha ofrecido a los responsables de trata oportunidades sin parangón, que ellos se han apresurado a utilizar para encontrar, vender y situar a mujeres y niños en condiciones de explotación sexual o incluso esclavitud, servidumbre o trabajos forzosos[12]12. Tal y como indica el Informe de Europol de 2006 del Crimen Organizado: «las ventajas que Internet ofrece, en términos de tecnología de información y comunicación, son extremadamente beneficiosas para el crimen organizado»[13].

Por otro lado, desde la sentencia del Tribunal Europeo de Derechos Humanos (TEDH) *Rantsev v. Chipre y Rusia*, las obligaciones positivas de los Estados derivadas del artículo 4 del Convenio Europeo de Derechos Humanos (CEDH) se extienden a los casos de trata, lo que ha elevado los estándares de protección exigidos a los estados.

A la luz de todas estas consideraciones, se plantean las siguientes cuestiones:

a) ¿Cuál es el impacto del *cybertrafficking* en el espacio de libertad, seguridad y justicia europeo?
b) A la luz del Protocolo de Palermo y Convenio de Varsovia sobre la trata de personas, así como la reciente STEDH *Rantsev v. Chipre y Rusia*, ¿cuáles son las obligaciones de los Estados de la UE respecto a la trata y por qué es importante combatir el *cybertrafficking*?
c) Teniendo en cuenta los objetivos recogidos en el Protocolo de Palermo y Convenio de Varsovia, así como las obligaciones de

11. J. L. De la Cuesta Arzamendi, A. I. Pérez Machío, C. San Juan, «Aproximaciones criminológicas a la realidad de los ciberdelitos», en *Derecho Penal Informatico* (Navarra, Aranzadi, 2010).

12. Hughes, D., The Impact of the Use of New Communications and Information Technologies on Trafficking in Human Beings for Sexual Exploitation: A Study of the Users, Council of Europe, 2001. Vid., Council of Europe, Final Report, Group of Specialists on the impact of the use of new information technologies on trafficking in human beings for the purpose of sexual exploitation, EG-S-NT(2002), 2002, p. 7. (En línea, consultado por última vez el 30 de septiembre de 2016). Disponible en: https://ec.europa.eu/anti- trafficking/sites/antitrafficking/files/group_of_specialists_on_the_impact_of_the_use_of_new_information_technologies_1.pdf

13. EUROPOL, EU Serious,Organised Crime Threat Assessment Report 2013, European Police Office, 2013, p.7.

los Estados derivadas de la STEDH *Rantsev v. Chipre y Rusia* en materia de trata, ¿es suficiente el tratamiento a nivel nacional e internacional para combatir el *cybertrafficking*?

A estas cuestiones trataremos de responder a lo largo de este trabajo.

2. El impacto del *cybertrafficking* en el espacio de libertad, seguridad y justicia europeo: la trata como un asunto de seguridad

En la actualidad el paradigma predominante es un concepto amplio de seguridad[14], más acorde con las transformaciones globales y en el que se integra la «seguridad humana»[15]. Este enfoque aparece reflejado en las actuaciones del Consejo de Seguridad, en el concepto de Seguridad Cooperativa de la OTAN, en la recientemente publicada Estrategia Global Europea y en la Estrategia de Seguridad Nacional española de 2013[16].

Uno de los problemas relacionados con la «seguridad humana» que actualmente genera más atención internacional es la trata de seres humanos, en gran parte debido a la acción de Estados Unidos, precursor del Protocolo de Palermo, que elabora anualmente los *Trafficking In Persons Reports* con los que condiciona las ayudas no humanitarias al cumplimiento de ciertos criterios relacionados con medidas de persecución, promulgación e implementación de políticas anti-trata y de protección de las víctimas.

14. En contraposición con la concepción clásica de seguridad del paradigma realista de las Relaciones Internacionales, de raíces hobbesianas, que identificaba seguridad con integridad territorial del Estado. Vid., G. Orozco, «El concepto de la seguridad en la Teoría de las Relaciones Internacionales», Revista CIDOB d'Afers Internacionals, núm. 72, 2005, 166.

15. «El concepto de 'seguridad humana' se refiere a la necesidad de proteger el desarrollo libre de las personas en zonas donde se vean amenazados y violados los derechos humanos, mostrando que la base y fundamento de las políticas de seguridad se entronca en la persona humana, pues el fin de toda institución debe ser proteger al ser humano de las amenazas a su integridad, frente a la integridad del Estado o por encima del interés nacional». *Cfr.*, Ibid, p. 175.

16. Ministerio de Defensa, Documento Marco 05/2011 sobre la evolución del concepto de seguridad, 2011. (En línea, consultado por última vez el 30 de septiembre de 2016). Disponible en:http://www.ieee.es/Galerias/fichero/docs_marco/2011/DIEEEM05-2011EvolucionConceptoSeguridad.pdf

La trata de personas como asunto específico que afecta a la paz y la seguridad fue debatido por primera vez en la sesión del Consejo de Seguridad de las Naciones Unidas de 16 de diciembre de 2015. En esta reunión se solicitó el refuerzo del compromiso político y la mejora de la implementación de las medidas legales para penalizar, prevenir y combatir la trata de personas, que menoscaba el Estado de Derecho y contribuye a otras formas de delincuencia organizada transnacional, exacerbando conflictos y aumentando la inseguridad.

Previamente ya se había tenido en cuenta como asunto de seguridad de forma más transversal, por lo menos en cuanto a trata con fines de explotación sexual se refiere. Así, partiendo de la Declaración y Plataforma de Acción de Beijing de 1995[17], que incluye la trata y la prostitución forzada en la definición de violencia contra la mujer, es relevante la Resolución 1325 del Consejo de Seguridad de las Naciones Unidas sobre mujer, paz y seguridad (junto a las resoluciones 1820, 1888 y 1960 que la complementan)[18], que insta a los Estados a aplicar el criterio de género en las situaciones de conflictos armados y reconstrucciones de paz, prestando especial atención a la promoción de la lucha contra la trata de mujeres y niñas con fines de explotación sexual.

En el ámbito regional europeo, tanto el Consejo de Europa como Unión Europea han mostrado un fuerte compromiso político para abordar el problema de la trata de seres humanos. Por ejemplo, al Consejo de Europa se debe el Convenio sobre la Lucha contra la Trata de Seres Humanos, de 2005, que establece obligaciones que van más allá de las recogidas en el Protocolo de Palermo, y la creación de un organismo de supervisión: el grupo GRETA.

Centrándonos en la UE, desde que el Consejo Europeo en la Cumbre de Tampere de 1999 incluyera la lucha contra la trata como uno de los objetivos para establecer un espacio de libertad, seguridad y justicia, en la UE ha proliferado el número de iniciativas, medidas, programas de financiación y normativa; se ha incluido en la Estrategia de Seguridad Interior de la UE como un aspecto de

17. En línea, consultado por última vez el 30 de septiembre de 2016. Disponible en: http://www.unwomen.org/~/media/headquarters/attachments/sections/csw/bpa_s_final_web.pdf

18. En línea, consultadas por última vez el 30 de septiembre de 2016. Disponibles todas ellas en: http://www.un.org/es/peacekeeping/issues/women/wps.shtml

la acción exterior y como un elemento a combatir en la Estrategia Global para la Política Exterior y de Seguridad de la UE.

España, aunque no lo identifica como un asunto clave en la Estrategia de Seguridad Nacional[19], establece las prioridades para abordarlo en el Plan Integral de Lucha contra la Trata de Mujeres y Niñas (2015-2018)[20]. No obstante, lo hace de forma parcial, ya que como anticipa el título, se refiere únicamente a una de las modalidades de la trata (la trata con fines de explotación sexual), y no hace mención al resto de modalidades (trata con fines de tráfico de órganos, o para el sometimiento a una situación de esclavitud, servidumbre o trabajos forzosos)[21].

Vemos por tanto cómo la lucha contra la trata de personas en general se ha convertido en un aspecto importante para el mantenimiento del Espacio de Libertad, Seguridad y Justicia de la Unión Europea, lo que convierte en prioritaria la necesidad de una mayor comprensión del fenómeno del *cybertrafficking*, por sus características y su capacidad de captar más fácilmente potenciales víctimas aprovechándose de las condiciones de vulnerabilidad.

2. A la luz del protocolo de palermo y convenio de varsovia sobre la trata de personas, así como la reciente *stedh rantsev v. Chipre y Rusia*, ¿cuáles son las obligaciones de los estados de la ue respecto a la trata y por qué es importante combatir el cybertrafficking?

Tanto el Protocolo de Palermo como el Convenio de Varsovia se refieren a la necesidad de un enfoque global de lucha contra la trata, que incluya medidas para prevenirla y proteger a las víctimas, así como castigar a los traficantes. Además, establece unas intensas obligaciones de cooperación. Se desprende de las

19. Aunque lo mencione en el apartado de «flujos migratorios irregulares» (p. 32).

20. En línea, consultado por última vez el 30 de septiembre de 2016. Disponible en: http://www.violenciagenero.msssi.gob.es/planActuacion/planContraExplotacionSexual/docs/Plan_Integral_Trat a_18_Septiembre2015_2018.pdf

21. Y eso a pesar de las recomendaciones del Grupo GRETA para España en 2013, que llamaban la atención sobre este extremo. *Vid.*, Consejo de Europa, Grupo de Expertos sobre la Acción contra el Tráfico de Seres Humanos (GRETA), *Informe relativo a la implementación de la Convención del Consejo de Europa Contra la Trata de Seres Humanos por España*, Consejo de Europa, 2013.

disposiciones de estos dos instrumentos que los Estados parte, incluida la casi totalidad de los Estados miembro del Consejo de Europa, han formado la opinión de que sólo una combinación de medidas destinadas a tratar los tres aspectos (prevención, protección y persecución) pueden ser eficaces en la lucha contra el tráfico. En consecuencia, el deber de penalizar y enjuiciar la trata es sólo un aspecto en la lucha para combatir el tráfico general; los Estados deben investigar potenciales casos de trata, y aquéllos que son Estados de origen o de tránsito están obligados a cooperar efectivamente cuando sean casos transnacionales.

Por su parte, el 7 de enero de 2010 el TEDH dictó la sentencia del caso *Rantsev v. Chipre y Rusia*, aclamada por mostrar la voluntad del tribunal de luchar contra la trata de mujeres. En esta sentencia se pone de relieve el coste humano de la trata y la aquiesciencia de las autoridades políticas ante la misma, cuando relata el caso de Oxana Rantseva, mujer rusa de 21 años que aterrizó en Chipre en 2001 y una noche más tarde estaba muerta. En el caso *Rantsev*, el TEDH afirmó que la trata, a pesar de no aparecer literalmente en el artículo 4 del CEDH[22], estaba incluida en el mismo. Y lo hizo aplicando las reglas de interpretación del Convenio de Viena de 1969 sobre el Derecho de los Tratados (sentido corriente de los términos del tratado, contexto, objeto y fin), ya que «la trata de personas, por su naturaleza y propósito de explotación, está basada en el ejercicio de los atributos del derecho de propiedad»[23]. Por ende, las obligaciones del artículo 4 del CEDH (perfiladas sobre todo en *Siliadin*, en *C.N. y V. v. Francia* en *C.N. v. Reino Unido*) son aplicables a los casos de trata.

¿Cuáles son estas obligaciones? En *Siliadin*, el TEDH indica que la vulneración del artículo 4 constituye una violación de valores democráticos fundamentales de las sociedades que conforman el Consejo de Europa, por lo que se requieren estándares muy altos para su protección[24]. Las obligaciones positivas que emanan del artículo 4 para los Estados son tanto penales como procedimentales[25]:

22. Según el art. 4 del CEDH: *1. Nadie podrá ser sometido a esclavitud o servidumbre.2. Nadie podrá ser constreñido a realizar un trabajo forzado u obligatorio.*

23. *Rantsev v. Chipre y Rusia*, ECHR, no. 25965/04, 1 julio 2010, párr. 281.

24. *Siliadin v. Francia*, ECHR, no. 73316/01, 26 julio 2005, párr. 82 y 112.

25. Recogidas en: *Siliadin*, párr. 89 y 112, *Rantsev,* párr. 283-289 y *C.N. v. Reino Unido*, párr. 65 y ss.

a) En primer lugar, la obligación de penalizar y perseguir efectivamente la situación de violación del artículo 4. El Tribunal considera que el espectro de las garantías establecidas en la legislación nacional debe ser adecuado para garantizar la protección práctica y efectiva de los derechos de las víctimas de la trata. «En consecuencia, además de las medidas penales para castigar a los tratantes, el artículo 4 exige a los Estados Miembros poner en práctica medidas adecuadas de regulación de las empresas [o medios] que se utilizan a menudo como una tapadera para el tráfico de personas»[26].
b) En segundo lugar, la obligación positiva de adoptar medidas de protección.
c) En tercer lugar, la obligación de investigar adecuadamente las situaciones de explotación potencial cuando el asunto llama la atención de las autoridades, y de adoptar medidas para evitarlo[27]. Para que surja una obligación positiva de adoptar medidas operativas en un asunto concreto, debe demostrarse que las autoridades del Estado conocían, o debían haber conocido, circunstancias que permitían albergar una sospecha plausible de que un individuo identificado se había encontrado en un riesgo real e inminente de ser objeto una de las violaciones que establece el artículo 4. En el caso de una respuesta positiva, se produciría una violación del artículo 4 cuando las autoridades no consigan adoptar las medidas apropiadas dentro del alcance de sus potestades, para apartar a dicho individuo de la situación o riesgo. Esta obligación debe ser interpretada de forma que no imponga una carga imposible o desproporcionada sobre las autoridades de un Estado[28]. Es una obligación de

26. *Rantsev*, párr. 274.

27. En el fondo, y aunque no lo diga directamente, el TEDH se está refiriendo al estándar de «diligencia debida», establecido por la Corte IDH en el caso *Velásquez vs. Honduras*. Si el aparato estatal se conduce de manera que permite violaciones de derechos humanos no punibles y el restablecimiento de las víctimas no se produce lo antes posible, el Estado habrá fracasado en el deber de asegurar el libre y pleno ejercicio de tales derechos a las personas que se hallan bajo su jurisdicción, por lo que se puede hacer responder directamente por el referido déficit.

28. *Rantsev,* párr. 218-219.

medios y no de resultado, y no hay violación del artículo 4 si el Estado condujo una investigación efectiva, objetivamente capaz de llevar a la identificación y castigo de los responsables.

3. ¿Es suficiente el tratamiento delcybertrafficking a nivel nacional e internacional?

3.1. *Propuesta de definición del delito de cybertrafficking*

Como acaba de señalarse, tanto el Protocolo de Palermo como el Convenio de Varsovia, así como la STEDH *Rantsev* obligan a los Estados (y entre ellos, a España) a luchar contra la trata desde un enfoque global: legislar para prevenirla, proteger a las víctimas y castigar a los tratantes. Ya hemos tenido ocasión de pronunciarnos sobre el enfoque parcial desde el que España aborda esta lucha al centrarse sólo en una de las modalidades de trata, como es la trata con fines de explotación sexual (*cfr.* Plan Integral de Lucha contra la Trata de Mujeres y Niñas). Recordemos que según el TEDH, el artículo 4 del CEDH exige a los Estados Miembros poner en práctica medidas adecuadas de regulación de las empresas o medios que se utilizan a menudo como una tapadera para el tráfico de personas.

Teniendo en cuenta esto, ¿qué hay de del uso de las Tecnologías de la Información y la Comunicación como medio para cometer o facilitar la trata de personas? ¿Existen instrumentos nacionales o internacionales suficientes para luchar desde un enfoque global contra la trata cuando se utilizan las TIC? A ello dedicaremos nuestras siguientes reflexiones. Parece razonable que el primer paso para luchar contra cualquier fenómeno sea definirlo, sobre todo teniendo en cuenta que no existe un concepto estándar de *cybertrafficking* a nivel nacional o internacional.

Para ello debemos referirnos en primer lugar a los llamados «delitos informáticos». Si bien no existe una categoría legal de delitos informáticos[29], el término resulta útil para hacer referencia a todas aquellas conductas delictivas que son llevadas a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware

29. M. A. Davara Rodríguez, *Manual de Derecho Informático* (Navarra, Aranzadi, 2016), 386-388.

o software[30]. Quizá la definición más sistemática de qué debe entenderse por delito informático la aporta Lima Malvido[31], quien considera que el delito informático es «cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel, ya sea como método, medio o fin».

Dentro de los delitos informáticos, debemos distinguir entre delitos cuyo bien jurídico protegido es un bien o un servicio informático (se los puede denominar de forma genérica como delitos de daños informáticos o de acceso ilícito, donde se protege la integridad de programas informáticos, documentos electrónicos y, en general, datos, *cfr.* art. 264 CP y arts. 2 a 6 del Convenio de Budapest sobre Ciberdelincuencia), de aquellos otros delitos que, pudiendo cometerse sin intervención de TIC, se sirven de éstas como medio comisivo. Entre los tipos penales asociados a esta segunda categoría de delitos informáticos (delitos cometidos a través de medios informáticos) se encuentran los delitos de falsedad informática (*cfr.* arts. 390 a 399 *bis* CP y art. 7 Convenio de Budapest sobre Cibercriminalidad), de estafa informática (*cfr.* art. 248.2.a y b CP y art. 8 Convenio de Budapest sobre Cibercriminalidad), los delitos contra la propiedad intelectual (*cfr.* art. 270.2 y 3 CP y art. 10 Convenio de Budapest sobre Cibercriminalidad), la revelación de secretos cuando se hace a través de medios electrónicos (*cfr.* art. 197.1 CP), el recientemente introducido delito de sexting (art. 197.7 CP), o los delitos relativos a la pornografía infantil (cfr. art. 189 CP y art. 9 Convenio de Budapest sobre Cibercriminalidad). Puede observarse respecto de éstos últimos tipos penales que protegen una amplia gama de bienes jurídicos, que no necesariamente están relacionados con la informática (patrimonio, intimidad, integridad e indemnidad sexual de los menores…) pero que, sin embargo, se encuentran en una posición especialmente vulnerable si se atacan a través de medios

30. Ibid., p. 389.

31. M. L. Lima Malvido, «Delitos electrónicos», *Revista Criminalia, Academia Mexicana de Ciencias Penales*, núm. 1-6 (Enero-Junio 1984), 100. Cit. por C. Velasco San Martín, *Jurisdicción y competencia penal en relación al acceso transfronterizo en materia de ciberdelitos* (Valencia, Tirant lo Blanch, 2016), 51. 32Sobre la cuestión del bien jurídico del delito de trata, ver C. Villacampa Estiarte, «El delito de trata de seres humanos en el Código Penal Español», en *Nuevos retos en la lucha contra la trata de personas con fines de explotación sexual: un enfoque interdisciplinar* (Navarra, Civitas, 2012).

informáticos (nos remitimos a las reflexiones del Consejo de Europa sobre el incremento de los delitos de pornografía infantil a causa de la creciente presencia de Internet en la vida cotidiana).

El delito de trata, cuyo bien jurídico protegido es la dignidad del sujeto pasivo del tipo[32], puede ser cometido íntegramente a través de medios informáticos si tenemos en cuenta que la mera captación es ya constitutiva del tipo y que ésta puede realizarse, por ejemplo, a través de foros o chats. Por otra parte, las TIC también pueden facilitar el transporte, el traslado, o la acogida o recepción de las víctimas, pues si bien estas acciones necesariamente deben producirse fuera de la red, ello no impide que los medios electrónicos contribuyan a facilitarlas. Cuando las TIC jueguen un papel relevante en la comisión del tipo de trata como método (captación online de víctimas a través de Internet) estaremos ante un delito de *cybertrafficking* o ciber-trata.

Por tanto, podemos decir que el delito de *cybertrafficking* es un delito cometido a través de medios informáticos, que tiene lugar cuando para la realización de alguna de las acciones que constituyen el tipo penal de trata (captación, transporte, traslado, acogida o recepción de personas) se utilizan Tecnologías de la Información y la Comunicación, bien para la realización íntegra del tipo (captación online a través de foros o chats), bien como medio para favorecer o facilitar cualquiera de las acciones que constituyen trata (captación offline, transporte, traslado, acogida o recepción de personas).

4.2. *Algunos instrumentos internacionales de lucha contra la ciberdelincuencia y su preocupación (o no) por el cybertrafficking*

Quizás, de todos los instrumentos internacionales de lucha contra la ciberdelincuencia, el más completo hasta la fecha sea el Convenio del Consejo de Europa sobre la Ciberdelincuencia, firmado en Budapest el 23 de noviembre de 2003 (Convenio de Budapest sobre Ciberdelincuencia), ratificado por España el 3 de junio de 2010, y en vigor desde el 1 de octubre de ese mismo

32. Sobre la cuestión del bien jurídico del delito de trata, ver C. Villacampa Estiarte, «El delito de trata de seres humanos en el Código Penal Español», en *Nuevos retos en la lucha contra la trata de personas con fines de explotación sexual: un enfoque interdisciplinar* (Navarra, Civitas, 2012).

año[33]. Existen otros, no obstante, que deben conocerse, como la Directiva 2013/40/UE del Parlamento y del Consejo, de 12 de agosto de 2013 relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión marco 2005/222/JAI del Consejo[34]; la Directiva 2011/92/UE del Parlamento y del Consejo, de 13 de diciembre de 2011, relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil y por la que se sustituye la Decisión marco 2004/68/JAI del Consejo; así como la Convención del Consejo de Europa de 25 de octubre de 2007 sobre la Protección de los Niños contra la Explotación y el Abuso Sexual[35]. Como puede observarse, estos últimos se centran en aspectos concretos: ataques contra sistemas de información (delitos de daños informáticos) y pornografía infantil (la Convención de 25 de octubre de 2007 no sólo trata la pornografía infantil desde el punto de vista de la ciberdelincuencia sino de forma global).

Por otra parte, más allá de los textos normativos señalados, existen numerosas iniciativas internacionales para combatir la ciberdelincuencia, como la Cumbre Mundial sobre Sociedad de la Información[36], el Foro para la Gobernanza de Internet[37], o la Unión Internacional de Telecomunicaciones[38], que en 2009 elaboró una extensa guía sobre ciberdelitos donde podemos encontrar un exhaustivo catálogo de delitos informáticos, entre los que

33. BOE n. 226, de 17 de septiembre de 2010. Disponible en: ttps://www.boe.es/diario_boe/txt.php?id=BOE-A-2010-14221

34. DOUE de 14 de agosto de 2013 (L 218/8 a 218/14). Disponible en: https://www.boe.es/doue/2013/218/L00008-00014.pdf

35. BOE n. 274, de 12 de noviembre de 2010. Disponible en: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2010-17392

36. Pueden consultarse los documentos de esta cumbre, desarrollada en dos fases (Ginebra 2003 y Túnez 2005) en el siguiente enlace: https://www.itu.int/net/wsis/index-es.html. Interesa destacar, sin ánimo de ser exhaustivos, el punto 58 de la Declaración de Principios titulada «Construir la Sociedad de la Información: un desafío global para el nuevo milenio» (Disponible en: https://www.itu.int/net/wsis/docs/geneva/official/dop-es.html), donde se reconoce la importancia de fomentar la «dignidad y el valor de la persona» en el contexto de la Sociedad de la Información, formando parte, recordemos, la dignidad y el valor de la persona en cuanto tal del bien jurídico protegido por el delito de trata.

37. http://www.intgovforum.org/multilingual/

38. Puede encontrarse información sobre la UIT en su página web: http://www.itu.int/es/about/Pages/default.aspx

no se encuentra el de *cybertrafficking*[39]. La Asamblea General de las Naciones Unidas también ha emitido resoluciones en materia de ciberseguridad orientadas sobre todo a crear una cultura global sobre ciberseguridad[40].

En el catálogo de delitos informáticos que contempla el Convenio de Budapest tampoco encontramos referencia alguna a la comisión del delito de trata. El único artículo que podría tener alguna incidencia (de carácter tangencial) respecto de casos concretos de trata es el referido a los delitos relacionados con la pornografía infantil (artículo 9). En este artículo se castiga la producción de pornografía infantil, la oferta, puesta a disposición, difusión, transmisión o adquisición de pornografía infantil por medios informáticos, y la posesión de pornografía infantil en un sistema informático. Todas estas situaciones pueden ser consecuencia, aunque no necesariamente, de un tipo concreto de trata (la trata de menores con fines de explotación sexual), pero no se ataca, a través de este tipo delictivo, las conductas constitutivas de trata en sí.

Otro tanto puede decirse de la Directiva 2011/92/UE, que además se refiere exclusivamente a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil. Por tanto, ni combate la ciberdelincuencia, ni tampoco la trata de personas desde un enfoque global; sin embargo, uno y otro fenómeno estarán presentes en la medida en que conecten la captación con fines la explotación sexual y la pornografía infantil.

Podemos afirmar, por tanto, que en los instrumentos normativos internacionales relativos a la lucha contra la ciberdelincuencia señalados no se presta la debida atención al fenómeno del *cybertrafficking* y que, como máximo, determinadas conductas castigadas en tales textos tienen una incidencia tangencial. Esto no parece

39. Unión Internacional de Telecomunicaciones, El ciberdelito: Guía para los Países en Desarrollo, 2009. Disponible en: http://www.itu.int/dms_pub/itu-d/oth/01/0B/D010B0000073301PDFS.pdf: Algunos de los delitos que recoge son: acceso ilícito y daños informáticos, fraude y estafas informáticas, delitos relativos a los contenidos en la red, delitos contra la propiedad intelectual e industrial, ciberterrorismo, guerra informática o ciberblanqueo de dinero o la «peska» (actuaciones orientadas a que las víctimas revelen información personal o secreta).

40.Puede accederse al contenido de estas resoluciones así como a otros documentos que no hemos tenido ocasión de mencionar a través de la plataforma Ciberdelincuencia.org: http://www.ciberdelincuencia.org/fuentes/resoluciones.php

muy coherente con la importancia que hemos visto que tiene para la seguridad a nivel global, y puede ir en detrimento de las obligaciones de cooperación contempladas en el Protocolo de Palermo (artículos 9 al 13, que incluyen, por ejemplo, la necesidad de intercambio de información y otras medidas procesales) y en el Convenio de Varsovia (artículos 5 a 9), puesto que la ausencia de una respuesta y posición común contra dicha modalidad de trata puede dificultar en la práctica la lucha contra este fenómeno.

4.3. *La tipificación de los delitos informáticos en España y la presencia (o no) del cybertrafficking en otros instrumentos*

La tipificación de los delitos informáticos en España no se distancia en exceso de los ejemplos ya señalados en textos internacionales, y fundamentalmente en el Convenio de Budapest sobre Ciberdelincuencia. Incluso, podemos encontrar desde la redacción original del Código Penal en 1995 nutridas referencias a delitos contra sistemas informáticos o cometidos a través de medios informáticos, si bien se han introducido modificaciones o incluso se han tipificado nuevos delitos. Así, están regulados en nuestro Código Penal los delitos de daños informáticos (art. 264 CP), descubrimiento y revelación de secretos, y acceso ilícito a sistemas informáticos (arts. 197 y ss CP), estafas electrónicas (art. 248.2 CP), delitos contra la propiedad intelectual e industrial (arts. 270 y ss CP), delitos contra el honor, que pueden ser cometidos a través de internet (vid. art. 211 CP, cuando habla de imprenta, radiodifusión o «cualquier otro medio de eficacia semejante»), los delitos de falsedad de documentos y tarjetas de crédito (art. 390 y ss CP, y especialmente el artículo 400 CP, cuya redacción ha sido modificada por la LO 1/2015 y que se refiere, entre otras conductas, al desarrollo, recepción, obtención o tenencia de programas informáticos específicamente destinados a la falsificación de documentos) y, finalmente, delitos relativos a proteger la indemnidad e integridad sexual de los menores (interesa especialmente a efectos de este estudio el artículo 189 CP, así como el artículo 183 bis). Tras la reforma de 2015 (LO 1/2015, de 30 de marzo) se recogen nuevos delitos informáticos hasta ahora carentes de una tipificación precisa: no sólo el grooming, sino también el sexting (art. 197.7 CP). Otras, como el phishing, quedan a la valoración de los tribunales respecto de si constituyen

o no un delito de estafa informática (*vid.* STS de 533/2007, 12 de junio, a favor de esta tesis, y la SAP de Las Palmas de 11 de febrero de 2013, en contra).

¿Cuál es la situación, pues, de la normativa penal española respecto del *cybertrafficking*? De los delitos informáticos señalados, el tipo más próximo se refiere a los delitos relativos a la indemnidad e integridad sexual de los menores (p. e., el grooming), aunque no sea equiparable a la trata por diversas razones: distinto bien jurídico y distinta acción típica. Por su parte, el artículo 177 bis del Código Penal castiga como reo de trata de seres humanos a quien «empleando violencia, intimidación o engaño, o abusando de una situación de superioridad o de necesidad o vulnerabilidad de la víctima nacional o extranjera, o mediante la entrega o recepción de pagos o beneficios para lograr el consentimiento de la persona que poseyera el control sobre la víctima, la captare, transportare, trasladare o recibiere, incluido el intercambio o transferencia de control sobre esas personas», con cualquiera de las finalidades siguientes: trabajo o servicios forzados, esclavitud o prácticas similares a la esclavitud, a la servidumbre o a la mendicidad, explotación sexual, incluyendo la pornografía, explotación para realizar actividades delictivas, extracción de sus órganos corporales, o celebración de matrimonios forzosos.

La configuración del tipo no excluye que la trata se cometa a través de redes sociales o de chats, o que los medios informáticos puedan contribuir de algún modo a la realización del tipo, aunque no menciona expresamente el *cybertrafficking*. De todos modos, el Código Penal tampoco parece ser el lugar más apropiado para hacer una referencia explícita a la incidencia de las TIC en la comisión del delito de trata.

Sin embargo, sí parece recomendable que en el marco de la Estrategia Nacional de Ciberseguridad se desarrollen actuaciones concretas que presten a este asunto la importancia que merece. No obstante, cuando examinamos la Estrategia de Ciberseguridad Nacional, entre cuyas líneas de actuación se recoge como objetivo nacional la persecución del ciberterrorismo y la ciberdelincuencia «en su doble vertiente de instrumento facilitador de sus actividades y de objeto directo de su acción»[41], no hace ninguna alusión

41. Gobierno de España, Presidencia del Gobierno, *Estrategia de Ciberseguridad Nacional*, 2013, Línea de acción 4, p. 35.

a tipos delictivos concretos más allá del crimen organizado y el blanqueo de capitales, y por ende, tampoco al *cybertrafficking*.

Conclusiones

En los últimos años, y con el cambio de paradigma realista a uno basado en la seguridad humana, la trata de seres humanos ha pasado a ser una cuestión de seguridad para los Estados, como demuestran las estrategias internacionales, europeas y nacionales de seguridad.

A lo largo del trabajo hemos visto que la obligación de combatir eficazmente la trata de personas emana del Protocolo de Palermo y, en el ámbito europeo, del Convenio de Varsovia. Particularmente, estos instrumentos contemplan la necesidad de perseguir y prevenir el delito, así como proteger a las víctimas, por lo que la cooperación entre los estados ocupa un lugar esencial en dichos convenios, dándosele un enfoque global.

Por otro lado, la STEDH *Rantsev v. Chipre y Rusia* extiende las obligaciones emanadas del artículo 4 del CEDH a los casos de trata de personas a pesar de no estar enunciada expresamente en el artículo. De este modo, se establecen unos elevados estándares de protección que se concretan en tres aspectos: (1) obligación de penalización y persecución efectiva; (2) obligación de adoptar medidas de protección de las víctimas; y (3) obligación de investigar adecuadamente las situaciones de explotación potencial y de adoptar medidas para evitarlo. Según el Tribunal de Estrasburgo, además de las medidas penales para castigar a los tratantes, el artículo 4 exige a los Estados Miembros poner en práctica medidas adecuadas de regulación de las empresas o medios que se utilizan a menudo como una tapadera para el tráfico de personas.

Hemos tratado de mostrar el evidente vínculo que existe entre el auge de Internet como fenómeno social y la comisión de actividades delictivas, especialmente en lo que se refiere a nuestro objeto de estudio, la trata de personas. Las Tecnologías de la Información y de la Comunicación están tomando cada vez un papel más relevante en la comisión de delitos, contribuyendo a que los casos sean mucho más complejos debido a las dificultades a la hora de determinar la jurisdicción competente o la normativa aplicable, así como los obstáculos derivados de las divergencias normativas y de preparación logística y formativa de muchos Es-

tados a la hora de combatir el cibercrimen. Los tratantes ya no necesitan recurrir a los viejos métodos como las «*red light areas*», ya que tanto la captación como los acuerdos de transacción de las víctimas pueden ser realizados de forma anónima (o aparentemente anónima) a través de Internet. De este modo, es menos probable que las víctimas despierten la atención de la policía, y surgen nuevos horizontes, posibilidades (y también obligaciones) vinculadas al control efectivo de las zonas potencialmente peligrosas en relación con actividades de trata, diseminadas una vez que se introducen los medios telemáticos.

Teniendo esto en cuenta, ¿se están cumpliendo estas obligaciones cuando en la comisión del delito de trata intervienen las Tecnologías de la Información y de la Comunicación? ¿Se han tomado medidas para investigar situaciones de explotación potencial de posibles víctimas de trata cuando tal situación de peligro potencial se produce en la red (por ejemplo, captación a través de foros o chats)?

Como hemos tratado de poner de manifiesto, la lucha contra el *cybertrafficking* (entendiendo éste como el delito cometido a través de medios informáticos que tiene lugar cuando para la realización de alguna de las acciones esenciales que constituyen el tipo penal de trata se utilizan medios telemáticos) brilla por su ausencia. Combatir penalmente tales conductas (necesario, sin lugar a dudas), como se hace en el artículo 177 bis CP con el delito de trata, no permite ni mucho menos entender que se esté abordando la lucha contra la trata de personas desde un enfoque global como exigen tanto el Protocolo de Palermo como el Convenio de Varsovia. No ya sólo porque se esté prestando una gran atención a la trata con fines de explotación sexual (de nuevo, necesaria) en detrimento de otras modalidades de trata, sino porque, en lo referido a los medios a través de los cuales puede cometerse, favorecerse o facilitarse la trata, se están ignorando o no se les está prestando suficiente atención a aquéllos que en los últimos años han contribuido a un mayor incremento de la actividad delictiva, como son los medios telemáticos.

Se hace necesario, por tanto, revisar las estrategias nacionales e internacionales tanto en materia de trata de seres humanos como de ciberdelincuencia, de manera que la importancia que tienen de facto las TIC en la comisión y favorecimiento del delito de trata de seres humanos se visibilice, contribuyendo de este

modo a que se luche contra la trata desde un enfoque global, tal y como proclaman los principales textos internacionales de referencia en la materia.

Agradecimientos

A todas las abuelas del mundo. Por contribuir a la divulgación científica al obligarnos a sintetizar los pensamientos complejos y expresarlos de manera accesible y sencilla.

Referencias bibliográficas

Allain, J., 2015, The Law and Slavery. Prohibiting Human Exploitation, Boston, Brill Nijhoff.

o 2012, *The Legal Understanding of Slavery: From the Historical to the Contemporary*, Oxford, Oxford University Press.

De La Cuesta Arzamendi, J. L. (ed.), 2010, *Derecho Penal Informático*, Navarra, Aranzadi.

Davara Rodríguez, M. A., 2016, Manual de Derecho Informático, 11ª Edición, Navarra, Aranzadi.

Gallagher, A., 2010, The International Law of Human Trafficking. Nueva York, Cambridge University Press.

Lara Aguado, A. (dir.), 2012, Nuevos retos en la lucha contra la trata de personas con fines de explotación sexual: un enfoque interdisciplinar, Navarra, Civitas, 2012.

Lima Malvido, M. L.,1984, Delitos electrónicos, *Revista Criminalia, Academia Mexicana de Ciencias Penales*, México D.F., Ed. Porrúa, n. 1-6, enero-junio 1984, p. 100.

Orozco, G., 2005, El concepto de la seguridad en la Teoría de las Relaciones Internacionales, *Revista CIDOB d'AfersInternacionals*, núm. 72.

Pérez Alonso, E., 2008, *Tráfico de personas e inmigración clandestina. (Un estudio sociológico, Internacional y Jurídico-Penal)*, Valencia, Tirant lo Blanch.

Scarpa, S., 2008, *Trafficking in Human Beings: modern slavery*, Oxford, Oxford University Press.

Sykiotou, A., 2007, *Trafficking in human beings: internet recruitment*, Council of Europe (En línea, consultado por última vez el 30 de septiembre de 2016). Disponible en: https://ec.europa.eu/anti-trafficking/sites/antitrafficking/files/trafficking_in_human_beings_internet_recruitment_1.pdf

Velasco San Martín, C., 2016, *Jurisdicción y competencia penal en relación al acceso transfronterizo en materia de ciberdelitos*, Valencia, Tirant lo Blanch

Informes, guías y documentos nacionales e internacionales

Comisión Europea, 2012, Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. *Estrategia de la UE para la erradicación de la trata de seres humanos* (2012-2016). COM/2012/0286 final. (En línea, consultado por última vez el 30 de septiembre de 2016). Disponible en: http://eur-lex.europa.eu/legal- content/ES/ALL/?uri=CELEX-%3A52012DC0286

Consejo de Europa, 2009, *Cybercrime training for judges: Training manual (draft)*, Project on Cybercrime. (En línea, consultado por última vez el 30 de septiembre de 2016). Disponible en: https://www.coe.int/t/dghl/cooperation/lisbonnetwork/meetings/Bureau/Training ManualJudges_en.pdf

Consejo de Europa, grupo de expertos sobre la acción contra el tráfico de seres humanos (GRETA), 2013, *Informe relativo a la implementación de la Convención del Consejo de Europa Contra la Trata de Seres Humanos por España*, Consejo de Europa, GRETA. Cumbre mundial sobre la sociedad de la información, 2004, Construir la Sociedad de la Información: un desafío global para el nuevo milenio (Disponible en: https://www.itu.int/net/wsis/docs/geneva/official/dop-es.html).

Hughes, D., 2001, *The Impact of the Use of New Communications and Information Technologies on Trafficking in Human Beings for Sexual Exploitation: A Study of the Users*, Council of Europe, *Vid.*, Council of Europe, Final Report, Group of Specialists on the impact of the use of new information technologies on trafficking in human beings for the purpose of sexual exploitation, EG-S-NT(2002), 2002, p. 7. (En línea, consultado por última vez el 30 de septiembre de 2016). Disponible en: https://ec.europa.eu/anti-trafficking/sites/antitrafficking/files/group_of_specialists_on_the_impact_of_the_use of_new_information_technologies_1.pdf.

EUROPOL, *EU Serious,Organised Crime Threat Assessment Report 2013*, European Police Office, 2013, p. 7.

NACIONES UNIDAS, UNODC, Manual para la lucha contra la trata de personas, Publicación de las Naciones Unidas, Nueva York, 2007, p. 88. En línea, consultado por última vez el 30 de septiembre de 2016). Disponible en: https://www.unodc.org/pdf/Trafficking_toolkit_Spanish.pdf.

NACIONES UNIDAS, ONU MUJERES, Declaración y Plataforma de Acción de Beijin, Pekín, 1995. (En línea, consultado por última vez el 30 de septiembre de 2016). Disponible en: http://www.unwomen.org/~/media/headquarters/attachments/sections/csw/bpa_s_f inal_web.pdf

Gobierno de Mónaco, «*Misuse of the Internet fortherecruitment of victims of trafficking in human beings*» (2005/DG2/VC/405).

Gobierno de España, Presidencia del Gobierno, Estrategia de Ciberseguridad Nacional. (En línea, consultado por última vez el 30 de septiembre de 2016). Disponible en: http://www.dsn.gob.es/es/estrategias- publicaciones/estrategias/estrategia-ciberseguridad-nacional

Gobierno de España, Presidencia del Gobierno, Estrategia de Seguridad Nacional. Un proyecto compartido, 2013. (En línea, consultado por última vez el 30 de septiembre de 2016). Disponible en: http://www.lamoncloa.gob.es/documents/seguridad_1406connavegacionfinalaces iblebpdf.pdf.

Gobierno de España, Ministerio de Defensa, Documento Marco 05/2011 sobre la evolución del concepto de seguridad, 2011. (En línea, consultado por última vez el 30 de septiembre de 2016). Disponible en:http://www.ieee.es/Galerias/fichero/docs_marco/2011/DIEEEM05-2011EvolucionConceptoSeguridad.pdf

Gobierno de España, Ministerio de Sanidad, Servicios Sociales e Igualdad, Plan Integral de Lucha contra la Trata de Mujeres y Niñas, 2015- 2018. (En línea, consultado por última vez el 30 de septiembre de 2016). Disponible en: http://www.violenciagenero.msssi.gob.es/planActuacion/planContraExplotacionS exual/docs/Plan_Integral_Trata_18_Septiembre2015_2018.pdf

J*urisprudencia de Tribunales Internacionales de Derechos Humanos*

Sentencia CIDH de 21 de julio de 1989. Caso Velásquez Rodríguez v. Honduras. (En línea, consultado por última vez el 30 de septiembre de 2016). Disponible en: http://www.corteidh.or.cr/docs/casos/articulos/seriec_07_esp.pdf

Sentencia TEDH de 26 de julio de 2005 (Demanda n. 73316/01). *Caso Siliadin v. Francia.* (En línea, consultado por última vez el 30 de septiembre de 2016). Disponible en: https://ec.europa.eu/anti- trafficking/sites/antitrafficking/files/siliadin_v_france_en_4.pdf

Sentencia TEDH de 7 de enero de 2010 (Demanda n. 25965/04). Caso *Rantsev v. Chipre y Rusia.* (En línea, consultado por última vez el 30 de septiembre de 2016). Disponible en: http://www.womenslinkworldwide.org/observatorio/documentos/gjo_ecthr Rant sev_c_Chipre_y_Rusia._es.pdf

LA DEFENSA DE LA PRIVACIDAD EN LA ERA DE LA CIBERSEGURIDAD

Ramón M. Orza Linares

Depto. Derecho Constitucional. Universidad de Granada

Resumen

El Tribunal Europeo de Derechos Humanos, en su Sentencia de 3 de abril de 2007 (Caso Copland), analizó si el seguimiento de las llamadas telefónicas, del uso del correo electrónico y de la navegación por Internet realizada por los responsables de un College universitario de Gales (Reino Unido) sobre una trabajadora del mismo, suponía injerencia en su derecho a la privacidad. En este asunto el Tribunal consideró que tales injerencias eran injustificadas. Esta doctrina, lejos de consolidarse, se sitúa en medio de un nuevo conflicto entre la libertad y la seguridad. Así, podemos asistir a una paulatina legislación, sobre todo en la Unión Europea, que busca una mayor protección de las libertades de los ciudadanos, al tiempo que la propia Unión Europea se dota de nuevas posibilidades e instrumentos que pueden suponer amenazas a la intimidad y a la vida privada de esos mismos ciudadanos.

Palabras claves

Privacidad, intimidad, libertad, derechos fundamentales, seguridad.

Introducción

La reacción ante los pasados atentados en Francia[1] y de otros países europeos, ha vuelto a poner de relieve la tensión existente

1. Nos referimos a los atentados ocurridos en Francia, el 7 de enero de 2015 que tuvo como objetivo el semanario «Charlie Hebdo» con un resultado de 12 muertos y 11 heridos, los atentados del 8 y 9 de enero de 2015, con un resultado de 5 fallecidos, entre ellos una policía municipal y cuatro clientes de un supermercado kósher en París, y ocho heridos; a los atentados del 13 de noviembre de 2015 en París en los que fallecieron 137 personas y 415 heridos, así como el atentado perpetrado el 14 de julio de 2016 en Niza en el que resultados fallecidas 85 personas y 303 fueron heridas, y, por último, el ataque contra una iglesia en Normandía, el 26 de julio de 2016, en que los atacantes mataron a un sacerdote, hirieron a otra persona y retuvieron como rehenes a cuatro personas más.

entre la defensa de la privacidad y la seguridad pública. Esta tensión, que se había manifestado de manera muy significativa tras los atentados del 11 de septiembre de 2001 contra las Torres Gemelas y el Pentágono en los Estados Unidos, han culminado con la adopción, a uno y otro lado del atlántico, de un variado catálogo de medidas que tienen como finalidad el refuerzo de la seguridad pública, a costa de un significativo aumento de los controles policiales sobre las personas.

Así, por lo que se refiere a los Estados Unidos, el 26 de octubre de 2001 fue aprobada el «USA Patriot Act» con la finalidad de ampliar la capacidad de acción del Estado para combatir el terrorismo.

Y, dentro de la Unión Europea, el 12 de febrero de 2015, se emitió una Declaración de los miembros del Consejo Europeo[2] en el que se manifestaba la voluntad de «reforzar las acciones contra las amenazas terroristas, en el pleno respeto de los derechos humanos y del Estado de Derecho», para lo que pedían «que los legisladores de la UE adopten con urgencia una Directiva europea sólida y eficaz sobre registro de nombre de los pasajeros, con sólidas garantías de protección de datos», así como que «se utilice plenamente el marco existente de Schengen para reforzar y modernizar el control de las fronteras exteriores», que «las fuerzas y cuerpos de seguridad y las autoridades judiciales intensifiquen el intercambio de información y la cooperación operativa, en particular a través de Europol y Eurojust» y, entre otras, «que los servicios de seguridad de los Estados miembros intensifiquen su cooperación». Todo ello, a estas alturas de 2016, ha supuesto la aprobación de varias directivas y de un reforzamiento institucional de la cooperación policial y judicial entre los Estados de la Unión.

Por lo demás, desde el 19 de septiembre de 2007 la Unión Europea ya contaba con un Coordinador de la lucha contra el terrorismo[3], cuyas tareas comprendían, entre otras, la de coor-

2. El texto íntegro de la Declaración se puede consultar en http://www.consilium.europa.eu/es/press/press-releases/2015/02/150212-european-council-statement-fight-against-terrorism/ [Consulta: 22 de septiembre de 2016]

3. Cargo que en la actualidad recae sobre el belga Guilles de Kerchove. En las Orientaciones estratégicas en materia de Justicia y Asuntos de Interior de junio de 2014, el Consejo Europeo reafirmó la importancia que reviste la función

dinar los trabajos del Consejo en la lucha contra el terrorismo, presentar recomendaciones y proponer al Consejo ámbitos de acción prioritarios o mejorar la comunicación en este ámbito entre la UE y terceros países.

No obstante, la reciente crisis de los refugiados, agudizada a partir del verano de 2015, procedentes principalmente de Siria y el resto de los países de Oriente Medio, pero también de África, los Balcanes Occidentales y del sur de Asia, junto con las incertidumbres políticas abiertas en la Unión Europea por la decisión británica de abandonarla, han acentuados las contradicciones existentes entre los países de la Unión Europea y han supuesto nuevas dificultades para organizar dentro de la Unión una respuesta armónica a los desafíos que presenta la garantía de la seguridad y el respeto a los derechos fundamentales.

En esta comunicación pretendemos analizar, por un lado, los instrumentos jurídicos que se han establecido para la defensa de la vida privada de las personas y, por otro —de manera contradictoria— las principales amenazas que, en aras de un reforzamiento de la seguridad pública, han sido establecidos legalmente por los Estados.

Por último, solo queda señalar que la perspectiva desde la que se ha elaborado la presente comunicación es la estrictamente jurídica, por lo que quedan fuera del análisis todas las informaciones más o menos relevantes o veraces sobre esta temática y la discusión sobre los instrumentos tecnológicos que están presentes en la mayoría de las amenazas que en la actualidad ponen en peligro el respeto a la intimidad y a la privacidad de los ciudadanos.

2.1. *Los instrumentos legales para la defensa de la vida privada*

2.1.1. *El origen de la protección de la intimidad y su regulación en los Estados Unidos*

Como es sabido, la defensa de la intimidad o de la vida privada de los ciudadanos tiene un origen norteamericano. La primera vez que aparece, en los Estados Unidos, el término de la «privacy» es en 1890, aunque apoyada en la construcción jurisprudencial

---

del coordinador de la lucha contra el terrorismo. Véase la página web: http://www.consilium.europa.eu/es/policies/strategic-guidelines-jha/ [Consulta: 10 de septiembre de2016].

que la consideraba como «el derecho a ser dejado solo»[4] y se concibe como un freno al poder de intromisión que en aquellos momentos estaba desarrollando la prensa. Se configuraba como un derecho de contenido negativo, individualista y de estructura semejante al derecho de propiedad.

Aunque este derecho no aparece citado expresamente en la Constitución norteamericana, su construcción se sustenta sobre la III, IV y V Enmiendas[5].

4. El origen del derecho a la vida privada se suele situar en el ensayo titulado «The Right to Privacy» escrito por Louis Brandeis, abogado y magistrado del Tribunal Supremo de los Estados Unidos de América y Samuel Warren, en 1890. Concretamente fue publicado en la *Harvard Law Review,* vol. IV No. 5(1890), págs. 194-220.Hay traducción española en Warren, S y Brandeis, L. *El derecho a la intimidad*, ed. a cargo de Pendás, B. y Baselga, P. Madrid, Civitas, 1995, pág. 22 y ss. El texto original puede consultarse en: http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html [Consulta: 15 de septiembre de 2016].

Algunos años antes, Thomas L. Cooley utilizó la expresión «the right to let alone» en su *Treatise on the law of torts* (Véase COOLEY, Th. M. (1879). *A Treatise on the Law of Torts or the Wrongs Which A rise Independently of Contract*, Chicago, Callaghan), expresión que fue utilizada por el Tribunal Supremo norteamericano en el caso *Boyd v. United States* en 1886. Un análisis pormenorizado de la gestación de este derecho, puede consultarse en Saldaña, M.N. (2012)««The Right to Privacy» La génesis de la protección de la privacidad en el sistema constitucional norteamericano: el centenario legado de Warren y Brandeis» *Revista de Derecho Político.* UNED, núm. 85, págs. 195-240. El texto de este estudio está disponible en la siguiente dirección electrónica: http://rabida.uhu.es/dspace/bitstream/handle/10272/7015/The_right_to_privacy.pdf?sequence=2 [Consulta: 10 de septiembre de 2016].

5. El texto de las Enmiendas es el siguiente:

Enmienda III

En tiempo de paz a ningún militar se le alojará en casa alguna sin el consentimiento del propietario; ni en tiempo de guerra, como no sea en la forma que prescriba la ley.

Enmienda IV

El derecho de los habitantes de que sus personas, domicilios, papeles y efectos se hallen a salvo de pesquisas y aprehensiones arbitrarias, será inviolable, y no se expedirán al efecto mandamientos que no se apoyen en un motivo verosímil, estén corroborados mediante juramento o protesta y describan con particularidad el lugar que deba ser registrado y las personas o cosas que han de ser detenidas o embargadas.

Enmienda V

Nadie estará obligado a responder de un delito castigado con la pena capital o con otra infamante si un gran jurado no lo denuncia o acusa, a excepción de los casos que se presenten en las fuerzas de mar o tierra o en la milicia nacional cuando se encuentre en servicio efectivo en tiempo de guerra o peligro público; tampoco

El contenido de la «privacy» ha sido ampliado jurisprudencialmente desde entonces y bajo su tutela se pueden señalar ámbitos protegidos: a) la intrusión en la intimidad o la soledad del ciudadano, o en sus asuntos privados, b) la divulgación pública de hechos privados embarazosos del ciudadano c) la publicidad engañosa que perjudica al ciudadano d) la apropiación del nombre o de la imagen del ciudadano, especialmente cuando supone beneficios económicos[6].

También protege la inviolabilidad del domicilio, y en general de la esfera personal, a través de la protección de la propiedad privada. Así como la facultad de guardar silencio sobre opiniones, actividades, afiliaciones políticas, o incluso el derecho de las asociaciones de no comunicar el listado de sus miembros. Últimamente se ha englobado dentro de este derecho la protección de la persona frente a la informática.

2.1.2. *La protección de la vida privada en Europa*

Por lo que se refiere a la regulación europea, ya el Consejo de Europa venía trabajando en estas materias desde 1967, cuando se creó una primera Comisión Consultiva. De sus trabajos surgió en 1968 la Recomendación 509 de la Asamblea del Consejo sobre «Los derechos humanos y los modernos logros científicos y técnicos»[7]. En este documento la Asamblea recomendaba que el Comité de Ministros dé instrucciones al Comité de Expertos en

---

se pondrá a persona alguna dos veces en peligro de perder la vida o algún miembro con motivo del mismo delito; ni se le compelerá a declarar contra sí misma en ningún juicio criminal; ni se le privará de la vida, la libertad o la propiedad sin el debido proceso legal; ni se ocupará la propiedad privada para uso público sin una justa indemnización.

Cfr. http://www.archives.gov/espanol/constitucion.html [Consulta: 15 de septiembre de 2016].

6. Cfr. al respecto Beard, A.M. (1978) The right to privacy vs. The first amendment: is a private person protected against the publicizing of his private facts?, se puede consultar el texto completo, en línea, en la siguiente dirección: http://www.alicemariebeard.com/law/privacy.htm [Consulta: 15 de septiembre de 2016].

7. Recommendation 509 (1968) Human rights and modern scientific and technological developments. Véase http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=14546&lang=en [Consulta: 18 de septiembre de 2016]

Derechos Humanos para «Para estudiar e informar de si, teniendo en cuenta el artículo 8 de la Convención de Derechos Humanos, la legislación nacional de los Estados miembro protege adecuadamente el derecho a la privacidad frente a violaciones que pueden ser cometidas por el uso de modernos métodos de la ciencia y de la técnica» y si la respuesta era negativa, le encargaba «hacer recomendaciones para mejor protección del derecho a la vida privada»[8].

También dentro del Consejo de Europa, entre 1973 y 1974, se aprueban dos Resoluciones sobre protección de la vida privada de las personas frente a los bancos de datos[9]. En ellas se recogen los principios de exactitud de los datos, finalidad de los registros, carácter público de los bancos de datos, que las informaciones sensibles no deben ser recogidas, conocimiento de los datos recopilados, etc.

En 1976 un nuevo Comité de Expertos se encarga de los trabajos preparatorios para la elaboración de un Convenio sobre estas materias. El Convenio 108, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal[10], sería el fruto de esos trabajos y entró en vigor, finalmente, el 1 de octubre de 1985. Este Convenio contiene siete capítulos con un total de 27 artículos. Entre sus finalidades destacaría el objeto de conformar «un núcleo irreductible», un mínimo común denominador en la protección de los derechos

8. Las violaciones podría venir, según el texto de la Recomendación por «phone-tapping, eavesdropping, surreptitious observation, the illegitimate use of official statistical and similar surveys to obtain private information, and subliminal advertising and propaganda» (párrafo 3).

9. Se trata de la Resolution (73) 22 «On the protection of the privacy of individuals vis-a-vis electronic data banks in the private sector» y de la Resolution (74) 29 «On the protection of the privacy of individuals vis-a-vis electronic data banks in the public sector». Cfr. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680502830, y https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804d1c51, respectivamente [Consulta: 22 de septiembre de 2016]

10. España ratificó el convenio el 27 de enero de 1984, siendo el cuarto país, y el quinto, condición para su entrada en vigor, fue Alemania, el 19 de junio de 1985. El texto oficial, se puede consultar en la página web del BOE, en línea, https://www.boe.es/buscar/doc.php?id=BOE-A-1985-23447 [Consulta: 10 de septiembre de 2016].

de los individuos, que pueda posibilitar la libre circulación de la información entre los países firmantes del convenio.

Finalmente, por lo que a la labor del Consejo de Europa se refiere, hay que mencionar el Protocolo Adicional al Convenio para la protección de las personas con respecto al tratamiento automatizado de los datos personales, relativo a las autoridades de control y a los flujos transfronterizos de datos personales[11]. Este Protocolo fue aprobado el 23 de mayo de 2001 por el Comité de Ministros del Consejo de Europa y abierto a la firma de los Estados signatarios del Convenio 108, el 8 de noviembre de 2001[12]. Los dos aspectos en los que centra su atención este Protocolo es la obligación, por parte de los Estados firmantes, de dotarse de Autoridades de control que velen por la correcta aplicación de los principios establecidos por el Convenio en orden a la protección de datos personales. El segundo aspecto que trata este protocolo es la regulación de los flujos transfronterizos de datos personales[13].

Y dentro de la Unión Europea, ya con anterioridad a la entrada en vigor de la «Carta de los Derechos fundamentales de la Unión Europea»[14], se adoptaron algunos Acuerdos celebrados al amparo del Título VI del Tratado de la Unión Europea sobre coo-

11. El Texto de este Protocolo adicional se puede consultar en http://www.coe.int/t/dghl/standardsetting/dataprotection/Global_standard/protocole%20additionnel%20ES.pdf [Consulta: 22 de septiembre de 2016]

12. La entrada en vigor de este Protocolo se produjo el 1 de julio de 2004 al obtener la ratificación de cinco países. A la fecha de la redacción de esta comunicación, son 36 países los que han ratificado este Protocolo Adicional. Entre los que no lo han ratificado se encuentran, entre otros, Italia, el Reino Unido, Rusia, Bélgica, Eslovenia, Islandia, Malta… España lo firmó el 24 de septiembre de 2009 y entró en vigor, tras su ratificación el 3 de junio de 2010, el 1 de octubre de 2010.

13. Un temprano análisis de este Protocolo Adicional lo podemos encontrar en Pavón Pérez, J.A. (2002) «La Protección de Datos Personales en el Consejo de Europa: el Protocolo Adicional al Convenio 108, relativo a las Autoridades de control y a los flujos transfronterizos de datos personales». *Anuario de la Facultad de Derecho.* Universidad de Extremadura, núms. 19-20, págs. 235-252. Se puede obtener en línea en https://dialnet.unirioja.es/descarga/articulo/831270.pdf [Consulta 22 de septiembre de 2016].

14. Acuerdo Internacional sobre «Carta de los Derechos Fundamentales de la Unión Europea», publicado en España el 30 de marzo de 2010. Véase su texto oficial en http://www.boe.es/buscar/doc.php?id=DOUE-Z-2010-70003 [Consulta: 10 de septiembre de 2016].

peración en asuntos de justicia e interior, entre los que destacan especialmente el Convenio de Schengen (1990)[15] y la creación de Europol (1995)[16].

Por lo demás, el artículo 7 de la Carta de Derechos Fundamentales señala en su artículo 7 que: «Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones» y el artículo 8, que «Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan» y en su párrafo 2º, que «Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación». Por últimos, dispone en su párrafo 3º que «el respeto de estas normas estará sujeto al control de una autoridad independiente. Por lo que se refiere al desarrollo normativo de estos principios, debemos destacar principalmente las siguientes:

—La Directiva 95/46/CE, de 24 de julio de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de dichos datos. Sus objetivos eran:
- Tutelar la intimidad y el resto de los derechos fundamentales.
- Garantizar el flujo de datos entre los Estados miembros.

15. Se trata del Instrumento de ratificación del Acuerdo de Adhesión del Reino de España al Convenio de aplicación del Acuerdo de Schengen de 14 de junio de 1985 entre los Gobiernos de los Estados de la Unión Económica Benelux, de la República Federal de Alemania y de la República Francesa, relativo a la supresión gradual de los controles en las fronteras comunes, firmado en Schengen el 19 de junio de 1990, al cual se adhirió la República Italiana por el Acuerdo firmado en París el 27 de noviembre de 1990, hecho el 25 de junio de 1991. Su texto, oficial, en el Boletín Oficial del Estado: https://www.boe.es/buscar/doc.php?id=BOE-A-1994-7586 [Consulta: 10 de septiembre de 2016].

16. La creación de una Oficina Europea de Policía (Europol) se acordó en el Tratado de la Unión Europea, de 7 de febrero de 1992, y se reguló en el Convenio, basado en el artículo K.3 del Tratado de la Unión Europea, por el que se crea una Oficina Europea de Policía (Convenio Europol). El texto del Convenio de 1995, que entró en vigor el 1 de octubre de 1998, se puede consultar en http://www.boe.es/diario_boe/txt.php?id=BOE-A-1998-22461 [Consulta: 10 de septiembre de 2016].

- El núcleo central de la protección otorgada se basa en el consentimiento, en la garantía de la autodeterminación individual, sin perjuicio de que, en determinados supuestos legales, puedan ser tratados datos sin consentimiento.

—La Directiva 97/66/CE, de 15 de diciembre de 1997, que se refiere al tratamiento de datos personales y protección de la intimidad en el sector de las telecomunicaciones. Trata de responder a la evolución de las tecnologías como por ejemplo, la aparición de la televisión interactiva o el vídeo bajo demanda y a la protección que se deben prestar a la intimidad en esos ámbitos. Es de destacar que trate de establecer un cierto anonimato en ciertos ámbitos como es el de la facturación o identificación de líneas

—La Directiva 2002/585/CE, de 12 de julio de 2002, que sustituye a la anterior, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas. Intenta abarcar la regulación de Internet y de los nuevos servicios asociados a la telefonía digital. Mantiene el principio del consentimiento e intenta establecer normas comunes a las nuevas modalidades comunicativas (correo electrónico, sms, etc.)

Y, por último, el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de fecha 27 de abril de 2016, relativo a «la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)»[17]. Sin embargo, hay que señalar que la entrada en vigor de este Reglamento se dilata hasta el 25 de mayo de 2018, por lo que hasta esa fecha tanto la Directiva 95/46 como las normas nacionales que la contemplan, siguen siendo plenamente válidas y aplicables[18].

17. Su texto oficial se puede consultar en https://www.boe.es/doue/2016/119/L00001-00088.pdf [Consulta: 16 de septiembre de 2016].

18. Por lo que se refiere a la legislación española relevante a estos efectos, la podemos encontrar contenida en la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, modificada por última vez por la Ley 2/2011, de 4 de marzo, y que en la actualidad está pendiente de una sustancial reforma en la línea del Reglamento (UE) 2016/679 ya señalado.

Por lo que se refiere a la interpretación que, de estos derechos, ha hecho la jurisprudencia europea, especialmente el Tribunal Europeo de Derechos Humanos, hay que referirse en primer lugar, a la Sentencia de 3 de abril de 2007, «Caso Copland»[19], en la que el Tribunal analizó si el seguimiento de las llamadas telefónicas, del uso del correo electrónico y de la navegación por internet realizada por los responsables de un «College» universitario de Gales (Reino Unido) sobre una trabajadora del mismo, suponía una violación de los derechos reconocidos en el Convenio Europeo de Derechos Humanos. En sus alegaciones, el Gobierno británico acepto que, en este caso, «si bien se efectuó cierto seguimiento de las llamadas, el correo electrónico y la navegación por Internet de la demandante con anterioridad a noviembre de 1999, no se llegó a interceptar las llamadas telefónicas ni a analizar el contenido de las páginas web visitadas por ella». Para el Gobierno inglés, «el seguimiento no consistió pues en nada más que un análisis de la información generada automáticamente para determinar si las instalaciones del College se habían usado con fines personales»[20]. Se trataba no de interceptar el contenido de las llamadas, o de los correos electrónico, sino de simplemente conocer a qué números se llamaba, a quién se enviaba los correos

---

Asimismo debemos tener en cuenta la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y del comercio electrónico, la Ley 59/2003, de 19 de diciembre, de firma electrónica y sobre todo, la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, modificada por la Sentencia del Tribunal Constitucional 20/2016, de 4 de febrero, que declaró inconstitucional parte de su artículo 34 y que también se ve afectada por la Sentencia del Tribunal de Justicia de la Unión Europea de 8 de abril de 2014, Asunto *Digital Rights Ireland Ltd contra Minister for Communications,* que declaró invalida, la Directiva 2006/24/CE, de 15 de marzo de 2006 sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE. Cfr. su texto en la dirección: http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30d64775543ef5314928987fb-1c534417b4f.e34KaxiLc3qMb40Rch0SaxuOb3f0?text=&docid=150642&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=260580 [Consulta: 12 de septiembre de 2016].

19. Sentencia del Tribunal Europeo de Derechos Humanos (STEDH) 23/2007, de 3 de abril. La jurisprudencia del Tribunal, usualmente en francés o inglés, puede consultarse en la página web http://www.echr.coe.int/.

20. Parágrafo 32

electrónico y el nombre o la dirección de las páginas web que se consultaba. Es más, según sus alegaciones, «En el supuesto de que el análisis de la relación de llamadas telefónicas, el correo electrónico e Internet se considerase una injerencia en el respeto de la vida privada o la correspondencia, el Gobierno señala que la injerencia estaba justificada»[21].

A pesar de esa argumentación, el Tribunal consideró que tales injerencias no estaban justificadas, ya que «según la reiterada jurisprudencia del Tribunal, las llamadas telefónicas que proceden de locales profesionales pueden incluirse en los conceptos de «vida privada» y de «correspondencia» a efectos del artículo 8.1 (Sentencias Halford [TEDH 1997, 37], previamente citada, ap. 44 y Amann contra Suiza [TEDH 2000, 87] [GC], núm. 27798/1995, ap. 43, TEDH 2000-II). Es lógico pues que los correos electrónicos enviados desde el lugar de trabajo estén protegidos en virtud del artículo 8, como debe estarlo la información derivada del seguimiento del uso personal de Internet»[22].

Asimismo, el Tribunal recordó que «la utilización de información relativa a la fecha y duración de las conversaciones telefónicas y en particular los números marcados, puede plantear un problema en relación con el artículo 8 (RCL 1999, 1190 y 1572), ya que dicha información es «parte de las comunicaciones telefónicas» (Sentencia Malone contra el Reino Unido de 2 agosto 1984 [TEDH 1984, 1], serie A núm. 82, ap. 84)» y el hecho de que el College obtuviese esos datos legítimamente, «en forma de facturas telefónicas», no es impedimento para «constatar una injerencia en los derechos garantizados por el artículo 8 (ibidem)» Y, lo que resulta más relevante, «el almacenamiento de datos personales

21. Parágrafo 33.

22. Parágrafo 41. El artículo 8 del Convenio Europeo de Derechos Humanos (4 de noviembre de 1950) señala que: *«Artículo 8: Derecho al respeto a la vida privada y familiar.*

1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.

2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás».

relativos a la vida privada de una persona se halla también en el ámbito de aplicación del artículo 8.1 (Sentencia Amann [TEDH 2000, 87], previamente citada, ap. 65)»[23]. Además el Tribunal considera que tal injerencia no estaba justificada ni por el derecho interno, ni por las normas internacionales[24].

Por todo ello, «el Tribunal considera que la recogida y almacenamiento de información personal relativa a las llamadas telefónicas, correo electrónico y navegación por Internet de la demandante, sin su conocimiento, constituye una injerencia en su derecho al respeto de su vida privada y su correspondencia, en el sentido del artículo 8 del Convenio»[25], concediéndole a la recurrente una indemnización por daño moral y obligando al Gobierno británico a correr también con los gastos del proceso[26].

Por lo que se refiere al Tribunal de Justicia de la Unión Europea, debemos remarcar su sentencia de 8 de abril de 2014, Asunto *Digital Rights Ireland Ltd contra Minister for Communications, Marine and Natural Resources y otros y Kärntner Landesregierung y otros, por petición de decisión prejudicial: High Court - Irlanda, Verfassungsgerichtshof - Austria*[27], que declaró invalida, en un decisión cuyas consecuencias legales todavía no se han concretado con

23. Parágrafo 43.

24. Parágrafos 45-48.

25. Parágrafo 44.

26. No obstante, la jurisprudencia mayoritaria del Tribunal Supremo considera que la obtención del número telefónico, por sí sólo no supone una injerencia en el ámbito protegido de la intimidad personal. Así, por ejemplo, la STS 921/2009 de 20 de octubre, considera, haciendo suyos unos votos particulares emitidos en la STS de 19 de febrero de 2007, que ««Los números identificativos con los que operan los terminales no pueden constituir, por sí mismos, materia amparada por el secreto de las comunicaciones, pues afirmar lo contrario supondría, a nuestro juicio, confundir los medios que posibilitan la comunicación con la comunicación misma», y ello porque «Sostener semejante criterio no supone contradicción alguna, en nuestra opinión, con la doctrina del Tribunal Europeo de Derechos Humanos, significativamente la contenida en la Sentencia del denominado «caso Malone», ni con la del Tribunal Constitucional ni, mucho menos aún, con la de esta misma Sala, pues esa doctrina se refiere a la extensión del ámbito protegido de la «comunicación» no tanto a los números telefónicos sino al hecho de que, a través de la averiguación de esos números, se conozcan extremos como el momento, la duración y, lo que es aún más importante, la identidad de las personas que establecen el contacto. Y eso sí que puede sostenerse que forma parte, auténticamente, de la "comunicación"».

27. Ya citada, véase nota 18.

claridad, la Directiva 2006/24/CE, de 15 de marzo de 2006, sobre la «conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE»[28].

En esta Sentencia, el Tribunal consideraba que al imponer la conservación de estos datos y al permitir el acceso a las autoridades nacionales competentes, la Directiva establecía «una excepción al régimen de protección del derecho al respeto de la vida privada… así como [a] la obligación de borrar o hacer anónimos estos datos cuando ya no son necesarios para la transmisión de una comunicación, salvo si son necesarios para la facturación y únicamente mientras exista esa necesidad»[29]. Y, además, «el acceso de las autoridades nacionales competentes a los datos constituye una injerencia adicional en ese derecho fundamental»[30]. Injerencia que resulta «de gran magnitud y debe considerarse especialmente grave», sobre todo si «la conservación de los datos y su posterior utilización se efectúen sin que el abonado o usuario registrado hayan sido informados de ello», lo que puede generar en las personas afectadas «el sentimiento de que su vida privada es objeto de una vigilancia constante»[31].

A ello se suma que la Directiva cuestionada «no establece reglas claras y precisas que regulen el alcance de la injerencia en los derechos fundamentales reconocidos en los artículos 7 y 8 de la Carta»[32]. Tampoco contiene garantías suficientes que permitan «asegurar una protección eficaz de los datos conservados contra los riegos de abuso y contra cualquier acceso y utilización ilícitos respecto de tales datos»[33], además de que tampoco la Directiva regula de manera clara y estricta la protección y la seguridad de la conservación de los datos en cuestión o, en fin, de que tales datos se conserven en el territorio de la Unión.

28. El texto de la Directiva declarada inválida puede consultarse en http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:ES:PDF [Consulta: 12 de septiembre de 2016].
29. Ibídem, parágrafo 32.
30. Ibídem, parágrafo 35.
31. Ibídem, parágrafo 37.
32. Ibídem, parágrafo 62.
33. Ibídem, parágrafo 66.

Por todo ello, el Tribunal considera que «al adoptar la Directiva 2006/24, el legislador de la Unión sobrepasó los límites que exige el respeto del principio de proporcionalidad en relación con los artículos 7,8 y 52, apartado 1, de la Carta»[34], por lo que procede declarar que «la Directiva 2006/24 es inválida»[35].

Y por otro lado, también debemos referirnos a la Sentencia del Tribunal de Justicia de la Unión Europea (gran Sala) de 13 de mayo de 2014 Asunto *Google Spain, S.L., Google Inc. contra Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, por petición prejudicial presentada por la Audiencia Nacional española[36].

Los aspectos más destacables de esta Sentencia, que contradice de manera muy importante el Dictamen del Abogado General[37], más cercano a las tesis defendidas por el Google, son los siguientes, siguiendo el resumen aportado por la propia AEPD:

—«La actividad de los motores de búsqueda como Google constituye un tratamiento de datos de carácter personal, del que es responsable el propio motor, dado que éste determina los fines y los medios de esta actividad.

—Ese tratamiento está sometido a las normas de protección de datos de la Unión Europea, dado que Google ha creado en un Estado miembro un establecimiento para la promoción y venta de espacios publicitarios y cuya actividad se dirige a los habitantes de ese Estado.

—Las personas tienen derecho a solicitar del motor de búsqueda, con las condiciones establecidas en la Directiva de protección de datos, la eliminación de referencias que les afectan, aunque esta información no haya sido eliminada por el editor ni dicho editor haya solicitado su desindexa-

34. Ibídem, parágrafo 69.

35. Ibídem, parágrafo 71.

36. La Sentencia del Tribunal de Justicia de la Unión Europea se puede consultar en http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=269153 [Consulta: 12 de septiembre de 2016].

37. Las Conclusiones del Abogado General Sr. Niilo Jääskinen, presentadas el 25 de junio de 2013, se pueden consultar en: http://curia.europa.eu/juris/document/document.jsf?docid=138782&doclang=ES [Consulta: 12 de septiembre de 2016].

ción. En caso de no atenderse su solicitud, las personas tienen derecho a recabar la tutela de las Agencias de Protección de datos nacionales y de los Tribunales.

—El derecho a la protección de datos de las personas prevalece, con carácter general, sobre el «mero interés económico del gestor del motor de búsqueda» salvo que el interesado tenga relevancia pública y el acceso a la información esté justificado por el interés público»[38].

De tal modo que se determina la prevalencia del derecho de protección de datos frente al derecho de los ciudadanos a acceder a la información disponible y lícita, salvo en casos de existencia de un interés público, que corresponde a los buscadores la responsabilidad de ponderar entre estos derechos y que, en definitiva, el «derecho al olvido» no es un mecanismo de «borrado automático». Y solo procederá cuando se justifique la necesidad de dicho borrado conforme a los criterios de la normativa sobre protección de datos.

Tal regulación del derecho al olvido se ha contemplado en el Reglamento (UE) 2016/679, que entrará en vigor, como ya hemos señalado, el 25 de mayo de 2018.

Finalmente, también debemos mencionar la Sentencia del Tribunal de Justicia de la Unión Europea de 6 de octubre de 2015[39] que ha anulado la Decisión de la Comisión 2000/520/CE en la que se otorgaba a las entidades de EEUU adheridas a ese acuerdo un nivel adecuado de protección de datos y las autorizaba a transferencias internacionales de datos y en la que considera que «una autoridad de control de un Estado miembro puede examinar la solicitud de una persona relativa a la protección de sus derechos y libertades frente al tratamiento de los datos personales que la

38. Cfr. este análisis en la página web de la propia Agencia Española de Protección de Datos: https://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2014/notas_prensa/common/may_14/NP_STJUE_derecho_olvido.pdf [Consulta: 12 de septiembre de 2016].

39. Se trata de la Sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala) de 6 de octubre de 2015, en asunto *Maximillian Schrems vs. Data Protection Commissioner* (Cuestión Prejudicial planteada por la High Court de Irlanda). El texto completo de la Sentencia se puede consultar en http://curia.europa.eu/juris/document/document.jsf?docid=169195&doclang=ES [Consulta: 22 de septiembre de 2016].

conciernen que se hayan transferido desde un Estado miembro a ese tercer país, cuando esa persona alega que el Derecho y las prácticas en vigor en éste no garantizan un nivel de protección adecuado». Las consecuencias de esta anulación de la normativa europea sobre lo que se dio en llamar «puerto seguro» todavía no se han concretado dentro de la Unión Europea, estando actualmente las transferencias de datos personales a empresas de los Estados Unidos en una situación de indefinición jurídica.

El 27 de septiembre de 2016 se conoció también la decisión del Comisionado de Hamburgo para la Protección de Datos y la Libertad de Información, de prohibir la transferencia de datos de los usuarios de la aplicación para teléfonos móviles, *WhatsApp,* a la red social *Facebook* —de los mismos propietarios—, sin el previo permiso de los usuarios y sin que éstos puedan decidir si desean esa transferencia de datos o no[40].

2.2. *Las amenazas a la protección de la vida privada*

2.2.1. *El marco legal que regula el control de la vida privada de los ciudadanos*

Sin embargo, las tendencia en aras de una paulatina mayor protección de la vida privada en los distintos países, sufrieron una importante inflexión tras los atentados del 11 de septiembre de 2001, contra las Torres Gemelas y el Pentágono.

En los Estados Unidos, la conmoción que produjeron esos atentados llevó a la aprobación de la conocida USA Patriot Act, escasamente un mes después de los atentados, el 21 de octubre de 2001[41], aunque su validez se limitaba, en principio, hasta el 31 de diciembre de 2005. Este plazo de caducidad fue ampliado

40. Puede consultarse la información en la página web del Comisionado: https://www.datenschutz-hamburg.de/news/detail/article/anordnung-gegen-massendatenabgleich-zwischen-whatsapp-und-facebook.html?tx_ttnews%5BbackPid%5D=170&cHash=4f6f211b21214425da19b5597eab4502 [Consulta: 3 de octubre de 2016].

41. El USA Patrio Act fue aprobado por una abrumadora mayoría de los congresistas norteamericanos. Concretamente en el Senado, sólo hubo un voto en contra y un senador que no votó, mientras que en la Cámara de Representantes la mayoría fue de 357 votos a favor, 66 en contra y 9 no votaron. El texto de esta norma puede consultarse en https://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf [Consulta: 15 de septiembre de 2016].

finalmente, introduciendo ligeras variaciones en su regulación, hasta que el 1 de Junio de 2015 fue sustituida por la actual USA Freedon Act, firmada por el Presidente Obama.

Entre las medidas más polémicas que contemplaba la Patriot Act se encontraban las de ampliar las facilidades para la interceptación y rastreo de las comunicaciones electrónicas, pudiendo las distintas agencias gubernamentales relacionadas con la seguridad a los datos de las comunicaciones, que debían ser almacenados durante 180 días, y retrasando las notificaciones a los afectados por las investigaciones. Además, cuando se estuvieren investigando intrusiones informáticas no era necesario contar con autorización judicial para interceptar las comunicaciones del presunto «hacker».

También permitía la existencia de mandatos para entrada y registros secretos, ya fuera física o virtualmente, sin dejar rastro evidente, aunque con obligación de informar al Tribunal que lo autorizó.

En fin, entre otros aspectos, también permitía emitir órdenes judiciales que omitieran describir los instrumentos, instalaciones o lugares vigilados, cuando se pensara que tal información pudiere frustrar la investigación en curso, entre otras facilidades.

Aunque parecía que la nueva administración del Presidente Barak Obama quería derogar el Patriot Act o, al menos, sus artículos más polémicos, lo cierto es que en febrero de 2010 el Congreso norteamericano amplío su cobertura un año más y que el 26 de mayo de 2011 firmó una extensión por cuatro años de tres artículos de esta ley: la que permitía las escuchas telefónicas itinerantes, la búsqueda de registros de negocios y la vigilancia de los individuos sospechosos de actividades terroristas no vinculados a grupos («lobos solitarios»).

Finalmente, el 2 de junio de 2015, esta normativa fue sustituida por la USA Freedom Act, actualmente en vigor, que limita algunos de los poderes que la anterior regulación otorgaba a la administración norteamericana, en especial a la Agencia de Seguridad Nacional (NSA).

Concretamente, se estableció que los datos de las llamadas telefónicas no fueran recolectados por la NSA, sino por las propias compañías telefónicas, aunque a esos datos podría acceder la NSA a través de una orden judicial con características especiales.

Así, la orden tendrá que ser firmada por un «Tribunal de Supervisión de Inteligencia Extranjera», formado por once jueces,

que desde 2001 son nombrados por el Presidente del Tribunal Supremo, que deberá decidir si la petición se ajusta a Derecho. La labor de este Tribunal ha sido fuertemente criticada[42], especialmente cuando se conoció que el 25 de abril de 2013 había emitido una orden, firmada por el juez Roger Vinson, que obligaba a la operadora de telefonía Verizon a que facilitara información de manera continua, y a diario, a la NSA, de todas las llamadas de teléfono efectuadas por sus clientes, y de sus metadatos, tanto dentro de los EEUU como a otros países, incluyendo llamadas telefónicas locales[43].

Además, la nueva regulación contemplada en la USA Freedom Act no afecta a la capacidad de los Estados Unidos para interceptar comunicaciones fuera de sus fronteras, que no necesita de ninguna clase de autorización adicional.

Todo ello ha llevado a que la labor en todos estos años de la NSA haya sido fuertemente criticada, especialmente a partir de la divulgación de los datos recolectados por Edward Snowden[44], siendo muy cuestionada la eficacia de la labor de esta Agencia[45].

42. Sin embargo la actuación de este Tribunal también está sujeta a polémica, ya que de las 24.082 solicitudes de autorización solicitadas por la NSA (entre los años 2001 y 2015), sólo 720 fueron modificadas y únicamente 12 fueron rechazadas. Los datos están obtenidos del Electronic Privacy Information Center (Cfr. https://epic.org/privacy/surveillance/fisa/stats/default.html [Consulta: 20 de septiembre de 2016]). La página web de la Foreign Intelligence Surveillance Court es: http://www.fisc.uscourts.gov/ [Consulta: 12 de septiembre de 2016]

43. Véase la información emitida por el diario The Guardian en su página web: https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order [Consulta: 15 de septiembre de 2016].

44. Se trataría de la filtración de una serie de documentos entre 2013 y 2015, extraídos por E. Snowden, que en conjunto superarían los 1,7 millones, además de miles de documentos secretos de las agencias de inteligencia de Estados Unidos, también contendrían miles de archivos secretos de países como Australia, Canadá o Reino Unido, gracias a su acceso a la exclusiva red Five Eyes, y los que tuvo acceso por su trabajo para Booz Allen Hamilton, uno de los mayores contratistas militares y de inteligencia del gobierno de Estados Unidos. Las primeras filtraciones fueron publicadas el cinco y el seis de junio de 2013 por los diarios The Guardian y The Washington Post y en España, por el diario El País Cfr. http://internacional.elpais.com/internacional/2013/06/07/actualidad/1370564066_752776.html [Consulta: 17 de septiembre de 2016].

45. Incluso el Parlamento Europeo se ha manifestado en varias ocasiones en contra del espionaje masivo a ciudadanos europeos realizados por las

En Europa, la desconfianza de las autoridades de la Unión Europea por el uso que los ciudadanos podían estar haciendo de internet llevó a la aprobación de la Directiva 2006/24/CE, que modificaba la anterior Directiva 2002/58/CE, en la que se establecía la obligación de los proveedores de acceso a internet de conservar los datos generados en las trasmisiones electrónicas.

Así, en los que podíamos considerar como la exposición de motivos de esa Directiva, se señalaba que, si bien los artículos 5, 6 y 9 de la anterior Directiva 2002/58/CE establecían como obligaciones de los proveedores que los datos obtenidos en las transmisiones a través de internet deberían borrarse o hacerse anónimos cuándo no se necesitaran para la transmisión, «salvo los datos necesarios para la facturación o los pagos por interconexión»[46], también se permitía que los Estados miembros limitasen esta obligación, siempre que tales restricciones constituyeran «medidas necesarias, apropiadas y proporcionadas en una sociedad democrática para fines específicos de orden público, como proteger la seguridad nacional (es decir, la seguridad del Estado), la defensa, la seguridad pública, o la prevención, investigación, detección y enjuiciamiento de delitos o la utilización no autorizada del sistema de comunicaciones electrónicas»[47]. Como varios Estados, entre ellos España[48], hicieron uso de esa posibilidad,

agencias de seguridad norteamericanas. Así, el 12 de marzo de 2014 el Pleno aprobó con 544 votos a favor, el informe realizado por la Comisión de Libertades Públicas denominado «US NSA surveillance programme, surveillance bodies in various Member States and impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs». Véase: http://www.europarl.europa.eu/news/es/news-room/20140307IPR38203/ee.uu.-debe-poner-fin-al-espionaje-masivo-o-afrontar-las-consecuencias y para el texto completo: http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2014-0230 [Consulta: 22 de septiembre de 2016]

46. Directiva 2006/24/CE, del Parlamento Europeo y del Consejo, de 15 de marzo, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones, que modifica la anterior Directiva 2002/58/CE. Parágrafo 3. Se puede localizar el texto de esta Directiva en la siguiente dirección: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:ES:PDF [Consulta: 210 de noviembre de 2012].

47. Artículo 15, apartado 1, de la Directiva 2002/58/CE.

48. En la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y del Comercio Electrónico.

aunque con una gran diversidad en sus legislaciones, su corrección e igualación venía obligada, que es lo que pretendía la nueva Directiva del año 2006.

Así, aunque «de conformidad con el artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales (CEDH), toda persona tiene derecho al respeto de su vida privada y de su correspondencia» y ello obliga a que no pueda existir injerencia de la autoridad pública en el ejercicio de este derecho, lo cierto es que esta injerencia podrá realizarse cuándo «esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria, entre otras cosas, para la seguridad nacional o la seguridad pública, la prevención de desórdenes o delitos, o la protección de los derechos y las libertades de terceros».

Por ello, el artículo 1 de la Directiva establecía, en su apartado 1, la obligación de los proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones de conservar determinados datos generados o tratados por los mismos, «para garantizar que los datos estén disponibles con fines de investigación, detección y enjuiciamiento de delitos graves, tal como se definen en la legislación nacional de cada Estado miembro», y en su apartado 2, que los citados datos son concretamente «los datos de tráfico y de localización sobre personas físicas y jurídicas y a los datos relacionados necesarios para identificar al abonado o al usuario registrado», pero no «se aplicará al contenido de las comunicaciones electrónicas, lo que incluye la información consultada utilizando una red de comunicaciones electrónicas»[49].

El periodo de conservación de tales datos era en una horquilla que iba desde los seis meses, como mínimo, a los dos años como máximo (Artículo 6).

Esta Directiva, sin embargo, fue anulada, en sus aspectos más polémicos, como ya hemos señalado, por el Tribunal de Justicia

49. Artículo 1 de la Directiva 2006/24/CE. Concretamente, en el artículo 5 se pormenorizan los datos que necesitan ser conservados. Además, en el apartado 2 de este artículo 5 se enfatiza de nuevo que «De conformidad con la presente Directiva, no podrá conservarse ningún dato que revele el contenido de la comunicación».

de la Unión Europea en su Sentencia de 8 de abril de 2014[50]. A ello se suma que la Directiva además de no establecer reglas claras, como ya hemos apuntado[51], tampoco contiene garantías suficientes que permitan «asegurar una protección eficaz de los datos conservados contra los riegos de abuso y contra cualquier acceso y utilización ilícitos respecto de tales datos»[52], además de que la Directiva no regula de manera clara y estricta la protección y la seguridad de los datos en cuestión ni que tales datos se conserven en el territorio de la Unión.

Por todo ello, el Tribunal considera que «al adoptar la Directiva 2006/24, el legislador de la Unión sobrepasó los límites que exige el respeto del principio de proporcionalidad en relación con los artículos 7,8 y 52, apartado 1, de la Carta»[53], por lo que procede declarar que «la Directiva 2006/24 es inválida»[54].

Como hemos señalado más arriba, las consecuencias de esta decisión todavía no se han trasladado a la legislación española, a pesar del tiempo transcurrido desde su publicación. De hecho, la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones[55], todavía vigente, fue aprobada con posterioridad a la fecha de la Sentencia del TJUE, y sobre las obligaciones de conservación de los datos, mantiene, en su artículo 42, la regulación que sobre esta materia contenía la Ley 25/2007, de 18 de octubre[56]. De hecho, la única modificación que ha tenido desde su aprobación, ha sido la obligada por la STC 20/2016, de 4 de febrero, que anuló parte de su artículo 34.

50. Sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala) de 8 de abril de 2014. Asunto «*Digital Rights Ireland Ltd contra Minister for Communications, Marine and Natural Resources y otros y KärntnerLandesregierung y otros», dictada por Petición de Decisión Prejudicial de High Court - Irlanda, Verfassungsgerichtshof – Austria*, ya citada.

51. Ibídem, parágrafo 62.

52. Ibídem, parágrafo 66.

53. Ibídem, parágrafo 69.

54. Ibídem, parágrafo 71.

55. El texto de la Ley se puede consultar en https://www.boe.es/diario_boe/txt.php?id=BOE-A-2014-4950

56. Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, modificada por la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones. Su texto se puede consultar en https://www.boe.es/buscar/act.php?id=BOE-A-2007-18243 [Consulta: 25 de septiembre de 2016]

Así, la Ley 25/2007, concretaba que la duración de la conservación de los datos fuera de doce meses[57]. A ello debemos sumar que el rango de datos que se debe conservar es muy amplio.

En cualquier caso, son muy importantes las dudas planteadas sobre las razones de mantener una regulación en España por aplicación de una Directiva que ha sido anulada por el Tribunal de Justicia de la Unión Europea, al considerarla una injerencia inadmisible sobre el derecho a la privacidad.

Tras los atentados en Francia, como ya señalamos, la preocupación por garantizar la seguridad de los ciudadanos europeos manifestada por los miembros del Consejo Europeo en Bruselas en el 2015, al que ya aludimos más arriba, se ha concretado en la acelerada aprobación de una Directiva para poner en marcha un Registro de Nombre de Pasajeros (PNR) de compañías aéreas, justificada por la necesidad de prevenir delitos graves y, especialmente, de naturaleza terrorista.

La propuesta de la creación de este Registro era una vieja aspiración de la Comisión, desde el año 2011, que fue rechazada, en su sesión de 24 de abril de 2013, por la Comisión de Libertades Civiles, Justicia y Asuntos de Interior del Parlamento Europeo[58]. En aquellos momentos los eurodiputados de los grupos socialista (S&D), liberal (ALDE) de Izquierda Unitaria (GUE) y Verdes (Greens/ALE) mostraron su preocupación por el posible riesgo que el PNR europeo supondría para la protección de datos personales de los pasajeros y la proporcionalidad de la medida, consiguiendo imponer su rechazo en la votación en la que se decidía sobre su puesta en marcha. Hay que tener en cuenta que, según apunta el Dictamen 6/2002, del Grupo de Trabajo sobre protección de datos del Artículo 29, de la Unión Europea, relativo a la transmisión de listas de pasajeros y otros datos de compañías aéreas a los Estados Unidos, el rango de datos que pueden ser incluidos bajo esta denominación PNR pueden incluir datos identificativos (apellidos, nombre, fecha de nacimiento, número de teléfono), número de reserva del PNR, fecha de la reserva, la agencia de viajes cuando corresponda, la información que se

57. Artículo 5 de la Ley 25/2007

58. Cfr. la página web del Parlamento Europeo http://www.europarl.europa.eu/ep-live/es/committees/video?event=20130424-0900-COMMITTEE-LIBE [Consulta: 25 de septiembre de 2016]

muestra en el billete, los datos financieros (número de tarjeta de crédito, fecha de caducidad, dirección del lugar de expedición, etc.), el itinerario, información sobre el transportista que opera el vuelo (número de vuelo, etc.), número de asiento y datos anteriores del PNR. En estos últimos pueden constar no solo los viajes completados en el pasado, sino también información de carácter religioso o étnico (elección de la comida, etc.), afiliación a un determinado grupo, datos relativos al lugar de residencia o los medios para contactar con una persona (dirección de correo electrónico, información sobre un amigo, lugar de trabajo, etc.), datos médicos (cualquier asistencia médica que se haya requerido, oxígeno, problemas relacionados con la vista, el oído o la movilidad, o cualquier otro problema que deba hacerse saber para garantizar un vuelo satisfactorio) y otros datos relacionados, por ejemplo, con los programas de viajeros frecuentes (*Frequent Fliers number*)[59]. El mismo informe también se refiere a que «el PNR puede contener datos que revelen el origen étnico o racial, las convicciones religiosas u otro tipo de información delicada en el sentido descrito en el artículo 8 de la Directiva 95/46/CE, que en principio prohíbe cualquier tipo de tratamiento de esta información a menos que se cuente con autorizaciones consentimiento explícito para su tratamiento con fines concretos, datos de carácter claramente público, etc.)»[60].

Sin embargo, los últimos atentados sufridos en varios Estados europeos, especialmente Francia, impulsaron de modo decidido la adopción de este Registro, que finalmente ha sido creado por la Directiva (UE) 2016/681, de 27 de abril de 2016[61]. Esta Directiva

59. Dictamen 6/2002, del Grupo de Trabajo sobre protección de datos del Artículo 29, de la Unión Europea, relativo a la transmisión de listas de pasajeros y otros datos de compañías aéreas a los Estados Unidos, aprobado del 24 de octubre de 2002 El texto íntegro del Dictamen se puede encontrar, en línea, en http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp66_es.pdf [Consulta: 20 de septiembre de 2016].

60. En el mismo sentido se pronunció el Gabinete Jurídico de la Agencia Española de Protección de Datos, en su Informe 0076/2009. Se puede consultar íntegro en https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/medidas_seguridad/common/pdfs/2009-0076_Nivel-de-seguridad-del-P.N.R.pdf [Consulta: 20 de septiembre de 2016].

61. Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativa a la utilización de datos del registro de nombres de los

fue aprobada por el Parlamento Europeo por 461 votos a favor, 179 en contra y 9 abstenciones, lo que ofrece una idea del amplio consenso que ha concitado esta nueva disposición y que contrasta con las dudas planteadas por los parlamentarios en 2013. La disposición prevé un plazo de dos años para que los distintos países incorporen esta normativa a su ordenamiento interno. En la actualidad, y mientras transcurre este plazo de dos años, se mantiene la obligación de las compañías aéreas de comunicar a las autoridades competentes de la Unión Europea los datos de información anticipada sobre pasajeros (API), que incluyen el número y tipo de documento de viaje que se ha utilizado, la nacionalidad, el nombre y apellidos completos, la fecha de nacimiento, el puesto fronterizo de entrada, el código del transporte, los horarios de salida llegada, el número de pasajeros y el lugar de embarque inicial.

Con la aprobación de esta nueva Directiva, los datos recopilados por las compañías aéreas y que deben ser comunicados a las autoridades, van a ser más completos –en el sentido apuntado más arriba- y además deben ser entregadas entre 24 y 48 horas antes de la hora programada para el vuelo e inmediatamente después del cierre del vuelo, nada más terminar el embarque, cuando todos los pasajeros están a bordo, el avión se dispone a despegar y es imposible subir o bajar de avión (artículo 8.3 de la Directiva)[62]. Todos los países deberán, asimismo, crear una Unidad de Información de Pasajeros (art. 4 de la Directiva), que recopilará todos estos datos y que deberá conservarlo durante cinco años, aunque deben despersonalizarse pasados seis meses, de forma que el interesado de ser identificado inmediatamente (artículo 12 de la Directiva), siendo la encargada de compartir los datos con los otros países y con las autoridades competentes en caso de que sea necesario para prevenir o investigar acciones terroristas o los delitos graves recogidos en el Anexo II de la Directiva (pertenencia a organización delictiva, trata de seres humanos, explotación sexual de niños y pornografía infantil, tráfico ilícito de estupefaciente y sustancias psicotrópicas, tráfico

---

pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave. El texto se puede consultar en: http://www.boe.es/doue/2016/119/L00132-00149.pdf [Consulta: 20 de septiembre de 2016].

62. La relación de datos que deben suministrar las compañías aéreas están indicados en el Anexo I de la Directiva.

ilícito de armas, corrupción, blanqueo del producto del delito y falsificación de monedas, delitos informáticos/ciberdelincuencia, fraude, espionaje industrial, homicidio, violación y secuestro, detención ilegal, toma de rehenes, tráfico ilícito de bienes culturales, incluidas las antigüedades y las obras de arte, etc.).

En relación a las cautelas que suscita esta nueva regulación, destaca el Consejo de Europa que ya ha mostrado su preocupación por esta Directiva, y apunta algunos aspectos que deberían ser contemplados para considerar a este Registro como respetuoso en relación a la protección de datos[63].

La Declaración de 2015 también indicaba la necesaria e inmediata adopción de medidas adicionales para controlar el mercado negro de armas de fuego dentro de la UE, así como establecer controles adicionales para la posesión legal de armas de fuego. También se proponían reforzar la labor que realizar la Agencia de Control del Fronteras de la UE (Frontex) e iniciar los trabajos con vista a la adopción de la Directiva sobre seguridad de las redes y de la información, dada la importancia de la ciberseguridad, junto con el fomento de la cooperación entre las policías de los distintos países y otras medidas en la misma dirección.

Llama la atención que en esa Declaración también se pida a los Estados que «se adopten medidas adecuadas, con arreglo a las constituciones nacionales, para detectar y eliminar los contenidos de Internet que fomenten el terrorismo o el extremismo, en particular mediante una mayor cooperación entre los poderes públicos y el sector privado a escala de la UE, también colaborando con Europol para establecer capacidades de notificación de contenidos de Internet» y que se creen «estrategias de comunicación para fomentar la tolerancia, la no discriminación, las libertades fundamentales y la solidaridad en toda la UE, incrementando en particular el diálogo interconfesional y entre otras comunidades, y potenciando los discursos que contrarresten las ideologías terro-

63. Comité consultatif de la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel(T-PD) «Avis sur les implications en matière de protection des données du traitement des dossiers passagers» Estrasburgo, 19 de agosto de 2016. Se puede consultar en línea, en http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD(2016)18rev%20Avis%20PNR_Fr.pdf [Consulta: 28 de septiembre de 2016]

ristas, por ejemplo dando voz a las víctimas» junto con el necesario desarrollo de «iniciativas en materia de educación, formación profesional, oportunidades de empleo, integración social y rehabilitación en el contexto judicial para abordar los factores que contribuyen a la radicalización, en particular en las prisiones»[64].

Como desarrollo adicional a esta Declaración, la Comisión Europea presentó el 28 de abril de 2016, una Agenda Europea de Seguridad, para el periodo 2015-2020[65], en la que se contiene un enfoque europeo común contra las amenazas terroristas internacionales. Por lo que respecta al objeto de esta comunicación, es de destacar el objetivo de esta Agenda de mejorar el intercambio de información y la interoperabilidad de las bases de datos y sistemas de información y, entre otras, reforzar el ECRIS (Sistema europeo de información de antecedentes penales), posibilitando también la inclusión de datos de personas de terceros países.

2.2.1. *Las amenazas a la privacidad desde el ámbito de las empresas y corporaciones privadas*

Pero también la protección de la vida privada y de la intimidad de las personas sufren amenazas desde el ámbito privado.

El primer aspecto que debemos remarcar es que la utilización de los datos personales que se vierten a la red, debe está siempre consentida por el ciudadano. Pero cada vez más, el ciudadano ni siquiera es consciente de que está suministrando datos personales en muchas de las actividades que realiza cuando utiliza el correo electrónico, los motores de búsqueda o la simple navegación. Es cierto que en muchas ocasiones, a la hora de utilizar distintas redes sociales o de instalar apps en sus dispositivos móviles, aparece una página inicial en la que debe aceptar distintos términos y condiciones de uso o la utilización por la aplicación de datos internos de esos dispositivos móviles (número de teléfono, de contactos, de ubicación, etc.), Pero tales términos y condiciones están escrito en un lenguaje excesivamente técnico o incluso críptico, que im-

64. «Declaración de los miembros del Consejo Europeo de 12 de febrero de 2015», ya citado.

65. El texto de la Agenda se puede consultar en http://ec.europa.eu/dgs/home-affairs/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf [Consulta: 23 de septiembre de 2016].

pide la correcta compresión de su significado o se refieren a una legislación ajena a la del país en la que se encuentra el usuario.

Por lo demás, las condiciones se ofrecen sin posibilidad de ser matizadas por sus usuarios que sólo tienen la opción de aceptarlas o rechazarlas en bloque —y ya conocemos los abundantes problemas derivados de los contratos de adhesión—. Por último, y no es un problema menor, tampoco existen controles fiables para que los menores de edad no estén aceptando —y por lo tanto, contratando— condiciones y términos legales que ni entienden ni están autorizados a suscribir.

Además, las grandes corporaciones que explotan sitios como «Microsoft», «Apple», «Google» o «Facebook», por citar las más conocidas, suelen situar sus sedes en Estados Unidos, dónde las regulaciones estatales de protección de los usuarios suelen tener una menor intensidad que, por ejemplo, en la Unión Europea.

Además, en relación a la protección del anonimato, se observa una tendencia creciente a buscar datos reales de las personas que utilizan las redes sociales. No es sólo que una persona ceda voluntariamente sus datos, sino que se establecen controles y cruces de información con otros usuarios para comprobar que los datos que se introducen son reales, pertenecen a personas físicas identificables a los que, además, se les incita de muy diversas maneras, a seguir incluyendo información de carácter personal (profesión, nombres de los cónyuges, edad, sexo, lugar de residencia, centros de enseñanzas, aficiones, gustos literarios y musicales, etc.). Y a todo ello se le suma la posibilidad de vincular fotografías y vídeos personales. En definitiva nos encontramos con una exposición absoluta de la intimidad personal. En este sentido es muy reveladora la denominada «política de nombres» de «Google+». Así, esta empresa no tiene ningún problema en señalar que «es importante que uses tu nombre para que las personas que quieran relacionarse contigo puedan encontrarte. Tu nombre es aquel por el que te conocen tus amigos, familiares y compañeros de trabajo». Y en caso de que exista alguna «incidencia de nombre», la empresa te pedirá que envíe una prueba de que ése es tu nombre verdadero, incluso enviando documentación oficial escaneada[66]. Lo mismo podemos decir para ejercitar el «derecho al olvido». Para que

66. Vid. http://support.google.com/plus/bin/answer.py?hl=es&answer=1228271 [Consulta: 15 de septiembre de 2016]

Google atienda nuestra petición de no encontrar informaciones que nos resulten perjudiciales, debemos solicitarlo a través de un formulario web en el que se nos pide que ofrezcamos a esa empresa un elenco de datos y elementos de verificación de los datos. De este modo no sólo Google podrá conocer y utilizar nuestros datos, sino que éstos están incluso verificados[67].

Especial atención debe prestarse también a los programas de reconocimiento facial. De hecho hemos venido observando en los últimos años un desarrollo acelerado de estas tecnologías.

Estas funcionalidades han supuesto una invasión tan importante en la privacidad que algunas de las autoridades de protección de datos han adoptado algunas medidas. Concretamente, la de Irlanda inició una investigación[68] en la que concluyó que el establecimiento de etiquetas de nombre en las imágenes, sin consentimiento de las personas interesadas, que estaba realizando «Facebook», no era admisible. Esta compañía posiblemente ante el temor de un endurecimiento de las políticas de privacidad en Europa, y antes de agotar el plazo de cuatro semanas que se le había otorgado (cuyo incumplimiento podría conllevar la imposición de una multa de 100.000 euros), actuó diligentemente desactivando ese servicio. Asimismo se comprometió a eliminar antes del 15 de octubre de 2012 cualquier patrón o modelo de datos que se usara como base para reconocer las caras de los usuarios.

67. El formulario que debe rellenarse se encuentra en la dirección https://support.google.com/legal/contact/lr_eudpa?product=websearch&hl=es. Para el buscador BING: https://www.bing.com/webmaster/tools/eu-privacy-request y para Yahoo, https://io.help.yahoo.com/contact/index?y=PROD_SRCH&token=w5FCchB1dWGbc2RE0kcjij0u65u86GoeqUkmqtTbcuO%2BLU%2FUQgc3BzwNZtXp6XEXn5YwJ6Wu6A9MCYnw7SzQy5BySKiGUpoj0xug9Sr7JfZdSQjOyA5v2Of2mZTMotlsehDS1xQqu1g%3D&locale=es_ES&page=contactform&selectedChannel=email-icon&isVip=false [Consulta: 25 de septiembre de 2016]

68. El informe se puede consultar en la siguiente dirección electrónica: http://dataprotection.ie/documents/press/Facebook_Ireland_Audit_Review_Report_21_Sept_2012.pdf [Consulta: 1 de octubre de 2016].

Otras autoridades de protección de datos, como las de Noruega, por ejemplo, también anunciaron a lo largo del verano de 2012 que iniciaban investigaciones sobre el reconocimiento facial en «Facebook» Cfr. http://www.bloomberg.com/news/2012-08-02/facebook-faces-norway-probe-over-facial-recognition-photo-tags.html [Consulta: 1 de octubre de 2016]

Significativamente, las recomendaciones de la Agencia Española de Protección de Datos van en una línea radicalmente diferente[69]. Así, por lo que se refiere a las peticiones de nombres, la Agencia recomienda que «No utilice su nombre real para configurar el ordenador, aplicaciones, móviles y otros servicios de internet para los que no sea realmente necesario». Es más, la Agencia recuerda que «en Internet no todo el mundo es quien dice ser». Por lo tanto «si cuando solicitan sus datos no dicen para qué los van a usar, o no entiende lo que le dicen, nunca dé sus datos».

Por lo que respecta a las redes sociales señala que «Las redes sociales son una importante fuente para la obtención de información sobre las personas. Debe garantizar la seguridad de su información mediante una configuración adecuada de su perfil y utilizando contraseñas adecuadas. Tenga presente que los buscadores pueden permitir a cualquier tercero obtener la información pública de los perfiles». En todo caso, «No publique en los perfiles de las redes sociales excesiva información personal».

Y, por último, en relación al correo electrónico la Agencia también indica que «Conviene utilizar una segunda cuenta, aparte de la personal, para acceder a servicios con interés temporal o comerciales».

En el mismo sentido, el Parlamento Europeo mantiene en su página web unas recomendaciones para «proteger su vida privada en la red»[70], en el que abogan por «limitar al mínimo la cantidad de información personal que revela», no aceptando «cookies» de terceros, vigilando la calidad de las claves que utilizamos, configurando las opciones de privacidad más estrictamente, limitando los posibles daños utilizando cuentas específicas para las compras por internet, leyendo la letra pequeña de los contratos, etc.

A pesar de ello no cabe ser muy optimista sobre la posibilidad de controlar de manera exhaustiva la información que cada ciudadano revela cuando utilizar internet y los servicios asociados a

69. Se trata de unas «Recomendaciones para una navegación más privada» en las que recoge numerosos consejos para la utilización responsable de internet. Puede consultarse en https://www.agpd.es/portalwebAGPD/jornadas/dia_internet_2016/recomendaciones-ides-idphp.php [Consulta: 10 de septiembre de 2016].

70. Se pueden consultar en la siguiente dirección electrónica: http://www.europarl.europa.eu/news/es/news-room/20131003STO21413/c%C3%B3mo-proteger-su-vida-privada-en-la-red [Consulta: 10 de septiembre de 2016]

ella (correo electrónico, mensajería, redes sociales, etc.), sobre todo cuando el negocio de los «Big data» se está revelando como uno de los más productivos para las grandes empresas[71]. Esther Mitjans se pregunta en relación con estos aspectos «¿Por qué los ciudadanos siguen dando tanta información personal?». En su opinión, «más allá de la necesidad humana de comunicarse, es la industria del entorno digital la que promueve activamente esta divulgación de datos», lo que le lleva a plantearse que la vigilancia en internet «es pues múltiple», y llevada a cabo no sólo por las instituciones sino que «también hay un entorno vigilante e invisible para muchos usuarios», de tal modo que «Google, Facebook u otro proveedor de servicios» puede controlar «nuestras relaciones y comportamientos, nuestro presente, nuestro pasado y, si es así, probablemente controlará nuestro futuro»[72].

Tampoco debemos dejar de mencionar el incremento del control de la vida privada de los ciudadanos, por manos privadas, a través de la creciente invasión de cámaras en lugares privados o públicos, la posibilidad de rastreo que ofrecen la multitud de dispositivos que incluyen sistemas de posicionamiento global, el control remoto de los dispositivos móviles (teléfonos, «smartphones», «tablets», etc.) o el importante campo que se abre con la internet «de las cosas».

Conclusion

En definitiva, con el aumento de las amenazas a la privacidad provenientes tanto del sector público como del privado, estamos lejos del panorama que dibujaba el documento de la Unión Europea conocido como el «Programa de Estocolmo. Una Europa abierta y segura que sirva y proteja al ciudadano»[73], cuando

71. Precisamente, una de las empresas más potentes en el negocio de los datos verificados es española. Su página web es http://www.adsalsa.com/ [Consulta: 25 de septiembre de 2016]

72. Mitjans, E. (2016) La múltiple vigilancia en el entorno digital». En *Monográfico de la Asociación Profesional Española de Privacidad, Día Europeo de Protección de Datos* 2016. On line en: http://www.apep.es/esther-mitjans-la-multiple-vigilancia-en-el-entorno-digital/ [Consulta: 26 de septiembre de 2016]

73. Este documento se puede consultar en: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:115:0001:0038:es:PDF . Un resumen del mismo también se puede consultar en http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=URISERV%3Ajl0034 [Consulta: 25 de septiembre de 2016]

afirmaba que al tratar de «evaluar la intimidad del individuo en el espacio de libertad, seguridad y justicia, prevalece el derecho a la libertad» de tal modo que «Principios básicos como la limitación en función del objetivo, la proporcionalidad, la legitimidad del tratamiento de datos, los límites del período de almacenamiento, la seguridad y la confidencialidad, así como el respeto a los derechos individuales, el control por unas autoridades de supervisión nacionales independientes y el acceso a recurso judicial efectivo deben quedar garantizados, y debe establecerse un sistema general de protección». Más bien al contrario, a lo que estamos asistiendo es a un creciente aumento de los instrumentos legales para controlar la vida privada de los ciudadanos. Aumento de estos instrumentos legales que viene acompañado de un incremento de las tecnologías –e incluso normas legales- que la hacen posible. La gestión y la trasmisión de ingentes cantidades de datos, no sería posible sin la existencia de poderosos ordenadores y de redes cada vez más capaces, que las faciliten.

Ante ese panorama, debemos acentuar la importancia de la responsabilidad a la hora de ceder datos y del consentimiento para su tratamiento. Debemos, por lo tanto, luchar para que ese mínimo instrumento que queda en manos de los ciudadanos no se dé por supuesto, que sea explícito, que se documente de un modo adecuado y que sea proporcionado, garantizando siempre el respeto al interés del ciudadano. Además deben reforzarse los derechos de los ciudadanos a acceder a la información registrada, a la oposición al tratamiento y a su rectificación y cancelación. Al tiempo, las autoridades deben velar por incrementar la información y la formación de los ciudadanos, especialmente de los menores de edad, para que el uso de las nuevas tecnologías se haga de un modo consciente y responsable.

Como señalaba la Declaración Francesa de los Derechos del Hombre y del Ciudadano «la ignorancia, el olvido o el menosprecio de los derechos del Hombre son las únicas causas de las calamidades públicas y de la corrupción de los Gobiernos». Esperemos que el acento que actualmente se pone en la seguridad, no lleve a la ignorancia o el menosprecio de la libertad individual y del derecho a una vida privada sin injerencias públicas o privadas.

Referencias bibliográficas

Anarte Borrallo, E. (2003). «Sobre los límites de la protección penal de los datos personales». *Derecho y conocimiento*. Universidad de Huelva. Vol. 2, pág. 225-254.

Beard, A.M. (1978) *The right to privacy vs. The first amendment: is a private person protected against the publicizing of his private facts?*, En línea, http://www.alicemariebeard.com/law/privacy.htm

Bru Cuadrada, E. (2007) «La protección de datos en España y en la Unión Europea. Especial referencia a los mecanismos jurídicos de reacción frente a la vulneración del derecho a la intimidad» *Revista de Internet, Derecho y Política*, Barcelona, UOC, núm. 5 (2007).

Campuzano Tomé, H. (2000). *Vida Privada y Datos Personales*, Madrid: Tecnos.

Carrillo López, M. (2003). *El derecho a no ser molestado*. Navarra: Aranzadi.

Cooley, Th. M. (1879). *A Treatise on the Law of Torts or the Wrongs Which A rise Independently of Contract*, Chicago, Callaghan.

Cotino Hueso, L. (2011), *Libertades de expresión e información en Internet y las redes sociales: ejercicio, amenazas y garantías*, Valencia: PUV (Publicaciones de la Universidad de Valencia).

Dans, E. (2011) «Sobre el anonimato y redes sociales», *El Blog de Enrique Dans*. En línea: http://www.enriquedans.com/2011/08/sobre-anonimato-y-redes-sociales.html

Electronic Frontier Foundation (S/F) «Anonymity». *Electronic Frontier Foundation. Defending your Rights en the Digital World*. En línea: https://www.eff.org/issues/anonymity.

Garriga Domínguez, A. (2004) *Tratamiento de datos personales y derechos fundamentales*. Madrid, Dykinson.

González Cifuentes, C. (2011) *El derecho a la intimidad de los altos cargos*. Tesis Doctoral, Universidad de Salamanca. En línea. http://gredos.usal.es/jspui/bitstream/10366/115568/1/DDPG_Gonzalez_Cifuentes_C._El_derecho.pdf

Guerrero Picó, M.ª C. (2006)*:»El impacto de internet en el derecho fundamental a la protección de datos de carácter personal»*. Madrid: Thomson-Civitas.

Heredero Higueras, M. (1997): *«La Directiva comunitaria de protección de los datos de carácter personal (Comentario a la Directiva del Parlamento Europeo y del Consejo 95/46/CE, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos)»*. Pamplona: Aranzadi.

Herrán Ortiz, A.I. (2001),: »La protección de datos de carácter personal en el marco de la Unión Europea», en *REDI*, núm. 39.

Less Andrade, Pedro (2009) «Google, protegiendo la privacidad en Internet». En *VI Encuentro Iberoamericano de Protección de Datos*. Cartagena de Indias, mayo de 2009 (en línea). Localización: https://www.agpd.es/portalweb/internacional/red_iberoamericana/encuentros/

VI_Encuentro/common/pla_privacidad_internet_vi_encuentro_iberoamerica.pdf

Lucas Murillo de la Cueva, P. L. (1990). El derecho a la autodeterminación informativa. Madrid: Tecnos.

Martínez Martínez, R. (2001). *Tecnologías de la información, policía y Constitución*. Valencia: Tirant Lo Blanch.

Masnick, M. (2011) «What's in a name: The importance of pseudonymity & the dangers of requiring 'Real Names'». *Techdirt*, En línea: https://www.techdirt.com/articles/20110805/14103715409/whats-name-importance-pseudonymity-dangers-requiring-real-names.shtml

Mitjans, E. (2016) La múltiple vigilancia en el entorno digital». En *Monográfico de la Asociación Profesional Española de Privacidad, Día Europeo de Protección de Datos* 2016. On line en: http://www.apep.es/esther-mitjans-la-multiple-vigilancia-en-el-entorno-digital/

Orza Linares, R. M. (2009) «¿Es posible la creación de nuevos derechos fundamentales asociados a las nuevas tecnologías de la información y de la comunicación?». Comunicación presentada al *IV Congreso de la Cibersociedad 2009*. En línea. Se puede consultar en http://www.cibersociedad.net/congres2009/es/coms/es-posible-la-creacion-de-nuevos-derechos-fundamentales-asociados-a-las-nuevas-tecnologias-de-la-informacion-y-de-la-comunicacion/991/

Orza Linares, R.M. (2010) «Las nuevas tecnologías de la información y comunicación y nuevos derechos fundamentales». En VV.AA. *Realidades y tendencias del Derecho en el siglo XXI* . Tomo VI. Bogotá: Ed. Universidad Javierana y Ed. Themis, págs. 251-285.

Orza Linares, R. (2011) «El derecho al anonimato en la Red» Revista *Telos,* Núm. 89: *Redes Sociales y democracia,* octubre-diciembre, 2011, págs. 24-33.

Orza Linares, R. y Ruiz Tarrías, S. (2011) «El derecho al olvido en Internet» En Carrillo i Martinez, A, Peguera, M, Peña-López, I. y Vilasau Sonala, M. (coord.) *Neutralidad de la red y otros retos para el futuro de Internet. Actas del VII Congreso Internacional Internet, Derecho y Política.* Universitat Oberta de Catalunya, Barcelona, Ed. Huygens. Págs. 371-389. (el texto, disponible en pdf, se puede obtener en http://goo.gl/bs4kO)

Orza Linares, R. (2012) «Derechos Fundamentales e Internet: nuevos problemas, nuevos retos». *ReDCE*, núm. 18. Se puede consultar en línea en: http://www.ugr.es/~redce/REDCE18/articulos/10_ORZA.htm

Orza Linares, R. (2012) «El derecho al olvido en internet: Algunos intentos para su regulación legal» *Libertad, transparencia y política en Internet: ejercicio, amenazas y garantías*. Madrid, Centro de Estudios Políticos y Constitucionales.

Pace, A. (1998) «El derecho a la propia imagen en la sociedad de los *mass media*» *Revista Española de Derecho Constitucional*, núm. 52, pags. 33-52.

Pavón Pérez, J.A. (2002) «La Protección de Datos Personales en el Consejo de Europa: el Protocolo Adicional al Convenio 108, relativo a las Autoridades de control y a los flujos transfronterizos de datos personales». *Anuario de la Facultad de Derecho.* Universidad de Extremadura, núms. 19-20, págs. 235-252.

Perales, A. (2016) «La vigencia del consentimiento en el futuro de la protección de datos personales». En *Monográfico de la Asociación Profesional Española de Privacidad, Día Europeo de Protección de Datos* 2016. On line en http://www.apep.es/alejandro-perales-la-vigencia-del-consentimiento-en-el-futuro-de-la-proteccion-de-datos-personales/

Prieto Gutiérrez, J.M.ª (1997): «La Directiva 95/46/CE como criterio unificador», *Poder Judicial,* núm. 48 Madrid.

Puente Aba, L.M.ª (2009) «Difusión de imágenes ajenas en Internet: ¿ante qué delitos nos encontramos?» En Carbonell Mateu, J. C. y otros (dir.) *Constitución, Derechos Fundamentales y sistema penal* tomo II. Valencia, Ed. Tirant lo Blanc, págs. 1541-1547.

Saldaña, M.N. (2012) «"The Right to Privacy»" La génesis de la protección de la privacidad en el sistema constitucional norteamericano: el centenario legado de Warren y Brandeis» *Revista de Derecho Político.* UNED, núm. 85 (2012), págs. 195-240.

Sánchez Bravo, A. (1998): *«La protección del derecho a la libertad informática en la Unión Europea»*. Universidad de Sevilla.

Viguri Perea, A. (1999): *«Intimidad versus informática (La protección de datos de carácter personal: perspectiva desde el derecho comparado)*», La Ley, Tomo de Jurisprudencia 2/1999.

Warren, S y Brandeis, L. (1890) *El derecho a la intimidad*, ed. y trad. a cargo de Pendás, B. y Baselga, P. Madrid, Civitas, 1995, pág. 22 y ss

SEGURIDAD DE APLICACIONES EN RED MEDIANTE DISEÑO POR CONTRATO Y ADA 2012

Alejandro R. Mosteo
Centro Universitario de la Defensa de Zaragoza
Instituto de Investigación en Ingeniería de Aragón

Resumen

Internet ha generalizado el intercambio y distribución de información. Cada vez más aplicaciones tienen puntos de entrada remota susceptibles de ataque por parte de entidades hostiles con fines de denegación de servicio o de acceso a información restringida. Este trabajo aborda uno de los puntos que pueden contribuir a hacer las aplicaciones más seguras: el propio código fuente, y lo hace examinando las nuevas características del lenguaje de programación Ada 2012 para el Diseño por Contrato. Ada fue el lenguaje oficial del Departamento de Defensa de los EE. UU. durante los años 90 y ha mantenido y mejorado con cada revisión su enfoque en seguridad y detección temprana de errores para aplicaciones críticas (aviónica, armamento, sistemas médicos, etc.). El trabajo estudia vectores habituales de ataque, y cómo las características de Ada 2012 pueden contribuir a mitigar cierto tipo de amenazas cibernéticas.

Palabras claves

Ada 2012, diseño por contrato, seguridad, Internet, ataques remotos.

1. Introducción

Los orígenes de Internet se sitúan comúnmente en el año 1969, cuando la red ARPANET (Salus 1995) ve la luz a iniciativa del Departamento de Defensa de los Estados Unidos (DoD). Según responsables del proyecto original sus propósitos eran amplios, debiendo cubrir las necesidades de mando y control del DoD frente a amenazas nucleares, permitir un control robusto

del arsenal nuclear y en general mejorar las capacidades tácticas y estratégicas para la toma de decisiones (Lukasik 2011). Sin embargo, el impacto más obvio de este proyecto y ya legado de toda la humanidad es su evolución en la red Internet, hoy omnipresente en múltiples ámbitos de aplicación que sería redundante enumerar.

La ubicuidad de Internet ha llevado a la situación en que la inmensa mayoría de equipos domésticos y aparatos móviles están permanentemente interconectados, siendo en muchos casos alcanzables remotamente. Incluso el estar detrás de enrutadores que deberían limitar las conexiones entrantes no es siempre garantía de seguridad, dadas las vulnerabilidades comunes que se siguen reportando sin visos de solución. En ámbitos más controlados, como empresas y organizaciones gubernamentales, las correctas prácticas informáticas señalan la necesidad de *zonas desmilitarizadas* (Bauer 2001) que aíslen por completo los equipos sensibles de otros con conectividad al exterior.

Si bien no es comparable el daño económico que se puede producir a una empresa, o el coste estratégico del robo de datos a una organización gubernamental, en caso de acceso ilícito, con el daño moral y económico que puede derivarse de la violación de la intimidad de un ordenador personal, en esencia la conclusión es la misma: toda vez que se pueda establecer una conexión entrante a un equipo, existe un vector de ataque explotable incluso sin la participación de seres humanos. Distinguiremos en este estudio, pues, los ataques con sustrato *social*, en que una persona es engañada para que facilite el acceso, de los ataques puramente telemáticos, en los que se requiere una vulnerabilidad en el sistema atacado. Dentro de éstos, además, descartaremos ataques debidos a fallos de diseño triviales, como por ejemplo los de fuerza bruta, para concentrarnos en los que se deben a limitaciones en la tecnología utilizada, como por ejemplo un desbordamiento de pila (Harsman y Hunt 2005).

Este último tipo de ataques son los que podrían mitigarse con el uso de tecnologías más adecuadas. Y, en definitiva, el elemento ineludible en todo sistema informático es el *software:* los sistemas operativos y programas que llevan a cabo todas sus tareas. Todo *software* de mínima complejidad se crea con un lenguaje compilado o interpretado, y sus capacidades de expresividad semántica se traducen en comportamientos y vulnerabilidades distintas. De

ahí que en este trabajo busquemos el señalar cuáles de las vulnerabilidades conocidas son mitigables con el uso de Ada 2012.

2. Perspectiva histórica

La historia del lenguaje Ada se remonta al año 1977 (Ichbiah 1984), cuando el DoD decidió poner coto a un maremágnum de más de 450 lenguajes informáticos por aquel entonces en uso dentro de la organización. El resultado fue un lenguaje estructurado perteneciente al paradigma imperativo, fuertemente tipado y de propósito general, pero con características que lo hacían apropiado tanto para grandes sistemas (dadas sus características de modularidad) como para el muy bajo nivel (con métodos para la representación de bits en la memoria y asociados a registros). Además, incorporaba los últimos avances en ciencias de la computación en cuanto a concurrencia, que muchos lenguajes de uso común hoy en día todavía no han superado.

2.1. *El mandato original*

El desarrollo de la especificación de Ada se produjo entre los años 1975, con la propuesta original *Strawman*, y 1980, con la aprobación del estándar militar MIL-STD-1815 (Ichbiah 1984). Sin embargo, no fue hasta el año 1983 que apareció el primer compilador validado (Softech Inc 1983). La validación era una nueva característica hasta la fecha por la que todo compilador debía pasar una batería de pruebas (hoy conocida como ACATS[1]) que demostraban su conformidad con la especificación (Tonndorf 1999). Este novedoso requerimiento hace que el lenguaje sea extremadamente portable y que la incidencia de errores por ambigüedad en el lenguaje (*undefined behavior*), sea mucho más limitada que en otros lenguajes con múltiples implementaciones como C.

Sin embargo, lo ambicioso de la especificación y lo extenso del lenguaje hicieron que las primeras herramientas disponibles fueran limitadas y poco potentes, dificultando el desarrollo (Hoare 1981). Además, los programas compilados no eran tan eficientes debido a dichas limitaciones en los compiladores de la

1. *Ada Conformity Assessment Test Suite.*

época y el amplio abanico de chequeos impuestos por la especificación (que, sin embargo, dan lugar a una mayor seguridad en los programas desarrollados, aspecto que particularmente interesa en este estudio).

En definitiva, tras más de una década, el mandato de uso de Ada para todos los proyectos del DoD estuvo en vigor entre los años 1991 y 1997 (con excepciones debidamente justificadas) (Rosen 2009). Se estima que el uso de distintos lenguajes se redujo de unos 450 a unos 37 hacia el año 1995 (Hook, y otros 1995).

2.2. *Ada tras el final del mandato*

Aunque podría argüirse el éxito del mandato, lo cierto es que la imposición no fue bien recibida en círculos tanto técnicos como de mando. Hacia el final había una percepción de que se habían alcanzado las metas en la reducción de complejidad de mantenimiento, pero de que se estaba entrando en un camino vicioso de falta de competitividad. Ésta es una de las razones aducidas para el abandono del mandato, con la intención de que el lenguaje compitiera en un mercado más abierto por sus propios méritos, pasando de ser una imposición a una recomendación (Hamilton 1997).

La herencia de los orígenes del lenguaje Ada está clara: es un lenguaje específicamente diseñado para facilitar el mantenimiento de sistemas complejos y críticos por encima de otras consideraciones. Tras el mandato su uso decayó progresivamente hasta la situación actual, en se le encuentra fundamentalmente en el nicho del software crítico: aviónica, satélites, control de tráfico aéreo, sistemas ferroviarios, etc. (Feldman 2014). Sus partidarios arguyen su solidez para esos objetivos y lamentan la falacia de la reducción de costes por el uso de otros lenguajes más populares (el argumento es que un desarrollador competente de C/C++ es barato y fácil de encontrar, mientras que Ada requiere formación dada la escasez de programadores que lo conozcan), alegando que el mayor coste en un proyecto informático es el mantenimiento (Pham 2003), un factor expresamente contemplado en el diseño de Ada.

Independientemente de estas alegaciones que no cuentan con soporte concluyente, Ada ha seguido modernizándose con sus estándares 95, 2005 y 2012, con los que se han incorporado al

lenguaje características de probada relevancia como las *interfaces* para la herencia múltiple o los predicados (pre- y post-condiciones e invariantes) destinados a la verificación formal del código (Barnes 2013), que son de particular interés en este estudio.

3. Ciberataques relevantes

En esta sección se examinan algunos ataques recientes, identificando aquéllos atribuibles principalmente a deficiencias en las herramientas informáticas. En particular, se han buscado ataques que hayan afectado a entidades gubernamentales o empresas de relevancia crítica, como de telecomunicaciones o infraestructuras.

3.1. *Vulnerabilidades relevantes*

De entre los múltiples ataques posibles, una vulnerabilidad de día cero en un servicio comúnmente a la escucha en un ordenador personal es posiblemente el vector de ataque más dañino y relevante para este estudio. Por su propia naturaleza de día cero, estas vulnerabilidades no tienen defensa conocida, y los atacantes que la conozcan tienen garantizada una vía de entrada en todo ordenador que ofrezca el servicio afectado (por ejemplo, servidores web o de llamadas remotas). En el pasado, algunas versiones de Windows fueron famosas por la extremada sencillez de infección a través de servicios presentes en todos los ordenadores, como el de RPC[2]: un ordenador que fuera instalado teniendo una conexión a Internet de IP pública, susceptible de ser usada por un gusano, era virtualmente infectado antes de que pudiera ser actualizado contra el ataque, con un tiempo medio hasta la infección de 4 minutos (Hutcheson 2008).

En un giro perverso de la cultura de actualizaciones, los actores maliciosos han usado en el pasado los parches oficiales de un sistema operativo para encontrar nuevas vías de ataque, como ocurrió con el gusano *Blaster* (Roberts 2003). Estos ataques, aunque no estrictamente de día cero, al anticiparse a la actualización de la mayoría de equipos han probado ser altamente eficaces. La mayoría de ataques, de hecho, se producen a través de vulnerabilidades ya conocidas, con algunas fuentes citando hasta un 85%

2. *Remote Procedure Call.*

del total de ataques (Public Safety Canada 2015). La demora en la aplicación de los parches de actualizaciones, ya sea por deficiente cultura de seguridad o por razones de servicio en infraestructuras de negocio críticas, es una causa todavía fundamental que explica en parte la abundancia de ataques exitosos.

3.2. *Ataques potenciales*

En esta sección discutimos algún vector de ataque que, aunque no haya sido usado de forma probada con fines maliciosos, es relevante por su pertinencia.

En general, incluso el sistema más aislado puede ser vulnerable a través de piezas de software aparentemente inofensivas. Cualquier programa que interpreta información sin los debidos chequeos puede conducir a la ejecución de código no deseado. Un ejemplo reciente afecta al intérprete de los documentos PDF en el popular navegador Chrome (MacGregor 2016). La incorrecta configuración de ciertas opciones de chequeo de desbordamientos de búfer conduce a que documentos maliciosamente creados puedan tomar el control del intérprete. Un problema similar ha sido identificado (CVE-2016-3319) en ciertas versiones del navegador de *Microsoft* en *Windows 10*. Este tipo de problemas ilustran la necesidad de practicar una programación defensiva para la que algunos lenguajes no están debidamente preparados.

Huelga decir que los lenguajes interpretados, aunque incorporen medidas de seguridad en el propio lenguaje, pueden estar expuestos a toda una nueva clase de ataques a través de la implementación de su máquina virtual (Govindavajhala y Appel 2003). Si bien lenguajes compilados como C, C++ y Ada están libres de este riesgo, Java y Flash, por poner dos ejemplos bien conocidos, han visto sus reputaciones duramente dañadas por la recua aparentemente interminable de vulnerabilidades que han conducido a recomendaciones por parte de actores tan importantes como el Departamento de Seguridad Nacional de los EE. UU. de eliminar totalmente su uso (Whittaker 2013).

3.3. *Ataques a entidades gubernamentales e infraestructuras críticas*

En el subsiguiente estudio de vulnerabilidades se incluyen únicamente ataques con un vector de entrada conocido. Las noticias informan con frecuencia de ataques a grandes empresas con

importantes robos de información (Privacy Rights Clearinghouse 2016), pero en muchos casos es difícil determinar el *modus operandi* de los atacantes, en parte por la reticencia de empresas y organismos a admitir públicamente negligencias en sus políticas de seguridad. Por ejemplo, la Corte del Estado de Washington sufrió el robo de más de un millón de registros relativos a datos privados de ciudadanos, presuntamente a través de una vulnerabilidad en *ColdFusion* de *Adobe*, cuya naturaleza se desconoce (CVE-2013-3336).

Del mismo modo, es difícil encontrar información fidedigna sobre ataques recientes que todavía están siendo investigados, por lo que los datos más fiables están en general disponibles para ataques con cierto tiempo de antigüedad. Además, para cuando los análisis se completan el código malicioso puede llevar ya mucho tiempo en funcionamiento, a veces desde fechas imprecisas. En general, los ataques se enumeran por orden de antigüedad. También se ha procurado recoger una muestra representativa de distintas vías de infección y propósitos ilegítimos, siempre entre ataques de alto impacto.

En 2015 se produjo el robo de información personal (Hirschfeld Davis 2015), entre ella registros de huellas dactilares, de entre 18 y 21 millones de empleados federales de los EE. UU. El robo costó el puesto a Katherine Archuleta, directora de la Oficina de Gestión de Personal, entidad víctima del ataque. El vector de ataque, atribuido a personas basadas en China, no ha sido publicitado pero se sospecha de componentes iniciales de ingeniería social y posterior uso de vulnerabilidades en productos de *Adobe* de escalada de privilegios (Gallagher 2015).

En 2014 se hizo pública la vulnerabilidad *Heartbleed*, corazón sangrante, (en alusión al módulo afectado, *Heartbeat*, latido), presente en código crítico de la librería *OpenSSL* desde 2012. Esta librería es un componente fundamental de la infraestructura de comunicaciones criptográficas seguras de Internet. El componente afectado, la capa segura de transporte (*Transport Secure Layer*), fallaba en comprobar el tamaño de cierta entrada (*bounds check*), un error por omisión relativamente sencillo de cometer en lenguajes que dependen fuertemente de la disciplina del programador, como C, al carecer de comprobaciones automáticas y apoyarse frecuentemente en aritmética de punteros. El parche (Moeller y Langley 2014) que corrige esta vulnerabilidad

ejemplifica cómo lenguajes que dependen de verificaciones y computaciones explícitas y manuales son un caldo de cultivo para código vulnerable. *Heartbleed* fue unánimemente considerado por la prensa especializada como un desastre de dimensiones sin precedentes, al permitir el robo de claves privadas en toda máquina afectada abierta a Internet. Entre las consecuencias probadas de la vulnerabilidad se encuentra el robo de la información personal de más de 4.5 millones de pacientes de la segunda cadena privada de hospitales de los EE. UU. (Frizell 2014), *Community Health Systems*. Además, se han producido alegaciones de que la Agencia Nacional de Seguridad (NSA) de los EE. UU. podría haber mantenido la vulnerabilidad en secreto para beneficio propio tiempo antes de su salida a la luz (Molina 2014). Ya en 2002, otro desbordamiento de búfer en la misma librería permitía acceso remoto a máquinas que usaran las versiones vulnerables (CVE-2002-0656).

Flame es un *malware* modular cuyos orígenes se han trazado hacia el año 2012 (sKyWIper Analysis Team 2012). Notablemente, este kit de espionaje no se aprovecha de ninguna nueva vulnerabilidad, sino que utiliza las mismas que utilizaba el gusano *Stuxnet* que se verá más adelante. Este hecho es un nuevo recordatorio del peligro de no reaccionar con presteza a las amenazas de seguridad. En un inesperado giro de los acontecimientos, los creadores de este *software* ordenaron su autodestrucción cuando se hizo evidente que había sido descubierto, en un esfuerzo por dificultar las actividades forenses. De sus tasas de infección y otros indicios se desprende que un plausible objetivo era el espionaje industrial a países de Oriente Medio y en particular a Irán (Damballa 2012). Otro *malware* relacionado frecuentemente con *Flame* y *Stuxnet* es *Duqu*, del año 2011, por la razón de que su objetivo parece ser el mismo, concretamente el sabotaje del programa nuclear Iraní. En este caso sí que se produce la explotación de una nueva vulnerabilidad de día cero, concretamente en el intérprete de fuentes *TrueType* de *Windows* (Bencsáth, y otros 2011).

En 2011, una vulnerabilidad en el verificador de código interpretado del popular (aunque ya en creciente desuso, en parte por haber sido causa de abundantes vulnerabilidades) lenguaje *Flash* condujo al robo de información privilegiada que podría haber permitido, con información adicional, suplantar elementos de seguridad de la compañía *RSA Security LLC*, irónicamente una empresa dedicada a la venta de soluciones contra ciberamenazas.

El ataque explotaba chequeos deficientes y ejecución de código en zonas supuestamente no ejecutables (Oh y Radu 2011).

En el mismo año, y aprovechándose de una variedad de vulnerabilidades que incluyen desbordamientos de búfer e insuficiente validación de datos, se propaga el troyano *ZeroAccess*. En este caso la motivación (Shearer 2013) es económica, pues el troyano aprovecha las máquinas infectadas para minar *Bitcoins* (Nakamoto 2008), entre otras acciones. Esta criptomoneda es una vía de lucro atractiva para los delincuentes ya que se puede liquidar siendo muy difícil trazar su procedencia. Entre otras particularidades destacables de este *software* se encuentra que utiliza redes P2P[3] distribuidas para su estructura de control y mando, haciéndolo altamente resistente a la neutralización.

En 2010 se descubrió uno de los ataques más sonados de la historia reciente, *Stuxnet* (Langner 2011), hoy en día considerado fruto de esfuerzos conjuntos de los EE. UU. e Israel. Este gusano es un ejemplo de cómo infraestructuras críticas y aisladas de Internet pueden ser atacadas a través de una combinación de métodos. El vector de ataque inicial se cree fueron unidades USB infectadas y abandonadas a propósito. Sin embargo, la característica más destacable es el uso de hasta cuatro vulnerabilidades de día cero, de alto valor para los atacantes, para asegurar su propagación dentro de las redes locales (Gostev 2010). Sin embargo, del análisis de propagación (Matrosov, y otros 2011) se desprende que todas las vulnerabilidades empleadas son de naturaleza lógica y por tanto independientes del lenguaje de programación utilizado. Sin embargo, varias de ellas se basan en accesos a recursos que deberían ser inaccesibles debido a insuficientes chequeos. Las características de prueba formal de Ada que se detallan más adelante podrían ser útiles en este sentido.

A finales del año 2009 se produjo la considerada peor infección desde 2003, debida al gusano *Conficker* (Markoff 2009). En este caso el vector de propagación era una vulnerabilidad en sistemas operativos de *Microsoft* que permitía la ejecución de forma remota a través del servicio RPC. Nuevamente, accesos a memoria fuera de rango propiciados por desbordamientos de búfer son la base de la vulnerabilidad (Minh y Minh 2009). El cometido de

3. *Peer to peer*, entre iguales.

este gusano era el acceso remoto para cualquier tipo de actividad hostil, por lo que el impacto de sufrir una infección iba mucho más allá de los inocentes virus de antaño. Entre sus consecuencias puede destacarse la prohibición de vuelo de aviones militares franceses tras resultar infectada su red de computadores *Intramar*, causando la imposibilidad de la distribución de planes de vuelo (Willsher 2009). También el Ministerio de Defensa del Reino Unido se vio afectado (Page 2009), resultando en el envío de correos no deseados desde la RAF[4] hacia Rusia, aunque supuestamente sin que se produjeran filtraciones de información clasificada.

Ese mismo año, vulnerabilidades del tipo inyección *SQL* fueron la vía de ataque para el robo de unos 750,000 dólares en cajeros de *Citibank* (Johnson 2009). Este tipo de vulnerabilidad permite la ejecución de instrucciones no autorizadas en bases de datos a través de servicios web u otros programas que hacen una verificación deficiente de datos proporcionados por el usuario.

El gusano *Zotob* se propagó en el año 2005, gracias a una vulnerabilidad de desbordamiento de búfer en el servicio *Plug and Play* de *Microsoft Windows 2000*. Sus propósitos eran aparentemente lucrativos, aunque parte de su fama se debe a que causó la caída temporal del canal de televisión *CNN live* (Ward 2005).

En el año 2004, el uso de un desbordamiento de búfer por el gusano *Sasser* privó de comunicaciones por satélite a la agencia *France-Presse* (AFP) durante varias horas, los trenes de *Australia Railcorp* dejaron de circular temporalmente, y se sospecha que algunos vuelos de Delta Airlines se vieron afectados por las incidencias en los equipos en tierra (BBC News 2004).

En 2003, el gusano *SQL Slammer* afectó a servidores que utilizaban *Microsoft SQL Server*, aprovechándose de un desbordamiento de búfer para ejecutar código arbitrario en el servidor (Moore, Paxson, y otros 2003). Aunque sus efectos fueron relativamente poco dañinos el potencial para robo de información al afectar a servidores de bases de datos no puede pasar desapercibido. Irónicamente, el alto tráfico causado por el gusano hizo que muchos enrutadores dejaran de funcionar, en lugar de rechazar o postergar el exceso de tráfico como sería lo apropiado, en otra señal evidente de deficientes prácticas de programación.

4. *Royal Air Force.*

Ese mismo año, el gusano *Blaster*, alias *LoveSan*, se propaga mediante un desbordamiento ya conocido de búfer en el servicio de RPC (Flashsky 2003), que generalmente estaba abierto a la sazón en máquinas de *Microsoft* y que los enrutadores no protegían por ser de uso común. La ausencia de un propósito malicioso evidente no impidió su impacto en infraestructuras críticas al causar el reinicio no programado de computadores, habiendo sido asociado a un importante apagón ocurrido en los EE. UU. (Verton 2003).

En el año 2001, el gusano *Code Red* se aprovechó de un desbordamiento de búfer en algunas versiones del servidor IIS[5] (Teeraruangchaisri 2001) para propagarse y ejecutar código malicioso de dos variedades: denegación distribuida de servicio (notablemente, a la web de la Casa Blanca) y corrupción de sitios web (*defacement*) de los sistemas afectados. Se estima que unas 359,000 máquinas fueron infectadas en menos de 14 horas. De éstas, al menos 136 máquinas dentro del dominio *.mil* y 213 dentro del dominio *.gov* se vieron afectadas (Moore y Shannon 2013). El potencial de robo de información restringida es evidente.

3.4. *Observaciones*

Como se ha visto, el desbordamiento es el tipo de vulnerabilidad predominante (Cowan, y otros 2000). Lejos de ser un problema resuelto o en vías de solución, es evidente que el acceso a información restringida es un negocio lucrativo para malhechores del siglo XXI. El seguimiento de bases de datos sobre accesos (Privacy Rights Clearinghouse 2016), (CVE 2016) se convierte en una necesidad para las organizaciones conscientes de la criticidad de sus datos y al mismo tiempo son un duro recordatorio del hostil entorno en que se ha convertido nuestro mundo digital. Adicionalmente, estudios periódicos muestran que la tendencia es estable en cuanto al número de intrusiones anuales que se producen (Verizon 2016), lo cual apunta a una difícil solución en el futuro próximo.

5. *Internet Information Services.*

3.5. *Una reflexión sobre los dispositivos móviles*

La masiva proliferación de los s*martphones* ha abierto una nueva vía de penetración, particularmente útil contra redes locales no alcanzables de otro modo. Estos dispositivos son a todos los efectos ordenadores portátiles, por desgracia estando expuestos al mismo tipo de peligros. Es más, al tratarse de dispositivos que suelen conectarse a distintas redes, y en particular no estando limitados a redes Wi-Fi, su atractivo para los atacantes es patente. Los dispositivos *Android*, además, han sido criticados por la fragmentación del mercado y la lenta respuesta de los fabricantes en instalar actualizaciones. Esto convierte estos aparatos en el objetivo ideal para una nueva generación de ataques. Por ejemplo, en el año 2016 han aparecido al menos dos vulnerabilidades críticas de escalada de privilegios para las cuales no hay esperanza de que se produzca un parcheo eficiente. Tomando como ejemplo la más reciente, a través de la vulnerabilidad *Quadrooter* (Check Point Research Team 2016) cualquier aplicación puede corromper ciertas estructuras del sistema operativo para acceder a memoria ya liberada (*use-after-free*), posibilidad que en combinación con otras técnicas habituales conduce a una escalada de privilegios que permite a la aplicación tomar el control del dispositivo. Otra colección de vulnerabilidades, en general relacionadas con desbordamientos de enteros (Drake 2015) es *Stagefright*, de nuevo afectando a la mayoría de dispositivos Android en circulación. Se considera que este ataque podría perpetrarse de forma totalmente subrepticia con el envío de mensajes MMS a un destinatario de interés; sin embargo a día de hoy no hay ejemplos conocidos de su uso. Una vez infectado el dispositivo, el código malicioso podría borrar dicho mensaje eliminando toda constancia del ataque.

4. Características relevantes de ADA 2012

Se han señalado en la introducción las raíces históricas que hacen del lenguaje Ada una opción particularmente indicada para desarrollos seguros. Se ahonda a continuación en aspectos específicos en relación con las vulnerabilidades presentadas.

4.1. *Cultura de seguridad*

En inglés se usan dos términos distintos para hacer referencia a distintos tipos de seguridad. Por una parte tenemos *safety*, cuan-

do estamos hablando de que algo es seguro de usar: por ejemplo un vehículo. Además, encontramos *security* en el sentido de defensa: la que nos puede otorgar una presencia policial. Se hace alusión a ambos conceptos en los objetivos de diseño de Ada: *safety, security and high-reliability* (AdaCore 2015). No es de extrañar, pues, que encontremos en el lenguaje características específicas para la detección temprana de fallos. En general, el lenguaje prima la seguridad y la ausencia de errores sobre la conveniencia en el momento de la escritura, puesto que se estima que el tiempo dedicado al mantenimiento e inspección del *software* es mucho mayor que el dedicado a su programación original (Koskinen 2015). Estos principios de diseño deberían ser en sí mismos un punto a favor del lenguaje, puesto que el paso de los años ha confirmado tanto su vigencia como el éxito de las distintas revisiones del lenguaje en aplicarlos.

4.2. *Comprobaciones en tiempo de compilación y ejecución*

Si nos concentramos en el origen de las vulnerabilidades presentadas, observamos que en su mayor parte (desbordamientos de búfer, desbordamientos aritméticos, acceso a memoria ya liberada) se deben a problemas que un compilador es capaz de detectar automáticamente insertando las comprobaciones adecuadas. Ada, por ejemplo, implementa chequeo de rangos, de desbordamiento y de ámbito de vida de punteros más puesta a cero de punteros liberados, respectivamente. Por desgracia, C no contempla dichos chequeos y C++, en su mayor parte, favorece una cultura de máxima eficiencia delegando en el programador la corrección del código (Phipps 1999). Esto está presente en, por ejemplo, la existencia de formas de acceso a tipos estructurados que omiten chequeos de rangos que pueden conducir a la aplicación de técnicas como las vistas en la vulnerabilidad *Quadrooter*. En definitiva, el uso de un lenguaje que no cae en las falacias de la optimización prematura (Flater y Guthrie 2013) y la infalibilidad del ser humano, como Ada, elimina de partida la causa fundamental de un elevadísimo porcentaje de las vulnerabilidades que se han visto explotadas.

En este sentido, Ada sigue siendo el único lenguaje de propósito general y uso extendido que no restringe la declaración de variables numéricas a tipos de datos hardware, sino que permite hacerlo en el dominio del problema (Taft, y otros 2013). Esta

capacidad básica permite al programador acotar con sencillez otro amplio abanico de ataques, que aparece en varias de las vulnerabilidades estudiadas, concernientes a la validación de datos de entrada. Nuevamente, es preferible que el compilador lo haga en todos los casos a que el programador deba recordar hacerlo en cada ocasión y prever cualquier circunstancia en la que puede ser necesario.

4.3. *Predicados y diseño por contrato*

En esencia, el problema fundamental en cuanto a vulnerabilidades de las metodologías de desarrollo que predominan en la industria es su naturaleza reactiva, dadas las prioridades de coste y tiempo al mercado. Las vulnerabilidades se corrigen y detectan a posteriori, haciendo que el sentimiento de estar jugando al ratón y al gato sea inevitable. Por ello, cuando la ausencia de defectos es primordial, se acude a la verificación estática del código, que prueba con métodos formales la inexistencia de condiciones imprevistas (German 2003). Los problemas obvios son el incremento en el coste y el menor ritmo de desarrollo. Sin embargo, en lugar de considerarse una posibilidad de todo o nada, se puede acudir a verificar subsistemas críticos o, en general, a adoptar todos los medios razonablemente posibles para el chequeo de asunciones en el código.

El diseño por contrato, que se basa en el establecimiento de promesas (contratos) entre los datos que recibe una subrutina (subprogramas: procedimientos y funciones, en terminología Ada) y los resultados que ésta genera, no es una idea nueva. De hecho, era uno de los pilares del lenguaje Eiffel, hoy en relativo desuso, y existe un cierto consenso sobre la utilidad de esta metodología para el desarrollo seguro de software (Rubio-Medrano, Ahn y Sohr 2013) (Sangiovanni-Vincentelli, Damm y Passerone 2012). En un nivel básico, los contratos son precondiciones y postcondiciones que se comprueban en el momento de la llamada a un subprograma (precondición) y al terminar ésta (postcondición). Si estos chequeos fallan, en el peor caso el programa se interrumpe, lo que puede conducir a una denegación de servicio pero no a una ejecución de código hostil; en el mejor caso, de la verificación de los contratos en ausencia de excepciones se puede deducir matemáticamente que un programa no puede incurrir en errores.

Ada 2012 pone al alcance del programador herramientas explícitas para la escritura de pre- y post- condiciones en el momento de la declaración de los subprogramas, tanto en sus interfaces públicas como privadas. Esto incrementa el nivel de chequeos del compilador y facilita la documentación de suposiciones en el diseño. Además, como se verá en la siguiente sección, estas condiciones pueden ser utilizadas por herramientas de validación formal para el chequeo estático del código.

Además, existe la posibilidad de declarar predicados estáticos y dinámicos asociados a tipos de datos (Taft, y otros 2013): en esencia, se pueden aplicar invariantes a los tipos de datos que se verifican en el momento de asignar valores a variables, añadiendo una poderosa forma de verificación automática al arsenal del programador y de la herramienta de verificación formal. Que sepamos, esta característica no existe en ningún lenguaje de programación de propósito general y uso destacable en la industria.

En resumen, el programador concienciado con la cultura de seguridad tiene nuevas herramientas cómodas y efectivas a su alcance para mejorar la calidad del código (Bigelow 2013): puede asociar contratos a todos aquellos subprogramas susceptibles de recibirlos, y puede aplicar invariantes a los tipos de datos que se manejan en el programa. Además, el poder expresivo del lenguaje hace que los chequeos no tengan que suponer una penalización demasiado onerosa en el ejecutable final.

4.4. SPARK

La inclusión de las características recién descritas en la última revisión de Ada no es casualidad: desde los años noventa (Ross 2005) existe un subconjunto del lenguaje, denominado SPARK (Carré y Garnsworthy 1990), cuyo propósito es permitir la verificación estática del código. Este código, al ser un subconjunto, puede compilarse normalmente con un compilador de Ada, mientras que herramientas específicas aprovechaban información adicional presente en comentarios de formato especial diseminados al efecto en las fuentes. El problema de esta aproximación es que crea una desconexión entre el código compilado y las anotaciones que lo acompañan para permitir la verificación formal, dejando en manos del programador nuevamente la responsabilidad de la equivalencia entre lo programado y lo declarado en los comentarios.

Sin embargo, la revisión más reciente, SPARK 2014, que va aparejada a nuevas características de Ada 2012 (los denominados aspectos), abandona estos comentarios (de los que el compilador de Ada hace caso omiso) en favor de los predicados descritos. De esta forma, se completa el vínculo entre la verificación formal y el chequeo dinámico del código en el momento de la ejecución: el mismo código que se ejecuta y que aplica las comprobaciones es la fuente de las pruebas matemáticas que garantizan la ausencia de defectos.

Aunque es imposible aplicar estas técnicas a la programación en masa, simplificar la tarea al programador, acercando a su repertorio estas facilidades de chequeo que se escriben una vez pero se comprueban en cada uso, debería redundar en una reducción de las tasas de fallo (German 2003).

Existen algunos ejemplos de código abierto de demostración de este tipo de desarrollos que pueden resultar de interés al programador concienciado. En el proyecto *Tokeneer*, la Agencia Nacional de Seguridad de los EE. UU. encargó el desarrollo del software de un sistema biométrico de seguridad utilizando estas tecnologías, cuyos resultados se pueden consultar íntegramente como parte de un acuerdo de transferencia. Otro proyecto con una componente de interés especial es *Crazyflie*, en el que se convirtió un estabilizador para cuadricópteros de lenguaje C a una combinación de Ada y SPARK (Gracio 2015). En el proceso se identificaron varios bugs gracias a la herramienta de verificación formal.

Conclusión

En este trabajo se ha hecho un recorrido histórico por la evolución del lenguaje informático Ada poniéndolo en perspectiva respecto a la evolución de Internet. Hoy más que nunca las redes basadas en TCP/IP, Internet e *intranets*, son un pilar fundamental en el que se asienta el intercambio de información de procesos tanto civiles como militares, de diversos niveles de criticidad. La convivencia de máquinas expuestas a ataques remotos con otras que de uso interno en redes que deberían ser seguras ofrece un vector de ataque que puede ser explotado para el robo de información privilegiada y la implantación de *malware* pernicioso. Similarmente, la proliferación de *Smartphones* con vulnerabilidades raramente resueltas abre una nueva vía de entrada a lugares aislados.

Con este análisis como marco de contexto se han presentado a continuación los atributos del lenguaje Ada 2012 y su subconjunto SPARK que los convierten en herramientas idóneas para desarrollos de alta fiabilidad, haciendo incluso posible la verificación formal de subsistemas críticos. Si bien el uso de Ada no es predominante fuera de ámbitos específicos, la conclusión de este estudio es que un mayor conocimiento de sus capacidades, enfocadas explícitamente a la seguridad y fiabilidad del código, y su uso en dichos desarrollos críticos, podrían contribuir a incrementar el nivel de seguridad informática y a reducir las tasas de fallos.

Agradecimientos

Este trabajo ha sido financiado por los proyectos SIRENA (CUD2013-05) y ALERTA (CUD2016-17).

Referencias bibliográficas

AdaCore. *Ada Answers: The Ada Programming Language [en línea]*. 2015. http://www.adacore.com/adaanswers/about/ada.

Barnes, John. «Ada 2012 rationale.» *Lecture Notes in Computer Science* (Springer) 8338 (2013): 1-204.

Bauer, Mick. «Paranoid Penguin: Designing and Using DMZ Networks to Protect Internet Servers.» *Linux Journal*, 2001.

BBC News. *Sasser net worm affects millions [en línea]*. 4 de mayo de 2004. http://news.bbc.co.uk/2/hi/technology/3682537.stm.

Bencsáth, Boldizsár, Gábor Pék, Levente Buttyán, y Márk Félegyházi. *Duqu: A Stuxnet-like malware found in the wild*. Budapest: Laboratory of Cryptography and System Security (CrySyS), 2011.

Bigelow, Daniel. *Embedded: Ada 2012: say what you mean, mean what you say [en línea]*. 29 de enero de 2013. http://www.embedded.com/electronics-blogs/industry-comment/4405929/Using-Ada-2012-to-say-what-you-mean.

Carré, Bernard, y Jonathan Garnsworthy. «SPARK - an annotated Ada subset for safety-critical programming.» *Tri-Ada: Government, industry, academia*. 1990. 392-402.

Check Point Research Team. *Quadrooter: new vulnerabilities affecting over 900 million android devices [en línea]*. 2016. https://www.checkpoint.com/downloads/resources/quadRooter-vulnerability-research-report.pdf.

Cooper, David. *Tokeneer ID Station EAL5 Demonstrator*. Praxis High Integrity Systems, 2008.

Cowan, C., F. Wagle, Calton Pu, S. Beattie, y J. Walpole. «Buffer overflows: attacks and defenses for the vulnerability of the decade.» *DARPA*

Information Survivability Conference and Exposition (DISCEX'00). Hilton Head, SC: IEEE, 2000. 119-129.

CVE. *Common Vulnerabilities and Exposures [en línea]*. 2016. http://cve.mitre.org/.

CVE-2002-0656. *Common Vulnerabilities and Exposures [en línea]*. 2 de julio de 2002. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0656.

CVE-2013-3336. *Common Vulnerabilities and Exposures [en línea]*. 6 de mayo de 2013. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3336.

CVE-2016-3319. *Common Vulnerabilities and Exposures [en línea]*. 15 de marzo de 2016. https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3319.

Damballa. *The Flame/Flamer/sKyWIper Malware [en línea]*. 29 de mayo de 2012. https://www.damballa.com/the-flameflamerskywiper-malware/.

Drake, Joshua. «Stagefright: Scary Code in the Heart of Android.» *Black Hat USA*. 2015.

Feldman, Michael B. *Who's Using Ada? Real-World Projects Powered by the Ada Programming Language [en línea]*. 2014. https://www.seas.gwu.edu/~mfeldman/ada-project-summary.html.

Flashsky. *Xfocus Team: The analysis of LSD's buffer overrun in Windows RPC interface [en línea]*. 25 de julio de 2003. http://www.xfocus.org/documents/200307/2.html.

Flater, David, y William F. Guthrie. «A case study of performance degradation attributable to run-time bounds checks on C++ vector access.» *Journal of Research of NIST*, 2013: 260-279.

Frizell, sam. *TIME: Devastating Heartbleed Flaw Was Used in Hospital Hack [en línea]*. 2014. http://time.com/3148773/report-devastating-heartbleed-flaw-was-used-in-hospital-hack/.

Gallagher, Sean. *Ars Technica: Why the «biggest government hack ever» got past the feds [en línea]*. 8 de julio de 2015. http://arstechnica.com/security/2015/06/why-the-biggest-government-hack-ever-got-past-opm-dhs-and-nsa/.

German, Andy. *Software Static Code Analysis Lessons Learned*. QinetiQ Ltd, 2003.

Gostev, Alexander. *SecureList: Myrtus and Guava, Episode MS10-061 [en línea]*. 14 de septiembre de 2010. https://securelist.com/blog/incidents/29747/myrtus-and-guava-episode-ms10-061/.

Govindavajhala, S, y A.W. Appel. «Using memory errors to attack a virtual machine.» *Symposium on Security and Privacy*. Oakland, CA: IEEE, 2003. 154-165.

Gracio, Anthony Leonardo. *How to prevent drone crashes using SPARK [en línea]*. 28 de mayo de 2015. http://blog.adacore.com/how-to-prevent-drone-crashes-using-spark.

Hamilton, Drew, entrevista de Magnus Kempe. *End of Mandate Q&A with AJPO Director Hamilton* AdaHome http://www.adahome.com/articles/1997-04/qa_ajpo.html, (22 de abril de 1997).

Harsman, Simon, y Ray Hunt. «A taxonomy of network and computer attacks.» *Computers & Security*, 2005: 31-43.

Hirschfeld Davis, Julie. *The NY Times: Hacking of Government Computers Exposed 21.5 million people [en línea]*. 9 de julio de 2015. http://www.nytimes.com/2015/07/10/us/office-of-personnel-management-hackers-got-data-of-millions.html?_r=1.

Hoare, C.A.R., entrevista de Communications of the ACM. *The Emperor's Old Clothes* (1981).

Hook, Audrey A., Bill Brykczynski, Catherine W. McDonald, Sarah H. Nash, y Christine Youngblut. *A Survey of Computer Programming Languages Currently Used in the Department of Defense*. Unclassified, Institute for Defense Analyses, Alexandria, VA: Defense Information Systems Agency, 1995, 1-95.

Hutcheson, Lorna. *InfoSec Handlers Diary Blog: Survival time on the Internet [en línea]*. 13 de julio de 2008. https://isc.sans.edu/diary/Survival+Time+on+the+Internet/4721.

Ichbiah, Jean. «Ada: past, present, future.» *Communications of the ACM*, 1984: 990-997.

Johnson, Bobbie. *The Guardian: Heartland hackers also behind $750,000 cash machine strike [en línea]*. 2009. https://www.theguardian.com/technology/blog/2009/aug/24/hacking-law.

Koskinen, Jussi. *Software Maintenance Costs*. Joensuu, Finlandia: University of Eastern Finland, 2015.

Langner, Ralph. «Stuxnet: Dissecting a Cyberwarfare Weapon.» *IEEE Security & Privacy*, 2011: 49-51.

Lukasik, Stephen. «Why the Arpanet Was Built.» *Annals of the History of Computing* (IEEE) 33, núm. 3 (2011): 4-21.

MacGregor, Alice. *The Stack: PDF exploit found in default Google Chrome reader [en línea]*. 2016. https://thestack.com/security/2016/06/09/pdf-exploit-found-in-default-google-chrome-reader/.

Markoff, John. *The NY Times: Worm infects millions of computers worldwide [en línea]*. 22 de enero de 2009. http://www.nytimes.com/2009/01/23/technology/internet/23worm.html.

Matrosov, Aleksandr, E Rodionov, D Harlye, y J Malcho. *Suxnet under the microscope*. ESET, 2011.

Meyer, Bertrand. «Applying «Design by Contract».» *Computer*, 1992: 40-51.

Minh, Bui Quang, y Hoang Xuan Minh. *How Conficker makes use of MS08-067 [en línea]*. 14 de abril de 2009. https://www.exploit-db.com/docs/320.pdf.

Moeller, Bodo, y Adam Langley. *Bugzilla: Add missing bounds checks for Heartbeat messages [en línea]*. 21 de marzo de 2014. https://bugzilla.redhat.com/attachment.cgi?id=883475.

Molina, Brett. *USA Today: NSA denies report it exploited Heartbleed for years [en línea]*. 11 de abril de 2014. http://www.usatoday.com/story/tech/2014/04/11/heartbleed-cisco-juniper/7589759/.

Moore, David, Vern Paxson, Stefan Savage, Colleen Shannon, Stuart Staniford, y Nicholas Weaver. «Inside the Slammer Worn.» *IEEE Security & Privacy*, 2003: 33-39.

Moore, David, y Colleen Shannon. *Caida: The Spread of the Code-Red Worm [en línea]*. 17 de julio de 2013. http://www.caida.org/research/security/code-red/coderedv2_analysis.xml.

Nakamoto, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System*. Cryptovest, 2008.

Oh, Jeong Wook, y Marian Radu. *A Technical Analysis on the CVE-2011-0609 Adobe Flash Player Vulnerability [en línea]*. 2011. https://blogs.technet.microsoft.com/mmpc/2011/03/17/a-technical-analysis-on-the-cve-2011-0609-adobe-flash-player-vulnerability/.

Page, Lewis. *The Register: MoD networks still malware-plagued after two weeks [en línea]*. 20 de enero de 2009. http://www.theregister.co.uk/2009/01/20/mod_malware_still_going_strong.

Pham, Hoang. «Software reliability and cost models: Perspectives, comparison, and practice.» *European Journal of Operational Research*, 2003: 475-489.

Phipps, Geoffrey. «Comparing observed bug and productivity rates for Java and C++.» *Software - Practice and Experience* 29, nº 4 (1999): 345-358.

Privacy Rights Clearinghouse. *Data Breaches [en línea]*. 2016. http://www.privacyrights.org/data-breach/.

Public Safety Canada. *Top 4 Strategies to Mitigate Targeted Cyber Intrusions*. 26 de noviembre de 2015. http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/tp-strtgs-eng.aspx.

Roberts, Paul. *Computerworld: Blaster worm spreading; experts warn of attack [en línea]*. 12 de agosto de 2003. http://www.computerworld.com/article/2571072/malware-vulnerabilities/blaster-worm-spreading--experts-warn-of-attack.html.

Rosen, J.-P. «The Ada paradox(es).» *ACM SIGAda Ada Letters*, 2009: 28-35.

Ross, Philip E. «The Exterminators: A small British firm shows that software bugs aren't inevitable.» *IEEE Spectrum*, 2005.

Rubio-Medrano, Carlos E., Gail-Joon Ahn, y Karsten Sohr. «Verifying access control properties with Design by Contract: framework and lessons learned.» *Computer Software and Applications Conference (COMPSAC)*. IEEE, 2013. 21-26.

Salus, Peter H. *Casting the Net: From ARPANET to Internet and Beyond...* Boston: Addison-Wesley Longman Publishing Co., Inc., 1995.

Sangiovanni-Vincentelli, A, W Damm, y R Passerone. «Taming Dr. Frankenstein: Contract-Based Design for Cyber-Physical Systems.» *European Journal of Control*, 2012: 217-238.

Shearer, Jarrad. *Trojan.Zeroaccess [en línea]*. 29 de noviembre de 2013. https://www.symantec.com/security_response/writeup.jsp?docid=2011-071314-0410-99.

sKyWIper Analysis Team. *SKyWIper (a.k.a. Flame a.k.a. Flamer): A complex malware for targeted attacks*. Budapest: Laboratory of Cryptography and System Security (CrySyS), 2012.

Softech Inc. *Ada Compiler Validation Summary Report: NYU Ada/ED, Version 19.7 V-001*. Waltham, MA: Ada Joint Program Office, 1983.

Taft, S.-Tucker, Robert A. Duff, Randall L. Brukardt, Erhard Ploedereder, Pascal Leroy, y Edmond Schonberg. *Ada 2012 Reference Manual. Language and Standard Libraries*. Springer, 2013.

Teeraruangchaisri, Kittipong. *Code Red and Code Red II: Double dragons*. SANS Institute, 2001.

Tonndorf, Michael. «Ada conformity assessments: a model for other programming languages?» *ACM SIGAda international conference on Ada*. New York: ACM, 1999. 89-99.

Verizon. *Data Breach Investigations Report (DBIR) [en línea]*. 2016. http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/.

Verton, Dan. *Computerworld: Blaster worm linked to severity of blackout [en línea]*. 29 de agosto de 2003. http://www.computerworld.com/article/2571068/disaster-recovery/blaster-worm-linked-to-severity-of-blackout.html.

Ward, Mark. *BBC news: Money motive drove virus suspects [en línea]*. 5 de septiembre de 2005. http://news.bbc.co.uk/2/hi/technology/4205220.stm.

Whittaker, Zack. *ZDNet: DHS warns to disable Java amid zero-day flaw [en línea]*. 2013. http://www.zdnet.com/article/homeland-security-warns-to-disable-java-amid-zero-day-flaw/.

Willsher, Kim. *The Telegraph: French fighter planes grounded by computer virus [en línea]*. 7 de febrero de 2009. http://www.telegraph.co.uk/news/worldnews/europe/france/4547649/French-fighter-planes-grounded-by-computer-virus.html.

FORMACIÓN EN CIBERDEFENSA
CURSO AVANZADO DE CIBERDEFENSA

David Copé de los Mozos
Academia de Ingenieros del Ejército de Tierra

Resumen

Vivimos en un mundo conectado por medio de Internet y aunque creemos que los sistemas están perfectamente protegidos, continuamente los medios de comunicación informan que algún sistema ha sido vulnerado. Por lo tanto, es fundamental la protección adecuada de nuestros sistemas de información para intentar reducir el impacto ante un ciberataque. Pero esta protección, debido a sus implicaciones tecnológicas requiere un alto grado de preparación del personal responsable de aplicar las medidas de seguridad necesarias para proteger estos sistemas. Además, la legislación, obliga a los diferentes organismos, entre ellos el Ministerio de Defensa, a formar al personal responsable de implementar estar medidas de seguridad. Con este motivo, se ha creado un Plan de Formación en Ciberdefensa que permitirá formar al personal con responsabilidades en ciberdefensa.

Palabras claves

Ciberdefensa, Ciberseguridad, Seguridad de los Sistemas de Información y Telecomunicaciones, Formación.

1. Introducción

Si hacemos un breve repaso de las noticias de las últimas semanas de los medios de comunicación, incluso no técnicos, aparecen algunas de estas en las que, de alguna forma, una o varias

* Diploma de Informática Militar.
* Academia de Ingenieros del Ejército de Tierra.
* Unidad Militar de Emergencias.

amenazas[1] han conseguido vulnerar determinados sistemas de información de algun colectivo o ha vulnerado la privacidad de determinadas personas a través del ciberespacio[2]. Estas amenazas pueden tener diferente motivación (ciberterrorismo, ciberespionaje, ciberdelito o cibercrimen o hacktivismo)[3]. El origen de estas amenazas, en muchas ocasiones, no es fácil de determinar, el anonimato que proporciona Internet conlleva una verdadera dificultad de atribución de los ciberataques[4] realizados a un determinado colectivo u organización y además, el coste que conlleva realizarlos es relativamente bajo, por lo que está al alcance de cualquiera. Por ello, para evitar que estos ciberataques puedan dañar nuestros activos[5] debemos protegerlos con la implantación de determinadas salvaguardas[6], para evitar un intento de vulneración de nuestro entorno, ya sea desde el exterior o interior de nuestra organización.

Proteger los sistemas de información y telecomunicaciones no es una tarea sencilla debido a la complejidad de los sistemas actuales, los cuales mezclan distintas tecnologías, por lo que aumenta la

1. «Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización». AENOR UNE 71504:2008.

2. «Dominio global y dinámico compuesto por infraestructuras de tecnologías de la información, redes de telecomunicaciones y sistemas de información.» MADOC: Glosario de Términos Militares, PD0-000, Ministerio de Defensa, 2014.

3. «Utilización no violenta de herramientas digitales ilegales o legalmente ambiguas persiguiendo fines políticos. Estas herramientas incluyen desfiguraciones de webs, redirecciones, ataques de denegación de servicio, robo de información, parodias de sitios web, sustituciones virtuales, sabotajes virtuales y desarrollo de software». Fuente: https://es.wikipedia.org/wiki/Hacktivismo

4. «Acción producida en el ciberespacio que compromete la disponibilidad, integridad y confidencialidad de la información mediante en acceso no autorizado, la modificación, degradación o destrucción de los sistemas de información y telecomunicaciones o las infraestructuras que lo soportan». MADOC: Glosario de Términos Militares, PD0-000, Ministerio de Defensa, 2014.

5. «Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos.» AENOR UNE 71504:2008.

6. «Aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo (estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización)». MAGERIT.

superficie de exposición y la probabilidad que se produzcan distintos fallos. Ello requiere un amplio y detallado conocimiento de cómo funcionan y se integran estas tecnologías y, además de esto, se requiere disponer de los conocimientos adecuados para saber cómo proporcionar la seguridad a estos sistemas, manteniendo en todo momento sus capacidades operativas. Para conseguir esto, es fundamental mantener al personal, que da soporte a nuestros sistemas de información y telecomunicaciones y a aquellos que operan con los sistemas, perfectamente formados en el ámbito de la ciberdefensa[7].

2. Legislación y normativa

Además de lo anterior, la propia legislación y normativa española y europea, nos invita e incluso nos obliga, a emplear los recursos necesarios para formar al personal que realice cometidos en ciberseguridad[8] o ciberdefensa, tal como veremos a continuación.

2.2. *Legislación y normativa nacional*

La Estrategia de Seguridad Nacional, en las *Líneas de Acción Estratégicas en Ciberseguridad* establece que habrá que realizar la «Promoción de la capacitación de profesionales en Ciberseguridad».

Por su parte, la Estrategia de Ciberseguridad Nacional, en el *Objetivo 5 de la ciberseguridad,* determina que se deberá «Alcanzar y mantener los conocimientos, habilidades, experiencia y capacidades tecnológicas que necesita España para sustentar todos los objetivos de ciberseguridad». Además, la *Línea de acción 6* establece que se debe «Desarrollar un Marco de Conocimientos

7. «Conjunto de recursos, actividades, tácticas, técnicas y procedimientos para preservar la seguridad de sistemas de mando y control de las Fuerzas Armadas y la información que manejan, así como permitir la explotación y respuesta sobre los sistema necesarios, para garantizar el libre acceso al ciberespacio de interés militar y permitir el desarrollo eficaz de las operaciones militares y el uso eficiente de los recursos.» MADOC: Glosario de Términos Militares, PD0-000, Ministerio de Defensa, 2014, pág. 27.

8. «Protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados». ISACA (Information Systems Audit and Control Association) Capítulo Monterrey.

de Ciberseguridad en los ámbitos técnico, operativo y jurídico».

También el Esquema nacional de seguridad[9], en el artículo 15 punto 2, determina que «El personal de las Administraciones públicas recibirá la formación específica necesaria para garantizar la seguridad de las tecnologías de la información aplicables a los sistemas y servicios de la Administración.» Además este Real Decreto, en el artículo 37 apartado c, asigna al Centro Criptológico Nacional la «Formación destinada al personal de la Administración especialista en el campo de la seguridad de las tecnologías de la información, al objeto de facilitar la actualización de conocimientos del personal de la Administración y de lograr la sensibilización y mejora de sus capacidades para la detección y gestión de incidentes». Seguidamente este documento, en la Disposición adicional primera. Formación, estipula que «el personal de las Administraciones públicas recibirá, de acuerdo con lo previsto en la disposición adicional segunda de la Ley de acceso electrónico de los ciudadanos a los Servicios Públicos[10], la formación necesaria para garantizar el conocimiento del presente Esquema Nacional de Seguridad, a cuyo fin los órganos responsables dispondrán lo necesario para que la formación sea una realidad efectiva».

Finalmente la Ley de acceso electrónico de los ciudadanos a los Servicios Públicos, en la disposición adicional segunda, tal como hemos indicado anteriormente establece que: «La Administración General del Estado promoverá la formación del personal a su servicio en la utilización de medios electrónicos para el desarrollo de las actividades propias de aquélla. En especial, los empleados públicos de la Administración General del Estado recibirán formación específica que garantice conocimientos actualizados de las condiciones de seguridad de la utilización de medios electrónicos en la actividad administrativa, así como de protección de los datos de carácter personal, respeto a la propiedad intelectual e industrial y gestión de la información».

Tal como hemos mostrado, la propia Administración y por ende el Ministerio de Defensa en su ámbito, deben emplear todos los medios disponibles para formar a su personal en este ámbito

9. Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

10. Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos (Vigente hasta el 02 de Octubre de 2016).

de la ciberdefensa, para permitir adecuadamente la protección de los sistemas ante las posibles amenazas.

2.2. *Legislación y normativa europea*

Además de lo anterior, también en el marco europeo la Estrategia de Ciberseguridad de la Unión Europea[11], la Comisión invita a los estados miembros a «Intensificar los esfuerzos nacionales en materia de educación y formación en seguridad de las tecnologías de la información y telecomunicaciones, mediante la introducción de: formación en seguridad de las tecnologías de la información y telecomunicaciones en las escuelas para el año 2014; la formación en seguridad de las tecnologías de la información y telecomunicaciones, desarrollo de software seguro y la protección de los datos personales para los estudiantes de informática; y formación básica seguridad de las tecnologías de la información y telecomunicaciones para el personal que trabaja en las administraciones públicas»[12].

Igualmente la Comisión Europea, conocedora de la necesidad de formación del personal técnico en estas materias, anima prestar especial atención a la formación en este ámbito de la seguridad de los sistemas de información.

3. Situación actual

Si partimos de la base que para ser un especialista o administrador en los Sistemas de Información y Telecomunicaciones, normalmente se requiere un elevado conocimiento técnico de distintas materias, por ejemplo, podemos tener especialistas en bases de datos relacionales, especialistas en «Big Data»[13], especialistas en virtualización, administración de redes, administradores de sistemas de gestión documental, especialistas en entornos

11. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.

12. «Step up national efforts on NIS education and training, by introducing: training on NIS in schools by 2014; training on NIS and secure software development and personal data protection for computer science students; and NIS basic training for staff working in public administrations».

13. «Concepto que hace referencia al almacenamiento de grandes cantidades de datos y a los procedimientos usados para encontrar patrones repetitivos dentro de esos datos. Fuente: https://es.wikipedia.org/wiki/Big_data

web, etc. Y como hemos dicho anteriormente, normalmente todas estas tecnologías están relacionadas unas con otras. Para poder proteger los sistemas, debido a la complejidad de estos, el personal que debe protegerlos requiere una formación muy especializada, ya que no solo debe ser un experto en el conjunto de tecnologías que desea proteger, además se requiere tener elevados conocimientos prácticos y procedimentales en la Seguridad de los Sistemas de Información (STIC).

Hasta hace poco, cualquiera de este personal técnico podría serlo en su ámbito sin tener muchos conocimientos de seguridad informática, normalmente la parte de la seguridad durante el ciclo de desarrollo de los sistemas no se trataba y, si acaso, lo común era dejarla para el final. Incluso, muchas veces para implementar la seguridad de un sistema, la única tareas a realizar solía ser una fortificación del perímetro. Sin embargo, actualmente ya nos estamos dando cuenta que la implantación de cualquier tecnología no puede olvidar la aplicación de alguna clase de una metodología de análisis y gestión de riesgos, debido a que un sistema se romperá por el eslabón más débil y por tanto, existiendo esta dependencia entre tecnologías, finalmente el sistemas completo podrá ser vulnerable e incluso otros sistemas colaterales que estén ubicados en la misma red.

Si estudiamos los contenidos de los planes de estudios de las carreras universitarias relacionadas con los sistemas de Información y Telecomunicaciones de hace unos pocos años, podemos comprobar que, estos planes de estudios solo incluían una mínima carga lectiva de asignaturas relacionadas con la ciberseguridad y además estas solían ser optativas. Sin embargo, actualmente en las universidades se están actualizando muchos planes de estudios de las carreras universitarias relacionadas con la gestión de los sistemas de información y telecomunicaciones. Y estás actualizaciones, suponen un aumento de la carga lectiva en los planes de estudios con asignaturas relacionadas con la ciberseguridad, tanto con carácter obligatorio como optativo. Además, ya se han creado numerosos Masters de postgrado relacionados con la ciberseguridad. Por lo tanto, podemos comprobar que el sector universitario es perfectamente conocedor de la demanda de personal con conocimientos en este ámbito y se está actualizando para hacer frente a esta creciente necesidad.

Por ello, es fundamental que hoy en día, la seguridad informática o ciberseguridad, debe incluirse en cualquier plan de

estudios en la formación del personal técnico en el ámbito de los sistemas de información y telecomunicaciones. Tal y como ocurre en los planes de estudios de los alumnos de formación del arma de Transmisiones y del Curso para la Obtención del Diploma de Informática Militar. Esta formación inicial servirá para tener conciencia de la importancia de la ciberdefensa y posteriormente podrá ser la base para que los conocimientos en este ámbito puedan ser ampliados.

4. Plan de formación de ciberdefensa

Según todo lo anterior, no es de extrañar que por Orden Ministerial[14], en el año 2013 se cree el Mando Conjunto de Ciberdefensa, al cual se le asigna, entre otros el cometido «Definir, dirigir y coordinar la formación y el adiestramiento especializado en materia de Ciberdefensa».

Además, el Real Decreto por el que se establece la organización básica de las Fuerzas Armadas[15], define las misiones del Mando Conjunto de Ciberdefensa y por otra parte, en el artículo 11.1.c de la Orden Ministerial 8/2015[16], le asigna la responsabilidad de «definir, dirigir y coordinar la concienciación, la formación y el adiestramiento especializado en materia de ciberdefensa».

Es por lo que, durante el año 2014 con la dirección del Mando Conjunto de Ciberdefensa se creó un grupo de trabajo, para la redacción del Plan de Formación de Ciberdefensa (FORCIBE), en el cual participaron, además del personal del Mando de Ciberdefensa, personal de la Dirección General de Reclutamiento y Enseñanza Militar (DIGEREM) y personal del Ejército de Tierra, Armada y Ejército del Aire.

En este plan se identificó esta formación en ciberdefensa como «aquélla orientada a conseguir la aptitud necesaria en materia de ciberdefensa para el desarrollo de las funciones y cometidos del puesto de trabajo considerado, mediante el necesario

14. Orden Ministerial 10/2013, de 19 de febrero, por la que se crea el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas.

15. Real Decreto 872/2014, de 10 de octubre, por el que se establece la organización básica de las Fuerzas Armadas.

16. Orden Ministerial 8/2015 , de 21 de enero, por la que se desarrolla la organización básica de las Fuerzas Armadas.

conocimiento de los medios y recursos disponibles en la materia, así como de las tácticas, técnicas y procedimientos con ellos relacionados, ya sean propios, aliados, o asociados con elementos potencialmente hostiles y enemigos, en su caso, que operen en el ciberespacio»[17].

El objetivo fundamental del Plan de formación en Ciberdefensa es «el de definir los requisitos de formación, en materia de Ciberdefensa que deberán alcanzar los profesionales del Ministerio de Defensa (MINISDEF) que ocupen puestos de trabajo relacionados con la Ciberdefensa. Por ello, el plan es de aplicación a todo el personal con responsabilidades en los Sistemas de Información de Telecomunicaciones (CIS), así como a personal con cometidos específicos de Ciberdefensa»[18].

Para la definición del Plan FORCIBE primero se identificaron los diferentes grupos de personal que deberían recibir formación en ciberdefensa y cuáles eras los conocimientos que deberían adquirir cada uno de ellos. A su vez se identificaron los siguientes tres grandes grupos: Grupos con Funciones Técnicas, grupos con Funciones de Asesoramiento y Otros Grupos.

Dentro de los Grupos con Funciones Técnicas se incluyeron los administradores de red, administradores de sistemas, administradores de seguridad, auditor de seguridad, supervisor de seguridad de las TIC, gestores de incidentes, expertos en malware, analistas forenses, operadores de monitorización y técnico de seguridad de dispositivos móviles.

En los Grupos con Funciones de Asesoramiento se incorporaron al asesor en ciberdefensa, asesor legal en Ciberdefensa y al analista de ciberinteligencia.

Y dentro de Otros grupos se incluyeron a: cuadros de mando, alta dirección, autoridades de los sistemas.

Una ver definidos estos grupos formativos, a continuación se identificaron todas las posibilidades de formación existentes en la actualidad de diferentes ámbitos a los que el personal del Ministerio de Defensa podría tener acceso: la propia formación en el Ministerio de Defensa y la específica de cada uno de los ejércitos, la de la OTAN, la que imparte el Centro Criptológico Nacional,

17. Plan de Formación de Ciberdefensa. 2015. 21 Plan de Formación de Ciberdefensa. 2015.

18. BOD. núm. 55, de fecha 21 de marzo de 2016. Resolución 220/03840/16..

y aquella que podemos encontrar en las Universidades y en las empresas privadas. Tras este estudio, se determinó que existía una amplia oferta de formación en este ámbito, pero esta formación no estaba estructurada adecuadamente a las necesidades actuales del Ministerio de Defensa.

Como no se podía basar el plan de formación del Ministerio en la oferta de formación existente, se definieron en detalle las necesidades de formación de cada uno de los grupos anteriores y se creó un itinerario formativo modular para cubrir cada una de las necesidades de formación de estos. Y dentro de cada itinerario formativo, se definieron una serie de módulos y para cada uno de ellos, se identificaron unas necesidades formativas mínimas que habría que cubrir.

Resultando de los trabajos realizados el siguiente esquema del plan de formación de ciberdefensa, del Anexo A.

El plan FORCIBE pretende que, todo el itinerario formativo definido tenga un carácter modular de tal forma que las necesidades formativas de cada grupo podrán ser cubiertas por uno o varios módulos normalizados implementados posteriormente sobre determinados cursos.

Los módulos definidos se pueden clasificar según a quién están orientados y según el tipo de función del puesto que se ocupe. Por ello, se dividen en formación generalista, especializada y técnica.

La formación generalista está orientada a personal no técnico sin conocimientos previos de ciberdefensa y que los necesita para desarrollar adecuadamente sus cometidos. Uno de estos cursos es el curso básico de ciberdefensa, que para personal sin conocimientos previos en ciberdefensa, es el curso inicial que daría la entrada para realizar posteriormente otros cursos, si es que estos son necesarios para el puesto que se ocupe. En este ámbito no técnico, además del curso básico de ciberdefensa, se identificaron otros dos módulos formativos: el de supervisor de seguridad de las tecnologías de la información y telecomunicaciones y el de asesor de ciberdefensa, para poder desarrollar sus cometidos de Asesoramiento al Mando y el Planeamiento en general.

La formación especializada está orientada a personal no técnico que tiene una formación específica en otros ámbitos pero que necesita esta formación para realizar cometidos en estos ámbitos específico aplicado a la ciberdefensa. Inicialmente se han

contemplado únicamente dos ámbitos, el de inteligencia y el de asesor legal.

La formación técnica está enfocada a enseñar las destrezas fundamentales, métodos, herramientas y técnicas necesarias para proteger las tecnologías de la información y telecomunicaciones contra las amenazas más frecuentes. Esta es una formación eminentemente práctica y totalmente de aplicación al puesto que se ocupe.

Como cuadro resumen resultante en el Anexo 2 se muestra una aproximación a la formación prevista para cada uno de los grupos de formación. Este cuadro es orientativo, ya que, como hemos dicho, esta formación estará ligada al puesto de trabajo y por tanto a las funciones que se realicen, por lo tanto dependerá también de la organización interna de cada una de las unidades u organismos que realicen tareas relacionadas con la ciberdefensa. Una vez definida las necesidades de formación se estableció que esta formación podría ser impartida por academias, escuelas y centros del Ministerio de Defensa, Universidades, así como por centros e instituciones privadas, no estando en este momento totalmente definidos quienes serán los encargados de impartirlos. Actualmente, solo se han definido en detalle tres cursos que serán los primeros en ser impartidos:

—El curso básico de ciberdefensa, del que ya se ha realizado la primera edición[19] durante el mes de junio de este año y ha sido impartido en la Escuela de Especialidades Antonio Escaño de la Armada con profesores del Centro Universitario de la Defensa del Ferrol. En el que fueron convocadas 20 plazas para suboficiales, de ellas, 10 para el EMAD, 4 para el Ejército de Tierra, 3 para la Armada y otras 3 para el Ejército del Aire. Y con una carga lectiva de 63 horas la fase no presencial y de 75 horas la fase presencial. Además, actualmente se está desarrollando la fase a distancia de la segunda edición[20] de este curso, aunque en esta edición las plazas han sido convocadas para oficiales, con la sigui-

19. BOD. núm. 184, de fecha 20 de septiembre de 2016. Resolución 220/13229/16.

20. RD. 339/2007, de 30 de abril, por el que se ordenan las enseñanzas de perfeccionamiento y de Altos Estudios de la Defensa Nacional.

ente distribución: 6 plazas para el EMAD, 6 plazas para el Ejército de Tierra, 4 plazas para la Armada y otras 4 para el Ejército del Aire.

—El curso de administrador de seguridad, cuya primera edición se desarrollará durante el año 2017 y se impartirá en la Escuela de Técnicas de Mando, Control y Telecomunicaciones Ejército del Aire ubicada en Madrid. El cual tendrá una carga lectiva de 120 horas impartidas de forma presencial.

—Y finalmente, el curso avanzado de ciberdefensa que actualmente se está desarrollando la primera edición en la Academia de Ingenieros del Ejército de Tierra, ubicada en Hoyo de Manzanares.

5. Curso avanzado de ciberdefensa

Una vez finalizado el Plan de Formación en Ciberdefensa se procedió a elaborar el currículo del curso avanzado de ciberdefensa. Este define a dicho curso a efectos de aplicación del Real Decreto 339/2015[21], como un curso militar conjunto y de especialización. Además se establece que este curso es de la Categoría A según la OM 59/1991, es decir, cursos nacionales de especialización inferior a seis meses de duración. Posteriormente y partiendo de las necesidades formativas del curso avanzado de ciberdefensa descritas en el Plan de Formación en Ciberdefensa, se definió el perfil de egreso, es decir, que capacidades o aptitudes debería obtener un alumno que finalizase este curso con aprovechamiento. A continuación, se establecieron los contenidos del Plan de Estudios de este curso para permitir a los alumnos obtener dichas capacidades, estos contenidos se dividieron en varios módulos, resultando los siguientes:

Módulo 1: Gestión STIC.
Módulo 2: Especialidades Criptológicas.
Módulo 3: Fundamentos de análisis de vulnerabilidades.
Módulo 4: Arquitecturas de redes seguras.
Módulo 5: Seguridad en el software.
Módulo 6: Ciberindidentes.

21. OM. 59/1991, de 07 de agosto, en la que establecen las categorías en las que quedan comprendidos los cursos de perfeccionamiento.

Consecutivamente con esto, se definió cual debería ser la duración aproximada del curso. Por ello, se determinó que la duración de la fase de presente debería ser alrededor de dos meses presenciales para que los alumnos egresados pudiesen conseguir los objetivos y capacidades previstas y además no sería conveniente que el personal que asistiese al curso se ausentase mucho más de su destino, para evitar la merma de las capacidades de las unidades de destino, ya que inicialmente estaba previsto que asistiese el personal técnico que se encuentra actualmente desarrollando tareas relacionadas con la ciberdefensa. También, se determinó que el curso debería incluir una fase a distancia en la que se impartirían los contenidos con carácter más teórico evitando así alargar la fase de presente. Finalmente, se detalló cual debería ser la duración, resultado:

—Una fase a distancia: con una carga lectiva de 50 horas, las cuales se desarrollarían en aproximadamente 4 semanas.
—Y una fase presencial: con una carga lectiva de 200 sesiones teóricas, prácticas o teóricos/prácticas, que se realizaran durante ocho semanas. A estas horas habría que añadir otras 200 horas de trabajo del alumno durante el desarrollo del curso. Debido a la alta especialización del curso, a que en las Academias y Escuelas del Ministerio de Defensa no disponen de personal que pueda impartir esta nueva formación y además el personal el experto en Ciberdefensa destinado en las Unidades de Ciberdefensa no puede detraerse de sus Unidades durante la duración del curso, se buscó la colaboración con determinadas Universidades nacionales, siendo finalmente seleccionado el Centro Universitario de la Universidad de Zaragoza para impartir el curso, debido a que dispone de personal totalmente cualificado y además las tareas de gestión se ven facilitadas por ya existir un convenio de colaboración de este centro con el Ministerio de Defensa.

Como se ha indicado, actualmente se está desarrollando la primera edición del curso, la cual se inició el 12 de septiembre con la fase a distancia y continuó el 10 de octubre con la fase de presente, la cual finalizará el 02 de diciembre.

En esta presente edición hay 21 alumnos: 10 del EMAD, 5 del Ejército de Tierra, 3 de la Armada y 3 de Ejército del Aire.

Conclusion

Tal como hemos visto, está claro que en la situación actual hay que hacer un esfuerzo en la formación del personal en el ámbito de la ciberdefensa, debido a que debemos proteger nuestras zonas de interés en el ciberespacio, para así proteger nuestros sistemas, tanto en territorio nacional como aquellos desplegados en las operaciones en el exterior.

También hay que tener en cuenta que, en este ámbito tecnológico todo evoluciona muy rápidamente, aparecen nuevas amenazas a las que hay que hacer frente, la capacidad del hardware aumenta constantemente lo que permite realizar determinadas tareas mucho más rápidamente y la creación de nuevo software que es accesible por cualquiera requiere que esta formación debe ser continua, para permitir la actualización de conocimientos y capacidades del personal con cometidos en ciberdefensa.

Por ello, los planes de formación en ciberdefensa deben actualizarse periódicamente, así como los cursos o módulos que lo compongan, aunque esto pueda suponer un gran esfuerzo en su gestión y también económico.

Referencias bibliográficas

Ministerio de Defensa. ET. MADOC. 2014: Glosario de Términos Militares.

AENOR. 2008. UNE 71504:2008 Metodología de análisis y gestión de riesgos para los sistemas de información. 2008-07-16.

Consejo Superior de Administración Electrónica. 2012. MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

Consejo de Ministros. 2013. Estrategia de Seguridad Nacional, de 31 de mayo de 2013.

Estrategia de Ciberseguridad Nacional 5 de diciembre 2013 Consejo de Seguridad Nacional.

España. 2010. Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

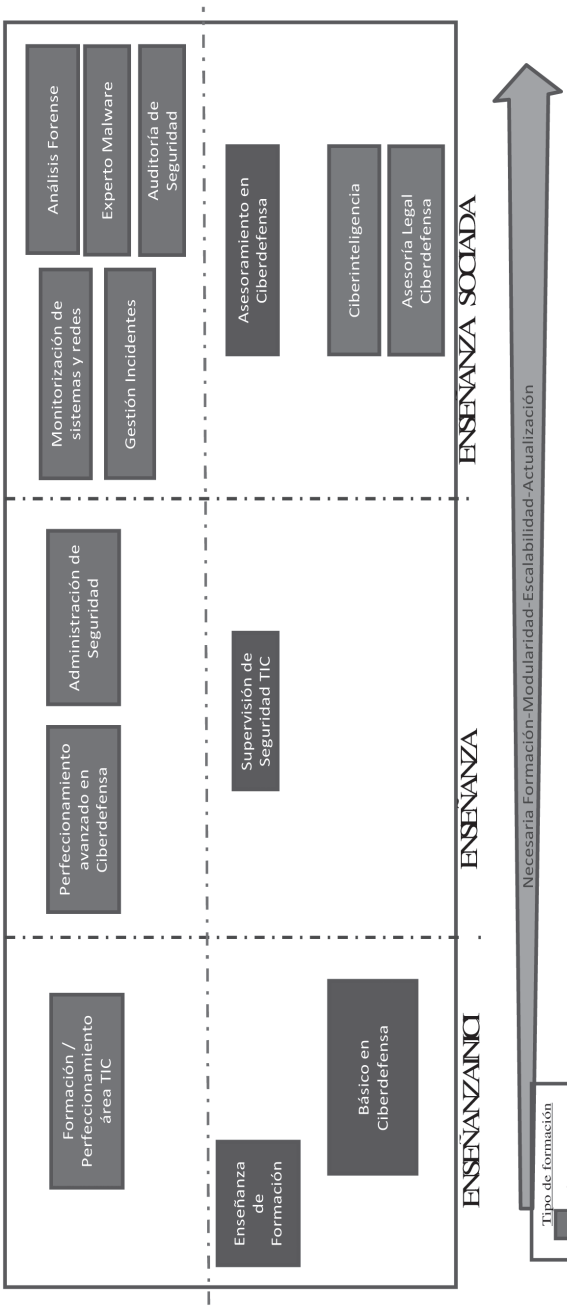
España. 2007. Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.

Comisión Europea. 2013. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.

Wikipedia. Consultada realizada en agosto de 2016. https://es.wikipedia.org/

Ministerio de Defensa. 2013. Orden Ministerial 10/2013, de 19 de febrero, por la que se crea el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas.
España. 2014. Real Decreto 872/2014, de 10 de octubre, por el que se establece la organización básica de las Fuerzas Armadas.
Ministerio de Defensa. 2015 Orden Ministerial 8/2015, de 21 de enero, por la que se desarrolla la organización básica de las Fuerzas Armadas.
Ministerio de Defensa. Boletín Oficial de Defensa. 2016.
EMAD. 2015. Plan de Formación de Ciberdefensa.

ANEXO A


ESQUEMA DEL PLAN DE FORMACIÓN EN CIBERDEFENSA
Formación / Perfeccionamiento área TIC
Básico en Ciberdefensa
Enseñanza de Formación
Perfeccionamiento avanzado en Ciberdefensa
Administración de Seguridad
Supervisión de Seguridad TIC
Monitorización de sistemas y redes
Gestión Incidentes
Análisis Forense
Experto Malware
Auditoría de Seguridad
Asesoramiento en Ciberdefensa
Ciberinteligencia
Asesoría Legal Ciberdefensa
ENSEÑANZA INICIAL
ENSEÑANZA
ENSEÑANZA SOCIADA
Necesaria Formación-Modularidad-Escalabilidad-Actualización
Tipo de formación
Técnica
Especial
Generalista

ANEXO B

FORCIBE FORMACIÓN POR GRUPOS			FORMACION											
			BÁSICA	SSTIC	FUNCIONES TÉCNICAS						OTRAS FUNCIONES			
			Formación Basica CD	Supervisión de Seguridad TIC	Formación Avanzada CD	Gestion de Incidentes	Administración de Seguridad	Monitorización de redes y sistemas	Analisis Forense	Experto Malware	Auditoria de Seguridad	Asesoramiento en CD	Ciberinteligencia	Asesoramiento Legal en CD
GRUPOS DE FORMACIÓN	FUNCIONES TÉCNICAS	Auditor de Seguridad			x		x				x			
		Supervisor de Seguridad de las TIC		x										
		Administrador de Seguridad (ASS)			x		x							
		Gestor de Incidentes			x	x								
		Operador de Monitorización			x			x						
		Analista Forense			x				x					
		Experto Malware			x					x				
		Administradores de red, sistemas y dispositivos móviles	A través de la Enseñanza de Formación. Ámbito específico/organizativo.											
	FUNCIONES DEAS OSARAMIENTO	Asesor Ciberdefensa	x		*							x		
		Analista Ciberinteligencia	x		*								x	
		Asesor Legal Ciberdefensa	x											x
	OTROS	Cuadros de Mando	A través de la Enseñanza de Formación y Ámbito específico/organizativo.											
		Alta Dirección	No se contempla formación particular dentro del Plan FORCIBE.											
		Autoridades de Sistemas	Para las Autoridades Operación de los sistemas (AOS/AOSTIC) y Autoridad de Seguridad TIC (ASTIC): No se contempla formación particular dentro del Plan FORCIBE. Cometidos según regulación vigente.											
			*	Debe haber realizado o la Formación Básica CD o Avanzada CD (en caso de proceder de entorno TIC)										

BLOQUE IV

CULTURA DE DEFENSA

UNA APROXIMACIÓN HISTÓRICO-JURÍDICA AL CONCEPTO DE GUERRA JUSTA EN LA EDAD CONTEMPORÁNEA

Marina Rojo Gallego-Burín
Universidad de Granada

Resumen

Uno de los mayores debates que se suscita ante cualquier conflicto, que no se resuelve pacíficamente, es si sería lícita o justa una intervención armada. Igual que ahora el ser humano se preocupa por legitimar y restringir el empleo de la fuerza, nuestros antepasados también tuvieron esa inquietud. Por tanto, resulta sugestivo comprobar cómo ha ido evolucionando el pensamiento en torno a esta problemática a lo largo de la Edad Contemporánea, poniendo especial énfasis en las opiniones de algunos autores como Kant, Rawls o Walzer, en la postura adoptada por el catolicismo y el islam, y en la tesis defendida por el Presidente de los Estados Unidos, Barack Obama.

Palabras claves

Guerra justa, literatura política, Iglesia Católica, Islam, «Doctrina Obama».

1. Introducción

La teoría de la guerra justa cuenta con unos orígenes ancestrales, nuestros antepasados ya sintieron la inquietud de legitimar y restringir el uso de la fuerza. Pretendemos poner nuestra atención en cómo ha sido tratada esta cuestión en la época más reciente de nuestra historia, la Edad Contemporánea, cronológicamente desde la Revolución francesa (1789) hasta nuestros días.

2. La guerra justa en la literatura política contemporánea

En el siglo XVIII diversos autores formularon variados proyectos de paz. Immanuel Kant (1724-1804), considerado como un teórico de la guerra justa, desde una posición que no se puede

encuadrar ni en un pacifismo extremo ni en un belicismo radical propuso un modelo, la Paz perpetua. Esto no era una idea original, en ella encontramos reminiscencias de Dubais en el siglo XIV, que fueron desarrolladas por el abate de Saint Pierre o el Duque de Sully con anterioridad. Kant en su obra *Sobre la paz perpetua,* idea un orden legal que erradique la guerra, establecie los requisitos que han de existir en las relaciones interestatales y resalta la incapacidad del Derecho Internacional para poner fin a los conflictos entre Estados. No obstante, para alcanzar esa utopia de la paz perpetua antes era imprescindible eliminar múltiples vilezas, como la avaricia o la ambición humana, pues Kant, como ya afirmó Hobbes, considera que la guerra es intrínseca a la naturaleza del hombre: «El estado de paz entre los hombres que viven unos juntos a otros no es un estado de naturaleza, que es más bien un estado de guerra, es decir, un estado en el que, si bien, las hostilidades no se han declarado, sí existe una constante amenaza». Se convierte en un deber abandonar ese estado: «no debe haber guerra», propone un nuevo modo de ordenación del sistema y de las relaciones internacionales, hasta que llegaran esos ansiados tiempos de paz perpetua la guerra debía ser regulada.

Por considerar este filósofo prusiano que la guerra está implícita en el hombre, y por la inseguridad que esta conlleva, admite la legitimidad de la guerra preventiva cuando existan graves amenazas o peligros. Pero al mismo tiempo rechaza hacer la guerra como un acto punitivo: «Ninguna guerra de Estados independientes entre sí puede ser una guerra punitiva,» ya que todas la naciones se encuentran en situación de igualdad, es legítima toda guerra que se destine a recuperar los derechos de los Estados que hayan sido violados. Concluye, como sostiene el internacionalista Truyol y Serra (Truyol y Serra, 1979, 61), que la finalidad de la doctrina del Derecho es la paz perpetua, la cual se alcanzará a través del Estado mundial, el Estado mundial de Derecho. Empero, como Kant es consciente de las graves dificultades que se plantean para alcanzar esa paz perpetua, establece una serie de prohibiciones para abolir la guerra, que aunque no son suficientes en sí mismas para acabar con la guerra, sí son necesarias: nunca se podría calificar como lícito ningún tratado de paz que cuente como intención oculta, para tiempos venideros, hacer la guerra. Tampoco se pueden adquirir o entregar las naciones independientes; las milicias se deberán extinguir; los

Estados no se endeudarán hipotecando su política exterior, así como no ejercerán ningún tipo de injerencia en otras naciones ni ninguna que se encuentre en guerra recurrirá a la agresión que impida una paz futura.

Otro teórico que es imprescindible mencionar es al general Carl von Clausewitz (1780-1831), cuya obra *De la guerra* —donde teorizó sobre la guerra y no sobre la paz— ha influido tanto a ideólogos como a estrategas. Este es un tratado cuya finalidad es demostrar que la guerra siempre cuenta con una misma causa: la política, «la guerra es sólo una parte del intercambio político y, por lo tanto, de ninguna manera constituye algo independiente en sí mismo». De dicha determinación deduce la legalidad y licitud de la Guerra y establece un axioma: la guerra es política y ella (la guerra) se emprende para alcanzar los objetivos de la política. Por tanto, existe una relación íntima entre la guerra y la política, la primera depende de la segunda, es su instrumento. Esta idea es de suma vigencia, como afirman García Caneiro y Vidarte, esa es una consideración asumida socialmente y «no sólo en el aparato racionalizador de la guerra, sino en su propia justificación» (García Caneiro y Javier Vidarte, 2002, 102).

Durante los últimos años del siglo XIX los gobernantes y políticos se ven imbuidos por una idea fundamental, que marcaría un nuevo ritmo en el mundo: la razón de Estado. Esto provocó que surgiera un «derecho de los Estados a la guerra» (Fernández Pons, 2010, 352), al cual podían recurrir si la situación o particularidades del momento lo consideraran pertinente. A partir de este momento lo más importante es defender a la nación, a lo que hay que aunarle distintos principios morales, anhelos de justicia, que contribuirán a restringir la cifra de los conflictos bélicos. En esos momentos se guerreaba con artillería de gran potencia: tanques, ametralladoras, aviones militares, gases letales, junto a armas bacteriológicas y atómicas, hay que mencionar esfuerzos, como el de codificar el Derecho humanitario y el de guerra, que trataban de poner coto a esta situación dramática.

Para lograr la paz y el desarme se celebraron dos conferencias. La primera en 1899 en La Haya y la segunda en 1907, en la misma ciudad. Estas conferencias se vieron influidas por el pensamiento del jurista holandés Hugo Grocio y por un acontecimiento histórico en los Estados Unidos: la Guerra de Secesión (1861-1865). Pues, los federales, tras esta contienda —por todas las atrocidades

que se cometieron— sintieron la necesidad de contar con un Código en el que se reuniera todo el Derecho de la guerra. Dicho compendio, aprobado por Abraham Lincoln el 23 de abril de 1863, fue encargado a Francis Lieber y se tituló *Instruction for the Goverment of Armies of the United States in the Field,* (Instrucciones para la conducción de los Ejércitos de Estados Unidos en campaña), conocido como Código Lieber, que a pesar de no constituir un tratado, es el primer intento de codificar las Leyes de la Guerra. En definitiva, es en la segunda mitad del siglo XIX cuando se trata de conjugar belicismo con protección humanitaria.

El siglo el XX, fue un tiempo de lo más desconcertante y contradictorio. Por primera vez el Derecho Internacional dictó en 1945 una norma imperativa que prohibía la guerra: la Carta de Naciones Unidas (art. 2.4), la ONU sólo intervendría en guerras justas. Pese a esta disposición fue un siglo marcado por lo sanguinario, con más de setenta guerras civiles, cincuenta de ellas posteriores a 1945. Al mismo tiempo que se produce algo histórico jurídicamente, como es el hecho de prohibir la utilización de la fuerza, es la época también en la que se produce el mayor número de conflictos internos. El único signo positivo fue la disminución de los enfrentamientos interestatales.

Respecto del siglo XX hay que mencionar a autores como John Rawls (1921-2002), que parte de una premisa importante: la de considerar al Derecho de gentes como una conjunción entre conceptos políticos, principios jurídicos, justicia y bien común. Para poder comprender la teoría de este profesor estadounidense, él mismo advierte cómo es conveniente tener en cuenta una serie de aspectos. En primer lugar, las potestades con que cuentan los gobiernos, respecto a la guerra, sólo son admisibles si ésta se incluye en un derecho de gentes razonable. Rawls presenta una teoría de la guerra justa absolutamente innovadora, no se asemeja a la sistemática seguida por otros autores, aunque se aprecia la influencia de san Agustín. Respecto del derecho de gentes diferencia dos teorías distintas; por una parte la ideal o de estricto cumplimiento y de otra la no ideal o inobservancia, con lo que podríamos establecer un paralelismo con la ciudad de Dios y la de los hombres, agustiniana. En la ideal las partes celebran tratados a los que se da cumplimiento, la conforman dos tipos de sociedades: «las democráticas liberales bien ordenadas» y las bien ordenadas y justas, jerarquizadas, con creencias religiosas, en las que no

existe separación Iglesia-Estado. Estas sociedades no luchan entre ellas, sólo hacen la guerra cuando tienen el convencimiento de que se encuentran amenazados por las naciones proscritas. Ello es debido a que el derecho de gentes sólo acepta que recurran a la Guerra, como legítima defensa, las «sociedades bien ordenadas, liberales y decentes, y a cualquier sociedad que acepte y respete un razonable derecho de gentes». Esta es una aseveración deducida de la práctica, desde el año 1800 no se han enfrentado entre sí este tipo de naciones, y en aquellas contiendas acontecidas entre una pluralidad de naciones, las democráticas han intervenido como aliadas. Las sociedades bien ordenadas pueden hacer uso del derecho a la legítima defensa, son las únicas que lo ostentan, aunque este derecho puede ser entendido de diferentes modos: las naciones liberales pueden guerrear en defensa propia, como una forma de preservar las «libertades básicas de sus ciudadanos, las instituciones democráticas y las tradiciones y formas de vida religiosas y no religiosas de la sociedad civil». Para Rawls, no es legítima la guerra cuyo fin sea la obtención de beneficios económicos, sólo es lícita aquella dirigida a proteger la libertad y las instituciones que tienen como función garantizar ésta. Los pueblos decentes también ostentan el derecho de defensa propia, pues entre su política se encuentra el respeto a los derechos humanos, este es el único requisito que se exige para ejercer este derecho. Dichas sociedades no hacen la guerra para aumentar el dominio de su territorio, sino que en ocasiones afirman acudir a ella para mantener su seguridad, cuando se trata de «operaciones encubiertas», como pueden ser las cuestiones financieras.

Por otro lado, respecto a la teoría no ideal de Rawls, la cual se corresponde con nuestro mundo actual y que no disfrutará de una justicia completa, cuenta con dos tipos de estados:

1. Los proscritos o criminales: rechazan el cumplimiento de un razonable derecho de gentes. Y además, legitiman el hacer la guerra, ya que con ella se pueden favorecer intereses nacionales, lo que no implica que sean razonables.
2. Los menos favorecidos: aquellos que padecen retraso tanto económico como de desarrollo tecnológico, lo que les impide gozar de un régimen «ordenado liberal o jerárquico».

Como hemos visto, las sociedades bien ordenadas son las únicas que cuentan con el derecho a la legítima defensa, para protegerse a sí mismas o a otras de su misma condición. Dichas consideraciones hacen que nos planteemos una cuestión que en los últimos años se suscita frecuentemente: ¿sería lícita la intervención de una nación bien ordenada en una proscrita o menos favorecida, para tratar de transformar a esta última en un Estado bien ordenado? Rawls defiende que sí es legítimo, pero sólo en el supuesto de que se traten de naciones abiertas o desarrolladas, de otro modo sería imposible inducirle al respeto de los derechos humanos. Con dicho planteamiento comprobamos cómo se restringe la potestad de realizar una guerra justa, se limita incluso la capacidad para poder declararla sólo a un tipo determinado de estados, los democráticos. Y se niega el poder de autodefenderse a los que no están bien ordenados. Esto es un planteamiento controvertido, pues por el hecho de que un Estado no se encuentre bien ordenado no se debe dejar a su población desamparada, despojarla del derecho a protegerse. Ello es por un loable propósito: que las naciones se aproximen a ese tipo de regímenes y de esta forma se extinga la guerra.

Actuamente el mayor exponente de la doctrina de la guerra justa, es el profesor norteamericano Michael Walzer (1935). Formula una teoría de la que se dice que es más «razonable que racional» (Walzer, 2001: 89). Plantea tesis actuales, teniendo presente nuestro pasado, de ahí que podamos encontrar en ella reminiscencias y semejanzas con las tesis más clásicas.

«La agresión es el nombre que damos al crimen de la guerra» (Walzer, 2001: 89), así considera este autor a la guerra, como un crimen. Michael Walzer comienza su teoría analizando la legítima defensa, la concibe como algo natural, aunque condicionado por las circunstancias bélicas: «La defensa de los derechos es una razón para luchar, (…) es la única razón». Todos los demás tipos de guerras, ya sea preventiva, de conquista… son rechazados; la legítima defensa es lo más conveniente y aconsejable, pues en caso de no responder a una agresión, aunque sea lícito el no hacerlo, el gobierno es responsable de los males que padecería su pueblo: «El propósito más profundo del Estado (…) es la defensa y lo mínimo que puede decirse es que muchos Estados actuales sirven ese propósito. Cuando su territorio se ve atacado o se presenta

un reto a su soberanía, tiene sentido buscar la existencia de un agresor y no creer simplemente en la realidad de un predador natural». (Walzer, 2001: 100).

También es abordada la guerra preventiva, su tesis se aproxima a las que en el siglo XVI enunciaran Vitoria y Grocio. Walzer define esta contienda como una «guerra en la que se lucha para mantener el equilibrio, para detener lo que se considera que trastoca un reparto uniforme del poder y lo transforma en una relación de dominio e inferioridad», en la cual para darse licitud tiene que existir una fehaciente amenaza de que se producirá una agresión inmediata. A pesar de ello, asevera que es una justa causa para declarar una guerra de este tipo la existencia de «miedo justo», expresión que toma de Bacon. Esto puede ser una causa arbitraria, por lo que para evitarlo añade una serie de casos que nunca podrían degenerar en una guerra: «los delirios jactanciosos a que a menudo son propensos los líderes políticos, el daño debe ser sugerido también en algún sentido material. Tampoco cuenta como amenaza el tipo de preparación militar que forma parte de la clásica carrera armamentística, a menos que viole algún límite formal o acordado tácitamente. Incluso lo que los juristas llaman actos hostiles que no llegan a la categoría de guerra. Y las provocaciones no son iguales que las amenazas».

2.1. *La guerra justa según la iglesia católica y el islam en la contemporaneidad*

Para conocer el tratamiento que ha recibido la teoría de la guerra justa en la Edad Contemporánea es necesario determinar como esta es abordada por las dos religiones más relevantes: el catolicismo y el islam.

El Catecismo católico, actualmente en vigor, establece las condiciones para que se emprenda una guerra justa. Ésta es aceptada, se legitima la guerra en defensa propia: «mientras exista el riesgo de guerra y falte una autoridad internacional competente y provista de la fuerza correspondiente, una vez agotados todos los medios de acuerdo pacífico, no se podrá negar a los gobiernos el derecho a la legítima defensa» (2308). Además, se fijan unos requisitos para realizar esta guerra defensiva, basados en los de la tradicional guerra justa: «Que el daño causado por el agresor a la nación o a la comunidad de las naciones sea duradero, grave y

cierto. Que todos los demás medios para poner fin a la agresión hayan resultado impracticables o ineficaces. Que se reúnan las condiciones serias de éxito. Que el empleo de las armas no entrañe males y desórdenes más graves que el mal que se pretende eliminar. El poder de los medios modernos de destrucción obliga a una prudencia extrema en la apreciación de esta condición».

Respecto a este tema es preciso mencionar a Pio XII, que se caracterizó por su profunda preocupación por la paz y la guerra. Podemos mencionar unas declaraciones suyas en las que repudia la guerra de agresión y defiende la creación de una organización supranacional que vele por la paz. Pio XII no aceptaba ningún tipo de guerra ofensiva, sólo era lícita la legítima defensa. Por primera vez se limita hasta tal extremo el recurso a la guerra, pero adviértase que el desvelo que sentía Pío XII por los conflictos bélicos y la llegada de la paz estaba justificado: el mundo se horrorizaba con la Segunda Guerra Mundial.

El Pontífice Juan XXIII va aún más lejos que su predecesor, rechaza todo tipo de contienda, incluso parece condenar la que se ejerce como defensa: «Se ha ido generalizando cada vez más en nuestros tiempos la profunda convicción de que las diferencias que eventualmente surjan entre los pueblos deben resolverse no con las armas, sino por medio de negociaciones y convenios. Esta convicción, hay que confesarlo, nace en la mayor parte de los casos, de la terrible potencia destructora que los actuales armamentos poseen y del temor a las horribles calamidades y ruinas que tales armamentos acarrearían. Por esto, en nuestra época, que se jacta de poseer la energía atómica, resulta un absurdo sostener que la guerra es un medio apto para resarcir el derecho violado».

Es pertinente comprobar cuál es la postura de la Iglesia Católica en la actualidad, para ello tenemos que acudir a la Encíclica *Gaudium et spes* de 1965, que promulgó Pablo VI en el Concilio Vaticano II. En ella existe una rotunda condena a la guerra: «El horror y la maldad de la guerra se acrecientan inmensamente con el incremento de las armas científicas. Con tales armas, las operaciones bélicas pueden producir destrucciones enormes e indiscriminadas, las cuales, por tanto, sobrepasan excesivamente los límites de la legítima defensa. (…) Toda acción bélica que tienda indiscriminadamente a la destrucción de ciudades enteras o de extensas regiones junto con sus habitantes, es un crimen contra Dios y la humanidad que hay que condenar con firmeza

y sin vacilaciones». Es tal el rechazo hacia la guerra que, incluso, para guerrear en defensa propia es preciso haber agotado todos los recursos de solución pacífica de las controversias para que se puedan catalogar como justas: «Mientras exista el riesgo de guerra y falte una autoridad internacional competente y provista de medios eficaces, una vez agotados todos los recursos pacíficos de la diplomacia, no se podrá negar el derecho de legítima defensa a los gobiernos. A los jefes de Estado y a cuantos participan en los cargos de gobierno les incumbe el deber de proteger la seguridad de los pueblos a ellos confiados, actuando con suma responsabilidad en asunto tan grave. Pero una cosa es utilizar la fuerza militar para defenderse con justicia y otra muy distinta querer someter a otras naciones».

En cuanto a las opiniones más recientes, podemos acudir a las palabras del Cardenal Ratzinger, ya el hecho de tomar el nombre de un Papa pacifista, como fue Benedicto XV, indica cuál es su pensamiento respecto a la guerra. Benedicto XVI antes de ser nombrado Sumo Pontífice, en 2004, se refirió a esta cuestión, lo hace a propósito de la Segunda Guerra Mundial, pues él mismo la vivió. Afirma que la responsabilidad que manifestaron las tropas Aliadas es el paradigma de un *bellum justum,* «porque su intervención tenía como finalidad el bien, incluso el de aquellos contra cuyo país se dirigía la guerra». De este conflicto pone de manifiesto, la insostenibilidad de un pacifismo radical, ello desemboca en la mayor de las injusticias y la violencia. Además, sostiene que existe una simbiosis entre la paz y el derecho, y la paz y la justicia: si el derecho y la justicia se corrompen, la paz se pondrá en peligro. En ocasiones luchar por el derecho conlleva recurrir a la fuerza, pero siempre debe ser de un modo proporcionado. Por otra parte, la fuerza del derecho también puede llevar a la injusticia, y es que este debe basarse en pautas de conductas reconocibles, por todos, como justas.

Tras conocer la tesis defendida por la Iglesia Católica en la actualidad, debemos analizar la postura adoptada por los musulmanes. Nos referimos a la *yihad*, tema de suma actualidad.

Los ulemas oficialistas contemporáneos, como el rector Mahmud Shaltut (1958- 1963), sostienen que los musulmanes cuentan con lo que para nosotros sería una guerra justa, la auténtica yihad defensiva, que precisa de causas como poner fin a una agresión o preservar la misión del islam. Son numerosísimos los ejemplos de

yihad defensivas que se han vivido a lo largo de la historia, las más importantes se sucedieron en el preludio del colonialismo (1785-1900) en el África Occidental. Los adalides del islam proclamaron la yihad contra los rusos (1830-1859); en Sudán contra ingleses y egipcios (1841-1956); italianos en Libia (1911-1951), o en Somalia (1899- 1920) y Argelia contra británicos, etíopes y franceses. Pero no sólo se han dado casos de yihad contra enemigos extranjeros, en tiempos de las cruzadas —enfrentamientos de cristianos contra cristianos— en la religión musulmana se dio el mismo supuesto: la «yihad intraislámica», como se vivió en Al-Ándalus entre almorávides y almohades. Los jariyíes luchaban contra gran parte de la comunidad musulmana, en defensa del mensaje profético al considerar que se estaba corrompiendo.

Una cuestión relevante es la relativa a la autoridad con potestad para declarar la yihad, esta es una grave problemática pues puede suponer que a cualquier persona se le reconozca la capacidad de hacer la yihad en nombre del islam. La persona llamada a realizarla es determinada por la *fiqh*, la jurisprudencia. Pero la doctrina no es uniforme, hay teóricos que establecen que es al gobernante a quien le corresponde el emprenderla, pudiendo constitutir un deber para todo el orbe musulmán el tener que participar en ella, rechazando que se trate de una responsabilidad individual, pudiendo eximirse solo a mujeres, discapacitados, menores de edad y enfermos. Sin embargo, existen opiniones discrepantes que sostienen la capacidad individual de cada fiel para poder hacer la yihad.

Los estudiosos liberales condenan la puesta en funcionamiento de la yihad actual. Para ello realizan distintas argumentaciones, por una parte alegan la afirmación del Corán: «No cabe coacción en religión» (2:256), defienden un modo pacífico para islamizar, pero en caso de que esto no fuera posible, se recurriría a un procedimiento político. La yihad defensiva hoy en día es la única causa justa desde un punto de vista jurídico, incluso ha sido admitida por la mayor parte de los países islámicos. Muhámed Yawad al. Mugniya (1904-1979), uno de los jefe chiís del Líbano, diferencia entre la yihad ofensiva y defensiva. La primera es llamada por el imán; ésta queda en estado latente hasta que este surja al final de los tiempos o en caso contrario nombre a un representante *ad hoc,* pues el imán permanece velado. La defensiva de la auténtica fe es provocada por esa posición de ocultamiento que tiene el

imán; puede ser emprendida por un muchtahidín. Esta jugó un papel esencial en 1979, cooperó para la victoria de la Revolución Islámica Iraní.

Desde la segunda mitad del siglo XX, la yihad se ha visto transformada con la aparición del yihadismo, que la concibe como un procedimiento de lucha contra la falta de fe, convirtiéndose la yihad en una obligación. Algunos sostienen que se percibe cierta tendencia a suprimir el sentido religioso de la yihad, la han hecho paladines como Yaser Arafat (mandatario no religioso) en 1978 en pro de la liberación de Palestina y Jerusalén, y también defiende que acudan a ella no musulmanes, por ejemplo el cabecilla de Al-Ázhar sostuvo que a la yihad contra Israel lucharan tanto coptos como los musulmanes de Egipto. Existen también supuestos en los que se combinan para llamar a la yihad sentimientos religiosos y nacionalistas, como el Movimiento de la Yihad Islámica de Palestina, que llama a la yihad a todos los musulmanes y tiene en el centro de su diana a Israel y Estados Unidos, contra los que hay que combatir, para conquistar Israel.

Como ya hemos apuntado, esto nos lleva hasta el yihadismo, el experto Gómez García diferencia tres clases: el revolucionario de los años 70, el internacionalista que surge en 1985, y el global que ve su aparición en 2001 (Gómez García, 2009, 363).

«El Imán de la yihad», Abdallah Azzam, profesor de Osama Bin Laden, que formó parte de los Hermanos Musulmanes de Jordania hasta 1980 (cuando defendieron el envío sólo de ayuda humanitaria y financiación a Afganistán y no de guerreros), defiende que la yihad es un deber individual. Sostiene que todos los musulmanes tienen una deuda mientras no recuperen todos los territorios que fueron musulmanes, como Al-Ándalus, Jerusalén o Samarcanda, deuda que pueden comenzar a saldar en Afganistán. Así lo expresan sus palabras: «Este deber no concluirá con la victoria en Afganistán; la yihad seguirá siendo una obligación individual hasta que todos los territorios que fueron musulmanes nos sean devueltos para que el Islam impere de nuevo: ahí están Palestina, Bujará, Somalia, Líbano, Chad, Eritrea, Somalia, Filipinas, Birmania, el sur de Yemen, Tashkent y Andalucía». Se comprueba cómo para el integrismo musulmán una causa justa para hacer la guerra es la recuperación de los territorios que en el pasado se encontraban bajo la influencia del Islam. Además, llamó a la yihad internacionalmente, para ello contaba con re-

quisitos procedimentales, establecía la obligación de advertir al adversario, lo cual nos explica la proliferación de webs islamistas desde 1995, y la presencia en los medios de comunicación desde 2001.Yihadismo que se reavivó con la lucha entre Irán y Estados Unidos en los años 80 y la desaparición de la URSS.

Azzam fue asesinado cuando iba a producirse un enfrentamiento entre dos doctrinas: la suya, que sostenía que no se debería extender la yihad hasta que no se instituyera en Afganistán el Estado islámico, contra la de Bin Laden, que insistía en llamar a la yihad en todo el Oriente Próximo, para luchar contra las potencias extranjeras, defender a aquellos territorios ya en teoría islámicos, pues se encontraban «infectados» por esas potencias. Así, desde el yihadismo internacional aparece el global, que se sintió alentado por el asentamiento de tropas estadounidenses en Arabia Saudí (el propio Bin Laden puso a disposición de los gobernantes saudíes una legión árabe para proteger sus fronteras, y evitar que esa labor la realizaran los estadounidenses, tal y como ocurrió) o la Guerra del Golfo. De tal modo, en 1998 diferentes valedores islamistas como Bin Laden o Al-Zawáhiri proclamaron el nacimiento del Frente Islámico Mundial para combatir a los Judíos y los Cruzados; se fusionó con el grupo Al-Qaeda en 2001, denominándose Base de la Yihad.

Bin Laden, en 1996, trazó la contienda frente a los cruzados del siguiente modo: «Es evidente que debe adoptarse un modo de combatir adecuado al desequilibrio de poder entre nuestras fuerzas armadas y las del enemigo (…) En una palabra, iniciar una guerra de guerrillas, donde tomen parte los hijos de la nación, y no las fuerzas militares».

El jefe operativo de los atentados del 11 de septiembre de 2001, Al-Zawahiri, publicó «Caballeros bajo el estandarte del Profeta», una especie de testamento político, en el que señala cómo tienen que ser las guerras en el futuro, Boix Alonso la sistematiza así: «realizar acciones que causen un número muy elevado de víctimas porque es el lenguaje que entiende Occidente; potenciar las operaciones de martirio; y elegir los objetivos y las armas con el fin de dañar lo más posible la estructura del enemigo y de disuadirle de la política que mantiene actualmente» (Boix Alonso, 1999: 8). A Al-Zawahiri, considerado como cerebro de Al- Qaeda, se le atribuye un gran poder de persuasión, sus teorías las acompaña de todo tipo de fuentes, para ratificar y otorgarles

la legitimidad que tan difícil es que posean hechos como los que defiende. Sus palabras van acompañadas de citas del Corán; establece paralelismos entre hechos de la historia musulmana con las efemérides presentes. Así por ejemplo, relaciona la aceptación de resoluciones de Naciones Unidas sobre Palestina por parte de algunos gobiernos árabes (lo que se puede considerar como irreligiosidad) con las Guerras de Ridda que se vivieron en el 633 y luchaban contra la apostasía tras el fallecimiento de Mahoma; la actitud de Pakistán después del 11 de septiembre de 2001, con la ausencia de creencias islámicas del pueblo de Mongolia y Al-Ándalus, desde tiempos de la reconquista, que se ha elevado a la categoría de mito, por el deseo que sienten por recuperarlo.

Los atentados de septiembre de 2001, de Nairobi o Dar es Salam de 1998, solo responden a esa concepción del yihadismo global que vivimos en la actualidad. Ese es el modo que consideran legítimo para luchar contra «los infieles con los que se han aliado los apóstatas» (Gómez García, 2009: 363). El 2 de mayo de 2011, diez años después de los atentados del 11 de septiembre, fue apresado y ejecutado «extrajudicialmente» el líder Bin Laden. La documentación encontrada en su escondite de Abbottabad muestran a una Al- Qaeda gestionada por el libio Atiyah Abd al Rahman, que aunque mermada en recursos nunca ha dejado de existir y se relacionaba con otras organizaciones yihadistas. Se presentaba una yihad global como un fenómeno organizado, con una estructura jerarquizada y con planteamientos estratégicos, en contra de lo que hasta entonces se consideraba, que la yihad global había derivado en un movimiento carente de organización, liderazgo y táctica que seguir. A lo que hay que sumar a esta organización estructurada en grupos reducidos, células e incluso individuos que de modo autónomo y solitario practican esa yihad, pues comparten ideología basada en el salafismo. Todo esto nos muestra la gran preocupación que sienten aquellos que la defienden por legitimar la yihad global. Este es un fenómeno que desborda todos los límites; grupos de personas son preparadas en campamentos para realizar la yihad; lo cual nos explica los sucesivos atentados que se han perpetrado en Europa, que se encuadran dentro de esa yihad global. En los últimos años se percibe una mayor organización, en 2004 se anunció la fusión entre la organización de Bin Laden con los islamistas de Irak, lo que se conoció como Base de la Yihad en Mesopotamia.

De este modo, se comprueba cómo dentro del islamismo existe una honda preocupación por legitimar, que sean calificadas como lícitas sus actuaciones, pues bajo su punto de vista, actúan movidos por una justa causa, están emprendiendo una guerra justa. La organización Al-Qaeda, tiene dos objetivos: derribar a aquellos soberanos islámicos que no cuentan con su misma creencia fundamentalista de la fe o apoyan a Occidente, teniendo que ser sustituidos por un Califato Islámico. Y segundo, la pretensión de poner fin a la sumisión que alegan padecer los musulmanes por parte de Norteamérica. El instituir tal Califato, no es una pretensión que comparta una mayoría de la población, sólo es la aspiración de un grupo radical, por lo que no se podría afirmar que existe una recta intención, no es algo a favor del bienestar y beneficio de la población. Ni se podría calificar como justa causa el obligar a profesar la fe de ese modo. Ellos alegan para atacar a Estados Unidos sus actuaciones en Irak o Palestina, pero aún en el supuesto de que esto fuera motivo suficiente, no se da ninguno de los requisitos para que sea una guerra justa: no hay recta intención, como hemos visto, tampoco se puede considerar a Al-Qaeda con autoridad legítima para emprenderla, ni existse la proporcionalidad en sus fines.

Hoy día no todos los pensadores defienden esa teoría integrista y fundamentalista, hay quienes no atienden tanto al sentido bélico del concepto, sino que prestan su atención al «sentido moral y espiritual» (López Pita, 2009: 172). A pesar de que las dos corrientes cuentan con la misma referencia, el Corán, el concepto de la yihad se encuentra determinado por la evolución histórica. Son divergentes las opiniones relativas a la yihad hoy día, la problemática no tiene visos de resolverse, pues es extremadamente difícil la de compaginar la tradición y los tiempos actuales.

De esto percibimos que la teoría de la guerra justa, tiene aún vigencia y entre todos los pueblos y las religiones, siempre se trata y se ha tratado de restringir la guerra, pero en ocasiones como es el caso de la yihad no son aceptables los criterios y argumentos establecidos por los que se quiere calificar como justa una lucha que en realidad no lo es.

2.2. *La «doctrina Obama»*

En el siglo XXI aún nos seguimos cuestionando ¿cuándo podemos hacer la guerra?, ¿tenemos que seguir aceptando este

procedimiento milenario de resolución de controversias? Para responder podemos acercarnos hasta la «Doctrina Obama», del actual Presidente de los Estados Unidos, considerado por el investigador Tovar Ruiz como «el presidente norteamericano más realista de los últimos 16 años, (…) que ha dejado atrás el idealismo filosófico de la postguerra Fría» (Tovar Ruiz, 2010). La política de Barack Obama se comienza a intuir en el discurso que pronunció en 2009 en la base de los Marines de Camp Legeune de Carolina del Norte, en el que hizo referencia a la retirada de las tropas de modo progresivo en Irak y el traspaso del gobierno a los iraquíes, o en un artículo del 2010 en la revista *Foreign Affairs* del Secretario de Defensa Roberts Gates en donde afirmaba que el empleo de la fuerza es siempre el último recurso, teniendo que ser su ejercicio multilateral. Pero ello no impide que en defensa de los intereses de Estados Unidos puedan recurrir a cualquier acción bélica de modo unilateral.

La «Doctrina de Obama», se vio reflejada en el discurso que pronunció en diciembre de 2009, cuando el Presidente estadounidense recibió el premio Nobel de la Paz. Este discurso lo tenemos que relacionar con el que pronunció meses antes, el 4 de junio de 2009, en el cual diferenció dos tipos de contiendas: el conflicto necesario, como el de Afganistán o Pakistán, pues al situarse en ese lugar extremistas violentos se hace necesario. Y guerras de elección, ejemplificada con la de Irak, la cual condenó, pues considera que los conflictos se deben resolver, cuando sea posible, por medios pacíficos.

Cuando recibió el Premio Nobel, el Presidente hizo alusión a la teoría de la guerra justa, la cual se incluye entre las necesarias, en esa necesidad se justifica. De sus palabras se deduce la importancia de conocer los orígenes de esta tesis, pues ellas nos transportan hasta las que Santo Tomás plasmara en su *Summa*. Barack Obama expresó la necesidad de concebir la guerra como un modo de intervención humanitaria. Ésta tiene que ser declarada por la autoridad competente y contar con el apoyo de la ciudadanía y la opinión pública. Y además es preciso que exista una causa justa, principalmente humanitaria, mantener la paz y siempre empleando la fuerza de un modo proporcionado.

Obama acepta la guerra como un medio de solución de controversias, pues en ocasiones a través de procedimientos pacíficos no es suficiente, por lo que se presenta como un fenómeno ne-

cesario: «Que no quede la menor duda: la maldad sí existe en el mundo. Un movimiento no violento no podría haber detenido los ejércitos de Hitler. La negociación no puede convencer a los líderes de Al-Qaeda a deponer las armas. Decir que la fuerza es a veces necesaria no es un llamado al cinismo; es reconocer la historia, las imperfecciones del hombre y los límites de la razón» (Obama, 2009). Ejemplo paradigmático de esta Doctrina del *Detente* (personificada con la doctrina de Obama) y de una guerra justa del siglo XXI es el caso de Libia, a través de la Operación *Odyssey Dawn*, que cumplió con todos los requisitos necesarios, contra las fuerzas de Gadafi: contó con el aval de la ONU, intervención de una fuerza multinacional, realizó unos ataques selectivos a objetivos militares y protegiendo a civiles.

En principio esta doctrina no sería reprobable moralmente, pues solo concibe la guerra como una intervención humanitaria cuando sea el último recurso y siempre tendrá que contar con la legalidad internacional, pero se podrían plantear ciertas cuestiones a su alrededor. Esta teoría nos recuerda a algunas afirmaciones que se realizaron con motivo de la guerra de Irak. El ministro de defensa francés Mme. Alliot- Marie no aceptó que su nación participara en tal contienda, manifestó que: «un ataque unilateral que no sea por consenso de la legalidad internacional, es pernicioso, porque amenaza crear un sentimiento de injusticia». De estas afirmaciones, se puede deducir que tanto este ministro como el Presidente Obama consideran que la legalidad de una guerra nace de la aprobación de la ONU.

Pero este tipo de consideraciones son controvertidas, el dejar residir la justicia en el acuerdo de un órgano político, como es el Consejo de Seguridad, puede llegar a ser algo peligroso, aunque también es cierto que es el único mecanismo con el que contamos. De hecho el escritor, ensayista y polemólogo español Rafael Sánchez Ferlosio no comparte estas determinaciones; afirma: «Dejando al margen la cuestión de facto de la dudosa o hasta extremadamente sospechosa libertad de cada uno de los 15 miembros, es decir, concediendo la ficción de *iure* de una total equipotencia de esas 15 libertades, el que la legitimación de la guerra contra Irak emanada por consenso de los 15 miembros de un organismo que es, incuestionablemente, de *derecho positivo* produjese efectivamente un sentimiento de justicia supondría nada menos que coronar virtualmente tal legitimación con la sacralidad de

un veredicto de derecho natural» (Sánchez Ferlosio, 2003). Para rechazar ese poder legitimador del Consejo de Seguridad alega hasta una norma jurídica del judaísmo post-exílico que dice que el reo que resultara condenado por unanimidad de los jurados debía ser inmediatamente absuelto y puesto en libertad; es Yavhé quien cuenta con una voz única, lo demás era un atrevimiento. Y esto es lo que ocurriría en la actualidad, tales consensos equivaldría a otorgar un poder omnipotente al consejo de Seguridad.

Sánchez Ferlosio considera temerario el universalismo en el derecho, esto provocaría la inutilidad de la ONU, como expresan sus palabras: «la ONU mostraría no ser más que una miserable oficina dedicada al suministro de coartadas, (…) para la protección de la buena conciencia de los hombres y los pueblos» (Sánchez Ferlosio, 2003).

Por otra parte, el establecer como justa causa una razón humanitaria, como hizo Obama, no se podría considerar reprobable. El problema se encuentra en que a veces esta se utiliza como un pretexto, es la excusa que se expone para hacer la guerra y justificar el horror. Dicha cuestión tan controvertida se comprobó hace poco tiempo, cuando se planteó la posible intervención en Siria por el empleo de armas químicas, y el presidente norteamericano manifiestó su voluntad de atacar incluso sin el apoyo de la comunidad internacional, en contra de su propia doctrina.

El planteamiento teórico de Obama no es reprochable, pero la realidad es confusa. Nos hallamos en un mundo complejo, poliédrico, movido frecuentemente por grandes intereses y donde las guerras justas tienen difícil cabida. Los analistas y expertos no dilucidan la realidad, ofrecen opiniones diversas, mientras que unos aceptan la versión «oficial», otros exponen las causas que califican de reales. Nos preguntamos si realmente se hace la guerra como una intervención humanitaria o esta es una mera excusa, por ello se suscitan cuestiones diversas ¿la guerra de Irak del 2003 tenía como propósito expandir valores democráticos?, ¿la de Libia en 2011, poner fin a la violación de los derechos humanos y la inseguridad? Estas causas podrían desencadenar una guerra justa, pero opiniones disidentes mantienen que esto son meros pretextos, pues las verdaderas causas son muy distintas, basadas en el mundo económico o político

Todo ello nos hace deducir la complejidad del asunto por la inmensidad de factores que se ven afectados en los conflictos.

Conclusión

Tras el análisis de algunos autores politicos de la Edad Contemporánea, así como haber indagado en cuales son las ideas defendidas por la Iglesia Católica y el Islam en la actualidad, junto al ideario del Presidente de los Estados Unidos, Barack Obama, se ha puesto de manifiesto cómo nos hallamos ante una doctrina que se erige entre dos posturas opuestas, el pacifismo y la aceptación sistemática de todas las guerras. En definitiva, se trata principalmente de consideraciones morales, que se han trasladado hasta el mundo jurídico.

El ser humano siempre ha tenido la necesidad de establecer unos criterios bajo los que determinar la legitimidad o no de las guerras, y así lo ha hecho desde tiempo inmemoriales. Pese a ser algo que siempre se ha cuestionado no existe unanimidad ni universalidad, se suceden las teorías. La guerra justa es una teoría en constante reformulación que ha ido evolucionando a lo largo del tiempo.

Tanto el cristianismo como el Islam, sin analogía entre ellos, se han planteado esta problemática. Han justificado el recurso a la fuerza, se han servido de causas para ellos calificadas como justas, para defender la auténtica fe.

A pesar de esos orígenes tan pretéritos es una doctrina de manifiesta vigencia. Tras los estudios del norteamericano Walzer, se ha contemplado su fuerte resurgimiento. A lo que hay que añadir que tras las repercusiones de la guerra de Irak, el presidente Barack Obama la adopta para su política, lo que la ha convertido en una tesis de plena actualidad.

Referencias bibliográficas

Allam, Magdi, *Vencer el miedo. Mi vida contra el terrorismo islámico y la inconsciencia de Occidente,* Ed. Encuentro, Madrid, 2008, págs. 187 y 188.

Baqués Quesada, Josep, *Los supuestos básicos de la teoría de la Guerra Justa,* Ed. Instituto Universitario General Gutiérrez Mellado, Madrid, 2006.

Bellamy, Alex J. *Guerras justas: De Cicerón a Irak,* Ed. Tezontle, Buenos Aires, 2009, págs. 226 y 227.

Boix Alonso, Luisa, «Al Qaeda: la nueva amenaza en la agenda de la seguridad nacional», *Cuadernos Constitucionales de la Cátedra Fadrique Furió Ceriol*, núm. 48 (2004), págs. 7-18.

Canal i Morell, Jordi y González Calleja, Eduardo, *Guerras Civiles. Una clave para entender la Europa de los siglos XIX y XX,* Ed. Casa Velázquez, Madrid, 2012.

Fazio Fernández, Mario, *De Benedicto XV a Benedicto XVI,* Ed. Rialp, Madrid, 2009.
Fernández Pons, Xavier, «Aplicación coercitiva del Derecho Internacional», en Sánchez, Victor M. (Dir.), *Derecho Internacional,* Ed. Huygens, Barcelona, 2010, págs. 351-372.
García Caneiro, José, y Vidarte, Francisco Javier, *Guerra y filosofía. Concepciones de la Guerra en la Historia del Pensamiento,* Ed. Tirant lo Blanch, Valencia, 2002.
García Cantalapiedra, D., *La «Doctrina Obama», la teoría de la «guerra limitada» y la nueva política exterior de EEUU: ¿Hacia una política neo-nixoniana?,* UNISCI Discussion Papers, núm. 28 (2012), págs. 145-153.
Gómez García, Luz, *Diccionario de islam e islamismo,* Ed. Espasa, Barcelona, 2009.
Herrero Cecilia, Ángel, *Historia del mundo contemporáneo. La época Napoleónica,* Ed. Akal, Madrid, 1994.
Juan XXIII, *Carta Encíclica Pacem in Terris. Sobre la paz entre todos los pueblos que ha de fundarse en la verdad, la justicia, el amor y la libertad*, Roma, 11 de abril, 1963.
Catecismo católico.
Kant, Immanuel, *Metafísica de las costumbres*, Ed. Tecnos, Madrid, 2005.
Kant, Immanuel, *Sobre la paz perpetua,* Edición de Abellán, José Luis, Ed. Alianza Editorial, Madrid, 2012.
López Pita, Paulina, «La guerra en el Corán y en la tradición musulmana», *Revista de Historia Militar*, núm. extra 1 (2009), págs. 141-176.
Mangas Martín, Araceli, *Conflictos armados internos y Derecho Internacional Humanitario,* Ed. Universidad de Salamanca, Salamanca, 1992.
Márquez Carrasco, María del Carmen, «Los crímenes contra la humanidad en perspectiva histórica (1899-1946)», en Vargas Gómez-Urrutia, Marina y Salinas de Frías, Ana, *Soberanía del Estado y Derecho Internacional. Homenaje al profesor Juan Antonio Carrillo Salcedo,* Ed. Universidad de Sevilla, Sevilla, 2005, tomo II, págs. 833-856
Obama, Barack, *Discurso pronunciado en la ceremonia de entrega del Nobel de la paz,* 2009.
ONU, Carta Naciones Unidas, Ginebra, 26 de junio de 1945.
Ortiz Sánchez, Luis, ¿Legitimidad de la guerra? *Una revisión de la teoría de la guerra justa,* Ed. Universitat de València, Valencia, 2011.
Pablo VI, *Constitución Pastoral Gaudium et Spes. La Iglesia en el mundo actual*, Roma, 7 de diciembre, 1965.
Parker, Geoffrey, *Historia de la guerra*, Ed. Akal, Madrid.
Pérez Mier, Laureano, *Pío XII y el Derecho Público,* Ed. Universidad Pontificia de Salamanca, Salamanca, 1956.
Rawls, John, *El derecho de gentes y «Una revisión de la razón pública»,* Ed. Paidós, Barcelona, 2001.
Reinares, Fernando, «¿Quién dijo que yihad sin líder? Lo que Abbottabad revela en torno a la situación y el funcionamiento de Al Qaeda»,

2011, [consultado el 18-2-2017] http://www.realinstitutoelcano.org/wps/portal/!ut/p/a0/04_Sj9CPykssy0xPLMnMz0vMAfGjzO318fEKcHX1NTZz9QgKNXI0NDSBAvyDbUREAbg0Kqw!!/?WCM_PORTLET=PC_Z7_3SLLLCAM54CNTQ27F30000000000000_WCM&WCM_GLOBAL_CONTEXT=/wps/wcm/connect/elcano/elcano_es/zonas_es/ari129-2011

Reinares, Fernando, «Reversión de la amenaza yihadista», *Nueva Revista,* núm. 143 (2013 junio).

Rubio Garrido, Rocio, «La fascinación de al- Ándalus o el delirio de al-Qaeda», en Thomas de Antonio, Clara María y Giménes Reíllo, Antonio (eds.), *El saber en Al-Ándalus,* Ed. Universidad de Sevilla, Sevilla, 2006, págs. 231-245.

Sánchez Ferlosio, Rafael, «Teodicea del universalismo», *ABC,* 5 enero 2003.

Tovar Ruiz, Julio, «El enigma de la doctrina Obama: un año de política exterior norteamericana», 2010 [consultado el 18-2-2017] http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/eeuu-dialogo+trasatlantico/dt2-2010

Von Clausewitz, Carl, *De la guerra,* Ed. La Esfera de los Libros, Madrid, 2005.

Walzer, Michael, *Guerras justas e injustas. Un razonamiento moral con ejemplos históricos.* Ed. Paidós, Barcelona, 2001.

DISEÑO Y VALIDACIÓN DE UN INSTRUMENTO DE RECOGIDA DE INFORMACIÓN EN ARCHIVOS MILITARES. EL CASO DE LOS ARCHIVOS MILITARES DE CEUTA Y MELILLA

Diego Becerril Ruiz
Universidad de Granada

José Manuel García Moreno
Universidad de Granada

Mónica Luque Suárez
Universidad de Granada

Resumen

En el marco del Proyecto de Investigación *La accion del ejército español en el Protectorado de Marruecos (1927-1956): antecedente de las operaciones de estabilización (COD. 26)* del Centro Mixto UGR-MADOC, estamos realizando una recopilación de información en diferentes archivos militares españoles. Para que dicha recogida sea útil a los objetivos del proyecto, hemos desarrollado y validado un instrumento para el registro de toda la documentación explorada a partir de los archivos Militares de Ceuta y Melilla. Dicho instrumento recoge los elementos que permiten operacionalizar esa información. Presentaremos cómo se ha articulado esta propuesta de instrumento como antecedente útil para investigadores en diferentes archivos militares que estudien operaciones de estabilización militar.

Palabras claves

Archivo militar, estabilización, validez de instrumento, protectorado, misión de paz.

1. Introduccion

Hasta el final de la *guerra fría*, las guerras o conflictos armados solían terminar con la victoria de una de las partes, o por vía de acuerdo negociado, que marcaba el cese de las hostilidades. Acto

seguido se procedía a la reparación y reconstrucción. Así ocurrió en Europa tras la Segunda Guerra Mundial y en conflictos posteriores. El fin de las hostilidades traía aparejada la llegada de la paz.

Pero desde la última década del siglo XX, marcada por la desaparición de la Unión Soviética y el neto predominio norteamericano, aparecen conflictos armados (Bosnia, Kosovo, Golfo Pérsico, Afganistán) en los que esta frontera entre guerra y paz dista de ser nítida.

Así comienzan a manejarse conceptos como guerras de cuarta generación, guerras híbridas, conflicto armado asimétrico, etc. En estos nuevos conflictos armados, se observa un espacio entre dos hitos: el hecho de ganar la guerra (objetivo militar) y el de conseguir la paz (objetivo estratégico). Este espacio entre la fase de intervención puramente militar y la normalización civil, está ocupado por una etapa de estabilización en la que se pretende consolidar lo obtenido en las operaciones, controlar y reducir el nivel de violencia residual e ir pasando el testigo a otros actores no militares hasta alcanzar una situación que permita retirar la fuerza militar.

> Entendemos por estabilización el conjunto de acciones coordinadas en tiempo, espacio y propósito, que llevan a cabo una diversidad de actores civiles y militares sobre un Teatro de Operaciones con la finalidad de permitir la creación, instauración y normal funcionamiento de las instituciones de gobierno de la nación (o en vías de convertirse en ella) anfitriona[1].

En esta línea, las operaciones de estabilización o de construcción de la paz, han pasado a convertirse en el tipo más habitual para las fuerzas armadas occidentales. Estas operaciones presentan cuatro características principales:

—El enemigo no está bien definido.
—La fuerza implicada debe colaborar y coordinar su acción con actores civiles, numerosos y de diversa naturaleza; porque el conflicto no tiene una solución puramente militar, aunque lo militar siempre forme parte de la solución.
—Es necesario cuidar el trato con la población civil del área de operaciones. Su actitud será un valioso indicador del grado de acierto de la actuación de la fuerza militar.

1. Publicación Doctrinal MADOC. PD3-303. ESTABILIZACION. Introducción.

—Las fuerzas de seguridad locales tienen un papel relevante, porque conocen la realidad social y cultural, permitiendo a la fuerza actuante conectar mejor con la población y prevenir errores.

—Son actividades de estabilización

> …aquellas que mediante el uso equilibrado de las capacidades coercitivas y constructivas de una fuerza militar contribuyen a establecer un entorno seguro y estable; facilitan la reconciliación entre adversarios de carácter local y regional; y apoyan el establecimiento y desarrollo de las instituciones políticas, sociales, legales y económicas, facilitando la asunción plena de las responsabilidades de gobierno por la autoridad legítima de la nación anfitriona[2].

Y estas actividades se agrupan en torno a cuatro categorías:

1. Apoyo a la Seguridad
2. Apoyo a la reforma del Sector Seguridad (SSR)
3. Apoyo a la restauración inicial de los Servicios.
4. Apoyo a las tareas iniciales de Gobierno.

El apoyo a la restauración inicial de los servicios se define como:

> Las actividades que puede realizar inicialmente la fuerza militar desplegada en una operación, durante un periodo limitado de tiempo, para colaborar en el restablecimiento de ciertos servicios e infraestructuras vitales o esenciales para la población, cuando no existen otros actores con capacidad para ejecutarlas[3].

Estas actividades tienen el propósito de crear expectativas de mejora entre la población impulsando el desarrollo político y social del área. Entre otros, incluye el abastecimiento de víveres y agua potable, asistencia sanitaria y restablecimiento de las vías de comunicación. Está claro que la reconstrucción de un país, tras un conflicto armado, es una tarea que rebasa las capacidades y las competencias militares.

No obstante, en el periodo inmediato posterior a la finalización del conflicto o de las operaciones, suele ser necesario que se acometan ciertas actividades, utilizando las capacidades militares existentes, para evitar a la población daños graves o irreparables.

2. PD3-303. ESTABILIZACIÓN. Las actividades de estabilización, p. 3-1.
3. PD3-303. ESTABILIZACIÓN. Las actividades de estabilización, p. 3-1.

Pero estas actuaciones estarán limitadas a la reparación inicial de servicios *vitales* (alimentación, agua, asistencia sanitaria, abrigo) y, excepcionalmente, de servicios *esenciales* (energía eléctrica, vías de comunicación, redes, infraestructura civil, economía, control sanitario e instalaciones hospitalarias, enseñanza, contratación local, limpieza de las zonas de operaciones, etc.).

Las acciones sobre servicios *vitales* evitan daños irreparables. Las de servicios *esenciales*, benefician a la población y favorecen su percepción sobre el papel de la fuerza militar y de sus propios órganos de gobierno o administración pública

Cuando se plantean, como en el caso de la estabilización, operaciones y actividades que parecen novedosas desde el punto de vista militar, es conveniente revisar nuestro pasado histórico en busca de experiencias afines. Porque, las tácticas, la organización y doctrina empleadas, debidamente procesadas, pueden aportar *lecciones aprendidas* aún válidas para el presente.

Aunque el interés de España en África es anterior y se intensificó en el cambio de siglo, el Protectorado de España en Marruecos, se estableció formalmente con la firma del Tratado Hispano-Francés de 27 de noviembre de 1912. La ocupación del territorio comenzó inmediatamente, aunque con resistencia por parte de la población que culminó con el llamado *Desastre* de Annual (1921) y terminó cuando España, con la colaboración francesa, consiguió controlar y pacificar el territorio en 1927, manteniendo su presencia en zona norte, hasta 1956.

Durante este periodo post-conflicto, la acción española en el Protectorado continuó dirigida por un Alto Comisario que, aunque formalmente dependía del Jalifa (representante del Sultán), de hecho era la máxima autoridad en la zona, organizada en tres distritos militares (Ceuta, Melilla y Larache).

La organización presidida por el alto comisario estaba estructurada en diversos departamentos, entre ellos, el de Asuntos Indígenas, que tenía representantes en los niveles regional, comarcal y local.

Era competencia de Asuntos Indígenas, entre otras, las relaciones con las cabilas; los asuntos de justicia islámica o especial; las escuelas y la sanidad e higiene.

En este ámbito competencial se tomarían medidas como la creación de una Junta de Enseñanza (en 1913), que incluía la formación del personal docente necesario. Asimismo, dado que

tampoco estaba organizada la salud pública, en 1916 se creó la Inspección de Sanidad que, venciendo recelos, llegó a realizar grandes campañas de vacunación.

Todas estas medidas iban encaminadas a favorecer la acción de gobierno del Jalifa y prestigiar su autoridad en un territorio que, hasta entonces, se había mantenido al margen de ella.

El jefe de la Oficina de Asuntos Indígenas era un militar y los militares predominaron en la administración de esta Dirección durante todo el Protectorado, siendo de su responsabilidad todos los servicios políticos, militares, de policía, comunicaciones, obras, sanidad y administración del territorio.

Si pensamos en los conflictos actuales en los que brilla esta «nueva» categoría de las acciones u operaciones de estabilización, como por ejemplo puede ser Afganistán, nos asalta la idea de que pueden apreciarse ciertas similitudes entre ambos casos.

Dejando al margen las diferencias, que las hay, a título indicativo cabe reseñar algunas coincidencias entre el caso de Marruecos (1927-1956) y, por ejemplo, el actual conflicto de Afganistán:

—En ambos casos la intervención de España se produce por interés nacional, pero impulsado y condicionado por compromisos o acuerdos multinacionales.
—La intervención asociada a las actividades de estabilización se desarrolla y alcanza su plenitud una vez pacificado el territorio.
—El escenario físico es particularmente inhóspito y carente de infraestructuras.
—La población sufre graves carencias, o simple inexistencia, con referencia a unos estándares mínimos de bienestar, en materia de transporte, vías de comunicación, energía, agua, sanidad e higiene.
—La sociedad se rige por códigos tribales y tradiciones o costumbres, sobre una base de interpretación rígida de los preceptos religiosos.
—No existe administración general o autoridad común que atienda a las necesidades mínimas de una sociedad estructurada: justicia, seguridad, educación, economía y finanzas, fomento, agricultura.
—Son sociedades donde, en muchas ocasiones, las diferencias se resuelven mediante el recurso a la violencia.

—Los primeros pasos en estos escenarios, terminadas las operaciones militares, corresponden también a la fuerza militar, que aún estará sobre el terreno y dispone de cierta capacidad residual para paliar o iniciar acciones en beneficio de la población.

Según lo expuesto, ¿por qué no indagar en la acción de España en el Protectorado de Marruecos? Pese a las diferencias, lo realizado allí incidía sobre la población y preparaba un mejor futuro para aquella sociedad, mediante la construcción de la paz, que no deja de ser la razón última de las actividades de estabilización.

2. Objetivos

Dado este marco introductorio donde es patente la necesidad de un estudio más detallado de la acción en el Protectorado como antecedente de las misiones actuales, nuestro objetivo principal es analizar la acción que el ejército español desempeñó en el protectorado de Marruecos entre los años 1927 y 1956. Los objetivos específicos se pueden agrupar en 2 apartados o fases que incluyen estos aspectos principales:

Fase 1: *Sanidad*

—Analizar las actuaciones sanitarias llevadas a cabo por el ejército en el periodo delimitado.
—Estudiar su mandato, construcción durante el protectorado
—Recopilar los posibles documentos gráficos de las acciones
—Analizar el desarrollo de estas acciones, su mantenimiento y posibles eventos asociadas a ellas (utilización, nuevas demandas, conflictos, …)
—Conocer el impacto social que tuvieron
—Intentar comprobar la incidencia que estas acciones tuvieron sobre la sanidad de la zona
—Conocer la permanencia o no de estas acciones una vez superado el protectorado

Vida social

—Analizar, desde una perspectiva sociohistórica la vida y dinámicas cotidianas de los militares españoles durante el periodo del protectorado español en Marruecos.

- Adaptación a los nuevos escenarios
- Relaciones familiares
- Enlaces y alianzas entre grupos sociales
- Dinámica e impacto de las relaciones cívico-militares

Fase 2: *Educación*

—Analizar las actuaciones educativas llevadas a cabo por el ejército en el periodo delimitado
- Construcción de escuelas u otro tipo de espacios
- Alfabetización y educación de la población
- Lenguas de alfabetización

—Empleo de recursos económicos y humanos
- Especial atención a la posible llegada de profesorado procedente de la península

—Recopilar los posibles documentos gráficos de las acciones
—Analizar el desarrollo de estas acciones
—Conocer el impacto social que tuvieron
—Comprobar la incidencia que estas acciones tuvieron sobre la educación de la zona
—Conocer la evolución y permanencia de estas acciones una vez terminado el protectorado

Infraestructuras

—Analizar la dotación de servicios esenciales durante el protectorado: vías de comunicación, obra civil, redes de saneamiento y agua potable, etc.
—Analizar la construcción de edificios públicos y de servicios (administrativos, colegios, mercados)
—Captación, transporte y aprovechamiento de fuentes de energía (electricidad, telefonía – telégrafo, etc.)
—Preparación de tierras de regadío: canalizaciones, drenajes, etc.

Todos estos objetivos se irán implementando a lo largo del proyecto pero para esta comunicación nos vamos a centrar en el diseño y validación del instrumento de recogida de información para archivos históricos militares, especialmente el caso de Ceuta y Melilla

3. Metodologia

Para dar cumplida cuenta de los objetivos de investigación se plantean el empleo de dos aproximaciones a la investigación: análisis de fuentes secundarias y el método biográfico. Aquí nos referiremos únicamente a la primera técnica.

El análisis de fuentes secundarias se está realizando a partir de los documentos recogidos en diferentes archivos históricos del ejército español. Fuentes de referencia son el Archivo General Militar de Madrid y el Centro de Historia Cultural y Militar del Ejército de Tierra, del cuál dependen los Archivos de Melilla y Ceuta. Se trataría, por tanto, de una investigación en la que se revisa, sistematiza y analiza diferente documentación recogida en forma de documentos – registros escritos y/o fotográficos relacionados con la acción del ejército español en el período contemplado (1927-1956).

Fotografía 1. Archivo Militar de Melilla

Fuente: Equipo de Investigación Proyecto Investigación COD.26
Centro Mixto UGR-MADOC

La investigación documental permite construir un marco conceptual referencial en relación al objeto de estudio, lo que ayudará a delimitar aspectos históricos, contextuales, así como de tipo normativo, organizacionales a la par que institucionales, de ahí la importancia de diseñar un instrumento para el registro de la información contenida en dichos archivos que permitan un posterior análisis eficaz y eficiente.

Tras la realización de algunas indagaciones, somos conscientes de la cantidad de documentación que hay disponible, así como los diferentes formatos y orígenes de la información con la que hay que trabajar. De ahí el interés por desarrollar un instrumento válido no ya para esta investigación sino para cualquiera que tuviera similares objetivos dentro del contexto de los archivos históricos militares en relación con las operaciones de estabilización.

Como ya hemos comentado, el instrumento (cuyo contenido presentamos en el apartado resultados) ha sido validado por el equipo de investigación. En este sentido cumple con criterios de validez y ha sido sometido a pruebas que así lo atestiguan. En primer lugar, es válido a los efectos del constructo que estamos tratando de medir, constructo que queda reflejado en los objetivos del proyecto al que responde esta investigación. Es decir, con la información que estamos recogiendo en las fichas preparadas a tal efecto podremos obtener información que nos ayude a dar cumplida cuenta de los objetivos de este estudio.

En este sentido, el instrumento de recogida de información permite la operacionalización mediante su sistematización de toda la información recogida en los archivos Militares de Ceuta y Melilla.

Este instrumento cuenta, por tanto, con lo que se conoce como validez de contenido. Es un tipo de validez de origen cualitativo que nos ayuda en enjuiciar la calidad del instrumento de medida. Esto es, los elementos que forman parte de él representan al constructo teórico que estamos midiendo en los términos en los que nos lo planteábamos en el proyecto de investigación. Así, el equipo de investigación desplazado a los archivos ha establecido que, con ese instrumento obtendremos información para conocer el papel del Ejército Español en el período del Protectorado contemplado así como para poder inferir elementos de asimilación con las operaciones de estabilización que se realizan en la actualidad.

En todo caso, ¿cuál ha sido el procedimiento de validación empleado? El primer paso dado por el equipo de investigación consistió en centrar bien cuáles eran los objetivos que, en concreto, queríamos responder mediante la información que se podía obtener de estos archivos. Es decir, analizamos bien nuestro proyecto desde el punto de vista conceptual. A partir de ahí, se estudió el tipo de temas que necesitaríamos encontrar

para dar respuesta a esos objetivos. El siguiente paso consistió en elaborar un primer borrador de dicha ficha de recogida de información por parte del equipo desplazado, en concreto, al Archivo de Melilla a partir de la revisión inicial de un conjunto aleatorio de expedientes-archivos. Dicho borrador fue revisado por el conjunto del equipo investigador (dando así cumplida cuenta de un criterio de calidad y de evaluación del instrumente que consiste en someterlo al juicio de terceras personas que no han participado directamente en la primera elaboración). Una vez revisado se aplicó de manera piloto con alguno de los expedientes que ya estaban a nuestra disposición. De esa forma pudimos ir ajustando la capacidad de dicho instrumento para poder conseguir con él la información esperada. Así los ítems —apartados se han conseguido ajustar de tal forma que, todos y cada uno de los expedientes pueden aportan información al objeto de investigación.

4. Resultados

Durante estos meses se ha desarrollado una continua labor de documentación y análisis de los documentos encontrados, siendo especialmente intensa en los archivos de Melilla. En un primer momento la tarea que se afrontó era comprender la sistematización y archivo de la documentación de estos archivos, para, posteriormente, diseñar el instrumento de recogida que mejor se adaptara tanto a la propia dinámica de los archivos militares como a los objetivos de nuestra investigación, tal y cómo hemos señalado con anterioridad.

4.1. *Los archivos de Melilla y Ceuta*

El archivo de Melilla es el Archivo Intermedio Militar, cuya titularidad estatal tiene una gestión por parte del Ejercito de tierra (Ministerio de Defensa). Este archivo se creó en 2003, ejerciendo como coordinador de los Archivos centrales de las UCOS (Unidades, Centros y Organismos) del Ejército de Tierra en Melilla, al igual que de la Delegación de Defensa. Sin embargo, los fondos históricos de la Comandancia General de Melilla (hasta 1927) se hallan en el Archivo General Militar de Madrid. Este archivo depende orgánica y funcionalmente del Instituto de Historia y Cultura Militar.

El archivo de Melilla se clasifica en cuatro áreas: Mando y administración territorial; Unidades de la fuerza; Apoyo a la fuerza; y reclutamiento.

Para tener una idea del volumen de cajas que supone el archivo de Melilla, hay que considerar que el área de Mando y Administración Territorial posee 2.264 cajas; Unidades de la fuerza, 1669 cajas; Apoyo a la fuerza tiene 354 cajas; y Reclutamiento son 13. En total el archivo dispone de 4.300 cajas.

Fotografía 2. Ejemplo de disposición de la información en el Archivo de Melilla

Fuente: Equipo de Investigación Proyecto Investigación COD.26 Centro Mixto UGR-MADOC

Por su parte, el archivo de Ceuta se crea en 1968, denominándose «Archivo regional militar de Ceuta». Su origen está relacionado con la necesidad de archivar la documentación procedente del ya extinguido Ejército del norte de África (E.N.A.) perteneciente a la Alta Comisaría de España en Marruecos y de la Comandancia militar de Ceuta. Según informa el propio ministerio de Defensa, la primera ubicación de este archive fue el Acuartelamiento «El revellín» , ya desaparecido. Se trasladó después a la Agrupación Logística núm. 23 en el acuartelamiento «El otero» y una vez más mudó a la antigua «Fábrica de Harinas» del ejército. Su sede final, terminado el traslado en 2009, es el acuartelamiento

«González Tablas», una vez se creó el Centro Regional de Historia y Cultura Militar por la Comandancia General de Ceuta.

El de Ceuta es un archivo intermedio del subsistema archivístico del Ejercito de tierra, ejerciendo de coordinador, receptor y custodio de los archivos centrales de las unidades, centros y organismos (UCOs) de la Comandancia General de Ceuta.

El archivo de Ceuta se divide en cinco áreas: Mando y administración territorial; Unidades de la fuerza; Apoyo a la fuerza; Reclutamiento; y Fondos de la justicia militar.

La cantidad de cajas que contiene el archivo son las siguientes. En el área de Mando y Administración Territorial, 7.549 cajas y 4.428 legajos; en Unidades de la Fuerza, 475 cajas y 6.921 legajos; en Apoyo a la Fuerza, 330 cajas y 314 legajos; en Reclutamiento, 27 cajas; y en Fondos de la Justicia Militar, 2.483 cajas. En total, pues, el archive de Ceuta atesora la cantidad de 10.864 cajas y 11.663 legajos.

4.2. *La construcción del instrumento de recogida de información*

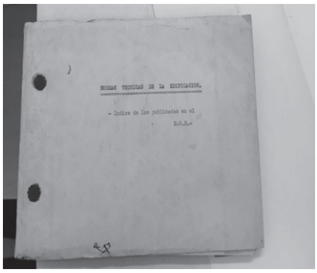
El actual director del Centro de Historia y Cultura Militar de Melilla es el Coronel D. José Félix Moreno Belmonte. Establecimos contacto con él para poder entrar y no ha habido ningún problema en tener, a nuestra entera disposición, el Archivo Militar para lo que quisiéramos investigar. Esto hay que destacarlo como un aspecto muy positivo para la investigación. Además existe la posibilidad, para cualquier ciudadano, de si desea solicitar información de cualquier tema de ámbito militar, enviar un correo a *centro_historia_cultura_militar_melilla@et.mde.es* solicitando información y ellos te envían una solicitud para rellenar, dándote de alta en una base de datos donde envían información periódica al respecto. Hay que decir que esta disposición por parte del ejército en materias para investigar, es poco conocido por la población en general y habría que potenciar más su conocimiento pues resulta muy beneficioso tanto para los investigadores especializados como para el público en general. En muchas ocasiones, pensando que la temática es militar, se cree que existirán mayores dificultades o impedimentos, pero muy al contrario, es información accesible y disponible sin grandes complicaciones.

Una vez se tuvo acceso a los Archivos, se abrieron cajas aleatoriamente, para comprobar que tipo de información contenían y

como se estructuraban. La unidad «caja» no ofrecía más información que la del soporte físico, pero poco sabíamos del contenido real de cada una de esas cajas.

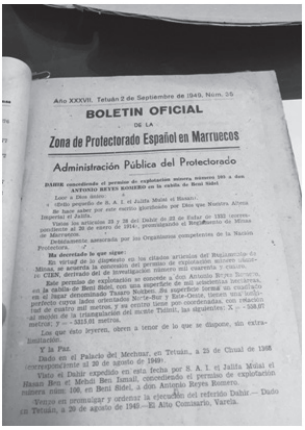
Con este «muestreo» de cajas se elaboró un primer borrador de ficha de registro de datos que posteriormente se ha ido perfeccionando una vez se abrieron y revisaron las cajas de una forma más sistemática, siguiendo el procedimiento de validación presentado en la metodología.

Fotografía 3. Ejemplo de expediente



Fuente: Equipo de Investigación Proyecto Investigación COD.26
Centro Mixto UGR-MADOC

Fotografía 4. Ejemplo de expediente

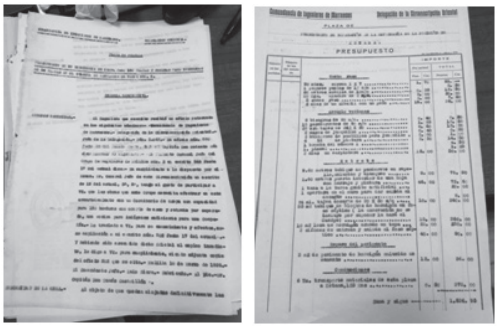

Año XXXVII. Tetuán 2 de Septiembre de 1949. Núm. 35

BOLETIN OFICIAL
DE LA
Zona de Protectorado Español en Marruecos

Administración Pública del Protectorado

Fuente: Equipo de Investigación Proyecto Investigación COD.26
Centro Mixto UGR-MADOC

Fotografía 5. Ejemplos de expediente



Fuente: Equipo de Investigación Proyecto Investigación COD.26
Centro Mixto UGR-MADOC

Finalmente, la ficha que como instrumento se ha diseñado y cumple de forma exhaustiva con toda la documentación encontrada, contiene los apartados siguientes:

1. Área:

Es la información acerca del área donde la información se engloba. En el proyecto se definieron 4 áreas: Sanidad, educación, infraestructuras y vida social. Cada ficha indica el área de la que forma parte. Para que la información sea acorde al proyecto debe estar englobada dentro de planes de estabilización y con una utilidad social, aunque sea secundaria. Por ejemplo, en infraestructuras, la construcción de cuarteles no se considera dentro del proyecto. Sin embargo, por poner un ejemplo, la construcción de depósitos en cuarteles pero cuyas aguas luego iban a riegos si se consideran.

2. Archivo:

El Archivo del que proviene la información. Por ahora el de Melilla y Ceuta pero será complementado con información de Archivos como el de Madrid o Ávila.

3. Institucion:

La institución que genera la información y es responsable de la acción que se vaya a realizar. Por ejemplo, en muchas casos de Melilla es la Comandancia de Obras.

4. Asunto:

Resumen del asunto sobre el que el expediente trata.

5. Fecha:

La fecha de la información.

6. Plaza de:

El lugar concreto donde la acción tiene lugar

7. Importe total:

Coste total de la acción que se va a realizar.

8. Órdenes recibidas (Resumen):

Un resumen de la orden, donde generalmente viene la procedencia concreta del inicio de la acción realizada

9. Necesidad de la obra (Resumen):

Muy interesante desde el punto de vista social es conocer la necesidad y justificación de la obra, lo que nos da una información privilegiada de los motivos que causaron la acción.

10. Descripción (Resumen):

Breve descripción de cuál es exactamente la labor que se va a llevar cabo.

11. Duración:

Tiempo estimado de duración de la acción.

12. Lugar de la obra:

Lugar exacto donde va a ejecutarse la acción.

13. Existen planos:

Respuesta afirmativa o negativa sobre la existencia de planos en el Archivo, que luego pueden ser consultados para conocer con mayor detalle el trabajo realizado.

ARCHIVO: Melilla
INSTITUCION: Delegación de Economía, Industria y Comercio
ASUNTO: Decreto Visirial autorizando a D. Antonio Borras para instalar en Tetuán una fábrica de azúcar de pilón

FECHA: 20 de septiembre de 1949
PLAZA DE: Tetuán
IMPORTE TOTAL: Lo que genere para el particular interesado.
ORDENES RECIBIDAS (Resumen): Vista la instancia y documentación presentada por D. Antonio Borrás Esteve, solicitando autorización para instalar en Tetuán una fábrica de azúcar de pilón con capacidad de producción de 18.000 kgs de azúcar diarios y 7440 de melaza. Visto el reglamento de nuevas industrias, ampliación, transformación y traslados de las existentes, debidamente asesorado por los Organismos competentes de la Nación Protectora se autoriza la instalación.

DESCRIPCION (Resumen): Condiciones para la Instalación:
Se autoriza la instalación de acuerdo a las siguientes condiciones:
1.- La presente autorización solo es válida para el concesionario, no pudiendo ser cedida o negoliada.
2.- La instalación de la industria y sus elementos tendrán que ajustarse en todas sus formas al proyecto presentado
3.- El plazo de puesta en marcha salvo fuerza mayor es como máximo de catorce meses tras la publicación de esta autorización ante la Inspección de Industria.
4.- Esta autorización no lleva implícita la importación de maquinarias, materias primas o elementos de trabajo. No se compromete pues la Administración a la aprobación sistemática de las peticiones de importación de azúcar centrífuga cruda que necesite la nueva industria, ni a la de azúcar pilón, que se acomodarán a las normas y circunstancias que sean de aplicación al solicitaria.
5.- El azúcar pilón a obtener en la nueva industria, habrá de tener siempre un precio de venta en fábrica no superior al que tenga en almacén, en igualdad de calidad, el pilón de fabricación española.
6.- Esta autorización no presupone exclusiva de venta alguna.
7.- La fábrica está sujeta a la intervención fiscal del Servicio de Aduanas en lo que se refiere a asegurar la legal percepción de los impuestos interiores de consumo
8.- La Administración se reserva el derecho de dejar sin efectos la presente autorización en el momento en que se presente y demuestre el incumplimiento de cualquiera de los preceptos anteriores.

DURACION: Como máximo 14 meses

LUGAR DE LA OBRA: Tetuán

EXISTEN PLANOS: NO

Documento 1. *Ejemplo de ficha cumplimentada*

Fuente: Equipo de Investigación Proyecto Investigación COD.26
Centro Mixto UGR-MADOC

5. Conclusiones

Esta sería la ficha que se ha validado y se ha demostrado como un instrumento excepcional para recoger información de forma sistemática de los archivos y asuntos que el proyecto plantea.

En cualquier caso, durante la realización de este proyecto se están hallando aspectos positivos y algunas dificultades que, por último, se quieren detallar. Un primer aspecto positivo a destacar es la disposición excelente para brindarnos información por parte del Ejercito y los encargados a todos los niveles. Otro aspecto positivo ha sido el hallazgo, dentro del archivo, de los Boletines trimestrales durante el periodo que estamos investigando, es decir, durante el Protectorado Español. En dichos boletines, encontramos información sobre toda las actuaciones que los militares

desarrollaban durante ese periodo y cómo repercutía directa o indirectamente a la ciudadanía indígena de la zona.

La principal dificultad y única, podríamos decir, ha sido que nos hemos encontrado muchísima información pero sin estar en una buena base de datos informatizada, es decir**,** ausencia de una base de datos formalizada en fechas, temáticas, etc. Esto nos ha generado, al principio, una desorientación en la búsqueda de información al respecto, ya que no podíamos seguir una línea en el tiempo, lo que nos ha llevado a realizar indagaciones más minuciosas en dichas búsquedas.

Es por esto, como conclusión, que se ha querido con este trabajo dar a conocer el proyecto realizado, con sus objetivos y metodología, y muy especialmente el instrumento de recogida. Con ello creemos que futuros investigadores tienen un recorrido realizado que le será muy útil en sus investigaciones.

LA ACTIVIDAD RESERVISTA AL SERVICIO DE LA CULTURA DE DEFENSA Y LA SEGURIDAD NACIONAL

Maújo Iglesias, Benigno Antonio
Díaz de Otazú Guerri, Francisco
López Díaz, José Antonio

Asociación ARES de Reservistas Españoles (Asturias), Delegación de Defensa en el Principado de Asturias

Resumen

La Reserva Militar de Voluntarios es una institución óptima para contribuir a la cultura de la defensa y la seguridad nacional, en especial cuando sus componentes no están activados, al ser difusores de las mismas en los ámbitos civiles donde se desenvuelven. Para ello es clave la organización de esfuerzos, definiendo una estrategia colectiva que encauce las diferentes acciones en torno a una visión y una misión compartidas. Se analiza todo ello, partiendo del estudio de campo del trabajo desarrollado en el trienio 2014-2016 por la asociación ARES en Asturias, en colaboración con la Delegación de Defensa: elaboración del documento estratégico, planes anuales de acción e indicadores de evolución (incremento de asociados; visibilidad social; impactos en medios de comunicación; actividades culturales y de formación militar).

Palabras claves

Reserva Voluntaria, Cultura Defensa, Seguridad.

1. Introducción

Los Reservistas Voluntarios son españoles que, en el ejercicio del derecho y el deber de defender a España, se vinculan de forma temporal y voluntaria con las Fuerzas Armadas, asumiendo un compromiso de disponibilidad para ser llamados a filas. Para ello ofrecen voluntariamente parte de su tiempo a las Fuerzas Armadas y aportan los conocimientos y la experiencia profesional adquirida en la vida civil, con una clara vocación de servicio y de entrega.

Pese a que la RV se haya creado formalmente por la Ley Orgánica 5/2005, de 17 de noviembre, de la Defensa Nacional,[1] encuentra su fundamento en la propia Constitución Española de 1978, en concreto en su artículo 30 al afirmar el derecho y el deber de los españoles de defender a España.[2]

El Reservista Voluntario encuentra sus antecedentes en la figura del voluntario que, con unas u otras singularidades propias de cada época histórica, ha existido desde siempre en la azarosa y bélica vida de España. En la monografía del Centro Superior de Estudios de la Defensa (CESEDEN) titulada *«De la milicia concejil al Reservista, una historia de generosidad»,* se recogen con detalle y amplitud los que, salvando distancias podrían ser considerados como antecedentes de una figura similar a la actual Reserva Voluntaria.[3]

Lo que ha dado en llamarse cultura de defensa, asociada a la seguridad nacional, es un campo muy propicio para el trabajo de los Reservistas Voluntarios, merced a su doble condición de militares cuando están activados y de civiles comprometidos con las Fuerzas Armadas cuando no lo están. Esa importante misión debe estar informada por los principios clásicos de la eficiencia y la eficacia en cada actuación, y para ello se considera que es primordial la organización y canalización de esfuerzos, al margen de una simple actitud voluntarista y de esfuerzos individuales, siempre loables pero escasamente rentables desde un punto de vista social. De tal manera que los Reservistas cumplirán mucho mejor la misión que les compete dentro de la defensa y la seguri-

1. BOE núm. 276, de 18 de noviembre de 2005. Artículo 29: «La aportación de otros recursos provenientes de la sociedad, se materializará de la siguiente forma: a) De acuerdo con el derecho y el deber que los españoles tienen de defender a España, según lo establecido en el artículo 30 de la Constitución, la incorporación adicional de ciudadanos a la Defensa se apoyará en el principio de contribución gradual y proporcionada a la situación de amenaza que sea necesario afrontar, en la forma que establezca la ley, mediante la incorporación a las Fuerzas Armadas de los reservistas que se consideren necesarios. b) La contribución de los recursos materiales a las diversas necesidades de la defensa se efectuará a través del órgano interministerial competente. Su composición y funciones se establecerán reglamentariamente».

2. Artículo 30.1*:*«Los españoles tienen el derecho y el deber de defender a España».

3. Centro Superior de Estudios de la Defensa, De la milicia concejil al Reservista, una historia de generosidad. (Madrid: CESEDEN) 2008.

dad nacional —básicamente en sus períodos de no activación— si están organizados que si no lo están.

2. El reservista voluntario

2.1. *Qué es un reservista*

La citada Ley Orgánica 5/2005, de 17 de noviembre, de la Defensa Nacional, que al establecer la incorporación adicional de ciudadanos a la defensa nacional, crea la figura del Reservista, tiene su antecedente en la derogada Ley 17/1999, de 18 de mayo, de Régimen del Personal para las Fuerzas Armadas[4]. En ésta, definía a los Reservistas como los españoles que podrían ser llamados a incorporarse a las Fuerzas Armadas para satisfacer las necesidades de la defensa nacional, clasificándolos en temporales, voluntarios y obligatorios.

La Ley 8/2006, de 24 de abril, de Tropa y Marinería[5], creó la figura del Reservista de Especial Disponibilidad, integrada por los militares profesionales de estos empleos al acabar sus compromisos de larga duración.

Y por último, la Ley 39/2007, de 19 de noviembre, de la Carrera Militar[6] señala que los Reservistas susceptibles de incorporarse a las Fuerzas Armadas en situaciones de crisis, son los Reservistas Voluntarios, los de Especial Disponibilidad y los Reservistas obligatorios, destacando la importancia de los primeros e impulsando esta figura. Además de lo anterior, esta Ley establece la posibilidad que tienen los militares de complemento y los profesionales de Tropa y Marinería que renuncien a su condición de militares (hay muchas circunstancias personales, laborales y familiares que motiven tan dolorosa decisión para un militar, sin perder por ello un ápice de su compromiso con la Nación) de continuar vinculados a las Fuerzas Armadas haciéndose Reservista.

Señala asimismo el orden de «llamamiento» o de incorporación ante una situación de crisis donde las necesidades de la defensa nacional no pueden satisfacerse con los profesionales. Los primeros, los Reservistas Voluntarios y los de Especial Disponibilidad bastando la decisión del Consejo de Ministros. Y sólo si

4. BOE núm. 119, de 19 de mayo de 1999.
5. BOE núm. 98, de 25 de abril de 2006.
6. BOE núm. 278, de 20 de noviembre de 2007.

aún no fuera suficiente, con la autorización del Congreso de los Diputados, los Reservistas obligatorios.

Y finalmente, en ejecución del necesario desarrollo reglamentario de la Ley, por medio del Real Decreto 383/2011, de 18 de marzo, se aprueba el Reglamento de Reservistas de las Fuerzas Armadas[7].

Se trata de la norma fundamental de la Reserva Voluntaria y a ella hay que remitirse para analizar la definición de Reservista, su clasificación, la forma de acceso, la formación, las activaciones, compromiso de permanencia y sus ampliaciones, empleos y ascensos, situaciones, entre otros contenidos.

De esta forma, son Reservistas los españoles que en aplicación del derecho y el deber de defender a España —artículo 30 de la Constitución— pueden ser llamados a incorporarse a las Fuerzas Armadas para participar en las misiones que correspondan legalmente.

2.2. *Clases de reservistas*

Pese a que el objeto del trabajo se centra en el Reservista Voluntario, por ser la figura más emblemática y mayoritaria entre el colectivo de Reservistas en general, hay varias clases. El artículo 2 del Reglamento señala las siguientes:

a) Reservistas Voluntarios: los españoles que sean seleccionados tras la correspondiente convocatoria pública, que superen los períodos de formación militar básica y específica y que se vinculen de manera temporal y voluntaria con las Fuerzas Armadas por un compromiso de disponibilidad. De esta definición se desprenden las dos notas más características de los Reservistas Voluntarios: voluntariedad y disponibilidad.
b) Reservistas de especial disponibilidad: los militares de Tropa y Marinería y los militares de complemento que adquieran dicha condición al acabar sus compromisos de larga duración.
c) Reservistas obligatorios: los españoles con una edad entre los diecinueve y los veinticinco años, declarados como tales por el Gobierno de acuerdo a la normativa de aplicación.

7. BOE núm. 70, de 23 de marzo de 2011.

2.3 *Requisitos para ser reservista voluntario*

Hay una convocatoria pública en el Boletín Oficial de Defensa (en adelante, BOD)[8], generalmente en el mes de septiembre de cada año, aprobada por el Subsecretario de Defensa tras la aprobación por el Consejo de Ministros de la provisión anual de plazas de las Fuerzas Armadas, que incluye el número máximo de Reservistas Voluntarios para cada año. Será el Ministro de Defensa quien fijará la distribución de efectivos entre el Ejército de Tierra, Ejército del Aire, la Armada y los Cuerpos Comunes de las Fuerzas Armadas.

Lógicamente, todo español podrá optar a las plazas de Reservista Voluntario que se ofrezcan en cada convocatoria anual, de acuerdo a los principios de igualdad, mérito y capacidad, así como los demás principios rectores para acceder a un empleo público. Estos son los requisitos generales para el acceso:

a) nacionalidad española
b) tener dieciocho años cumplidos y no alcanzar la edad máxima de los cincuenta y ocho años para los empleos de Oficial y Suboficial, y de cincuenta y cinco años para Tropa y Marinería
c) no tener antecedentes penales
d) no estar procesado o imputado en algún procedimiento judicial por delito doloso
e) no estar privado de los derechos civiles
f) no haber sido separado del servicio por expediente disciplinario en cualquier Administración Pública, ni estar inhabilitado con carácter firme para la función pública
g) aptitud psicofísica necesaria según la convocatoria, para el personal de las Fuerzas Armadas
h) no haber resuelto el compromiso como Reservista Voluntario con anterioridad, ni como militar de complemento ni como militar profesional, por las causas legales señaladas

8. Resolución 452/38137/2015, de 23 de septiembre, de la Subsecretaría de Defensa, por la que se convoca proceso de selección para el acceso a la condición de reservista voluntario de las Fuerzas Armadas. BOE núm. 232, de 28 de septiembre de 2015. La convocatoria para 2016 previsiblemente salga de manera inminente en los primeros días de octubre, muy similar a la de 2015 en cuanto a número de plazas y requisitos.

i) no haber sido denegada la ampliación del compromiso como Reservista Voluntario.
j) no ser militar profesional, Guardia Civil o personal estatutario de los servicios de inteligencia nacionales.

En cada convocatoria se relacionan en Anexo, las plazas ofertadas y los requisitos de cada una de ellas (titulación, experiencia y otros requisitos), así como la unidad y localización correspondiente.

Para los empleos de Oficial se exige titulación universitaria con carácter general; para Suboficial, título de Bachiller o formación profesional de grado superior; y para Tropa y Marinería, el graduado en educación secundaria obligatoria o equivalente.

Tras las pruebas selectivas señaladas en cada convocatoria, los seleccionados ordenados por puntuación, son nombrados aspirantes y se proponen para realizar el período de formación militar básica y la formación específica (ya en la unidad correspondiente a la plaza asignada), con la finalidad de capacitarles militarmente para poder desempeñar sus funciones en el área de trabajo y cometido de la plaza obtenida. La primera fase tiene una duración de treinta días y la segunda dependerá del grado de adecuación de la profesión civil del aspirante a la plaza obtenida, sin que exceda nunca de treinta días.

2.4. *Compromiso inicial y posibles ampliaciones*

El Reservista Voluntario firma un compromiso inicial de tres años, a contar desde la publicación de la resolución de su nombramiento. Excepcionalmente cabe que sea sólo un año, en situaciones de crisis cuando el Consejo de Ministros decrete su incorporación.

De igual forma, podrán ampliar el compromiso inicial, por períodos de tres años, siempre que no se rebase la edad máxima de sesenta y un años para oficiales y suboficiales y cincuenta y ocho años para tropa y marinería.

La concesión de la ampliación de compromiso requiere la superación del preceptivo reconocimiento médico, conforme al reglamento de aptitud psicofísica del personal de las Fuerzas Armadas. Así como los informes favorables de su Unidad y de la Delegación de Defensa de la que dependa el Reservista Voluntario.

Además, la segunda ampliación requería haber sido activado, al menos, una vez en los últimos tres años y tres veces en los últimos

seis. Esta exigencia conllevó la pérdida de la condición como Reservista de varios de ellos, al coincidir con una etapa donde las activaciones prácticamente no existían. La misma Administración que tenía potestad para conceder la activación era la que expulsaba al Reservista por falta de activaciones, sin que el Reservista pudiera hacer nada salvo solicitar una y otra vez ser activado. Esta clara disfunción fue corregida por el Real Decreto 176/2014, de 21 de marzo, por el que se regula el procedimiento para la tramitación de las iniciativas y quejas relativas al régimen de personal y a las condiciones de vida que pueda plantear el militar[9]. No obstante, mientras estuvo vigente, más de setenta Reservistas Voluntarios perdieron su condición por no haber sido activados, contra su voluntad expresa[10].

2.5. *Empleos y ascensos*

Los Reservistas Voluntarios tendrán inicialmente los empleos de Alférez (RV) o Alférez de Fragata (RV), Sargento (RV) y Soldado (RV) o Marinero (RV), según la categoría a la que hayan accedido en la correspondiente convocatoria.

Posteriormente, podrán alcanzar los empleos siguientes:

a) Oficiales: Teniente (RV)/Alférez de Navío (RV) y Capitán (RV)/Teniente de Navío (RV)
b) Suboficiales: Sargento Primero (RV) y Brigada (RV)
c) Tropa y Marinería: Cabo (RV) y Cabo Primero (RV)

Para que se produzca el ascenso han de concurrir las siguientes condiciones:

a) Seis años en el empleo anterior y acreditar un mínimo de sesenta días de activación, sea prestación de servicio o formación.
b) Informe favorable por el Jefe de la Unidad y por el Delegado de Defensa del que dependa.

9. BOE núm. 84, de 7 de abril de 2014.

10. https://cisde.es/observatorio/defensa-rectifica-ya-no-tendra-que-echar-a-sus-reservistas-por-no-haberlos-activado.

Aún hoy siguen a la espera de una solución. Se han planteado varias demandas ante la jurisdicción de lo contencioso-administrativo. Desde ARES se llegó a enviar al Ministerio de Defensa una propuesta de disposición que les devuelva a su condición de Reservista Voluntario.

c) Haber aceptado y realizado todas las activaciones para seguir los programas de formación continuada para las que fue requerido, durante los años de permanencia necesarios para el ascenso. No se tendrán en consideración las no realizadas por las causas de suspensión de incorporación previstas en este reglamento.
d) No haber sido separado del servicio, mediante expediente disciplinario, de cualquiera de las Administraciones Públicas, ni hallarse inhabilitado con carácter firme para el ejercicio de la función pública.
e) Haber sido declarado Apto en la preceptiva evaluación para el ascenso.

2.6. *Activaciones*

El término «activación» se corresponde con la situación del Reservista Voluntario cuando presta servicios, o recibe formación o adiestramiento, en las Fuerzas Armadas, ya sea en su Unidad o en otra diferente. Previamente a la activación, debe pasarse un reconocimiento médico de aptitud.

Los Reservistas Voluntarios podrán permanecer, como máximo, en la situación de activados treinta días al año si es para participar en programas de formación continuada; y si fuese para prestar servicio, el tiempo señalado para la propia activación.

Mientras estén activados, tendrán condición militar a todos los efectos, deberán cumplir las reglas de comportamiento militar y estarán sujetos a las leyes penales y disciplinarias militares, así como al régimen de personal correspondiente. Y por supuesto tienen el derecho y el deber de usar el mismo uniforme que los militares profesionales de su empleo y unidad, con el distintivo de Reservista Voluntario.

Mientras no estén activados, permanecen en situación de disponibilidad. Y puesto que las Delegaciones de Defensa contactan periódicamente con ellos para mantener actualizada la información, asumen la obligación de comunicar todos los cambios de domicilio, en el plazo de un mes.

2.7. *Derechos y deberes*

Conforme al artículo 43 del citado Reglamento, cuando no están activados, tienen derecho en actos castrenses y sociales, al

uso del uniforme que les correspondan en razón a su empleo y Unidad, y para ello sólo deberán comunicarlo previamente a la Delegación de Defensa de adscripción.

El tiempo como Reservista Voluntario se considera como mérito para acceder a la enseñanza militar de formación en las Fuerzas Armadas, así como en los sistemas de selección respecto de los cuerpos, escalas, plazas de funcionario y actividades de carácter laboral de las Administraciones públicas, en todos los supuestos en que sus funciones guarden relación con los servicios prestados como Reservistas.

De igual manera tienen derecho a tarjeta de identificación militar para personal Reservista.

Respecto a los derechos económicos, durante el período de activación para prestar servicio, percibirán las retribuciones fijadas para los militares profesionales con empleo equivalente Y durante los períodos de instrucción y adiestramiento o cursos de formación y perfeccionamiento, percibirán una indemnización calculada sobre el salario mínimo interprofesional diario que va desde el doble del SMI hasta el triple, en función del empleo.

Asimismo, mientras dure su activación, se les aplicará el régimen de Seguridad Social establecido para los militares profesionales que mantienen una relación de servicios de carácter temporal.

2.2. *Asociaciones de reservistas*

La Ley 39/ 2007, de 19 de noviembre, de la Carrera Militar[11], en su articulo 124 señala que «Las Administraciones Publicas apoyarán a las asociaciones de reservistas que ayuden a mantener relaciones entre sus propios miembros y de la sociedad con sus Fuerzas Armadas». En su desarrollo el vigente Reglamento también las contempla en el artículo 5. Son aquéllas constituidas con personal Reservista, conforme a la normativa reguladora del derecho de asociación[12].

Las Administraciones Públicas tienen la obligación de apoyar el asociacionismo reservista como vía para mantener las relaciones entre sus miembros, con la sociedad y con las Fuerzas Armadas; para difundir la cultura de seguridad y defensa; para promover la

11. BOE núm. 278, de 20 de noviembre de 2007.

12. Ley Orgánica 1/2002, de 22 de marzo, reguladora del Derecho de Asociación. BOE núm. 73, de 26 de marzo de 2002.

renovación del juramento o promesa ante la Bandera de España; y para colaborar con los organismos militares en la participación de reservistas en actividades de carácter militar.

De igual manera se promoverán acuerdos y convenios con asociaciones de reservistas voluntarios y con la federación de todas ellas, participando en los foros internacionales de Reservistas en los que España tiene presencia.

A este respecto, aún continúa pendiente un procedimiento muy común en otros ámbitos de la Administración Pública con presencia de asociaciones, sindicatos u órganos similares de participación social, como es la realización de una auditoría de representatividad. De esta forma, con la certificación y posterior comprobación oficial de los asociados de cada asociación, es sencillo determinar la representatividad mayor o menor de la que goza cada una, huyendo de cualquier otro procedimiento más opaco, menos riguroso y muy poco veraz.

La Asociación ARES de Reservistas Voluntarios cuenta con casi setecientos asociados en España, siendo la más grande y hegemónica entre los Reservistas Voluntarios[13].

2.3. *Cultura de defensa y seguridad*

No existe una definición comúnmente aceptada de la cultura de defensa. Se usa y hasta se abusa del término, pero pocos de nuestros compatriotas podrían —aún hoy en día— definirla con más o menos precisión.

La cultura de defensa es mucho más que algo propio de militares o que los civiles aplaudan en los desfiles. Debe ser una

13. La Asociación ARES de Reservistas Españoles es la mayor asociación de Reservistas de España. Es una asociación de civiles con una profunda vocación militar y compromiso con las Fuerzas Armadas, con la misión de difundir los fines de la Reserva Militar de Voluntarios, de ayudar al mantenimiento de las relaciones entre nuestros propios miembros y de la sociedad con sus Fuerzas Armadas, de promover los valores de seguridad y defensa, y colaborar en la Defensa Nacional y en el establecimiento de una auténtica Cultura de Defensa en España. Está Inscrita en el Registro Nacional de Asociaciones con el número 585627, Grupo 1, Sección 1, y está amparada por la Ley 39/ 2007, de 19 de noviembre, de la Carrera Militar (BOE núm. 278, de 20 de noviembre de 2007). En su articulo 124 señala que «Las Administraciones Publicas apoyarán a las asociaciones de reservistas que ayuden a mantener relaciones entre sus propios miembros y de la sociedad con sus Fuerzas Armadas». www.ares.resvol.es

empresa conjunta, de un pueblo soberano y sano que conociendo su pasado —asumiéndolo y respetándolo—, conoce y también asume los riesgos del presente, proyectándolo al futuro en clave de compromiso colectivo. La cultura de defensa es el eje que da cobertura a nuestra forma de vida, a los valores propios de nuestra civilización y cultura. Y esto es tan serio e importante que no puede dejarse sólo en manos de una parte de la sociedad —de la que lleva uniforme—, puesto que nos compete a todos.

El Sargento Primero (RV) Santiago Carrasco Díaz-Masa, Presidente Honorífico de la Asociación ARES de Reservistas Españoles, afirma que la cultura de defensa puede resumirse en algo tan simple como que la sociedad civil adquiera la formación y la convicción necesarias para que apoye a las Fuerzas Armadas al mejor cumplimiento de su misión. Sin embargo, algo tan sencillo no se ha conseguido en España, pese a la positiva valoración que de las Fuerzas Armadas tienen los españoles.

El Sargento Primero (RV) Carrasco Díaz-Masa argumenta que el concepto va unido al modelo de Fuerzas Armadas que se quiera implantar. Y que un modelo adecuado para España es sin duda alguna el modelo de Fuerzas Armadas profesionales, que España tiene sobre el papel pero del que carece en la práctica. Señala que a su juicio, al modelo le faltan tres de las cuatro columnas necesarias: la industria de defensa, el personal civil al servicio de las Fuerzas Armadas y por último la Reserva Militar. La columna representada por el militar profesional, y principal del modelo, es insuficiente para soportar por sí sola el peso del modelo, la superficie y la población a la que debe servir[14].

14. «La industria de defensa atraviesa grandes dificultades cuando no es desmantelada, a causa entre otras razones, de la delgadez de la primera columna y la repercusión que esto tiene para la I+D, factor clave para tener éxito comercial extra fronteras. El personal civil al servicio de las FFAA no goza en la mayoría de los casos de la confianza, la consideración y la retribución necesarias para sentirse implicado en la defensa nacional. Y por último la Reserva Militar, columna imprescindible en el modelo de Fuerzas Armadas Profesionales, sin la cual simplemente no existen Fuerzas Armadas Profesionales, está aún por implantar. España carece de un contingente de Reserva Militar suficiente, instruido e integrado en este modelo profesional de cuatro columnas imprescindibles todas ellas para garantizar la defensa de la nación». Presentación de Santiago Carrasco Díaz-Masa en José Antonio López Díaz, La Reserva Militar Voluntaria en España: urdimbre y retroprogresión (Oviedo: AC Ediciones, 2014). Prólogo.

Por su parte, el Alférez de Fragata (RV) José Antonio López Díaz, afirma que en España no sólo falta cultura de defensa, sino que lo que también falta y es ello mucho más preocupante, es el concepto básico de Nación. Y que uno de los grandes problemas es precisamente el desconocimiento de las diferencias entre Nación y Estado, relacionado éste con el poder.[15]

El mismo autor señala que por ello el ejército forma parte de la defensa de la Nación y no del Estado. «Es parte de la defensa del dominio, de la soberanía del pueblo sobre el territorio y todo lo demás. Pues la defensa de la Nación es la defensa del pueblo y del territorio, para eso es para lo que está el ejército»[16].

Relacionado con este concepto, la defensa nacional era definida en la Ley Orgánica 6/1980, de 1 de julio, por la que se regulan los criterios básicos de la Defensa Nacional y la Organización Militar, como «la disposición, integración y acción coordinada de todas las energías y fuerzas morales y materiales de la Nación, ante cualquier forma de agresión, debiendo los españoles participar en el logro de tal fin. Tiene por finalidad garantizar de modo

15. «No sólo falta cultura de defensa, sino que faltan conceptos básicos de lo que es la Nación. Así, el derecho y el deber de defender a España es un acto coherente con la defensa de la nación, pero el problema ese gran desconocimiento de este país sobre la materia, la nación no tiene nada que ver con el estado. La nación tiene que ver con un dominio, con un territorio, con sus gentes. El punto esencial es que el sujeto soberano de la nación es el pueblo. Sería un autodominio: es el pueblo el que ejerce su autodominio sobre un territorio, una cultura y unas instituciones. No tiene nada que ver la nación, con el poder; es el estado el que tiene que ver con el poder. Ahí está, probablemente, unos de los problemas que tenemos que resolver en España. Un problema de ignorancia, de confundir elementos de poder con objetos de dominio. El dominio no pertenece al rey, no pertenece al gobierno, no pertenece al estado. El dominio, el propietario de la nación, es el pueblo. Esa es la cuestión». José Antonio López Díaz, La Reserva Militar Voluntaria en España: urdimbre y retroprogresión (Oviedo: AC Ediciones, 2014), 9.

16. «En resumen: la Nación se debe entender, en nuestro ordenamiento donde la soberanía reside en el pueblo español, como el sujeto de todo el proceso. La nación es un concepto de dominio. La nación tiene que ver con la soberanía y la soberanía tiene que ver con el pueblo; por decirlo de alguna forma: la Nación es la urdimbre y el Estado sería el poder. El ejército al menos en nuestro sistema, en nuestra Constitución, no está para defender al estado; sí lo está en cuanto a producto de la nación, no como producto del poder». José Antonio López Díaz, La Reserva Militar Voluntaria en España: urdimbre y retroprogresión (Oviedo: AC Ediciones, 2014), 10.

permanente la unidad, soberanía e independencia de España, su integridad territorial y el ordenamiento constitucional»[17].

Una definición plena de sentido, que reafirma la misión colectiva de todos los españoles, como un deber, poniendo todos los recursos materiales y morales al servicio de la unidad y la independencia de la Patria.

Tanto la normativa posterior como los sucesivos documentos sobre Defensa (Directivas de Defensa Nacional, revisiones estratégicas, Planes directores,…) hacen hincapié en la necesidad que la sociedad española comprenda, apoye y se comprometa con el objetivo de la seguridad, al que sirve la defensa, y que constituye junto a la libertad y la justicia uno de los pilares del Estado de Derecho[18].

Por lo que se refiere a la seguridad nacional, hay que remitirse a la importante Estrategia de Seguridad Nacional (ESN, en adelante), elaborada en 2013 en el Departamento de Seguridad Nacional de Presidencia del Gobierno. Define de forma integral a la seguridad nacional, como «la acción del Estado dirigida a proteger la libertad y el bienestar de sus 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*»[19].

Tiene carácter de servicio público, objeto de una política de Estado que reclama el compromiso y la responsabilidad al más alto nivel, quedando bajo la dirección y el liderazgo del Presidente del Gobierno, e implicando a todas las estructuras del Estado, a todas las Administraciones Públicas y también a toda la sociedad.

Por lo tanto el compromiso de la seguridad nacional también nos compete a todos y, en su garantía, el apoyo y la colaboración de los españoles resulta imprescindible. Como señala la ESN debe abordarse bajo el principio de la unidad de acción. Esta unidad

17. *BOE* núm. 165, de 10 de julio de 1980 (vigente hasta el 8 de diciembre de 2005). artículo 2.

18. Pedro Bernal Gutiérrez, La cultura de seguridad y defensa en España. Sus orígenes y evolución, en La cultura de seguridad y defensa, un proyecto en marcha. Cuadernos de Estrategia 155. (Madrid: Ministerio de Defensa. Instituto Español de Estudios Estratégicos, 2011), 29-31.

19. Estrategia de Seguridad Nacional. Un proyecto compartido. Acuerdo del Consejo de Ministros de 7 de junio de 2013. (Madrid, 2013), 7.

se caracteriza por la visión integral de la seguridad nacional, con la participación de todos los agentes de interés, su coordinación y su gestión armónica de forma que se garantice la optimización de los recursos disponibles, la eficacia y eficiencia del sistema.

Esta es una de las grandes utilidades de la Reserva Voluntaria (RV) o Reserva Militar de Voluntarios, ya que el Reservista no deja de ser un civil que se convierte en militar por un tiempo determinado —cuando está activado— y cuando no lo está, continúa su relación con las Fuerzas Armadas al estar en situación de disponibilidad.

2.4. *Experiencia de la delegación de ares en asturias 2014-2016*

Hasta aquí se ha expuesto qué es la figura del Reservista Voluntario —aún desconocida para una gran parte de nuestros compatriotas—; los conceptos de cultura de defensa y seguridad nacional; la obligación de la Administración de apoyar y fomentar las Asociaciones de Reservistas; y como corolario de todo ello, el papel que los Reservistas Voluntarios deben tener en la defensa y seguridad nacional.

A continuación, se analizará la experiencia de la delegación de ARES en Asturias tratando de ejercer ese papel durante en el trienio 2014-2016, y los indicadores de su actividad como método de medir los resultados.

2.4.1. *Visión*

La Asamblea General de ARES Asturias aprobó en enero de 2014, el documento «Visión», por entender que era la base sobre lo que se debía ir construyendo el resto. Se pretendía exponerlo a la Asamblea de Reservistas y que fuese un documento comúnmente aceptado. Sin una visión común, pocas actuaciones posteriores podrían llevarse a cabo. Tras un análisis DAFO de la situación actual de la Reserva Voluntaria, se aprobó la Visión con los siguientes contenidos:

1. Se aprecia una evidente infrautilización de actual modelo de Reserva Voluntaria. Se traduce en bajas voluntarias y una desmoralización palpable en el colectivo. Las activaciones por otra parte son escasas y las pocas que hay están muy concentradas. Los cometidos y funciones en

el destino son en ocasiones desilusionantes, apreciándose en bastantes ocasiones que en las Unidades no saben que hacer con su Reservista. Por otra parte, las actuales exigencias para el ascenso se valoran como un obstáculo insalvable en muchas ocasiones. Otras cuestiones menores como la renovación del vestuario, acceso al PCAMI, acceso a descuentos y promociones, alojamiento en residencias militares, entre otras, suponen una discriminación negativa en absoluto ilusionante para el colectivo Reservista.

2. Aún hay un gran desconocimiento por la sociedad de la Reserva Voluntaria. La indudable importancia que la misma puede tener para divulgar la cultura de defensa y el papel que podríamos tener en la seguridad nacional, están claramente desaprovechados.
3. Antes que buscar responsables o soluciones al margen de nosotros mismos, tenemos que actuar para mantener la vinculación y cohesión interna, reforzar el sentido de pertenencia y asegurar una adecuada formación y unas habilidades mínimas relacionadas con el entorno militar.
4. Se hace preciso conseguir mayor visibilidad en el entorno próximo, siendo capaces de generar noticias propias y actividades que provoquen un mayor conocimiento por parte de la sociedad.
5. ARES, como asociación hegemónica de la Reserva Voluntaria, debe desempeñar un papel muy activo, aportando organización.

Se considera que la organización aporta valor y rigor, y es más eficiente y eficaz que las actuaciones debidas a esfuerzos individuales o iniciativas meramente voluntaristas.

6. Siendo realistas tampoco es posible exigir nada a las respectivas Delegaciones de Defensa, ya que aunque con buena intención, la insuficiencia de recursos lastra cualquier posibilidad.
7. Es indudable que estamos ante una etapa difícil para la Reserva Voluntaria. Este hecho debe aprovecharse más como oportunidad que como lamento, y ocasión de mostrar de nuevo nuestro compromiso. Somos Reservistas siempre, auque no estemos activados. La ausencia de activaciones no puede ser una excusa para el desaliento ni para el abandono.

8. Y ello sólo puede conseguirse desde una actuación organizada, cohesionada y estructurada, con una estrategia clara y unas acciones concretas que la desarrollen.
9. Es necesario imprimir en todas las acciones, el valor añadido que genera dicha organización, que permita colaborar mejor con la Delegación de Defensa y trabajar mejor para la Reserva Voluntaria.

2.4.2. *Estrategia*

Tras tener encuadrada la Visión, se definió y aprobó la Estrategia para poder desarrollar aquélla.

1. Al servicio de esa visión, es necesario fortalecer el papel de la Asociación, asumiendo el rol de liderazgo que de la misma se desprende.
2. Es preciso trasladar al Reservista la importancia —y más en estos tiempos— de asociarse y de participar activamente en la misma.
3. Por ello, las actuaciones que se desarrollen deben estar sujetas a la visión y a la estrategia definida previamente. Deben estar soportadas por una organización por encima de los individuos. Y deben ser desarrolladas en un plan de acción, con objetivos y acciones concretas, y con un plan de actividades. Todo lo anterior, junto a una eficaz política de relaciones con los medios de comunicación, serán los factores clave de éxito de esta operación.

2.4.3. *Organización*

La Visión y la Estrategia deben estar soportadas y deben ejecutarse en el marco de una Organización que canalice los esfuerzos y aporte rigor y eficacia a todas las actuaciones.

1. La organización, como elemento de soporte de las actividades, debe encontrar su referencia en los propios Estatutos de la organización. De esta forma, se debe constituir formalmente la Delegación de ARES Asturias, actuando escrupulosamente conforme a esa normativa interna.
2. Por ello, el primer paso debe ser constituir formalmente la Delegación de ARES en Asturias, que será gestionada por una Junta Directiva.

3. Esta Junta será el elemento principal de soporte de la organización, y la que dirigirá y coordinará las actividades que se desarrollen o en las que colabore la asociación. Nada debiera hacerse de manera individual, sino como colectivo organizado.
4. La Junta Directiva, según los Estatutos, debe contar al menos con un Delegado, dos Subdelegados, Tesorero, Secretario y Vocales, que estarán encargados de las diferentes Secciones que cabría constituir. Se consideran prioritarias las siguientes: Sección Deportiva (para actividades deportivas y operativas), Sección de Formación (conferencias, cursos, …) y Sección de Comunicación (medios, web, twitter, whatsapp).
5. Las convocatorias de las Asambleas Generales anuales, las convocatorias de reuniones ordinarias de Junta Directiva, las convocatorias de actividades, etc., deben efectuarse con el mayor rigor posible —tanto formal como materialmente—, según los Estatutos de la asociación o los procedimientos internos definidos.

2.4.4. *Planeamiento*

Tras la Visión, la Estrategia y la Organización como soporte de todo ello, se abordó la planificación de actividades. Para ello se seleccionaron varios objetivos, que se despliegan en acciones, en el marco general de colaboración con la Delegación de Defensa, con una visión global y asegurando la mayor coordinación, aún partiendo de la indudable autonomía de ARES Asturias.

Se determinaron los siguientes objetivos:

Objetivo 1: Potenciar la delegación de ARES en el Principado de Asturias.

Acciones:

1.1 Mantener contacto con todos los Reservistas asturianos —en toda su clasificación— dando a conocer la asociación y su finalidad.
1.2 Ofrecer apoyo al Reservista ante incidencias, consultas y trámites, manteniendo una adecuada interlocución con la Delegación de Defensa.
1.3 Incrementar el número de asociados de la delegación de ARES.

1.4 Convocar una Asamblea General de asociados para fijar la visión y las líneas estratégicas, constituyendo una Junta Directiva y en ella, al menos varios Secciones para fortalecer la organización y desarrollar actividades.
1.5 Elaborar un documento de presentación oficial de la delegación, entregable a autoridades militares y civiles, sobre nuestra organización y las actividades que se desarrollan.
1.6 Disponer de algún material corporativo (camisetas técnicas, banderas de mochila, lotería).
1.7 Presentar una candidatura anual a los Premios Defensa.

Objetivo 2: Divulgar los valores Reservistas y la cultura de defensa.

Acciones:

2.1 Desarrollar un ciclo de conferencias de carácter anual y colaborar en aquellas otras ajenas que sean de interés común.
2.2 Participar en Congresos o Reuniones sobre temas militares, de seguridad y defensa, con el objetivo de presentar ponencias o comunicaciones.
2.3 Publicar artículos o colaboraciones en prensa escrita, a modo de tribuna de opinión, sobre la Reserva Voluntaria y su misión en la cultura de defensa.
2.4 Enviar a los medios y personal interesado en general, tanto las convocatorias de actividades como las notas de prensa sobre su ejecución, para aumentar nuestra visibilidad.

Objetivo 3: Colaborar en las actividades que desarrolle la Delegación de Defensa y entidades afines:

Acciones:

3.1 Colaboración para mantener el plan de activaciones cortas en la Delegación de Defensa y tratar de iniciarlo en la Comandancia Naval de Gijón.
3.2 Apoyar a la Delegación de Defensa en los actos del día de la Delegación con la entrega de diplomas a Reservistas (nombramientos, ascensos, méritos, …).
3.3 Colaborar en otros actos externos como las visitas a Unidades, Juras de Bandera, Día de la Fiesta Nacional, Escoltas de Honor, entre otros.

3.4 Colaborar en las tareas de recuperación del patrimonio militar de la Delegación de Defensa.
3.5 Impulsar la colaboración con las Asociaciones de Veteranos, y otras afines como ARAMA (Asociación para la Recuperación de la Arquitectura Militar Asturiana), ARHCA (Asociación de Recreación Histórico Cultural de Asturias) y Sociedad de Amigos del País.
3.6 Participar en todos los actos castrenses que se desarrollen en Asturias, con invitación previa o gestionando la misma. Se pondrá especial interés en incrementar la relación con el Regimiento Príncipe núm. 3.

Objetivo 4: Mantener la comunicación e información entre los Reservistas asturianos:

Acciones:

4.1 Celebrar varios encuentros reservistas anuales, con invitación extensiva a las delegaciones de provincias limítrofes, Asociaciones de Veteranos y afines.
4.2 Mantener el envío periódico de información a través del correo electrónico sobre temas reservistas, militares y de la cultura de defensa en general.
4.3 Implantar un grupo de whatsapp como medio de información y comunicación rápida entre Reservistas para temas de interés del colectivo.
4.4 Actualizar de forma permanente la sección de noticias de la delegación en la web corporativa de ARES.
4.5 Abrir una cuenta de Twitter de ARES Asturias.

Objetivo 5: Impulsar la formación y mejorar las habilidades deportivo-militares de los Reservistas:

Acciones:

5.1 Impartir cursos de formación básica en instrucción y orden cerrado, defensa personal, emergencias y primeros auxilios, orientación y topografía, marchas de montaña, actividades acuáticas, entre otros.
5.2 Formación básica en manejo de armas de fuego.
5.3 Hacer prácticas mensuales de tiro.
5.4 Hacer ejercicios de combate de airsoft con un equipo de ARES Asturias.

5.5 Participar en el Raid de ARES a nivel nacional
5.6 Reanudar el Aula de Formación en la Delegación de Defensa

2.4.5. *Actuaciones*

La ejecución del plan de acción se concreta en las actividades llevadas a cabo en cada año en el trienio 2014-2016.

En este período, la delegación de ARES en Asturias llega a celebrar una media de sesenta actividades anuales, de las que la gran mayoría son organizadas directamente por la propia organización.

Debe destacarse que todas las actividades son organizadas con recursos propios, financiadas en su mayor parte por los propios Reservistas participantes. No se recibe ni un solo euro en ayudas o subvenciones públicas ni privadas, salvo ayudas puntuales y de escasa cuantía procedentes de la Junta Nacional de ARES.

Las actividades pueden agruparse en los siguientes bloques:

—De carácter deportivo y de formación en habilidades militares: defensa personal (mensual), tiro olímpico (mensual), montañismo, recorridos de tiro policial y de combate, tiro con armas históricas de avancarga, recarga de cartuchería metálica, emergencias, submarinismo, instrucción y orden cerrado, orientación topográfica, seguridad y autoprotección, uso de la fuerza y reglas de enfrentamiento, combates de airsoft, prevención de riesgos laborales en el ámbito militar, piragüismo, equitación, protocolo militar, organización y despliegue militar.

—De carácter cultural y divulgativo de los valores de la cultura de defensa: presentaciones de libros de temática militar (en el trienio se han presentado seis libros)[20], conferencias (se organiza una media de cinco al año y se asiste como delegación a otras tantas), artículos en prensa escrita (se publican tres al año), asistencia a programas de televisión (en el período en tres ocasiones), asistencia a Congresos y reuniones militares.

20. Destaca por encima de todas, la presentación del libro «La Reserva Militar Voluntaria en España: urdimbre y retroprogresión» (Oviedo: AC Ediciones, 2014), cuyo autor es el Alférez de Fragata (RV) Don José Antonio López Díaz y miembro de ARES Asturias, al ser el primer libro escrito en España sobre la Reserva Voluntaria.

—De carácter social y de interés militar: escoltas de Honor en procesiones y actos religiosos (seis escoltas anuales), visitas a instalaciones militares y/o policiales, reuniones anuales, celebraciones señaladas (siempre se conmemora la Pascua Militar, el Día de las Fuerzas Armadas y el Día de la Fiesta Nacional, con comida, cena o en su defecto vino español), celebración del Día del Reservista con acto público en la calle, asistencia a actos de asociaciones afines (Veteranos de la Armada, de la Legión, de COE 72 y de Caballeros Legionarios Paracaidistas, principalmente), colocación del Belén de Cumbres, recogida para el Banco de Alimentos de Asturias, concierto benéfico.
—De colaboración con la Delegación de Defensa: Día de la Delegación, rehabilitación e inventario del patrimonio histórico-militar, visitas institucionales, montaje y atención del Museo de armas históricas, Noche Blanca de Oviedo, entrega de Bandera a un Colegio Público. Y con la Comandancia de Marina de Gijón, en los servicios de control de accesos en visitas a buques.

2.4.6. *Indicadores*

Para analizar cuantitativamente la evolución de la Delegación de ARES en Asturias, se utilizan los siguientes indicadores:

1. Número de asociados

AÑO 2014	AÑO 2015	AÑO 2016 a 1 de octubre
23	31	37

2. Visibilidad exterior (se utiliza el criterio de presencia de Reservistas con uniforme militar en la calle, fuera de recintos militares)

AÑO 2014	AÑO 2015	AÑO 2016 a 1 de octubre
7	13	17

3. Impactos en medios de comunicación (se utiliza el criterio de noticias aparecidas en prensa escrita, radio y televisión)

AÑO 2014	AÑO 2015	AÑO 2016 a 1 de octubre
9	10	24

4. Número de actividades

AÑO 2014	AÑO 2015	AÑO 2016 a 1 de octubre
41	69	55

Con carácter singular debe destacarse que el Premio Defensa 2016 se otorgó —ex aequo— a la candidatura presentada por ARES Asturias, en la persona de uno de sus Reservistas y miembro de ARES.

Conclusión

Tras el análisis de la Reserva Voluntaria y de los conceptos de defensa, cultura de defensa y seguridad nacional, pudiera decirse sin ningún atrevimiento por nuestra parte, que los segundos no podrían entenderse desde una visión global y de unidad de acción, sin la primera.

La Reserva Militar de Voluntarios en España, con todas las serias deficiencias del modelo actual, con la antipatía de algunos y el desconocimiento de otros, es un instrumento eficaz (útil para el fin pretendido) y eficiente (con limitado consumo de recursos) para divulgar la cultura de defensa, al servicio de la defensa y la seguridad nacional.

Las dos notas más características de la Reserva Militar de Voluntarios —la voluntariedad y la disponibilidad— junto a la entrega, la generosidad y el compromiso con España y sus Fuerzas Armadas, encajan a la perfección con ese proyecto compartido que debe ser la defensa y seguridad nacional, tal como lo denomina la ESN. Si mientras está activado es evidente que el Reservista Voluntario es un militar más a todos los efectos, cuando no está activado se convierte en un agente de interés privilegiado para difundir, concienciar y responsabilizar a los ciudadanos de tales conceptos.

No debe olvidarse su doble condición de civil insertado en las Fuerzas Armadas —que cuando está activado es un militar más— y de militar insertado en la parte civil de la sociedad —ya que cuando no está activado sigue siendo un Reservista Voluntario.

Desaprovechar ese caudal de entrega, de disponibilidad y de voluntariedad –cuando no hay activación por medio, se insiste-, no sólo es una necedad impropia de estructuras desarrolladas, sino que es un lujo que España, su defensa y su seguridad, no se puede permitir.

A este respecto, basta pensar en qué no haría una empresa privada con un colectivo entusiasta de sus productos, conocedor de los mismos, racionalmente entregado, con formación, experiencia y trayectoria intelectual acreditada en tantísimos casos (en la Reserva Voluntaria forman excelentes profesionales de todas las ramas, la mayoría titulados universitarios con carreras exitosas) y voluntariamente disponible.

Si hubiese aún alguna duda acerca de lo anterior, bastaría con acudir a la normativa específica que atribuye este papel a los Reservistas y a las asociaciones que pudieran constituir.

Esa misión de los Reservistas tiene efectos multiplicadores si se ejecuta de forma ordenada y hasta sistematizada. Esa es la conclusión que se puede extraer de la experiencia en Asturias en el período 2014-2016, cuando en el año 2014 se constituyó la Junta Directiva de la delegación asturiana de ARES, que fue poniendo en marcha su propio sistema de trabajo.

La definición de la visión y la estrategia, soportadas ambas por una organización rigurosa y unos procedimientos de actuación conforme a los Estatutos de la asociación, hace mucho más sencilla la determinación de los objetivos, la planificación de actividades y la ejecución de las mismas.

Los resultados se plasman en los indicadores de actividad señalados, que son fundamentalmente cuantitativos, sin entrar a valorar otros aspectos cualitativos que siendo importantes, pudieran tener sesgo de opinión. Tales resultados demuestran la valoración positiva del método de trabajo adoptado en 2014, donde el elemento diferencial es el soporte de organización que conlleva la asociación de Reservistas.

Con una simple observación a los datos, cabe afirmar sin temor a equivocación alguna, que pocas instituciones y organizaciones habrán podido hacer más por la cultura de defensa, la defensa y la seguridad nacional, con menos recursos. Se insiste como se ha

dicho ya, en que son los propios Reservistas y demás participantes los que sufragan todos los gastos, sin ninguna financiación añadida. Para paliar en parte este inconveniente y a la vez disponer de recursos propios, la Junta Directiva decidió por primera vez y para el año 2016, la venta de participaciones de lotería con un pequeño recargo a modo de donativo.

El incremento de socios va parejo al crecimiento en el número de actividades organizadas y ejecutadas por ARES Asturias en su mayor parte, en el número de actividades donde los Reservistas están en la calle participando en diversos actos (comisionados por la Delegación de Defensa) y lo hacen vistiendo el uniforme con normalidad, y sobre todo en la presencia en medios de comunicación —con un repunte muy destacado en 2016—, aportando una creciente visibilidad a este importante pilar de la defensa y seguridad nacional que es la Reserva Voluntaria.

Agradecimientos

Los autores agradecen a la Asociación ARES de Reservistas Españoles el apoyo recibido y la colaboración prestada para que esta comunicación pudiera ver la luz. Y a todos los Reservistas que forman la Delegación de ARES en Asturias, por su implicación y entusiasmo en la divulgación de los valores de las Fuerzas Armadas, la defensa y la seguridad nacional.

De igual forma, se hace extensivo dicho agradecimiento a la Delegación de Defensa en el Principado de Asturias y a la Comandancia Naval de Gijón, por la atención dispensada a todos los Reservistas asturianos y, en especial, por su colaboración hacia todas las actividades organizadas por ARES Asturias.

Abreviaturas

ARAMA (Asociación para la Recuperación de la Arquitectura Militar Asturiana
ARES: Asociación de Reservistas Españoles
ARHCA (Asociación de Recreación Histórico Cultural de Asturias)
BOD: Boletín Oficial de Defensa
BOE: Boletín Oficial del Estado
CESEDEN: Centro de Estudios Superiores de la Defensa
COE: Compañía de Operaciones Especiales
ESN: Estrategia de Seguridad Nacional
PCAMI: Parque y Centro de Abastecimiento de Material de Intendencia

Referencias bibliográficas

Bernal Gutiérrez, Pedro. 2011. *La cultura de seguridad y defensa en España. Sus orígenes y evolución*. En *La cultura de seguridad y defensa, un proyecto en marcha*. Cuadernos de Estrategia 155. Madrid: Ministerio de Defensa. Instituto Español de Estudios Estratégicos.

Centro Superior de Estudios de la Defensa. 2008. *De la milicia concejil al Reservista, una historia de generosidad*. Madrid: CESEDEN

Constitución Española (*BOE* núm. 311, de 29 de diciembre de 1978).

Estrategia de Seguridad Nacional. Un proyecto compartido. Acuerdo del Consejo de Ministros de 7 de junio de 2013.

López Díaz, José Antonio. 2014. *La Reserva Militar Voluntaria en España: urdimbre y retroprogresión*. Oviedo: AC Ediciones.

Ley 17/1999, de 18 de mayo, de Régimen del Personal para las Fuerzas Armadas (*BOE* núm. 119, de 19 de Mayo de 1999).

Ley Orgánica 6/1980, de 1 de julio por la que se regulan los criterios básicos de la Defensa Nacional y la Organización Militar (*BOE* núm. 165, de 10 de julio de 1980).

Ley Orgánica 1/2002, de 22 de marzo, reguladora del Derecho de Asociación (*BOE* núm. 73, de 26 de marzo de 2002).

Ley Orgánica 5/2005, de 17 de noviembre, de la Defensa Nacional (*BOE* núm. 276, de 18 de noviembre de 2005).

Ley 8/2006, de 24 de abril, de Tropa y Marinería (*BOE* núm. 98, de 25 de abril de 2006).

Ley 39/ 2007, de 19 de noviembre, de la Carrera Militar (*BOE* núm. 278, de 20 de noviembre de 2007).

Real Decreto 383/2011, de 18 de marzo, se aprueba el Reglamento de Reservistas de las Fuerzas Armadas (*BOE* núm. 70, de 23 de marzo de 2011).

Real Decreto 176/2014, de 21 de marzo, por el que se regula el procedimiento para la tramitación de las iniciativas y quejas relativas al régimen de personal y a las condiciones de vida que pueda plantear el militar (*BOE* núm. 84, de 7 de abril de 2014).

Resolución 452/38137/2015, de 23 de septiembre, de la Subsecretaría, por la que se convoca proceso de selección para el acceso a la condición de reservista voluntario de las Fuerzas Armadas (*BOE* núm. 232, de 28 de septiembre de 2015).

BLOQUE V

ECONOMÍA E INDUSTRIA DE DEFENSA

LA ESTRATEGIA DE SEGURIDAD NACIONAL Y LA PERCEPCIÓN DE LA AMENAZA: LA INESTABILIDAD ECONÓMICA Y FINANCIERA

Claudia Pérez Fornies
Cátedra Paz, Seguridad y Defensa
Universidad de Zaragoza

Resumen

El objetivo de la comunicación es el tratar de dilucidar si la ciudadanía española y de otros lugares del mundo, en un contexto geográfico y temporal, sienten como amenaza para la seguridad nacional la inestabilidad económica.
Como resultado de la investigación, indica que, efectivamente, para la ciudadanía española, se sitúa en primer lugar dicha amenaza. Pero, al mismo tiempo, destaca el hecho paradójico que las políticas de austeridad derivadas de la crisis han producido importantes mermas en los presupuestos en seguridad interior y exterior, instrumentos muy importantes para reducir los niveles de riesgo de otras amenazas.
Sólo el crecimiento económico y la salida de la crisis pueden llevar a controlar esta amenaza y, por tanto, dedicar más recursos a la seguridad y defensa.

Palabras claves

Estrategia de Seguridad Nacional, Seguridad Nacional, Percepción de las amenazas, estabilidad económica.

1. Introducción

En mayo del año 2013, el Gobierno del presidente Rajoy aprobó la Estrategia de Seguridad Nacional «Un proyecto compartido» en la que se recogían los riesgos y amenazas que acechan a un mundo sumergido en cambios profundos y constantes. Una de las novedades importante es la inclusión de la Inestabilidad Económica y Financiera como amenaza recogida ya en la Estrategia de Seguridad Nacional de 2011.

En la Estrategia de Seguridad Nacional (2013) se recogen doce amenazas muy distintas entre sí. La amenaza que nos ocupa, la inestabilidad económica y financiera, no se estudia en profundidad por el Centro de Investigaciones Sociológicas hasta 2013, en un estudio realizado para el Ministerio de Defensa en el que se recoge la valoración que la ciudadanía realiza acerca de las amenazas. Nos enfrentamos a conceptos muy amplios: la seguridad nacional, la inestabilidad económica financiera, la crisis económica y las amenazas.

Pero además, el concepto de Seguridad viene ligado a la percepción que los ciudadanos realizan de las amenazas y su nivel de riesgo. Las sociedades como la nuestra, están dispuestas a asumir cierto nivel de riesgo, asunto completamente subjetivo, y que es fruto del mensaje que la ciudadanía reciba de las instituciones y de los medios de comunicación social.

No se trata de que hoy el mundo sea necesariamente más inseguro que ayer, sino que el ciudadano del primer mundo exige un nivel de seguridad mucho mayor, y frente a mayor número de riesgos, muchos de ellos grandes desconocidos. La seguridad es amplia, multidireccional, difusa y exige la intervención coordinada de múltiples actores, uno de ellos las Fuerzas Armadas.

La crisis económica es la causa de la introducción de la inestabilidad económica y financiera como amenaza para la seguridad y la defensa porque la genera. ¿Pero la percibe como amenaza la ciudadanía española? ¿Y el resto del mundo es sensible a esta amenaza?

La respuesta es afirmativa. La ciudadanía española la siente como primera amenaza para la Seguridad. Pero al mismo tiempo se produce un hecho paradógico, las políticas de austeridad derivadas de la crisis han mermado los presupuestos en seguridad interior y exterior, uno de los instrumentos para reducir los niveles de riesgos de otras amenazas.

Por lo tanto, nos encontramos en una encrucijada. Sólo el crecimiento económico y la salida de la crisis nos pueden llevar a controlar esta amenaza y otras porque nos permitirá dedicar más recursos en seguridad y defensa. En primer lugar, vamos a delimitar cuál es la percepción que los ciudadanos realizan de la amenazas en particular de la inestabilidad económica y financiera para, a continuación, establecer el escenario en el que se desarrolla la situación económica actual y las perspectivas de futuro.

2. La seguridad en la era de la globalización: la percepción de la amenaza

El punto de partida de este trabajo no puede ser otro que el que se fundamenta en la delimitación del concepto Seguridad ya que es un elemento esencial para el desarrollo y el progreso de una sociedad libre.

Al enfrentarnos a la pregunta ¿qué es la seguridad? Encontramos dos respuestas bien diferentes que nos plantean un primer dilema. La primera se centra en el poder y la segunda en la paz. El eterno debate en la teoría de las relaciones internacionales, la escuela realista y la escuela idealista.

Según Buzan (1991), la Seguridad consiste en liberarse de la amenaza y ser capaz, bien sean los estados o las sociedades, de mantener su independencia en lo que se refiere a su identidad y a su integración funcional, frente a fuerzas de cambio consideradas hostiles.

Aparecen los conceptos de amenazas, riesgos, conflictos. Muchas veces utilizados indistintamente, por un mal uso. La amenaza es un fenómeno provocado por otro Estado, Grupo no estatal o individuo que causa daños. El riesgo es algo potencial, una señal de alarma que nos pone en alerta. Así que se pueden gestionar los riesgos para intentar conseguir que no se materialicen las amenazas y por lo tanto los conflictos y materializarlos según la siguiente ecuación:

Riesgo= Amenaza* Vulnerabilidad
Vulnerabilidad= Exposición* Susceptibilidad/Resilencia

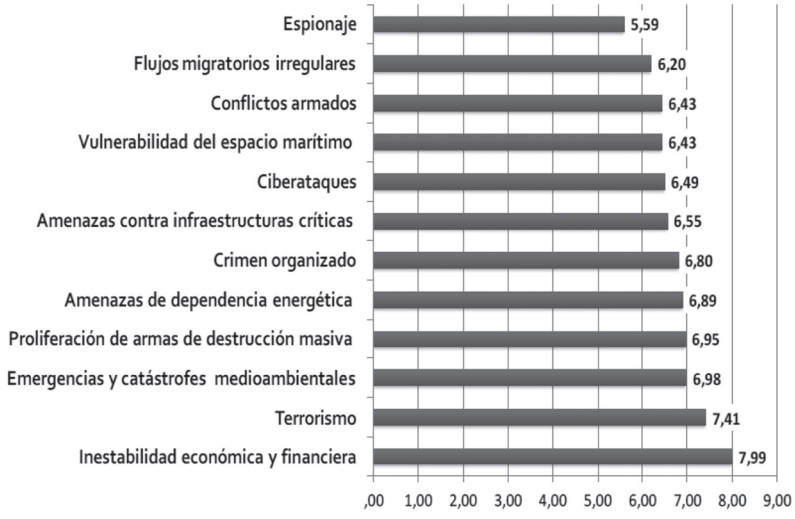
La caída del Muro de Berlín supone un cambio en los conceptos de seguridad. La seguridad debe tener distintos niveles de análisis (interdependiente, compartida y global) y debe mostrar su carácter multidisciplinar (militar, política, económica, social y medioambiental). Se abandona el concepto encorsetado que asociaba la seguridad a la defensa militar. Pero sí que nos debemos mover en el nivel de seguridad estatal: afecta a todos los individuos que componen un Estado.

Nuestro objetivo es observar la percepción que los ciudadanos tienen de todos esos problemas, amenazas y conflictos, en particular la inestabilidad económica y financiera. Porque la clave es presentar la Seguridad como un concepto con un contenido

importante subjetivo, depende de cada uno de nosotros, de nuestro nivel de información, de nuestra localización, del momento del tiempo, de nuestra educación, de un sin fin de cosas. Y para intentar recoger estos vectores (información, tiempo, lugar) analizaremos a continuación diferentes percepciones de la amenaza, en distintos momentos del tiempo, del espacio y de cultura.

Para determinar cuál es la percepción de la amenazase presenta a continuación un análisis de lo particular a lo general. De España a otras zonas geográficas y el mundo. Utilizamos para el análisis la fuente oficial del Centro de Investigaciones Sociológicas que de forma mensual realiza los barómetros del CIS para tomar el pulso de la población española en diferentes cuestiones. Pero los estudios en relación a la valoración de la amenaza no se recogen en los barómetros mensuales. Pero sí que se analizan en estudios específicos que el CIS realiza en materia de seguridad y relaciones internacionales.

Gráfico 1: Valoración de riesgos y amenazas en España



Fuente: Instituto Español de Estudios Estratégicos (2013)

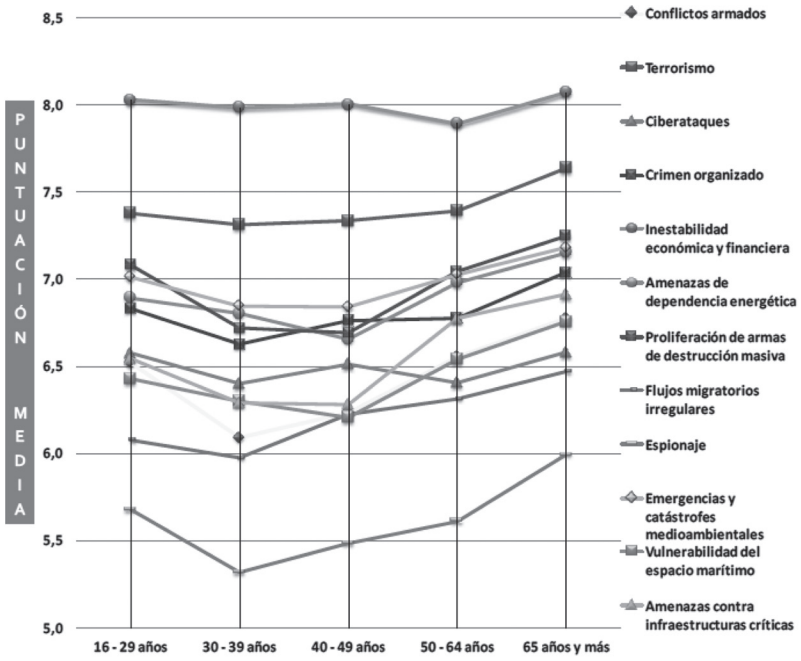
En el gráfico 1 se encuentran ordenadas, de acuerdo con la importancia dada por los encuestados, las amenazas recogidas en la ESN 2013. La puntuación refleja, en orden creciente, la media de todas las respuestas facilitadas por los encuestados, según una escala de 0 a 10. Sobre una muestra de 2.500 personas, población

española mayor de 16 años con la realización de entrevistas personales en los domicilio en septiembre de 2013.

La inestabilidad económica financiera y el terrorismo se presentan como las alternativas que la población española siente como mayores riesgos para la seguridad nacional. Por el contrario, es el espionaje el aspecto que es percibido como menos peligroso para esta sociedad.

La posibilidad de que existan conflictos armados no es considerada en la sociedad como un riesgo o amenaza muy relevante.

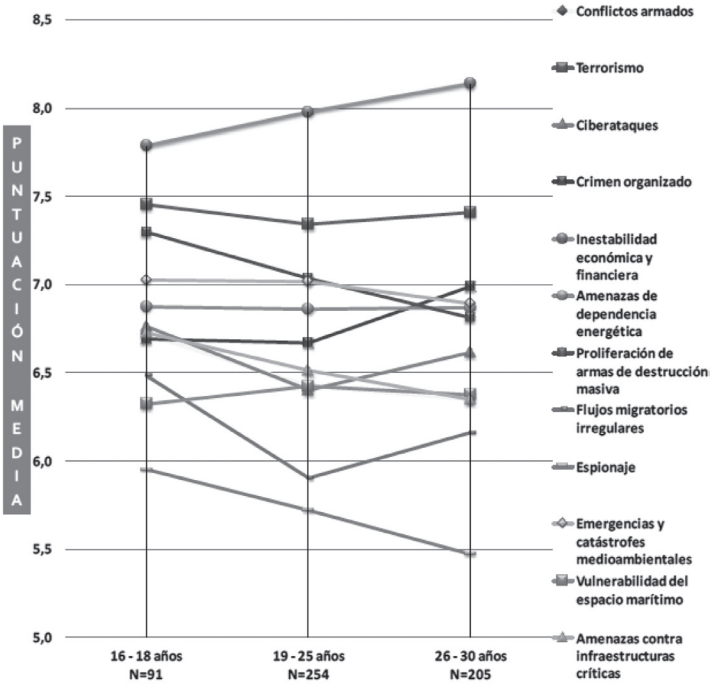
Gráfico 2: Valoración de riesgos y amenazas en España por edades



Fuente: Instituto Español de Estudios Estratégicos (2013)

La edad no es un factor que influya sustancialmente a la hora de hacer sus valoraciones sobre los riesgos y amenaza que puedan afectar a nuestra nación. Aunque sí que se observa un aumento de la preocupación frente a otros segmentos de edad ante cualquier tipo de amenaza cuando la gente pasa el umbral de los sesenta y cinco años.

Gráfico 3: Valoración de riesgos y amenazas en España entre los jóvenes



Fuente: Instituto Español de Estudios Estratégicos (2013)

Sin embargo se manifiestan algunas diferencias entre los jóvenes. Parece que conforme maduran perciben, en mayor proporción, la inestabilidad económica y financiera como amenaza y, por el contrario, sienten menos riesgo con el espionaje.

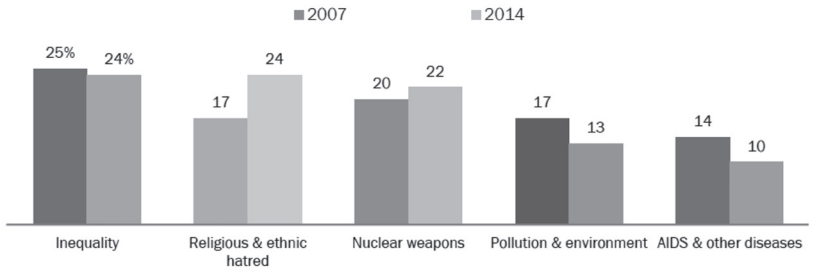
En cualquier caso destaca la amenaza económico financiero. Es un sesgo que la situación económica introduce. Después de seis años de crisis económica con altas tasa de paro es normal que sea la mayor preocupación.

Pero España presenta unas peculiaridades que la dotas de rasgos deferenciales con otros países del mundo. ¿Cuál es la percepción del resto del mundo acerca de las amenazas que les rodean? Para presentar un análisis de la percepción de la amenaza en el mundo utilizamos los datos proporcionados por el Pew Research Center (Think Tank) de Washintong. Este Instituto realiza una encuesta (telefónicas y personales a una población mayor de 18 años) en 44 países a 48.643 (unas 1000 personas por país) personas de marzo a junio de 2014.

Su trabajo analiza la percepción de los individuos de la muestra por áreas acerca de tres *problemas*, algunos son amenazas y otros potenciadores de la amenaza y no coinciden con las doce amenazas que acabamos de presentar pero es relevante su estudio:

1. Problemas étnicos y religiosos
2. Desigualdad
3. Contaminación y medio ambiente
4. Armas nucleares
5. SIDA y otros

Gráfico 4: Percepción de riesgos y amenazas en el mundo



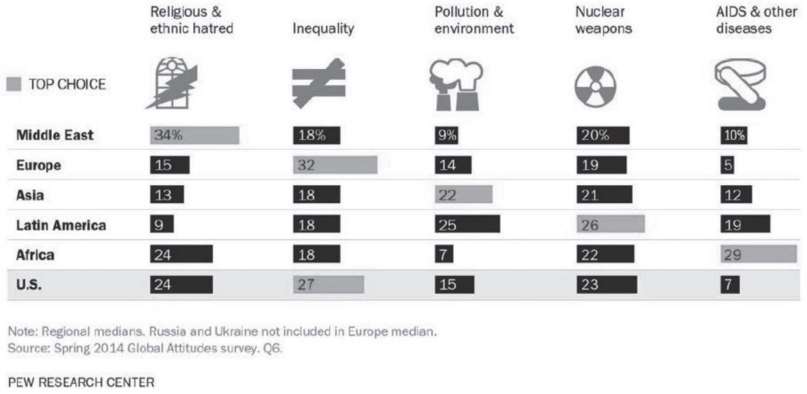
Note: Global median percent based on 28 countries surveyed in 2007 and 2014.

Source: Spring 2014 Global Attitudes survey. Q6.

PEW RESEARCH CENTER

En perspectiva temporal, desde 2007 hasta 2014, a nivel global se observa un aumento en la preocupación sobre todo en un tema: los problemas étnico religiosos. Pero si centramos nuestra atención únicamente en el año 2014, (la variable es la media de los porcentajes de los diferentes países) los problemas que toman un mayor protagonismo y por los que sienten mayor preocupación los habitantes del mundo son los problemas étnico religiosos y los problemas derivados de las desigualdades económicas: el punto de inflexión que suponen los atentados del 11 de septiembre de 2001 en EEUU, los posteriores de Madrid y Londres; el desarrollo posterior de Al Qaeda y sus franquicias por medio mundo, llevando la inestabilidad al continente africano; las Guerras de Afganistán, Irak, Siria; el eterno conflicto palestino- israelí; y algún conflicto más ya que son tantos que es difícil repasarlos todos es lo que produce el aumento en la variable conflictos religiosos. De la misma forma que la irrupción de la crisis económica en 2008 explica perfectamente la amenaza desigualdad de la renta.

Gráfico 5: Percepción de riesgos y amenazas por zonas geográficas



A continuación, se desciende al estudio de las áreas geográficas zonas geográficas y de los países ya que la localización geográfica y el momento temporal son las dos variables fundamentales que explican los cambios y diferencias que existen en la valoración que de la amenaza hacen los diferentes ciudadanos del mundo.

Las zonas geográficas son la siguierntes: Oriente Medio. Europa. Asia, Hispanoamérica, África y Estados Unidos. Es evidente la preocupación en Oriente Medio acerca de los problemas religiosos de forma que como acabamos de ver no sólo se manifiesta allí sino en otras partes del mundo como Estados Unidos y Europa. Los expertos mantienen que la potenciación de este problema en el futuro se va a convertir en la gran amenaza global si no lo ha hecho ya.

Sin embargo, los mundos desarrollados, como Europa y EEUU, muestran su mayor preocupación por las desigualdades sociales, fundamentalmente en los niveles de renta. La crisis de 2008 nos ha llevado a valorar un potenciador de la amenaza que en otros periodos de tiempo no le dábamos prácticamente importancia. Asia y América Latina valoran más los niveles de contaminación y las Armas Nucleares y África el SIDA y otras enfermedades contagiosas.

Pero si descendamos un nivel más y analizamos la percepción de la amenaza por países observamos que la mayor preocupación de los países de la Europa occidental se centra en las desigualdades económicas: las diferencias entre ricos y pobres y sobre todo el aumento en los niveles de pobreza derivada de la fuerte crisis económica. A diferencia de la Europa oriental que reflejando el conflicto actual y sus peculiaridades geopolíticas temen por la pro-

liferación de armamento nuclear. Cinco de siete países de Oriente Medio sienten como mayor amenaza los conflictos religiosos.

En Asia la percepción del conflicto es muy distinta por países. Desde la preocupación Japonesa y Pakistaní por el armamento nuclear, pasando a la preocupación por los radicalismo islamista de Indonesia, India y Malasia y terminando con la preocupación medioambiental de China, Filipinas, Tailandia y Vietnan.

En América Latina reparten su preocupación entre armamento nuclear y la contaminación. Y en África su mayor preocupación es el SIDA y otras enfermedades contagiosas como es el caso del ébola.

Gráfico 6: Percepción de riesgos y amenazas por países

Views in:	Nuclear weapons %	Inequality %	Religious & ethnic hatred %	Pollution & environment %	AIDS & other diseases %	Top choice
U.S.	23	**27**	24	15	7	Inequality
Spain	17	**54**	14	9	5	Inequality
Greece	23	**43**	10	14	9	Inequality
Germany	19	**34**	32	13	1	Inequality
Poland	28	**32**	14	13	9	Inequality
Italy	20	**32**	15	25	6	Inequality
France	14	**32**	**32**	17	5	Inequality/Religious hatred
UK	14	25	**39**	16	4	Religious & ethnic hatred
Ukraine	**36**	15	23	11	12	Nuclear weapons
Russia	**29**	19	27	13	10	Nuclear weapons
Lebanon	20	17	**58**	3	2	Religious & ethnic hatred
Palest. ter.	19	18	**40**	9	10	Religious & ethnic hatred
Tunisia	25	18	**39**	7	10	Religious & ethnic hatred
Egypt	12	27	**34**	11	14	Religious & ethnic hatred
Israel	27	23	**30**	12	8	Religious & ethnic hatred
Turkey	**34**	17	29	7	10	Nuclear weapons
Jordan	19	**31**	25	11	11	Inequality
Thailand	9	29	11	**36**	13	Pollution & environment
Philippines	19	22	11	**34**	14	Pollution & environment
China	26	14	9	**33**	13	Pollution & environment
Vietnam	21	13	9	**32**	22	Pollution & environment
Malaysia	22	13	**32**	16	12	Religious & ethnic hatred
Bangladesh	19	16	**30**	22	11	Religious & ethnic hatred
Indonesia	18	18	**26**	13	22	Religious & ethnic hatred
India	19	22	**25**	14	10	Religious & ethnic hatred
Japan	**49**	12	16	20	2	Nuclear weapons
Pakistan	**30**	29	13	3	7	Nuclear weapons
South Korea	26	**32**	11	29	2	Inequality
Chile	**30**	27	8	22	12	Nuclear weapons
Venezuela	**29**	16	8	21	24	Nuclear weapons
Brazil	**28**	19	19	13	20	Nuclear weapons
El Salvador	**27**	18	16	19	19	Nuclear weapons
Mexico	**26**	19	11	**26**	17	Nuclear weapons/Pollution
Colombia	22	17	8	**36**	15	Pollution & environment
Peru	23	12	7	**35**	22	Pollution & environment
Nicaragua	25	12	9	**29**	25	Pollution & environment
Argentina	17	**32**	12	25	12	Inequality
Uganda	21	20	7	8	**44**	AIDS & other diseases
Tanzania	16	12	25	4	**41**	AIDS & other diseases
South Africa	10	29	12	9	**35**	AIDS & other diseases
Kenya	24	17	24	3	**29**	AIDS & other diseases
Senegal	23	13	27	7	**28**	AIDS & other diseases
Nigeria	31	18	**38**	4	7	Religious & ethnic hatred
Ghana	22	**25**	17	13	20	Inequality

Fuente: Pew Research Center

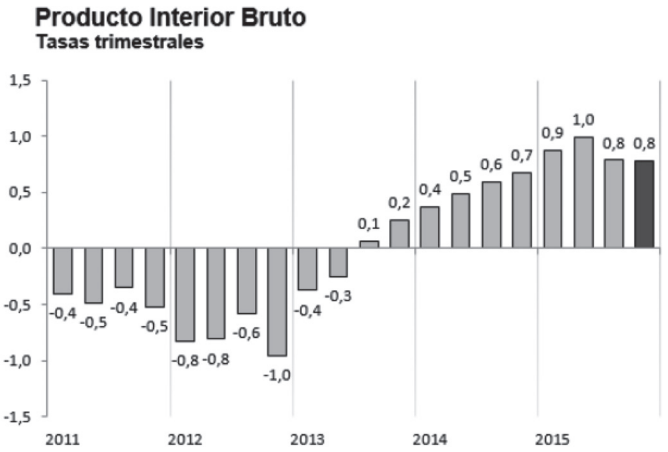
En definitiva, los ciudadanos del primer mundo sienten como principal amenaza a aquellos elementos derivados de la crisis económica. Por lo tanto, estos resultados coinciden con los ofrecidos por los estudios realizados para España. Una vez delimitada cual es la precepción que los ciudadanos acerca de la amenazas vamos a intentar acotar cuál es la situación económica actual y nuestras perspectivas de futuro.

3. La situación economica actual: pasado, presente y futuro

El crecimiento económico ha vuelto a la economía española, desde el tercer trimestre de 2013 el crecimiento ha sido positivo. Tras diez trimestres consecutivos de crecimientos negativos, las noticias no podían ser mejores. El crecimiento anual del PIB en 2015 ha sido de 3.2%, en el IV Trimestre de 2015 el crecimiento ha sido de 0.8%, mientras que la UE-28 y la UEM-19 han crecido un 0.3%. Por lo tanto, España ha crecido más de medio punto que el crecimiento que se ha producido en la Zona Euro. Sin embargo, no debemos olvidar que nuestra tasa de paro (20.9%) triplica la de los países de la OCDE y duplica la de la media de la UE (Portugal- 12%) y el más endeudado con el exterior, en términos relativos con respecto a la renta, del mundo. No debemos ser pesimistas, ni tampoco optimistas debemos ser conscientes de los lastres que tenemos derivados del pasado y que pesan para crecer.

El Objetivo es generar crecimiento económico, es decir, crecer con la suficiente intensidad como para paliar los desajustes. Si crecemos disminuiremos la amenaza inestabilidad económica, el crecimiento conlleva trabajo y mejoras en los niveles de renta y mejoras en la desigualdad de la renta. Todo ello disminuirá la desafección social y la pérdida de la credibilidad de las instituciones por parte de la ciudadanía.

Gráfico 7: PIB (tasas trimestrales)

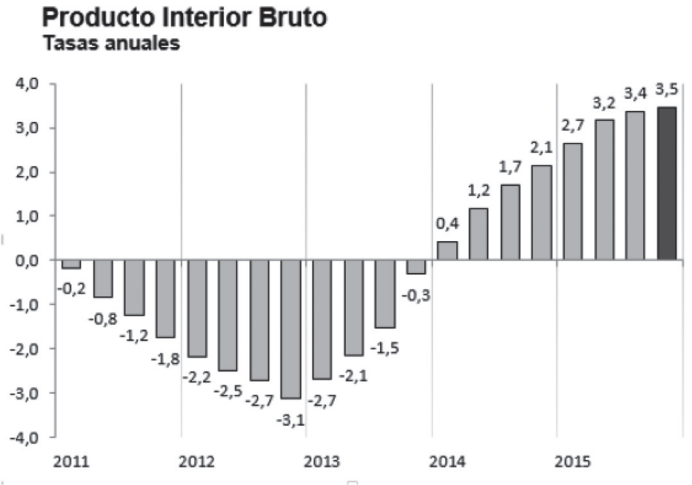


Producto Interior Bruto

Tasas	2013				2014				2015			
	Tr. I	Tr. II	Tr. III	Tr. IV	Tr. I	Tr. II	Tr. III	Tr. IV	Tr. I	Tr. II	Tr. III	Tr. IV
Anuales	-2,7	-2,1	-1,5	-0,3	0,4	1,2	1,7	2,1	2,7	3,2	3,4	3,5
Trimestrales	-0,4	-0,3	0,1	0,2	0,4	0,5	0,6	0,7	0,9	1,0	0,8	0,8

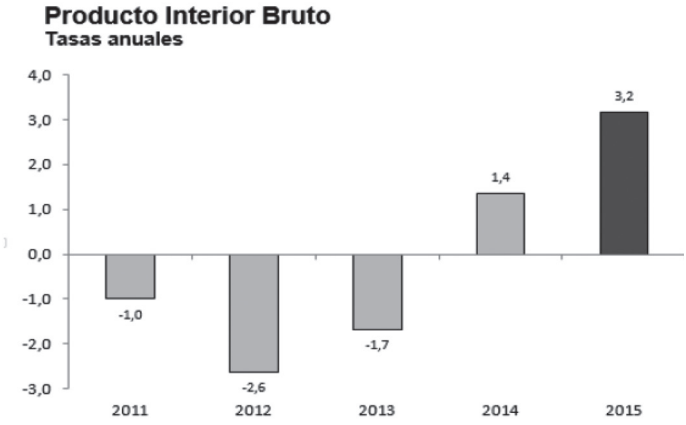
Fuente: INE

Gráfico 8: PIB (tasas anuales por trimestres)



Fuente: INE

Gráfico 9: PIB (tasas anuales)



Fuente: INE

Para entender la situación actual debemos desentrañar los desequilibrios tremendos que se derivan de la crisis del 2008 además de otros problemas de carácter estructural[1]. Siguiendo lo expuesto Serrano Sanz (2016) y (2015) se analizarán a continuación la situación económica actual, los problemas del pasado y las perspectivas de futuro.

3.1. *Los desequilibrios coyunturales*

El primero de los desequilibrios se concreta en un conjunto de excesos inversores que se materializan en un enorme stock de viviendas y de infraestructuras públicas, símbolo de la mala gestión, la ineficiencia y el despilfarro.

En una situación de auge económico, la iniciativa privada funciona y por lo tanto el sector público debe dar un paso atrás. Su intervención será clave en momentos de crisis para incentivar el mercado. Pues bien, mientras la iniciativa privada construía a

1. En esta situación, no debemos olvidar que los instrumentos que el gobierno español posee para subsanar los desequilibrios económicos se han reducido sustancialmente con la pertenencia de España a UEM, es decir, la pertenencia a la zona euro: se acabó la posibilidad de hacer política monetaria y política de tipo de cambio. Hemos tenido que devaluar el país de una forma muy dura: bajando los salarios, conteniendo el gasto y aumentando los impuestos.

niveles nunca vistos, la iniciativa pública se volvía loca haciendo lo mismo. La consecuencia de todo esto es la inmensa deuda que debemos pagar. Pero además, España tuvo necesidad de financiación exterior en los años de bonanza económica (1999-2012) lo que ha generado unos efectos perniciosos que se mantendrán en el tiempo.

Una posición internacional tan negativa limita el crecimiento futuro. Por un lado, debo pagar lo que debo y por otro, mi economía se vuelve muy vulnerable a cualquier perturbación exterior. Todo esto conlleva a una pérdida generalizada de confianza.

A todo esto se suma la crisis del sistema financiero español que colocó a España a borde del precipicio en el verano de 2012. Algunos Bancos y principalmente las Cajas –aunque no todas- alentaron a los excesos y finamente se convirtieron en víctimas. Cuando la crisis internacional cortó la liquidez y la construcción se desplomó, los balances de las entidades financieras implicadas no valían nada. Afortunadamente en agosto del 2012 llego el rescate financiero a España: un tema bien resuelto. Por todo ello, podemos decir que en el momento actual el sistema financiero español se encuentra en excelentes condiciones en términos comparados tal y como han demostrado los test a los que nos el Banco Central Europeo ha sometido a nuestras entidades financieras.

Pero no todos los problemas actuales derivan de la mala gestión de los años de crecimiento, ni mucho menos, algunos son estructurales, casi crónicos en España.

3.2. *Los problemas estructurales*

Desde mediados de los años ochenta se viene produciendo una pérdida importante del sector industrial en la economía, del mismo modo que en Europa y EEUU. En 1985 la industria suponía un 24,5 % de PIB español ahora está en torno a un 16,8%.

La industria es un sector que genera elevados crecimientos de la productividad del trabajo (la clave del crecimiento económico) por su capacidad para incorporar avance tecnológico y capital físico y humano. Por lo tanto, es la clave para el crecimiento económico. Si cada vez tenemos menos industria y más servicios (generadores de bajas tasas de productividad) tenemos un problema.

Además, la empresa española se caracteriza por un tamaño de PYME por muchos factores (factores productivos, baja tecnología,

etc). Si la recuperación económica pasa por la demanda externa y en el mundo globalizado vender en los mercados exteriores pasa por tener empresas de elevada dimensión.

Sin embargo, el problema estructural más grave que padece la economía española es en el mal desarrollo de su mercado de trabajo. Nuestro mercado de trabajo es incapaz de adaptarse a los ciclos económicos. Tan intolerable es una tasa de paro del 27% como hemos tenido recientemente como una del 8% en 2007. Las reglas del mercado de trabajo deben cambiarse radicalmente, hasta ahora sólo se han puesto parches. Reglas inadecuadas y deficiencias en la formación de la mano de obra están en la raíz de un problema que está minando la convivencia y el futuro del país.

Superada la crisis técnicamente desde el tercer trimestre de 2013, el escenario español de los últimos meses mucho ha cambiado y no debido a la economía si no a la política. Nada crea tanta incertidumbre como la inestabilidad institucional. Como estamos muy endeudados todavía necesitamos mayor estabilidad institucional. Nuestra gran vulnerabilidad es el exceso de endeudamiento que amenaza el crecimiento económico y por lo tanto la estabilidad económica y financiera. España se enfrenta a varios focos que destruyen su credibilidad institucional: la desafección de los ciudadanos y el desafío secesionista de Cataluña y la interinidad gubernamental. Sin lugar a dudas, la posible repetición de las elecciones por tercera vez en un año llevaría a nuestro país a una situación de descrédito internacional. Una evolución negativa estos parámetros puede dar al traste con las posibilidades de recuperación económica.

Del mismo modo que antes tenía sentido decir que la crisis económica podía derivar en un problema político, ahora la inestabilidad política puede erigirse en obstáculo central para la recuperación económica. Pero a esto hay que sumarle la situación internacional cambiante. El futuro es incierto.

4. Conclusión

Es necesario poner el valor todo lo positivo, que sin lugar a dudas, es mucho. Hemos conseguido el equilibrio exterior sólo con una devaluación interior, estamos creciendo más de lo esperado y somos ejemplo para otros según las autoridades comunitarias. Sin embargo, la percepción de la ciudadanía no cambiará

hasta que se reduzca apreciablemente el paro y las desigualdades en los niveles de renta. Hay que hacer política económica de alto perfil si queremos remontar la crisis y alejar los fantasmas del estancamiento. Tenemos que centrarnos en la reindustrialización, la formación de la mano de obra, la rigidez del mercado de trabajo.

En estas circunstancias, en el año 2016, el contexto internacional se sitúa en posiciones de riesgo y además se presenta repleto de incertidumbres institucionales lo que nos hace sospechar que no supone el mejor caldo de cultivo para llevar a cabo las políticas económicas necesarias sin que a nadie le tiemble el pulso.

Queremos sentirnos menos amenazados por la situación económica, hemos emprendido el camino correcto, pero ahora hay que hacerlo. No dejemos que la desafección social, el problema catalán y el populismo acaben con la posibilidad de salir de la crisis. Pero para todo esto necesitamos de un gobierno aunque algunos argumenten que la economía va bien a pesar de la interinidad que vive el país. Pues bien, el globo del crecimiento económico ha soportado el tirón nueve meses y se está vaciando de oxígeno ya que las perspectivas de futuro próximo muestran una ralentización de la economía española.

5. Bibliografía

Barbé, Esther, *La seguridad en la nueva Europa: Una aproximación institucional: Unión Europea, OTAN y UEO*. Madrid. Ed. Los Libros de la Catarata. 1995. 251 págs.

Buzan, Barry, «New patterns of global security in the twenty-first century». *International Affairs (Royal Institute of International Affairs 1944-)*, vol. 67, núm. 3, 1991, págs. 431-451

La Defensa Nacional y las Fuerzas Armadas X, Centro de Investigaciones Sociológicas, Estudio CIS núm. 2998, Madrid, 2013.

La Defensa Nacional y las Fuerzas Armadas IX. Centro de Investigaciones Sociológicas, Estudio CIS núm. 2912. Madrid, 2011.

Informe de resultados del X estudio del CIS: La Defensa Nacional y las Fuerzas Armadas, Instituto Español de Estudios Estratégico, Ministerio de Defensa, 2013.

Estudio encuesta «Defensa Nacional y Fuerzas Armadas», Instituto Español de Estudios Estratégico, Ministerio de Defensa, 2011.

Estadísticas nacionales, Instituto Nacional de Estadística (varios años), Ministerio de Economía y Competitividad.

Middle Easterners see religious and ethnic hatred as top global threat. Europeans and Americans focus on inequality as greatest danger, Pew Research Center, 2014, 27 págs.

La Estrategia de Seguridad Nacional: un proyecto compartido. Departamento de Seguridad Nacional. Presidencia de Gobierno, 2013.

Barómetro DEL Real Instituto Elcano (BRIE), 35ª oleada, Resultados de Abril de 2014, Real Instituto Elcano, Madrid, 2014, 74 págs.

La economía en una nueva legislatura, Círculo Cívico de Opinión, Madrid, 2016

Economía española: el realismo obligado. La hora de la política. Círculo Cívico de Opinión, Madrid, 2015.

UNA PERSPECTIVA ECONÓMICA DE LA PARTICIPACIÓN ESPAÑOLA EN LAS OPERACIONES DE MANTENIMIENTO DE LA PAZ

Juan José Aizpuru Díaz de Terán
Cátedra Paz, Seguridad y Defensa
Universidad de Zaragoza

Resumen

En los 27 años que España lleva participando en misiones internacionales se han invertido algo más de 10.000 millones de euros, en las que han intervenido más de 137.000 soldados en cuatro continentes han avalado el papel de España en la comunidad internacional, pero, al mismo tiempo, han exigido unos sacrificios tanto en personal como en material normalmente superiores a los recursos que las Fuerzas Armadas (FAS) disponían. Esta mayor notoriedad que suponen las misiones en el exterior de nuestras FAS, se ha traducido en un continuo incremento de los fondos que las sustentan, alcanzando en el año 2015, el 12,39% del presupuesto asignado al Ministerio de Defensa. La peculiaridad que supone la forma de financiación ha permitido superar las particularidades que entrañan la puesta en marcha y el normal funcionamiento de estas misiones. Teniendo en cuenta el número de misiones activas en estos momentos y el clima de crisis económica en el que nos encontramos, la cuestión de la financiación de las mismas se vuelve cada vez más fundamental.

Palabras claves

Gasto en Defensa, Economía de Defensa, Operaciones de Paz, Seguridad Nacional.

1. Introducción

En las últimas décadas, numerosos condicionantes han generado un cambio sustancial y radical en el panorama estratégico: por un lado, se ha producido la desaparición de los bloques que sustentaban la estrategia de la guerra fría; por otro, aparecen nuevas formas de violencia e inestabilidad.

Desde mediados de los ochenta, España se ha incorporado a organizaciones y alianzas internacionales de seguridad y defensa asumiendo responsabilidades en política exterior y de seguridad común, obligando a reorganizar los objetivos de seguridad y defensa y exigiendo un continuo incremento de los recursos económicos destinados a estos fines entre los que se encuentra la financiación de nuestra participación en operaciones de mantenimiento de la paz.

El objetivo de esta comunicación se materializa en el estudio del proceso de financiación y presupuestación de las Operaciones de Mantenimiento de la Paz (OMP) así como la cuantificación de los compromisos políticos nacionales con la comunidad internacional.

2. Antecedentes

La participación española en OMP se inicia oficialmente en 1989[1], cuando el entonces Secretario General de las ONU, Pérez de Cuellar, solicita la presencia española en la misión de verificación de la retirada de tropas cubanas de Angola (UNAVEM) con el envío de siete observadores militares. Desde entonces, más de 137.000 efectivos han participado en más de 50 misiones internacionales y de ayuda humanitaria, realizando un importante esfuerzo económico para sufragar todos los gastos de estas misiones cuyo importe total durante este periodo asciende aproximadamente a algo más de 10.000 millones de euros[2].

Aunque la participación de España en las misiones en el extranjero tiene una corta historia de algo más de 25 años, la presencia de sus FAS en el exterior, ha contribuido a aumentar y fortalecer el prestigio que la sociedad española tiene de sus Fuerzas Armadas.

El apoyo de España a la comunidad internacional en la prevención y solución de los conflictos en el mundo, da cumplimiento a uno de los principios contemplados en el preámbulo de la Constitución: «Colaborar en el fortalecimiento de unas relaciones

1. El 3 de enero de 1989, las FAS españolas se sumaron por primera vez en una operación de las NNUU, al amparo de la Resolución 632/89 del CSNU.

2. En julio de 2016 se encuentran 2109 militares desplegados en 15 operaciones en el exterior.

pacíficas y de eficaz colaboración entre todos los pueblos de la tierra».

La Ley Orgánica 5/2005 de la Defensa Nacional[3] y recogido en la Directiva de Defensa Nacional 1/2012, establece que España ha de desempeñar un papel cada vez más destacado en la esfera internacional y por ello, sus Fuerzas Armadas han de ser el instrumento de la acción exterior a través de su participación en las diversas organizaciones internacionales de seguridad y defensa[4], especialmente en el marco de la Unión Europea y de la Política Europea de Seguridad y Defensa[5].

La aparición en 2013 de la Estrategia de Seguridad Nacional (ESN)[6] en la que quedan reflejados los riesgos y amenazas a los que es necesario hacer frente en una situación global en continuo cambio, recoge la contribución de España a la seguridad internacional, junto a nuestros socios y aliados, en cumplimiento de los compromisos adquiridos. En los mismos extremos se expresa la Ley 36/2015 de Seguridad Nacional[7].

La Ley 2/2014 de la Acción Exterior y del Servicio Exterior del Estado[8] establece que la actuación de las FAS en el ámbito internacional se enmarcará en el conjunto de la acción exterior del Estado, como elemento esencial para garantizar la seguridad y defensa de España y para contribuir a nuestra proyección internacional y al mantenimiento de la paz y seguridad internacionales.

3. Ley Orgánica 5/2005, de 17 de noviembre, de la Defensa Nacional.

4. Art. 15.2 Las Fuerzas Armadas contribuyen militarmente a la seguridad y defensa de España y de sus aliados, en el marco de las organizaciones internacionales de las que España forma parte, así como al mantenimiento de la paz, la estabilidad y la ayuda humanitaria .

5. Durante el primer semestre de 2016, España despliega en todas las operaciones y misiones de la UE siendo el tercer contribuyente de fuerzas.

6. Estrategia de Seguridad Nacional, aprobada en Consejo de Ministros del 31 de mayo de 2013.

7. Ley 36/2015, de 29 de septiembre, de Seguridad Nacional. Artículo 3.- Se entenderá por Seguridad Nacional 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 adquiridos.

8. Ley 2/2014, de 25 de marzo, de la Acción y del Servicio Exterior del Estado.

El compromiso español con las OMP se desarrolla en paralelo con el proceso de transformación estructural de las FAS cuyos elementos característicos fueron la profesionalización, la transformación de un ejército territorial en otro funcional y proyectable, la internalización al estar cada vez más implicadas nuestras FAS en misiones en el exterior y la modernización e interoperabilidad, que supuso la normalización y consolidación de la presencia española en organizaciones de seguridad y defensa y, muy especialmente, en la OTAN y UE.

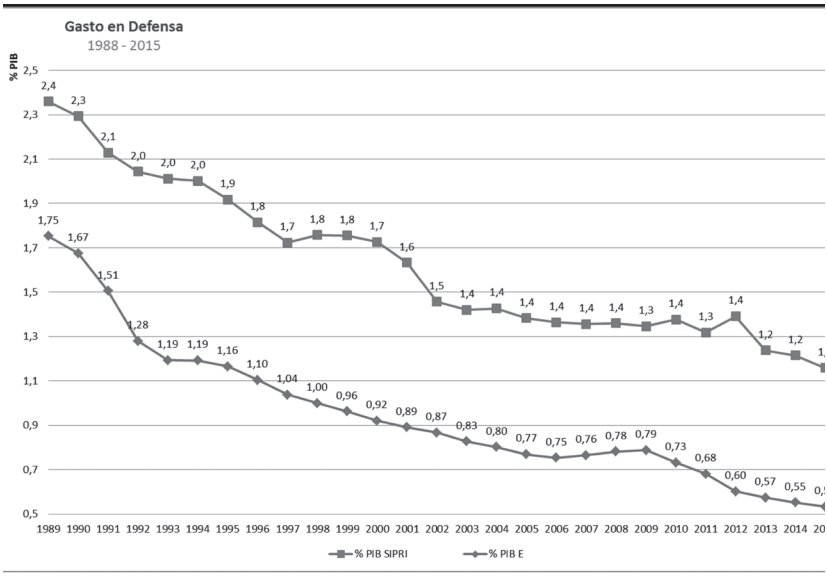
En el terreno presupuestario podemos decir que en ningún momento de la historia reciente de España se ha producido una situación de suficiencia financiera para el Ministerio de Defensa. Los presupuestos han sido siempre bajos y las situaciones de crisis han empeorado el escenario financiero. A esto hay que añadir la escasa cultura de Defensa de los ciudadanos, que les impide ser conscientes de los riesgos y amenazas que afectan a nuestro entorno. La plena asunción de los compromisos y responsabilidades en la esfera internacional exige un continuo incremento de los recursos económicos destinados a estos fines, bien para hacer frente a la creciente presencia, permanente o temporal, de nuestras FAS en el extranjero, bien para financiar nuestra actividad en operaciones de mantenimiento de la paz, bien para abonar nuestras cuotas de participación en dichas organizaciones internacionales.

3. Evolución del presupuesto de defensa

España mantiene una política de contención del gasto en Defensa, como la mayor parte de los países europeos, independiente de la situación de crisis actual, que contrasta con sus crecientes compromisos internacionales. Esta situación genera distorsiones lo que obligó a buscar más fuentes de financiación: las modificaciones presupuestarias de las OMP,s. con cargo al Fondo de Contingencia de ejecución presupuestaria, la venta de patrimonio militar (Instituto de la Vivienda y Equipamiento para la Defensa - INVIED) y los anticipos a través del Ministerio de Industria, Energía y Turismo que financian los grandes programas de la Defensa. En el Cuadro 1 se representa la evolución del Presupuesto de Defensa respecto al PIB a precios corrientes desde el año 1989 al 2015 y, al mismo tiempo, se representa el esfuerzo en Defensa realizado por España, en el mismo periodo, pero considerando el

criterio definido por el Stockholm International Peace Research Institute[9] (SIPRI). Como se puede observar, el descenso ha sido continuado en el esfuerzo inicial en Defensa en el periodo considerado, situándose por debajo del 2% recomendado por la OTAN, y que desde 1999 se sitúa por debajo del 1%.

Cuadro 1: Esfuerzo en Defensa como porcentaje del PIB

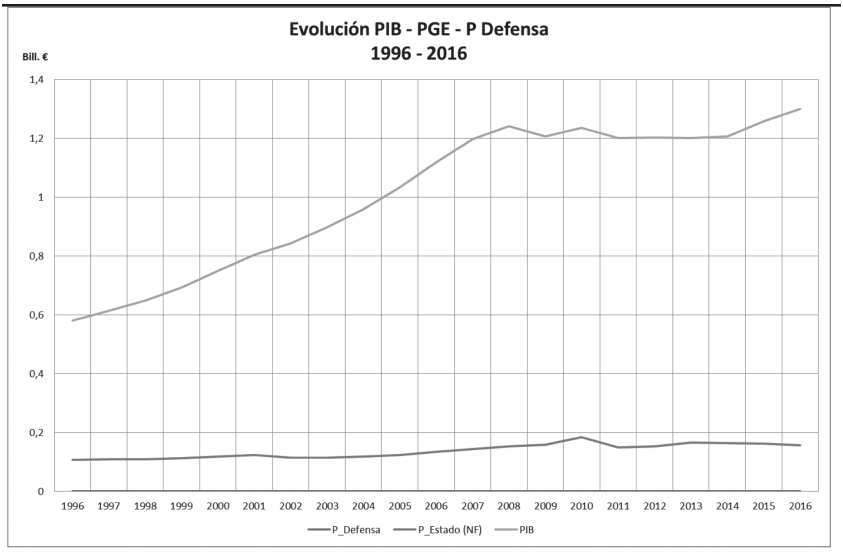


A la vista del Cuadro 2 que refleja la evolución del PIB nacional, los Presupuestos iniciales del Estado (no financiero) y Defensa, en el periodo 1996-2016. Podemos afirmar que los Presupuestos de Defensa son independientes de la evolución del

9. Los datos utilizados por SIPRI se basan en la definición OTAN de los gastos de defensa incorporando todos los gastos relativos a las FAS, incluidas las fuerzas de mantenimiento de la paz, los ministerios de defensa y demás organismos del gobierno que participan en proyectos de defensa; las fuerzas paramilitares, si se consideran que están entrenadas y equipadas para operaciones militares; y las actividades en el área militar. Dichos gastos incluyen el personal militar y civil, incluidas las pensiones de retiro del personal militar y servicios sociales para el personal, operación y mantenimiento, compras, I+D militar y ayuda militar (en el país donante). No incluye la defensa civil y los gastos corrientes de actividades previas, como los beneficios para veteranos, desmovilización, conversión y destrucción de armas.

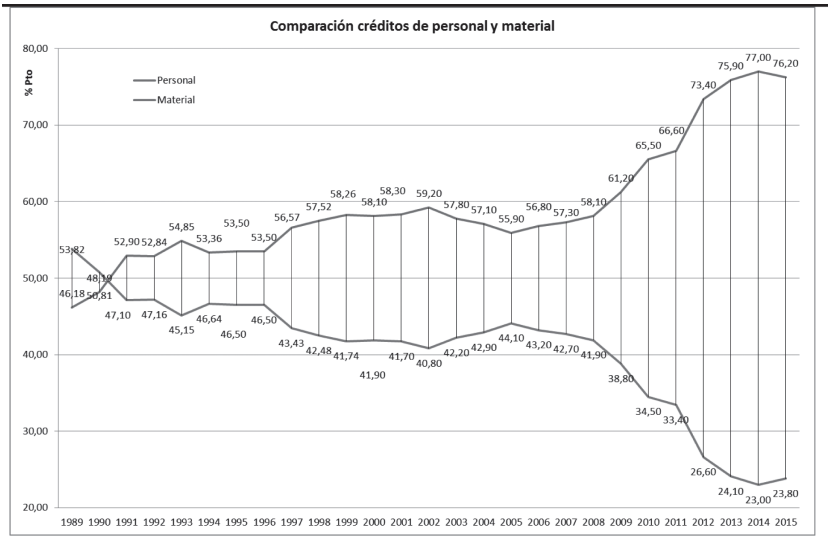
PIB Nacional, es decir, independientes del ciclo económico, no existiendo una correlación entre el aumento experimentado en los últimos 20 años en el PIB y el Presupuesto de Defensa.

Cuadro 2: Evolución PIB / PGE / P Defensa



En el cuadro 3 queda reflejada la importancia del gasto de personal del Ministerio de Defensa, llegando en los últimos años a representar valores superiores al 75% del presupuesto total, que supone una severa restricción al resto de partidas presupuestarias: las correspondientes a Gastos Corrientes (capítulo 2) que contribuyen a mejorar la operatividad de las fuerzas y reforzar la seguridad y la calidad de vida de los militares profesionales y las que contribuyen a la modernización y mantenimiento de los sistemas recogidas en el capítulo 6 de los presupuestos.

Cuadro 3: Comparación créditos de personal y material



Como consecuencia de la crisis, los continuos recortes presupuestarios efectuados desde el 2008 al 2015, el Presupuesto de Defensa ha disminuido un 36%, lo que ha situado a las FAS bajo mínimos no pudiendo asegurar su operatividad por la falta de recursos, excepto aquellas Unidades que están implicadas en operaciones de paz al recibir una financiación para ello.

4. La financiación de las misiones en el exterior

En el marco de las organizaciones internacionales (ONU, OTAN y UE) las operaciones en el exterior son financiadas totalmente con fondos públicos. Los mecanismos de financiación son básicamente dos: a través del presupuesto de la respectiva organización y mediante las aportaciones directas de los Estados miembros.

Las aportaciones nacionales pueden ser recursos materiales como contingentes militares, armamento e infraestructuras y recursos financieros en forma de pagos monetarios conforme a distintas fórmulas de financiación. La característica común a todos los sistemas de financiación es que las organizaciones no disponen de personal y equipos propios, sino que se apoyan en las capacidades nacionales de los miembros. Estas formas de aportación son las que van a particularizar los distintos mecanismos de

financiación. Así, la financiación de las operaciones de la ONU procede en su mayor parte de un presupuesto específico de la propia organización. En el caso de la OTAN, la contribución proviene en una mínima parte del presupuesto de la organización, siendo la contribución de los Estados miembros la parte principal de su financiación. Con respecto a la UE, la financiación está fragmentada entre las aportaciones de los Estados a la Política Exterior y de Seguridad Común (PESC) y las realizadas a la Política al Desarrollo y de la Oficina de Ayuda Humanitaria (ECHO).

En los puntos siguientes analizamos brevemente el sistema de financiación de las organizaciones antes indicadas.

4.1. *Naciones Unidas (NN.UU.)*

La decisión de establecer, mantener o ampliar una operación le corresponde al Consejo de Seguridad de Naciones Unidas (CSNU), pero la financiación de las mismas es responsabilidad colectiva de todos los Estados miembros, conforme a lo dispuesto en el artículo 17 de la Carta de NN.UU.[10].

Las aportaciones de la Asamblea General a los gastos derivados de las operaciones de paz se basan en una escala especial que se establece mediante una fórmula compleja establecida por los propios Estados miembros, en la que se tiene en cuenta, entre otras cosas, la riqueza nacional[11].

El proceso de inicio de una operación comienza con la propuesta por el Secretario General al Consejo de Seguridad mediante un informe en el que se incluye una primera estimación de su coste. Una vez autorizado por el CSNU, el Departamento de

10. 1. La Asamblea General examinará y aprobará el presupuesto de la Organización.

2. Los miembros sufragarán los gastos de la Organización en la proporción que determine la Asamblea General.

3. La Asamblea General considerará y aprobará los arreglos financieros y presupuestarios que se celebren con los organismos especializados de que trata el artículo 57 y examinará los presupuestos administrativos de tales organismos especializados con el fin de hacer recomendaciones a los organismos correspondientes.

11. La escala de cuotas para el prorrateo de los gastos de las operaciones de NN.UU. para el mantenimiento de la paz, durante el periodo 2016-2018, fue aprobada por la Asamblea General, Resolución 70/246, el 23 de diciembre de 2015.

Operaciones de Mantenimiento de la Paz (DOMP) prepara el presupuesto de la operación que es aprobado siguiendo los mismos trámites que el presupuesto ordinario, es decir, por la Asamblea General, previo informe de la Quinta Comisión.

El presupuesto se realiza por cada operación, durante un periodo que abarca desde el 1 de julio al 30 de junio y en el que se incluye el Memorando de Entendimiento (MOU) que cada país participante en la operación y el DOMP han firmado. El MOU detalla el despliegue operativo a realizar, incluyendo los medios personales (personal militar y de policía, personal civil) y materiales (transporte, instalaciones e infraestructuras, comunicaciones, etc.) a utilizar, así como las responsabilidades y las reglas de mantenimiento y necesidades de autoabastecimiento. A través de este desglose se puede determinar los reembolsos que NN.UU. pagará al Estado participante por la utilización de dichos medios, que se calculan en función de una serie de importes individuales que se actualizan periódicamente por la Asamblea General[12].

La financiación de las operaciones de NN.UU. se basa en un sistema de reembolso a las naciones participantes. Básicamente NN.UU. «contrata» a una Unidad de un Estado para cumplir una misión y le resarce de los gastos ocasionados. Esto hace que los mayores contribuyentes con tropas a las operaciones sean Estados de África y Asia que ven, de esta forma, una fuente de ingresos complementaria en sus presupuestos.

El sistema de reembolsos es un arma de doble filo. Por un lado, favorece la participación de las naciones, ya que, en el peor de los casos, aliviará la carga sobre los presupuestos nacionales respectivos. Pero, por otro lado, las naciones que son las mayores contribuyentes con tropas (Bangladesh, Etiopía, India y Pakistán) no ofrecen o no tienen las más modernas capacidades. Esto produce carencias en los sistemas de mando y control, inteligencia y otras capacidades más avanzadas.

En el cuadro 4 se reflejan los diez principales Estados proveedores de financiación en las en el periodo 2013-2015[13] así

12. El procedimiento de reembolso está recogido en la Resolución 50/222 de 10 de mayo de 1996, de la Asamblea General, así como la aplicación del Documento de la Quinta Comisión A/C.5/66/8, de 27 de octubre de 2011, *Manual sobre el equipo propiedad de los contingentes.*

13. A/67/224/Add.1.

como los diez Estados principales contribuyentes de tropas a 31 de diciembre de 2015.

Cuadro 4: Principales contribuyentes de tropas y proveedores de financiación

Estados / efectivos (31-XII-2015)		**Estados / % financiación** (Periodo 2013-2015)	
Bangladesh	**8.496**	Estados Unidos	**28,38**
Etiopía	**8.296**	Japón	**10,83**
India	**7.798**	Francia	**7,22**
Pakistán	**7.643**	Alemania	**7,14**
Ruanda	**6.077**	Reino Unido	**6,68**
Nepal	**5.344**	China	**6,64**
Senegal	**3.475**	Italia	**4,45**
Ghana	**3.198**	Federación Rusa	**3,15**
China	**3.045**	Canadá	**2,98**
Nigeria	**2.954**	España	**2,97**

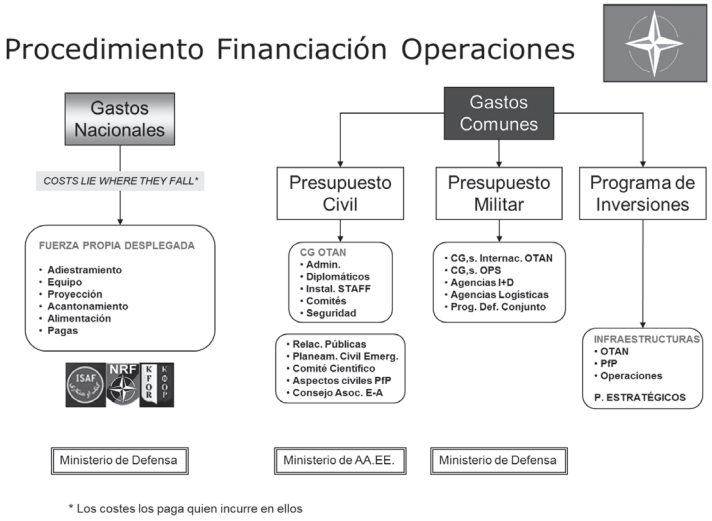
Fuente: Elaboración propia a partir de los datos obtenidos de www.un.org

4.2. *Organización del Tratado del Atlántico Norte (OTAN)*

La mayor parte de la financiación de las operaciones OTAN proviene de las aportaciones directas de sus Estados miembros al operar bajo el principio «*Costs lie where they fall*»[14]. Si embargo hay actividades cuyo coste no puede atribuirse a una nación determinada (por ejemplo, un Cuartel General internacional) para lo cual se desarrolló la denominada «financiación común» que consiste en un reparto de los costes entre todas las naciones aliadas conforme a su respectiva capacidad económica y al proceso de negociación política en cada caso. En el cuadro 5 se detalla un esquema del procedimiento de financiación en la Organización.

14. Los costes los paga quien incurre en ellos.

Cuadro 5: Esquema de la financiación OTAN



OTAN ha articulado el concepto *NATO Response Force* (NRF) a efectos de afrontar las posibles crisis que pudieran aparecer. El NRF es una fuerza multinacional de respuesta rápida compuesta por unidades terrestres, aéreas, marítimas y de fuerzas especiales proporcionada por los Estados miembros, que pueden desplegarse en cualquier momento en caso de conflicto, compuesto por aproximadamente trece mil efectivos en turnos rotatorios de doce meses y una fuerza de reserva que pueda sustituir a la anterior en caso necesario.

La carga financiera que deben soportar los Estados de guardia en el NRF en caso de implementación de una operación es enorme (creación de pistas de aterrizaje, construcción de infraestructuras logísticas, etc.) por lo que puede llegar a disuadir a las naciones a ser el primero en ofrecerse en la operación, podría aumentar la desmotivación en la participación en el NRF y afectar negativamente a la OTAN en el Área de Operaciones en el futuro, en el caso de que los Estados que más aportan a las operaciones no vean una mayor implicación por parte del resto de Estados.

4.3. *Unión Europea (UE)*

El estudio de la financiación de las operaciones en el marco de la UE es todo un desafío en la medida en que se incardina en

la de por si conflictiva y fragmentada financiación de la Política Exterior y de Seguridad Común (PESC). En 1999 la UE, en el marco de la Política Común de Seguridad y Defensa (PCSD), como parte integrante de la PESC, empezó a desarrollar sus propias capacidades y actividades de apoyo a la paz y a la seguridad internacional, liderando, desde 2003, más de una treintena de operaciones de mantenimiento de la paz en el exterior, distinguiendo entre operaciones civiles y operaciones militares.

Precisamente esa distinción entre lo civil y lo militar es la base del sistema de financiación de la PESC en general y de sus operaciones en particular. La existencia de estas dos fuentes de financiación es recogida en el artículo 41 del actual Tratado de Lisboa:

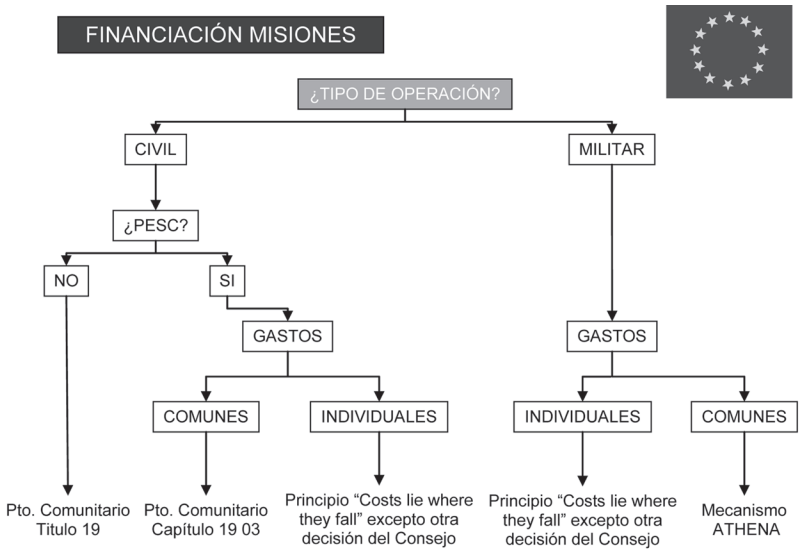
—Los gastos de carácter administrativo, es decir, los gastos de funcionamiento así como el conjunto de los gastos de carácter operativo como consecuencia del ejercicio de sus funciones y/o de puesta en marcha de las actuaciones derivadas de la PESC, se financiarán a través del Presupuesto de la UE.

—Los gastos derivados de las operaciones con repercusiones en el ámbito militar o de la defensa, así como aquéllos otros casos establecidos por el Consejo por unanimidad, correrán a cargo de los Estados miembros con arreglo a una clave de reparto basada en el producto nacional bruto[15].

En el cuadro 6 se presenta un esquema de cómo se financian las misiones de la UE.

15. Como excepción, aquéllos Estados cuyos representantes en el Consejo hayan efectuado una declaración formal con arreglo al párrafo segundo del apartado 1 del artículo 31 (regla de la abstención constructiva), no estarán obligados a contribuir a su financiación cuando se trate de operaciones que tengan repercusiones en el ámbito militar y de defensa. Dinamarca es el único Estado que ha decidido separarse de la aplicación de la PESC.

Cuadro 6: Esquema financiación misiones UE



Por tanto, la PESC es financiada por el presupuesto comunitario salvo por lo que respeta a las operaciones militares y aquellas que el Consejo decida excluir para cuya financiación ha creado un mecanismo intergubernamental específico: el mecanismo ATHENA[16], creado en 2004 cuando el Consejo adoptó la Decisión 2004/197/PESC.

Athena es un organismo dotado de personalidad jurídica, capacidad de obrar y sin ánimo de lucro, que actúa en nombre de los Estados; dispuesto ante cualquier operación militar de la UE, bajo la autoridad de un Comité Especial compuesto de un representante de cada Estado miembro participante y cuenta con un Administrador, nombrado por el Secretario General del Consejo, el Comandante de cada operación y el Contable, nombrado también por el Secretario General del Consejo.

Athena gestiona los gastos comunes originados por las operaciones militares, distinguiéndose las siguientes categorías, recogidas en los anexos I al IV de la Decisión (PESC) 2015/528:

16. La regulación actual está recogida en la Decisión (PESC) 2015/528 del Consejo, de 27 de marzo de 2015, por la que se crea un mecanismo para administrar la financiación de los costes comunes de las operaciones de la UE que tengan repercusiones en el ámbito militar o de la defensa.

—Costes comunes que estarán a cargo de Athena siempre que se generen, por ser gastos que no pueden vincularse a una operación (Anexo I).
—Costes operativos comunes correspondientes a la fase preparatoria de una operación, que incluyen gastos adicionales para las misiones de exploración y los preparativos para el lanzamiento de una misión (Anexo II).
—Costes de la fase activa de la operación, es decir, desde su lanzamiento, que suele coincidir con el nombramiento del Comandante de la operación, hasta la finalización de la misma (Anexo III).
—Costes operativos comunes relativos a la conclusión de una operación que estarán a cargo de Athena, que son los gastos derivados del destino final de las infraestructuras y equipos comunes, así como los del establecimiento de las cuentas de la operación (Anexo IV).

Los ingresos de Athena están constituidos por las cuotas de los Estados participantes que se calculan en función de la clave de reparto basada en el producto nacional bruto contemplada en el artículo 41, apartado 2, del Tratado y de conformidad con lo dispuesto en la Decisión 2014/335/UE-Euratom, por las aportaciones de terceros Estados que participen en la operación (en función del acuerdo bilateral formalizado entre las partes) y otros ingresos diversos (que incluyen los intereses percibidos, los ingresos procedentes de las ventas y el saldo de ejecución del ejercicio anterior, después de que lo haya determinado el Comité Especial).

Para los gastos individuales por la participación de un Estado en una operación militar rige el principio «*Cost lie where they fall*», al igual que en OTAN, por lo que también pueden ocurrir los mismos peligros en el caso de que los Estados que más aportan a estas operaciones no vean una mayor implicación por parte del resto de Estados.

5. Financiación de las operaciones de mantenimiento de la paz en España

Desde 1989, año en que se llevó a cabo la primera misión española en el exterior, hasta la actualidad, la participación en estas misiones no ha dejado de incrementarse con el consiguien-

te incremento del gasto, pasando de 18 millones de euros en el ejercicio 1990 los 1.000 millones de euros en el año 2015.

La financiación de la participación de las FAS españolas en las OMP hasta el año 2011, se realizaba con cargo a los créditos de un concepto presupuestario que se crea en 1990 específicamente para este fin: el concepto 228, inicialmente con la denominación «Gastos originados por la participación de las Fuerzas Armadas Españolas en operaciones de la ONU»[17], en la que se incluyen todos los gastos de personal, funcionamiento e inversiones ocasionados por las Unidades que participen en las operaciones.

La imputación de todos los gastos de estas operaciones en un único concepto, 228, dentro del capítulo 2 «Gastos corrientes en bienes y servicios», supone una excepción a los criterios generales de clasificación económica que rigen el gasto público, que exigen la imputación de estos gastos en los capítulos 1 «Gastos de personal», capítulo 2 «Gastos corrientes en bienes y servicios» y 6 «Inversiones reales», según corresponda.

Este concepto, desde el punto de vista de la clasificación funcional, está enmarcado en el programa presupuestario 122 M «Gastos operativos de las FAS» y asignado a la Secretaría de Estado de Defensa (SEDEF) como centro de responsabilidad del gasto, que incluye los créditos necesarios para la preparación y funcionamiento de todas las Unidades encuadradas en la Fuerza.

Desde el año 2011 y de conformidad con las recomendaciones efectuadas por el Tribunal de Cuentas[18], se desglosó el concepto 228 en dos nuevos conceptos: 128 para recoger los gastos de personal participante en OMP y el 668 (inversiones) para los gastos en repuestos y mantenimiento originados por la participación de las FAS en OMP.

17. Resolución de la Dirección General de Presupuestos del Ministerio de Economía y Hacienda, de 6 de noviembre de 1990, por la que se determinan los criterios de imputación de gastos a esta rúbrica presupuestaria, que para justificar la creación exponía que con ello se consigue *dotar a las asignaciones presupuestarias previstas para esta finalidad de la flexibilidad precisa para cubrir con la prontitud adecuada las necesidades operativas que se planteen, sin que por ello se limite el control que para la gestión de los referidos créditos se establecen en las disposiciones legales y reglamentarias vigentes*».

18. Informe de fiscalización de la participación de las Fuerzas Armadas Españolas en misiones internacionales, ejercicios 2009 y 2010. Núm. 943 de 28 de junio de 2012.

Los tres conceptos, 128, 228 y 668, son de naturaleza ampliable[19], es decir, el crédito inicial puede incrementarse a lo largo del ejercicio, con carácter extraordinario y dentro del límite y las condiciones legalmente establecidas para este tipo de créditos, con cargo actualmente al Fondo de Contingencia de Ejecución Presupuestaria[20].

La peculiaridad de este tipo de créditos consiste en que no es su importe inicial el que limita el gasto sino que es el gasto el que determina el importe final del crédito. Gracias a ello los gestores no tienen que acoplarse inicialmente a un límite predeterminado sino que, una vez autorizado el comienzo de las operaciones preparatorias de la OMP, pueden programar los gastos, puesto que el crédito será ampliado hasta la cobertura total de las obligaciones incurridas. Este sistema busca, sobre todo, la flexibilidad, puesto que la naturaleza ampliable del crédito y su dotación con cargo a un fondo de reserva automático permite responder inmediatamente a cualquier tipo de necesidad.

Pero, tiene como inconveniente el del control parlamentario previo, pues se limita al importe de la dotación inicial. En consecuencia las Cortes sólo pueden conocer a posteriori el gasto finalmente ejecutado, a través de la información que se remite con carácter periódico, sin que les sea posible autorizarlo en su totalidad. No obstante, esa falta de control previo está mitigada por el hecho de que las Cortes sí autorizan el importe del Fondo de Contingencia y éste tiene carácter limitativo, con lo que la responsabilidad de asignar prioridades a los gastos cuyo crédito es ampliable se traslada al Gobierno.

19. Artículo 54 de la Ley 47/2003, de 26 de noviembre, General Presupuestaria: Créditos destinados a atender obligaciones específicas del respectivo ejercicio, derivadas de normas de rango de ley, que de modo taxativo y debidamente explicitados se relacionen en el estado de gastos de los Presupuestos Generales del Estado y, en su virtud, podrá ser incrementada su cuantía hasta el importe que alcancen las respectivas obligaciones.

20. El Real Decreto Legislativo 2/2007, de 28 de diciembre, por el que se aprueba el Texto Refundido de la Ley General de Estabilidad Presupuestaria, establece en su artículo 15 que dentro del límite de gasto fijado anualmente por el Estado, se incluirá una Sección Presupuestaria bajo la rúbrica «Fondo de Contingencia de ejecución presupuestaria» por importe del 2 por 100 del citado límite. Este Fondo destinará, cuando proceda, a atender necesidades de carácter no discrecional y no previstas en el presupuesto inicialmente aprobado, que puedan presentarse a lo largo del ejercicio.

Los importes consignados inicialmente en el presupuesto del Ministerio de Defensa han pasado de 300.000 euros en 1990 a algo más de 14 millones de euros en los últimos once años, mientras que el gasto final, como podemos ver en el cuadro 7, ha pasado de los 28M de euros en los primeros años a cuantías superiores a los 700 M de euros en los últimos años financiadas con ampliaciones de crédito. Nos encontramos ante cantidades que en 1990 significaban el 0,33% del Presupuesto final del Ministerio de Defensa a representar, en estos últimos años (a partir del 2006), porcentajes superiores al 8%, alcanzando en el año 2015 el 12,40%.

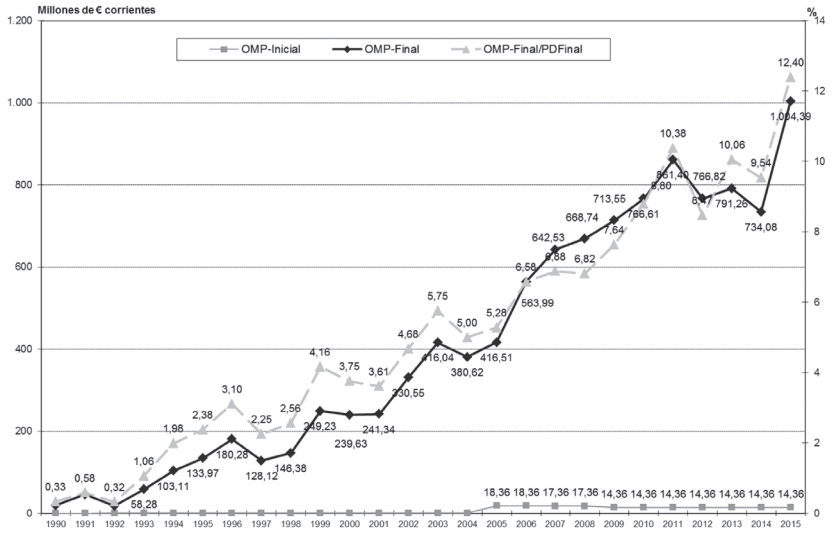
Desde un punto de vista normativo el Tribunal de Cuentas[21], en distintos informes de fiscalización[22], revela falta de rigor y realismo en la presupuestación y plantea la posibilidad de que, ante una consignación presupuestaria inicial tan baja y habida cuenta que estas misiones de esporádicas han devenido en permanentes, la presupuestación debe ser más realista teniendo en cuenta los compromisos adquiridos con los organismos internacionales. Si bien se puede objetar que la intensidad en la participación en estas misiones depende de decisiones políticas no previsibles, a priori, al estar condicionadas por la cambiante situación internacional. Pero, también es igualmente cierto que, sin perder el carácter de ampliable que su naturaleza requiere, la dotación inicial bien pudiera ser, cuando menos, del 50% de la ejecución final del ejercicio anterior, salvo que se prevea fundadamente la reducción de efectivos y/o escenarios del momento en el ejercicio siguiente.

21. Cossío y Alonso Rodríguez (2005).

22. Tribunal de cuentas. Informe núm. 564. Fiscalización de los gastos derivados de la participación de las Fuerzas Armadas en operaciones internacionales, ejercicios 1997-1998, de 25 de junio de 2002.

Informe núm. 943. Fiscalización de los gastos derivados de la participación de las Fuerzas Armadas en operaciones internacionales, ejercicios 2009 y 2010, de 28 de junio de 2012.

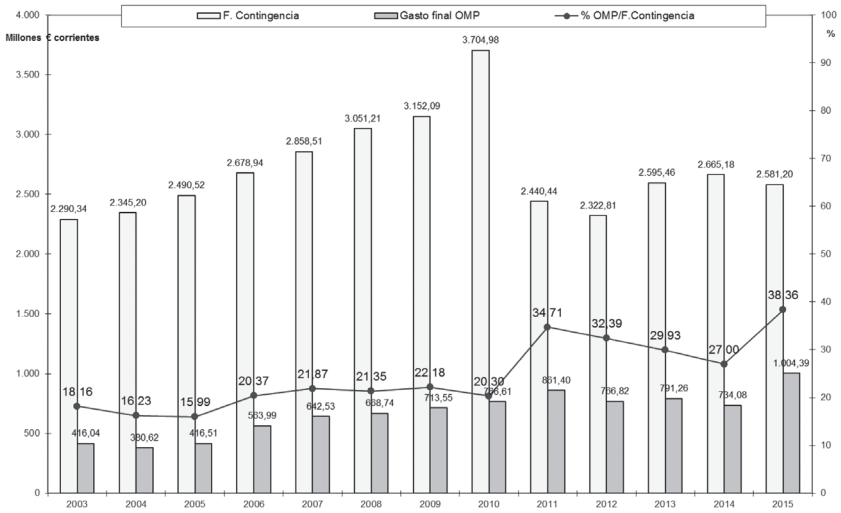
Cuadro 7: Evolución Gasto OMP (millones de euros corrientes)



Ahora bien, el problema estriba en la financiación que se realiza con cargo al Fondo de Contingencia de Ejecución Presupuestaria. En 2015, el importe total de este Fondo, para la totalidad de los Presupuestos Generales del Estado, ascendió a 2.581,20 millones de euros de los que, aproximadamente, 990 millones se destinaron a cubrir las necesidades de ampliación de crédito para los gastos de operaciones de paz.

Como se puede observar en el Cuadro 8, el crédito de OMP ampliado ha ido representando un porcentaje cada vez más alto, pasando del 18,16% en 2003 al 38,36% del total del Fondo en 2015, que en periodos de bonanza económica y superávit presupuestario puede ser asumible, pero no así cuando la economía crece menos que las previsiones macroeconómicas y en un entorno de déficit presupuestario, como el actual, será difícilmente sostenible, siendo la única alternativa la disminución de otros créditos.

Cuadro 8: Comparativa Fondo de Contingencia / Crédito OMP



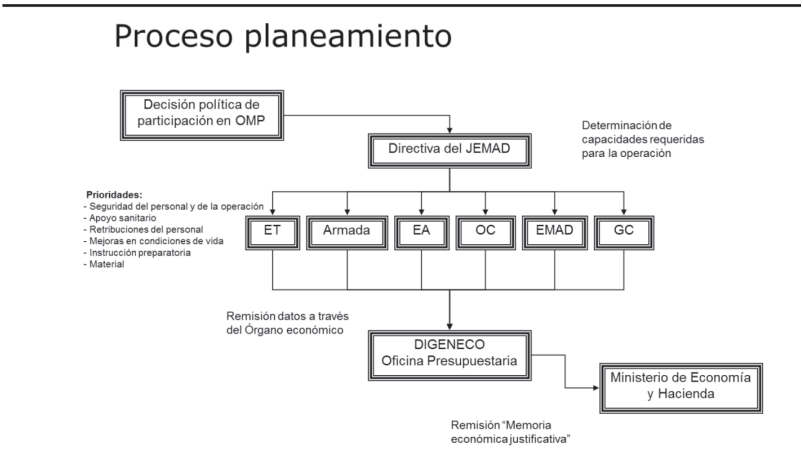
Como se ha indicado, el gasto en OMP está incluido en los tres conceptos: el 128, 228 y 668, pero a la hora de la estimación de los gastos debe realizarse separadamente por cada una de las operaciones. La Dirección General de Asuntos Económicos (DIGENECO) del Ministerio de Defensa[23] es la responsable de elaborar el expediente de ampliación de crédito[24].

El proceso de planeamiento presupuestario, como podemos ver en el Cuadro 9, comienza una vez que la Autoridad política ha decidido la participación de nuestras FAS en una operación fuera del de territorio nacional, ésta puede dar continuidad a una operación abierta o puede tratarse de poner en marcha una nueva misión. En base a esa decisión el Jefe de Estado Mayor de la Defensa (JEMAD) establece el tipo de fuerzas que será necesario para llevar a cabo la misión encomendada

23. Artículo 5 del Real Decreto 454/2012, de 5 de marzo, modificado por el Real Decreto 524/2014, de 20 de junio, que desarrolla la estructura orgánica básica del Ministerio de Defensa.

24. DIGENECO tiene elaborada una Instrucción interna con objeto de establecer los procedimientos de gestión y control de los recursos financieros destinados a financiar las operaciones de paz y ayuda humanitaria.

Cuadro 9: Proceso de planeamiento OMP.



Fuente: Elaboración propia a partir de datos de DIGENECO

Se inicia así la presupuestación en cada uno de los órganos, Ejército de Tierra, Armada, Ejército del Aire, Guardia Civil y Estado Mayor de la Defensa (EMAD), de acuerdo con su estructura y distribución de responsabilidades valorando las necesidades a satisfacer.

En el ámbito del Ejército de Tierra, el General de Ejército Jefe de Estado Mayor del Ejército (GEJEME), define las prioridades para atender las necesidades derivadas de la operación, así como sus variaciones, en función de la misión y situación, en consonancia con los aspectos derivados de la seguridad del personal y seguridad de la operación, apoyo sanitario, las retribuciones del personal, mejoras en las condiciones de vida, la instrucción preparatoria y el material necesario.

Para solicitar los créditos, cada ejército participante realiza una petición, justificada e individualizada por operación, de cada gasto con rigor y racionalidad económica, ajustando el gasto propuesto a las necesidades reales a satisfacer, teniendo en cuenta la evaluación de costes y los actuales escenarios. DIGENECO ha establecido una desagregación de los tipos de gastos que se atienden en los siguientes «conceptos» y «subconceptos», como podemos ver en el Cuadro 10:

—Concepto A: Retribuciones (Concepto presupuestario 128).
—Concepto B: Funcionamiento (Concepto presupuestario 228).
—Concepto C: Inversiones y Mantenimientos (Concepto presupuestario 668).

Con la información recibida, DIGENECO elabora una memoria justificativa que acompaña a la solicitud de aprobación de la ampliación de crédito que remite al Ministerio de Economía y Hacienda[25]. Todo este procedimiento supone un periodo importante desde su inicio hasta que el crédito se encuentra realmente a disposición de los gestores, lo que provoca en muchas ocasiones que no se disponga de los recursos necesarios para atender las necesidades existentes y se tenga que utilizar los créditos del presupuesto corriente para realizar, posteriormente, el cambio de financiación.

Cuadro 10: Conceptos de gastos

CONCEPTOS DE GASTO (Subconceptos)	
A.- RETRIBUCIONES	C.- INVERSIONES Y MANTENIMIENTO
B.- FUNCIONAMIENTO	C.1.- Armamento y equipo individual
B.1.- Arrendamientos	C.2.- Material móvil terrestre
B.2.- Combustibles	C.3.- Equipos de comunicaciones
B.3.- Vestuario	C.4.- Material de campamento
B.4.- Alimentación	C.5.- Obras civiles
B.5.- Material Sanitario	C.6.- Equipos diversos
B.6.- Transportes	C.7.- Municionamiento
B.7.- Otros gastos de vida y funcionamiento	C.8.- Mantenimiento de aeronaves
B.8.- Indemnizaciones por razón del servicio	C.9.- Mantenimiento de material móvil terrestre
	C.10.- Mantenimiento de equipos de comunicaciones
	C.11.- Mantenimiento de buques
	C.12.- Mantenimiento de equipos diversos

En el cuadro 11 representa la evolución del gasto total en OMP (euros corrientes) y los principales hitos en los incrementos producidos como consecuencia la participación en operaciones. Podemos observar que de los 18,75 millones de euros que en 1990 se destinaron a la operación «Alfa-Kilo» en el Kurdistán, se han pasado a más de 1.000 millones de euros en el 2015, lo

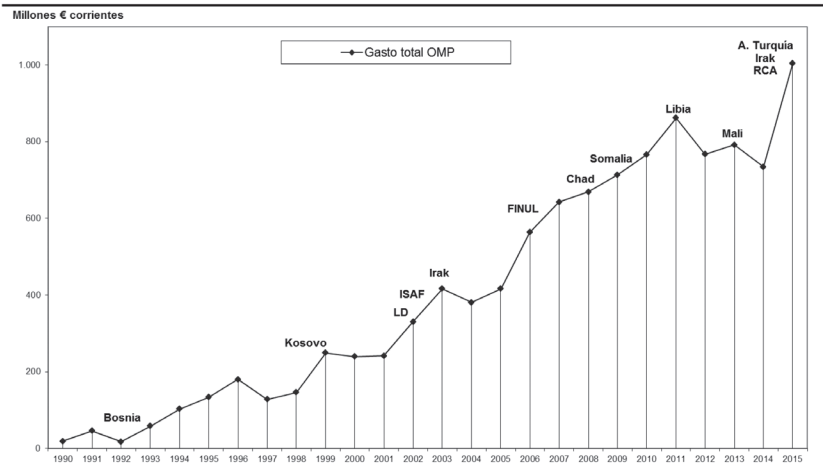
25. El artículo 62.1 d) de la Ley 47/2003, establece que corresponde al Ministerio de Economía y Hacienda la autorización de las ampliaciones de crédito previstas en el artículo 54.1.

que supone un incremento de más del 5000% desde esa primera participación.

En euros corrientes el gasto total, durante estos 27 años de participación de nuestras Fuerzas Armadas en las OMP, se ha elevado a más de 10.000 millones, de los que aproximadamente el 74,67% se ha realizado en la última década (2005-2015), motivado por la participación en operaciones que han requerido más financiación como Afganistán (ISAF), Líbano (FINUL) y Somalia (Atalanta) que representan el 43,88%, 20,29% y el 9,52% respectivamente del total del gasto (aproximadamente 8.000 millones de euros) en el periodo 2005-2015.

Con respecto a los conceptos de gasto (periodo 1990-2015) podemos indicar que, aproximadamente, el 18% corresponde a gastos de personal, el 32% a gastos de funcionamiento y el 50% a inversiones y mantenimiento.

Cuadro 11: Gasto total en OMP en millones de € corrientes



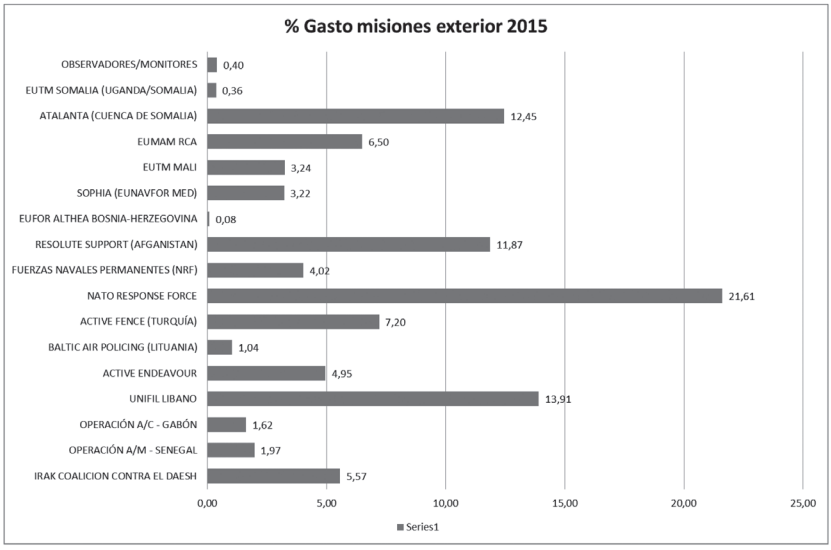
Fuente: Elaboración propia a partir de datos de DIGENECO

En la actualidad, nuestras FAS se encuentran participando en operaciones[26] en doce países (Afganistán, Bosnia-Herzegovina, Cabo Verde, Gabón, Irak, Líbano, Mali, República Centroafricana,

26. Disponible en http://www.defensa.gob.es/misiones/en_exterior/actuales/

Senegal, Somalia, Turquía y Yibuti), en tres continentes (África, Asia y Europa) y en cuatro zonas marítimas (mar del Norte, mar Mediterráneo, golfo de Guinea y océano Índico), lo que supone el mayor despliegue en cuanto número de escenarios en su historia.

Cuadro 12: Operaciones en el exterior a 31-diciembre-2015



Fuente: Elaboración propia a partir de datos de DIGENECO. Ministerio de Defensa.

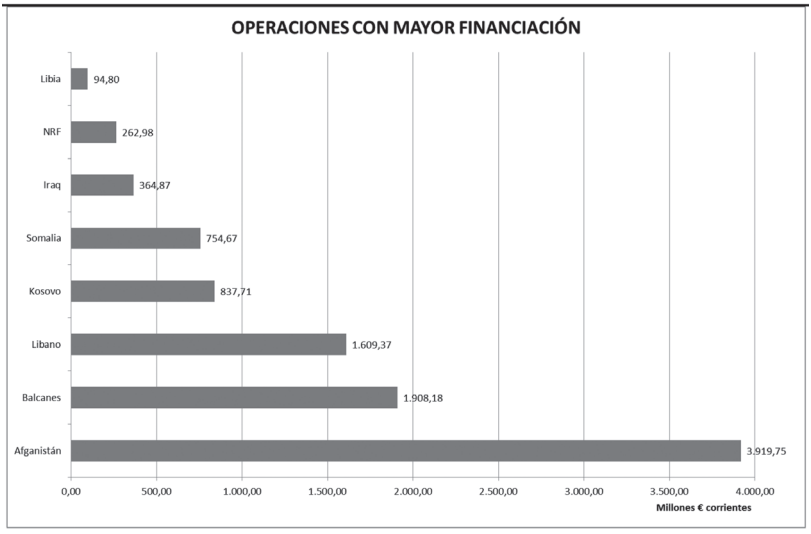
Por último, en el cuadro 13 se representan, las operaciones por volumen de financiación en el período 1990-diciembre 2015. Como se puede observar es Afganistán (Libertad Duradera, ISAF y Resolute Support) con 3.919,75 millones de euros, aproximadamente el 36,91% del gasto total en el período 1990-2015, la región que ha requerido de mayor financiación.

La segunda región que ha requerido mayor financiación corresponde a los Balcanes: Bosnia desde 1992 y bajo distintas banderas (IFOR, SFOR, UNPROFOR, ALTHEA) y Kosovo (KFOR, UNMIC) desde 1999 han generado un gasto de 2.745,89 millones de euros, aproximadamente el 25,86% del total del periodo.

La tercera región es el Líbano (FINUL) con un gasto de 1.609,37 millones de euros y aproximadamente el 15,15% del total del gasto.

El gasto en estas tres regiones representa el 77,92% de todos los recursos que el Ministerio de Defensa ha destinado a las OMP desde 1990.

Cuadro 13: Gasto total por OMP 1990-2015 (€ corrientes)



Fuente: Elaboración propia a partir de datos de DIGENECO. Ministerio de Defensa.

Conclusion

Las Operaciones de Paz en el marco de las organizaciones internacionales estudiadas brevemente se financian totalmente con fondos públicos, existiendo dos mecanismos básicos de financiación: a través del presupuesto de la respectiva organización y mediante contribuciones directas de los recursos nacionales, siendo éstas de dos tipos: recursos físicos (contribuciones en especie) y recursos financieros (pagos monetarios).

El principal problema que adolecen las tres organizaciones con respecto a su financiación es la insuficiencia de recursos, siempre por debajo de las aspiraciones políticas, estratégicas y operativas de las organizaciones y limita sus ambiciones para abordar operaciones de paz. Para conseguir una mayor sinergia en el empleo de los recursos deben ser capaces de adaptarse a situaciones cambiantes, a generar sus propias capacidades y a cooperar entre sí.

Con respecto a NN.UU., el sistema de reembolso supone una ayuda económica a los Estados que participan en las operaciones. Esto deriva que los Estados en vías de desarrollo sean los mayores contribuyentes de tropas, pero no disponen de las capacidades militares de los Estados más desarrollados.

El principio básico de la financiación en OTAN y UE: «Cost lie where costs fall», supone un importante lastre para el desarrollo de sus capacidades como organización. Las propuestas de futuro van dirigidas a convertir en gastos comunes gastos soportados por los Estados participantes y conseguir un mejor reparto de la carga financiera y militar que alivie la presión sobre los presupuestos nacionales.

La financiación de las OMP en España viene recogida, desde 2011, en tres conceptos presupuestarios: 128, 228 y 668 que tienen la consideración de ampliables contra el Fondo de Contingencia de ejecución presupuestaria. En este concepto, ampliable, es el gasto el que determina el importe del crédito. El sistema tiene la flexibilidad precisa para cubrir con la prontitud adecuada las necesidades operativas que se planteen, sin que por ello se limite el control que para la gestión de los citados créditos se establece en las disposiciones legales y reglamentarias. No obstante, la insuficiencia de crédito inicial y la demora en la aprobación de los expedientes de ampliación de crédito, pueden determinar que durante diferentes periodos de tiempo, especialmente en el primer trimestre del ejercicio, no se disponga de los recursos necesarios para atender las necesidades existentes y se tenga que utilizar los créditos del presupuesto corriente y realizar posteriormente el cambio de financiación. Una dotación inicial tan baja no parece compatible con la internalización de la seguridad, con la mayor proyección de las Fuerzas Armadas y con el compromiso de España con el mantenimiento de la paz y seguridad.

La acción exterior de España ha ido afianzando su presencia en las organizaciones internacionales que participa, lo que conlleva una creciente aportación de recursos humanos y económicos para alcanzar mayores niveles de seguridad. Consolidar el papel que desempeña España en el ámbito de la seguridad internacional implica un esfuerzo económico coherente con los nuevos desafíos y las nuevas misiones de las Fuerzas Armadas.

Referencias bibliográficas

Aranda Álvarez, E., «La Ley de Defensa Nacional y la participación de España en operaciones de mantenimiento de la paz», *Revista de Administración y Cidadanía,* Escola Galega de Administración Pública Vol.2 núm. 1, 2007, Santiago de Compostela, págs. 23-48.

Aranda Soria, Sonia, «El e-government al servicio de la transparencia en la rendición de cuentas en Defensa», Tesis doctoral, Universidad de Zaragoza, 2012, 371 págs.

Blanco y de la Torre, Félix, «ONU. Coste y financiación de las operaciones de mantenimiento de la paz», *Documento de opinión 51/2016*, Instituto de Estudios Estratégicos, Ministerio de Defensa, 2016, 16 págs.

Cossío Capdevila, A y Sara Alonso Rodríguez, S. «Análisis de la participación de las FAS españolas en Operaciones de Mantenimiento de la Paz de distintas organizaciones internacionales y su control». *Revista Española de Control Externo, Tribunal de Cuentas*. Vol. VII, núm. 19, 2005, Madrid, Págs. 103-130.

Cossío Capdevila, Ana, «La financiación de las operaciones militares de la Unión Europea y su control. El Mecanismo ATHENA», *Revista Española de Control Externo Tribunal de Cuentas*. Vol. XII, núm. 34, 2010, Madrid, págs. 151-174.

Unión Europea, Decisión del Consejo (2014/335/UE, Euratom), de 26 de mayo de 2014, sobre el sistema de recursos propios de la UE, *Diario Oficial de la Unión Europea* 7/06/2014, L168, págs. 105-111.

Unión Europea, Decisión (PESC) 2015/528 del Consejo, de 27 de marzo de 2015, por la que se crea un mecanismo para administrar la financiación de los costes comunes de las operaciones de la unión Europea que tengan repercusiones en el ámbito militar o de la defensa (Athena) y por la que se deroga la Decisión 2011/871/PESC, *Diario Oficial de la Unión Europea* 28/03/2015, L84, págs. 39-68.

Directiva de Defensa Nacional 01/2012, Presidencia del Gobierno, 2012

La Estrategia de Seguridad Nacional: un proyecto compartido. Departamento de Seguridad Nacional, Presidencia del Gobierno, 2013, 68 págs.

Fuente Cobo, Ignacio, «Las Operaciones de Paz para el siglo XXI: Un concepto en evolución», *Centro de Estudios y Análisis de Seguridad*, Universidad de Granada, 2003, 21 págs., www.ugr.es/

García Sánchez, Daniel, «Las operaciones de paz y el cambio institucional de los Ejércitos. Un análisis de la transformación de los ejércitos ante la adopción de nueva funciones determinadas por un nuevo entorno», Tesis Doctoral, Universidad Autónoma, Madrid, 2006, 705 págs.

España, Ley 47/2003, de 26 de noviembre, General Presupuestaria, *Boletín Oficial del Estado* de 27 de noviembre de 2003, núm. 284, 92 págs.

España, Ley Orgánica 5/2005, de 17 de noviembre, de la Defensa Nacional, *Boletín Oficial del Estado* de 18 de noviembre de 2005, núm. 276, 11 págs.

España, Ley 2/2014, de 15 de marzo, de la Acción y del Servicio Exterior del Estado, *Boletín Oficial del Estado* de 26 de marzo de 2014, núm. 74, 33 págs.

España, Ley 36/2015, de 29 de septiembre, de Seguridad Nacional, *Boletín Oficial del Estado* de 29 de septiembre de 2015, núm. 233, 12 págs.

Liñan Nogueras, DJ y Roldan Barbero, J. (Edit), *El Estatuto jurídico de las Fuerzas Armadas españolas en el exterior,* Plaza y Valdés Editores, Madrid, 2008, 450 págs.

Dirección de Doctrina, Orgánica y Materiales del Mando de Adiestramiento y Doctrina, *Doctrina de Empleo de las Fuerzas Terrestres (DO.001)* (3.ª edición), Granada, 2003,

Martínez Isidoro, Ricardo, «Las Operaciones de Apoyo a la Paz». *Documento de trabajo 25/2009. Real Instituto Elcano,* 2009,27 págs., www.realinstitutoelcano.org

Presupuestos de Defensa (varios años), Dirección General de Asuntos Económicos, Ministerio de Defensa.

Montoya Cerio, Fernando, «Brexit», ficción o realidad: impacto sobre la PCSD de la UE. *Documento de opinión 64bis/2016. Instituto de Estudios Estratégicos.* Ministerio de Defensa, 2016, 19 págs.

Moreno Izquierdo, Rafael, «España y las misiones de paz: retos y oportunidades». *Misiones de paz de las Fuerzas Armadas españolas.* Seminario en Zaragoza 7 de junio de 2007, Fundación Alternativas, págs. 7-14, http://www.falternativas.org/

Moreno Izquierdo, Rafael, «La contribución del Ministerio de Defensa Español a la reconstrucción y la acción humanitaria durante 2008», *Documentos iecah. Instituto de Estudios sobre Conflictos y Acción Humanitaria*, Madrid, 25 págs.

Moreno Zamora, Juan Ignacio, «Problemática de la financiación de las nuevas misiones de la Unión Europea», *Revista General de Marina,* Vol. 269, núm. 1 (julio), 2015, págs. 93-98.

Navas Córdoba, Julio, «El futuro de las misiones de la ONU: el papel de las organizaciones internacionales», *Documento de opinión 25/2012, Instituto de Estudios Estratégicos*, Ministerio de Defensa, 18 págs.

Pérez Forniés, Claudia, «Aspectos económicos de la Seguridad y Defensa: la Economía de la Defensa» en *Introducción a los estudios de seguridad y defensa.* Cueto C. y Jordan J. (Coord.) Editorial Comares, Granada, 2001, págs. 139-154.

Pérez Muinelo, Francisco, *El gasto de Defensa en España 1946-2009.* Ministerio de Defensa, Madrid, 286 págs.

España, Real Decreto Legislativo 2/2007, de 28 de diciembre, por el que se aprueba el Texto Refundido de la Ley General de Estabilidad Presupuestaria, *Boletín Oficial del Estado* de 31 de diciembre de 2007, núm. 313, 9 págs.

España, Real Decreto 524/2014, de 20 de junio, que modifica el Real Decreto 454/2012, de 5 de marzo, por el que se desarrolla la estructura orgánica básica del Ministerio de Defensa, *Boletín Oficial del Estado* de 21 de junio de 2014, núm. 151, 8 págs.

Fiscalización de los gastos derivados de la participación de las Fuerzas Armadas españolas en operaciones de paz de organizaciones internacionales, ejercicios 1996,1997 y 1998, de 25 de junio de 2002. Tribunal de Cuentas, Informe 564, 2002, 49 págs.

Fiscalización de los gastos derivados de la participación de las Fuerzas Armadas españolas en operaciones internacionales, ejercicios 2009 y 2010, de 28 de junio de 2012. Tribunal de Cuentas, Informe 943, 2012, 108 págs.

Sepúlveda, Isidro (ed), «España en las operaciones internacionales de pacificación». *Actas del III Congreso Internacional de Historia de la Defensa*. Instituto Universitario General Gutiérrez Mellado, Madrid, 546 págs.

Valiño Castro, Aurelia, «Evolución reciente del presupuesto y el gasto español en Defensa», *Cuadernos de información económica*, núm. 248, Septiembre/octubre 2015, 11 págs.

Vázquez Ramos, Alfredo, «Elementos de cambio y permanencia: potenciales escenarios de financiación de las misiones internacionales», *Documento de opinión 80/2011. Instituto de Estudios Estratégicos*. Ministerio de Defensa, 13 págs.

Páginas WEB:

https://www.sipri.org/

http://www.un.org/es/peacekeeping/resources/statistics/contributors.shtml

http://www.europarl.europa.eu/atyourservice/es/displayFtu.html?ftuId=FTU_6.1.2.html

http://www.igae.pap.minhap.gob.es/

http://www.defensa.gob.es/

http://www.iecah.org

http://www.nato.int

ESTUDIO SOBRE LOS MODELOS DE FINANCIACIÓN DE LA DEFENSA: PRESUPUESTOS PÚBLICOS E I+D PARA GARANTIZAR LA COMPETITIVIDAD DEL SECTOR

Elia Breijo Pena
Universidad Complutense de Madrid

José Ignacio López Sánchez
Universidad Complutense de Madrid
Cátedra Paz, Seguridad y Defensa de la Universidad de Zaragoza

Resumen

Desde 2007, la crisis económica ha provocado un profundo cambio en el mercado maduro de la defensa: la anterior dependencia de los *ciertos* presupuestos públicos se ha tornado en contra de las principales potencias, provocando dolorosos ajustes y un fuerte golpe de timón en busca de un puesto en un mercado con nuevas exigencias. Con base en la fortaleza de su mayor empresa nacional, se analizan las principales magnitudes de las naciones estudiando las grandes cifras de negocio de las empresas. Concluimos con una adaptación de la herramienta DAFO, con el fin de comprender la situación actual de cada mercado y el devenir del sector de la defensa. La capacidad de adaptación a las nuevas exigencias civil-militares, la inversión I+D y el esfuerzo exportador serán las piedras de toque para la conseguir la ansiada competitividad.

Palabras claves

Competitividad, Defensa, Presupuestos, Investigación y Desarrollo.

1. Introducción

Históricamente, la Defensa siempre ha sido un pilar fundamentar de todas las civilizaciones, desde los homínidos hasta las civilizaciones más avanzadas como la romana o la egipcia han tenido un sistema de defensa, más o menos rudimentario. La

técnica se ha sofisticado, mejorado y hasta deshumanizado, pero la idea sigue siendo la misma: la necesidad de defender lo que uno considera propio, de manera pasiva (defensa disuasoria) o activa.

La globalización ha provocado una atmósfera de colaboración entre personas y empresas civiles, capaces de conectar talentos en tiempo real, multiplicando hasta niveles inimaginables su potencial. Sin embargo, la globalización ha provocado el efecto contrario en el sector de la defensa por una sencilla razón: el aumento exponencial de riesgos y la dilución del concepto de soberanía en el entorno cibernético actual. Nadie defiende un país mejor que sus propios soldados, eso está claro. Pero en un mercado tan complejo donde las inversiones en investigación y desarrollo son muy dispares, muchos países se han visto forzados a compartir y ceder parte de su soberanía en términos de defensa con el objetivo de sumar fuerzas y poder plantar cara a las grandes potencias, con el fin de tener un cierto poder disuasorio. Lo mismo ha ocurrido con las empresas del sector.

En el mundo existen miles de empresas que se dedican al negocio de la defensa, sin embargo, debido a las crecientes elevadas inversiones que las empresas se ven forzadas a hacer para estar en la frontera del conocimiento, muchas han desaparecido o se han visto absorbidas por otras para poder seguir siendo competentes en un mercado muy controlado. Tal es la concentración de las inversiones, que casi el 50% de las ventas de armas las realizan únicamente las 10 empresas de defensa más grandes del mundo[1].

El elevado riesgo y el largo plazo son las características fundamentales de las inversiones en defensa. Mientras que todos los años se lanzan al mercado varios modelos de teléfonos móviles, los grandes programas armamentísticos suponen décadas de inversión y coordinación entre diferentes países. Esto, unido a la necesidad de compartir información sensible y a los intereses partidarios de que cada país quiere que sus empresas nacionales sean parte del programa, provoca que en demasiadas ocasiones la viabilidad y competitividad de una empresa esté ligada al esfuerzo inversor en defensa del país en cuestión; ya que para entrar en

1. The Sipri Top 100 Arms-Producing And Military Services Companies, 2014. Sipri Fact Sheet. Dec 2015.

un programa se debe tener un nivel tecnológico inalcanzable sin una fuerte inversión previa.

¿Existe correlación entre la competitividad de una empresa de defensa con el esfuerzo inversor en defensa de su país? Siguiendo esta línea, ¿el esfuerzo en investigación y desarrollo de una empresa, repercute en un aumento de las ventas? Estas son las preguntas que se analizarán a lo largo del trabajo.

2. Objetivo y metodología

Este trabajo tiene como objetivo el ayudar a comprender las variables que inciden en las variaciones de la inversión que tienen lugar en el sector de la defensa, buscando en todo momento las interrelaciones existentes entre las variables macroeconómicas de los grandes países y las principales empresas del sector de la defensa de dichos países.

Con el fin de conseguir dicho objetivo se analizarán los países de las empresas seleccinadas mediante el análisis PEST[2] Después, se pasará a estudiar la evolución de las principales magnitudes de la empresa más grande en el sector de la defensa para cada país.

Para concluir, se realizará un análisis DAFO de cada empresa en su entorno con la idea de poder extrapolar los resultados a las empresas del mismo sector, gracias a la metodología del caso. Para mantener el análisis simple, el objetivo principal de esta herramienta es la identificación de las tendencias del mercado y la recomendación de acciones en base a estas líneas generales.

Todas las herramientas y técnicas utilizadas en el estudio fueron enseñadas en el Master en Logística y Gestión Económica de la Defensa de la UCM en cooperación con el CESIA.

3. Los grandes inversores en Defensa: estado actual de la cuestión

Con el fin de identificar los países a estudiar y poder llevar a cabo un estudio posterior coherente con las empresas, se ha to-

2. La herramienta de análisis PEST es una técnica de análisis estratégico para definir el entorno de una compañía a través del análisis de una serie de elementos externos que la afectan. Dentro de los elementos a estudiar se encuentran: Políticos, Económicos, Sociales y Tecnológicos.

mado la lista de las empresas con mayores ventas del mundo del portal de referencia Defense News[3,4].

De esta manera, se ha tomado la empresa con mayor facturación de los países teniendo en cuenta la clasificación de 2015:

Tabla 1. Empresas más grandes de Defensa por cuantía de ventas

Posición	Compañía	País
1	Lockheed Martin	EEUU
2	Boeing	EEUU
3	BAE Systems	Reino Unido
4	Raytheon	EEUU
5	General Dynamics	EEUU
6	Northrop Grumman	EEUU
7	*Airbus Group*	*Holanda**
8	United Technologies	EEUU
9	Finmeccanica	Italia
10	L-3 Commmunications	EEUU
11	*Almaz-Antey*	*Rusia***
12	Thales	Francia
28	Rheinmetall	Alemania
88	Indra	España

Fuente: Defense News

Se ha elegido:
EEUU con su mayor empresa Lockheed Martin
Reino Unido con su mayor empresa BAE Systems
Italia con su mayor empresa Finmeccanica
*Holanda no se ha tomado ya que su mayor empresa es el conglomerado franco-alemán Airbus Group. Debido a la

3. La elección de esta fuente por encima de otras como SIPRI se ha basado en el hecho de que DefenseNews tiene en cuenta toda la venta en el sector de la defensa que realiza la empresa, no solamente la venta de armamento, que es el caso de SIPRI. Además, empresas como BAE Systems utilizan esta fuente en sus cuentas anuales para clasificarse dentro del mercado.

4. La elección de las empresas se ha hecho en base a la metodología del caso: la toma de un ejemplo —véase una empresa de defensa— con el objetivo de extrapolar los resultados al resto del mercado— el sector de defensa. La elección de esta técnica se basa en la incapacidad de estudiar y analizar la totalidad del sector, por lo que se opta por estudiar la empresa más grande por volumen de facturación. En base a esta elección, se estudia su entorno nacional.

incapacidad de separar de manera objetiva y efectiva cuánto porcentaje pertenece a Francia y cuánto a Alemania dentro de sus ventas de defensa, se ha optado por coger la siguiente empresa francesa y alemana más grande[5].

Francia con su mayor empresa Thales

Alemania con su mayor empresa Rheinmetall

**Rusia no se ha tomado debido a la falta de transparencia en sus inversiones de defensa y con el objetivo de simplificar el estudio entre las grandes potencias: EEUU/Europa.

España con su mayor empresa Indra. Como se puede observar, Indra está en la posición número 88 de 100, por lo que hay muchos países representados antes de ella. Sin embargo, se decide tenerla en cuenta en este estudio en aras de comparar su modelo de inversión con el de las grandes potencias.

Con el fin de mantener la máxima homogeneidad entre los análisis de los diferentes países, se realizará el análisis PESTEL en base a los indicadores de competitividad publicados cada año por el World Economic Forum. El último informe, y en el que se basa este trabajo, se publicó en Octubre 2015.

En la tabla del Anexo I se exponen las principales conclusiones del estudio realizado sobre los seis países seleccionados.

Las principales conclusiones que se pueden sacar de este estudio en las diferentes variables es:

—Político: Debido a la crisis económica, los diferentes países se han visto obligado a priorizar sus presupuestos, enfocando sus esfuerzos en la reactivación económica: mayor gasto social y políticas económicas. Los diversos *White Papers* definen nuevas amenazas como internet y los nuevos grupos terroristas —que precisan de un nuevo tipo de respuesta: ciberseguridad y cooperación. Cabe destacar el rol fundamental de EEUU en las políticas de defensa: debido a sus grandes presupuestos (muy superiores a los del resto de sus aliados), sus procedimientos y normativas son un referente para el mundo— así como su tecnología e innovación.

5. Sí se usarán los datos de Airbus durante el estudio con el fin de no desvirtuar la inversión europea en defensa.

—Económico: Las consecuencias de este cambio de estrategia política son claras: aumento de la deuda pública y caída de los gastos «no prioritarios» como los de defensa. Debido a esto, los diferentes ministerios han visto en la cooperación internacional un filo en el que relajar sus estrechos presupuestos. Conceptos como el Pooling and Sharing[6] comienzan tomar forma. Aunque la crisis fue dura en todos los países, es importante destacar el duro golpe que ha supuesto a los países mediterráneos: un enorme aumento de la deuda pública, graves casos de corrupción y una débil recuperación.

—Socio-culturales: todas las potencias estudiadas tienen una gran variedad de culturas. Cabe destacar países como Reino Unido, Francia, España o Italia, cuya Historia militar se cuenta por siglos y milenios, no así la estadounidense.

—Tecnológicas: en general, todos los países gozan de un nivel innovador bastante alto. Cabe destacar el caso de EEUU con una excelente colaboración entre la industria y las universidad, base fundamental de su éxito tecnológico. Así mismo, los países europeos y Reino Unido también tiene una buena capacidad innovadora, basada en sus excelentes universidades de ingeniería. Un caso especial es el de España, generadora de talento, pero debido a si pobre sistema innovador —en comparación con el resto de los países estudiados— le supone un gran esfuerzo retenerlo o atraerlo de fuera del país. La crisis ha provocado una disminución de los presupuestos para innovación en los países estudiados en los últimos años; aunque existe una voluntad por parte de los países de al menos mantener los niveles actuales ya que reconocen en la innovación, un pilar fundamental de su competitividad.

6. El concepto de Pooling and Sharing viene del inglés: pooling significa hacer un fondo común y sharing compartir. La idea detrás es que varios países hagan una aportación al fondo (de defensa en este caso) y con este fondo se adquiere, mantienen o defienden todos los miembros del fondo. La ventaja es que para el nivel de seguridad que obtienen los miembros, su desembolso individual hubiera sido muy superior que el de creando un fondo común. Fuente: Instituto Español de Estudios Estratégicos.

2. Las empresas de Defensa

2.1. *EEUU-Lockheed Martin*

La empresa estadounidense más grande por ingresos en defensa es Lockheed Martin.

En el Anexo II, Tabla A, se puede encontrar un estudio sobre las grandes magnitudes de la empresa a lo largo de los último años[7]. Cabe destacar del estudio la evolución positiva de las ventas de la empresa, viéndose afectada por la crisis financiera únicamente un año (2008). A partir del año 2008 hasta el 2014, las ventas de la empresa se dispararon. En el año 2015, Lockheed Martin presentó unas ventas que alcanzaban los 46 mil millones de dólares. El margen de beneficios de la empresa ronda la cifra del 9%, superándolo con creces en el año 2014; a pesar de ser el año en el que la empresa se vio afectada por una fuerte disminución en su *goodwill*[8] debido al hecho de que EEUU estaba en pleno proceso de reducción de operaciones en el extranjero, lo que provocaba un aumento de la competición nacional por los contratos —dejando un margen de maniobra menos amplio a la empresa para ganar beneficios. Lockheed Martin calculó que su *goodwill* en libros estaba 107 millones de dólares por encima de lo que percibía el mercado[9]. Este hecho es importante ya que pone de relieve la complicada situación que las empresas de defensa estadounidenses están sufriendo: la incertidumbre, la creciente competición y la necesidad de mirar al mundo civil para seguir creciendo.

Cabe destacar, asimismo, que los gastos en I+D de la empresa no rebasan en ningún momento el 2% de las ventas[10]. Como

7. No se ha tenido en cuenta el año 2015 por cuestiones de homogeneización con el resto de las empresas que publican sus cuentas más tarde que la empresa americana.

8. Es un activo intangible que refleja las conexiones de un negocio de atención al cliente, la reputación y otros factores similares. Muestra el valor de la reputación de una empresa, que puede afectar a la situación en el mercado de la misma, tanto positiva como negativamente. Fuente: Debitoor. Glosario de Contabilidad. Consultado: 09/04/2016. URL: https://debitoor.es/glosario/definicion-goodwill

9. Loockheed Martin Annual Report. Pag. 66-67. «Goodwill»

10. En este análisis, los datos de esfuerzo I+D diferencian el esfuerzo de la empresa del que hace el estado. De esta manera, no aparecen reflejados en I+D de este estudio la parte de los contratos de Investigación que sufraga el Estado; solamente el esfuerzo privado. Ver más: Lockheed Martin Annual Report de cualquier año en «Research and Development».

veremos posteriormente en las comparaciones, es un porcentaje bastante más bajo que el de los países europeo[11].

En el Anexo III se puede consultar el resto del estudio donde se analizan las cifras de la empresa en el sector de defensa, así como la aparente dependencia/independencia del gobierno.

2.2. *Reino Unido-BAE Systems*

BAE Systems es el segundo contratista de defensa más grande del mundo y la mayor de Reino Unido.

En la Tabla B del Anexo I, muestra el estudio hecho a las grandes cifras de las cuentas anuales en los últimos diez años a BAE Systems. Cabe destacar del estudio la evolución inestable del nivel de ventas, que alcanza su punto máximo en 2009 con casi 33 mil millones de dólares y su cifra más baja en 2014 con 24 mil millones de dólares. A pesar de la desigual evolución de las ventas de la empresa, el nivel de EBITDA sí se ha mantenido cerca de los 3 mil millones de dólares —mostrando una gran capacidad de ajuste de los costes operativos de la empresa[12]. El margen de beneficio no es tan alto como el de Lockheed Martin, con un margen de beneficio mínimo de 1.28% en el año 2009 y un máximo de 14.11% en el año 2008. En el año 2009 además de tener el margen de beneficio mínimo, sus ingresos netos[13] son negativos en 108 millones de euros. A diferencia de Lockheed Martin, sus gastos en I+D suponen en cualquier año más del 5% de las ventas, llegando al 13.15% en el año 2005; esfuerzo y cifras muy superior a las que maneja la empresa norteamericana.

En el Anexo III se puede consultar el resto del estudio donde se analizan las cifras de la empresa en el sector de defensa, así como la aparente dependencia/independencia del gobierno.

2.3. *Italia-Finmeccanica*

Finmeccanica es el segundo grupo industrial italiano y el primero en el sector de la defensa. Su tecnología está muy enfocada

11. Se verá más adelante que el amplio presupuesto de EEUU en términos de I+D en defensa, provoca que el esfuerzo que tiene que hacer es sector privado sea muy inferior al de sus socios europeos.

12. Entendiendo los costes operativos como aquellos que se deducen directamente a las ventas y de cuya resta se obtiene el EBITDA.

13. P/G del Periodo. Beneficio Neto.

a las aplicaciones duales entre en mundo civil y militar. Al igual que en las empresas anteriores, se ha hecho un estudio de las grandes cifras de las cuentas anuales desde 2006. Como se puede observar, las ventas de la empresa están en declive desde el año 2009, prácticamente desde el inicio de la crisis. Sin embargo, la cuota de sus ventas procedentes de defensa son solo la mitad de sus ventas, excepto en el año 2005 y 2011 que rebasaron el 60%. En lo que respecta al margen de beneficio, la empresa es bastante inestable, teniendo en 10 años un máximo de 10.9% de margen de beneficio en el año 2006 y un mínimo negativo de 13.72% sólo cinco años después en el 2011- aunque más adelante se estudiarán estos bruscos cambios, cabe destacar que en el año 2011 Finmeccanica vendió su participación (45%) en la filial Alsando Energia que tuvo un efecto directo en las cuentas con una reducción total del 7% y una caída del 5% en su cartera[14]. más adelante se estudiarán estos cambios tan bruscos en las cuentas. En lo que se refiere a los gastos de Investigación y Desarrollo, se puede observar que Finmeccanica realiza un gran esfuerzo, teniendo un ratio que supera en todos los años el 10%, incluso cuando tiene márgenes de beneficio negativos de dos cifras.

En el Anexo III se puede consultar el resto del estudio donde se analizan las cifras de la empresa en el sector de defensa, así como la aparente dependencia/independencia del gobierno.

2.4. *Francia-Thales*

Thales es un grupo francés dedicado a la electrónica y al desarrollo de sistemas de información y servicios. En el análisis de las principales cifras de la empresa[15], se puede ver una cierta fluctuación en el nivel de las ventas a lo largo de los años. En términos generales, aunque las ventas hayan fluctuado, el EBITDA

14. Finmeccanica, Press Release. Publicado: Roma 27 marzo 2012.

15. En este estudio se han utilizado las cifras obtenidas de la base de datos Orbis, si bien estas cifras no coinciden completamente con las publicadas oficialmente por la empresa. Esto puede provenir de los parámetros que la base de datos utilizada utilice para medir las magnitudes de la empresa, lo que ha supuesto un reto a la hora de explicar la variación de las partidas a lo largo de los años. Con el fin de mantener el estudio lo más homogéneo posible, se ha optado por hacer el análisis completo con la base de datos Orbis.

se ha mantenido más o menos estable rondando siempre los 1.5 mil millones de dólares. Tanto el margen de beneficio como los Ingresos netos sí han sufrido una fluctuación más grande, llegando incluso el margen de beneficio a ser negativo en dos años consecutivos: 2009 y 2010, los años con más presión por parte de los reducidos presupuestos del estado en materia de defensa. En dichos años la cartera de pedidos también se retrajo un 6% en comparación con el año pasado, motivado principalmente por la pobre actuación de la división de defensa (-26% en comparación con el año anterior) debido al declive de contratos y caída de los presupuestos de los gobiernos en esta materia.[16] Por otro lado, los malos resultados en el sector de la defensa fueron parcialmente compensados por los de Transporte y Espacio con un aumento del 26% con respecto al año anterior. Este espectacular aumento se debe principalmente al sector espacio que doblaron su cartera de pedidos con respecto a 2009 gracias a contratos como los de Iridium (filial estadounidense) por valor de 1.1 mil millones de euros para la construcción de una constelación de 81 satélites[17]. Aunque en el año 2011 la empresa no obtuvo mejores resultados en su nivel de ventas, sí consiguió mejorar su EBITDA (claro reflejo del esfuerzo de ajuste y optimización de la empresa) y empujar su margen neto hasta el 4.62%, muy superior al -2.9% del año 2010. No sería hasta el año 2012 cuando Thales realmente vuelve a tener unos buenos resultados impulsados por la adquisición del 35% de la empresa DCNS (naviera francesa) que provoca un aumento del 9% de sus ventas, en vez del 1.5%, sin el impacto de la adquisición. Cabe destacar, así mismo, el año 2014 en el que a pesar de la disminución de las ventas del grupo, incluso por debajo de los niveles de 2011, su EBITDA es de 1.5 mil millones de dólares y su margen neto llega a ser el más alto de los últimos 5 años con un 7.52%, gracias principalmente a la gran año de espacio y la recuperación de la división de defensa y seguridad que por primera vez tiene un aumento del 24% de EBIT sobre ventas. Por otro lado, el año 2014 no fue bueno para la división de

16. Thales Group. Annual Report 2010. Página 10.

17. El contrato entero de 1.1 mil millones de euros no ha caído en el año 2010, sólo parcialmente con la construcción de la constelación O3B, satélites de observación (Francia y Turquía) y varias satélites de telecomunicaciones. (Yaman Gazprom Apstar y Eutelsat).

transporte que sufrió una caída del 3% en sus ventas y una caída del 67% en su nivel de EBIT sobre ventas.

En lo que respecta a los gastos en I+D, la línea de la empresa es coherente con las anteriores empresas europeas ya que incluso en los años de malos rendimientos, el esfuerzo no ha sido nunca inferior al 3% de las ventas. De hecho, desde el año 2009 el esfuerzo en I+D no ha dejado de crecer hasta llegar a rozar el 5% de las ventas en el año 2014. En número de empleados, se puede observar un claro ajuste desde el año 2011, síntoma del constante esfuerzo de la empresa por ajustar sus costes y el aumento de la presión presupuestaria.

En el Anexo III se puede consultar el resto del estudio donde se analizan las cifras de la empresa en el sector de defensa, así como la aparente dependencia/independencia del gobierno.

2.5. *Alemania-Rheinmetall AG*

Rheinmetall es el mayor fabricante de armas de Alemania con sus tres fábricas principales situadas en Düsseldorf, Kassel y Unterlüß y su central situada en Düsseldorf.

Como se puede ver en la Tabla E del primer anexo, las ventas de la empresa son menos cuantiosas en términos generales que las anteriores, es esto es porque es la empresa número 28 del mundo en ingresos de defensa. Las ventas a lo largo de los años han sufrido variaciones pero son mucho más estables que las del resto de las empresas; siempre rondando entre los 5.5 y los 6 mil millones de euros. Esta estabilidad se debe al carácter recurrente de su core: munición[18]. El EBITDA de la empresa sí ha sufrido más fluctuaciones que las ventas debido, entre otros factores, a la dependencia de las materias primas de alta calidad como el acero o el hierro para fabricar sus productos tanto para su sección civil como la de defensa. El margen de beneficio de la empresa tuvo su mejor año en el 2011 con un 6.5% y peor año en el 2014 con apenas un 0.46%. De hecho, el margen de beneficio de la empresa ha menguado desde el año 2011 de manera continua. El esfuerzo de la empresa en I+D está en línea con la de sus socios europeos: estable en un 4%, así como el número de empleados.

18. Puede ser que un gobierno no necesite un vehículo nuevo o un nuevo cargamento de cañones pero sí de balas y misiles para dichos cañones.

En el sector de defensa, se puede ver cómo la cuota de ventas de defensa se ha mantenido estable a lo largo de los años suponiendo entre un 40% y un 50%, alcanzando su cifra más alta en el año 2009 con un 55%. Los gastos de I+D en defensa, como en el resto de las empresas, se ha supuesto proporcional al de la empresa.

En el Anexo III se puede consultar el resto del estudio donde se analizan las cifras de la empresa en el sector de defensa, así como la aparente dependencia/independencia del gobierno.

2.6. *España-Indra*

Indra es una multinacional española que ofrece servicios y soluciones de una gama muy diversa de productos: Defensa y Seguridad; Transporte y Tráfico; Energía e Industria; Telecomunicaciones y Media; Servicios financieros; y Administraciones públicas y Sanidad. El análisis de las grandes cifras de Indra se puede ver en la Tabla F del anexo. En dicho análisis se puede ver que las magnitudes de la empresa soy muy inferiores a las del resto de las empresas estudiadas[19]. Las ventas de la empresa se han mantenido relativamente estables a lo largo de los años, rondando los 3.5 y 4.0 mil millones de dólares. El margen de beneficio de la empresa ha sufrido una de variaciones más grandes de las magnitudes estudiadas pasando de 4.84% en el año 2013 al -3.68% en el año 2014. Esta gran inestabilidad en el margen de beneficio denota una baja flexibilidad en la estructura de costes de la empresa —muy especialmente palpable en la enorme caída del EBITDA en el año 2014, al contrario que en las anteriores donde se podía observar una relativa estabilidad en las ventas y los niveles de EBITDA. En relación con los gastos de I+D, se puede ver una evolución muy diferente a la de las otras empresas: mientras que el resto de las empresas europeas realizan un gran esfuerzo (por encima del 4% del nivel de ventas) en I+D, Indra sólo tiene dos años con un nivel por encima del 3%: 2012 y 2013; de hecho, en la mayoría de los años, el esfuerzo de la empresa en I+D ronda el 0%. Este modelo de I+D sería muy parecido al estadounidense en el que el esfuerzo

19. Indra es la empresa de este estudio con el puesto más bajo del ranking y primera (y única) empresa española en el top 100 de mayores empresas de defensa del mundo por ingresos. Fuente: DefenseNews.

innovador lo realiza el Estado y la empresa no tiene necesidad/motivación de realizarlo. De acuerdo con la base de datos de Orbis, el esfuerzo innovador para el año 2014 es del 0% —lo que confirmaría dicho modelo de financiación— aunque significa un cambio radical con respecto a la inercia que tenía de años anteriores de I+D (por encima del 6% de las ventas del año)[20]. Otra gran diferencia con el resto de las empresas analizadas es el número de empleados: desde la crisis en el año 2007 las empresas europeas y la americana estudiada han mantenido un nivel estabilizado de número de empleados o incluso disminuido. Sin embargo, desde el año 2008 los empleados de Indra no han dejado de crecer, a pesar de que sus cifras no mejoraran de manera proporcional[21].

En el Anexo III se puede consultar el resto del estudio donde se analizan las cifras de la empresa en el sector de defensa, así como la aparente dependencia/independencia del gobierno.

3. Estudio del entorno específico

En esta última parte del trabajo, se hará balance de los dos análisis posteriores con el fin de encontrar los diferentes modelos de financiación de la defensa y destapar las futuras oportunidades de negocio que se pueden abrir gracias al cambio de entorno.

El mundo actual es un sistema holístico[22] en el que todo está interconectado y la descompensación de una variable afecta al resto de manera directa o indirecta. El devenir de la economía afecta de lleno en los presupuestos de defensa, tachados de abusivos o desproporcionados en tiempos de crisis con una emer-

20. En las cuentas anuales de Indra para 2014, sí aparece que Indra realiza un esfuerzo de «Desarrollo» superior a los 100 millones de euros. Sin embargo, la base de datos en la que se basa el estudio diferencia el esfuerzo estatal del privado y esto supone que Orbis no considera los 100 millones como esfuerzo de la empresa.

21. Esto unido al hecho de que la gran mayoría de los empleados están en España, es coherente con el estudio PEST elaborado en el anterior epígrafe donde se especificaba que la inflexibilidad del mercado laboral en España es un problema a la hora de hacer negocios.

22. «Lo anterior se expresa en términos de Management con la expresión holístico, dando a entender que una comprensión de la empresa precisa considerar al mismo tiempo todas sus partes en movimiento y no de forma estática». Fuente: «Humanismo, nuevo paradigma empresarial», Editorial Académica Española, 2013, pág. 28. Rafael Alé-Ruiz

gencia social. Dichos presupuestos, por la naturaleza del sector que alimentan, condicionan mucho la competitividad de las empresas de defensa nacionales por el concepto de la soberanía nacional: los presupuestos de defensa de un país irán destinados principalmente a sus empresas nacionales con el fin de apoyar la industria de defensa y poseer una tecnología autónoma y de alta calidad que aporte al bien común global que es la seguridad y la defensa. En el estudio que se realizará a continuación se hará un simple DAFO en el que el lector se pone en la piel de la empresa de defensa antes descrita en su propio país, que necesita decidir su estrategia tras los cambios acontecidos en el mercado.

3.1. *EEUU: en la piel de Lockheed Martin*

Para ver el estudio en detalle, ir al Anexo IV

Actualmente Lockheed Martin está intentando utilizar sus fortalezas para poder beneficiarse de los nuevos mercados que suponen una oportunidad – esto lo podemos ver en su interés e inversión en su división de ciberseguridad y la búsqueda de aplicaciones civiles para sus productos. Además, su estrategia también contempla ajustes de su estructura a la nueva situación, como fue el despido de cientos de empleados durante los últimos años. En definitiva, una mezcla de estrategia ofensiva (utiliza sus fortalezas para obtener oportunidades) y defensivas (utiliza sus fortalezas para defenderse de las amenazas) ya que por un lado busca nuevas oportunidades y se defiende de las amenazas que ha estudiado en su mercado (disminución de los presupuestos y aumento de la competitividad) y en el extranjero.

En lo que respecta al modelo de I+D estadounidense, como se ha explicado anteriormente, los ajustes presupuestos y la caída del esfuerzo público a la investigación de defensa, ha obligado a la empresa a aumentar su esfuerzo privado para seguir siendo igual de competitivo. Para el futuro, el modelo estadounidense se comenzará a parecer más y más al europeo donde existe una fuerte cofinanciación y las empresas tienen que hacer un gran esfuerzo para poder mantenerse competitivas. Si bien es verdad que la presión innovadora sin la administración estadounidense se prevé menor, dejando margen de maniobra a empresas que hasta el momento no tenían ninguna oportunidad de ser competitivas, tanto estadounidenses como europeas o incluso asiáticas.

Aunque es una empresa gigante con más de cien mil empleados, su cartera le otorga un tiempo de reacción que debe aprovechas sabiamente y no despistarse ni dormirse en la comodidad del presupuesto estadounidense. La directiva de la empresa es consciente de los fuertes ajustes acometidos por la administración y ha comenzado a actuar para asegurar la viabilidad y fortaleza de la empresa en el largo plazo. La crisis de 2007 ha forzado un cambio de estrategia a la que Lockheed Martin está respondiendo mediante la diversificación y la defensa de su posición[23].

3.2. *Reino Unido: en la piel de BAE Systems*

Para ver el estudio en detalle, ir al Anexo IV

Actualmente BAE Systems está utilizando sus fortalezas para atajar las amenazas del sector, e incluso es capaz de transformar sus debilidades – como el de ser una empresa muy grande estructuralmente —en fortalezas— gracias a la flexibilidad de su estructura de costes. Esta estrategia defensiva le surte efecto gracias a su posición privilegiada en el mercado más grande del mundo en defensa y a su capacidad innovadora soportada por un gran esfuerzo de inversión año tras año. Además, al igual que Lockheed Martin, BAE Systems lleva a cabo una estrategia ofensiva utilizando sus fortalezas para identificar y conseguir las oportunidades del mercado —como así atestigua su focalización en la ciberseguridad.

En lo que respecta a la inversión I+D, el modelo de financiación es radicalmente opuesto al estadounidense. Mientras que en EEUU las empresas reciben una gran aportación a sus proyectos de I+D, las empresas británicas pueden contar con ese apoyo por lo que deben aumentar su esfuerzo propio. Observando las últimas cifras, BAE Systems es consciente de la necesidad de estar en la frontera del conocimiento, diferenciarse y ser competitivo su inversión en I+D tiene una clara tendencia al alza.

Una saneada cartera, una gran capacidad de adaptación e innovación y la posibilidad de aumentar su cartera de clientes y

23. Por la naturaleza del mercado de defensa, siendo un bien común global y necesario, no tiene sentido buscar la salida del mismo ya que es un mercado seguro, pero en declive por la situación. El mercado de defensa es el eterno mercado maduro.

productos así como la de adaptar los ya existentes, otorga a BAE Systems una posición privilegiada para afrontar los recortes y la nueva situación del mercado.

3.3. *Italia: en la piel de Finmeccanica*

Para ver el estudio en detalle, ir al Anexo IV.

En el estudio hecho a Finmeccanica, se puede ver una clara estrategia por parte de la empresa de utilizar sus fortalezas para acometer las nuevas oportunidades (ofensiva), así como su firme compromiso de centrar su actividad en su *core*, eliminando las actividades que le debilitan (supervivencia).

A pesar de las debilidades de la empresa, muy especialmente remarcable es el freno debido a su baja capacidad de financiación comparada con otras empresas del sector, cabe destacar la firmeza en su estrategia (coherente durante los últimos años, equilibrada sin cambios bruscos), su enorme capacidad innovadora (constantemente alta), su flexibilidad y su competitividad exportadora. Pese al desequilibrio nacional, Finmeccanica es capaz de buscar y encontrar fuera de sus fronteras lo que nacionalmente no encuentra, posicionándose por encima de otras empresas con mayor ayuda estatal como es Thales o Indra.

3.4. *Francia: en la piel de Thales*

Para ver el estudio en detalle, ir al Anexo IV

En el estudio hecho a Thales se puede ver la estrategia de buscar oportunidades gracias a sus fortalezas (ofensiva), como es la compra de la empresa Vormetric, o la utilización de sus productos de defensa/civiles en dentro de su propia organización o entre divisiones. Sus duplicidades en términos de productos específicos para cada país e ineficiencias vienen derivadas en muchos casos de la necesidad, por ley, de tener una filial en el país y un producto 100% del país de destino si se quiere hacer negocio de defensa allí. Este tipo de estrategias son de supervivencia y Thales no puede hacer nada al respecto porque la alta regulación del sector de la defensa nacional en cada país no es algo que pueda controlar.

Ante el competitivo mercado que se avecina, Thales es una empresa preparada para llevar a cabo los proyectos que se deban hacer. Si bien debe tener especial cuidado de la poca flexibilidad de su estructura de costes, las duplicidades y las ineficiencias que

acarrea tener una empresa con filiales en cada continente. Sus filiales pueden ser su punto de apoyo para la ampliación y puesta en marcha de la tecnología, si están debidamente gestionadas y controladas.

3.5. *Alemania: en la piel de Rheinmetall*

Para ver el estudio en detalle, ir al Anexo IV.

En el estudio realizado a Rheinmetall se puede observar una clara estrategia por parte de la empresa de utilizar sus fortalezas, como es su negocio recurrente mediante el fortalecimiento de su posición en el mercado, contra la amenaza del aumento de la presión presupuestaria (ofensiva). Por otro lado, la empresa está fijando sus esfuerzos en la optimización de su estructura de costes y el aumento de su inversión I+D con el fin de poder ampliar su negocio con nuevas oportunidades —clara estrategia de reorientación.

La alta especialización, experiencia y calidad de sus productos le han dado a Rheinmetall una posición de referencia en el mercado. Sin embargo, el entorno en el que actualmente se mueve Rheinmetall y de donde procede la mayor parte de sus ventas va a volverse muy hostil y deberá tomar su gran capacidad exportadora e innovadora como bandera para encontrar una posición en el mercado que llega, así como el de ampliar sus fronteras y entrar en nuevos mercados.

3.6. *España: en la piel de Indra*

Para ver el estudio en detalle, ir al Anexo IV.

En el estudio realizado a Indra se puede observar cómo la empresa utiliza sus fortalezas para conseguir nuevas oportunidades, tal es el caso de sus soluciones en ATM, ferroviario…etc en Latinoamérica (estrategia ofensiva). Asimismo, Indra es capaz de poner barreras de entrada en su mercado nacional gracias a su lobby, experiencia y posicionamiento en el cliente (defensiva).

Mientras que el resto de los países europeos invierten cantidades grandes, aunque menguantes, en sus empresas de defensa, España realiza una inversión pequeña y en declive; por lo que la única manera de que Indra se puede hacer competitiva en este mercado, es mediante una fuerte inversión en I+D, que le dé la ansiada competitividad y gane concursos fuera de sus fronteras –

estrategia que siguen Finmeccanica y Rheinmetall; empresas de defensa con un fuerte poder exportador. Aunque la situación de la empresa es complicada, debido a la rigidez de su estructura y la mala situación de su mercado nacional —en gran parte por la priorización por parte de la administración estatal de las inversiones públicas en fines sociales y de reactivación de la economía— Indra tiene la oportunidad de adelantarse a los cambios del mercado. El ajuste de su estructura de costes, el aumento de su esfuerzo innovador y la exportación serán claves para determinar la futura competitividad de la empresa.

4. Un vistazo hacia delante: extrapolación de resultados

El estudio realizado y los datos analizados tienen el objetivo de entender la dinámica del mercado actual, y es gracias a esta dinámica que estamos en disposición de hacer el ejercicio de mirar al futuro: ¿qué se puede esperar del mercado de defensa para los próximos años?

Durante todo el trabajo queda claro que la crisis financiera del año 2007 hizo emerger diferencias estructurales en el mercado de la defensa con la existencia de dos velocidades claras– EEUU y el resto del mundo. Mientras que EEUU copaba gran parte del mercado en defensa, tanto en gasto militar como en innovaciones y comercialización de armas, Europa sólo podía defenderse de este imponente mercado mediante la innovación y la defensa de sus fueros nacionales con, por ejemplo, programas europeos de innovación o la concentración de sus empresas para poder plantar cara a su competidor al otro lado del Atlántico (tal es el caso de Airbus Group con Boeing). La crisis, sin embargo, rompe el mercado y obliga a los gobiernos a cambiar sus prioridades de gasto: sacrificando parte de su esfuerzo en la defensa, en beneficio de fines sociales. Las empresas han detectado este cambio y sus consecuencias: el aumento de la competencia. En la defensa, mercado puramente tecnológico, sobreviven las empresas que venden los mejores productos, los más avanzados… en definitiva, los más innovadores. La respuesta de las empresas estadounidenses ha sido la de aumentar su esfuerzo en I+D a sabiendas del cambio que se cierne sobre el mercado: caída de la contratación pública, aumento de la competencia, disminución de los márgenes en los programas y caída en el nivel de ventas.

Las empresas europeas superan en porcentaje el esfuerzo innovador de las estadounidenses, sin embargo, todavía están muy lejos de su nivel de ventas y contratación.

La globalización está diluyendo las fronteras. Actualmente con un solo *click* se puede conectar, defender, atacar o vigilar cualquier parte del mundo desde cualquier lugar. Las naciones no sólo se deben defender físicamente de invasores o terroristas, si no también deben defender su espacio cibernético: su información sensible de personas u organismos malintencionados. Estamos en una realidad extraña: mientras que se diluyen las fronteras favoreciendo el comercio, el movimiento de talento, la creación de oportunidades… también crecen los riesgos. El aumento de la libertad, aumenta los riesgos sobre la seguridad nacional y la necesidad de control —lo que supone una limitación de la libertad: un auténtico paradigma.

El mercado de la defensa está respondiendo a esta nueva realidad: creciendo desde la defensa física de las fronteras hasta la defensa de la información en la red. La ciberseguridad se perfila como una pieza importante en el futuro cercano y ya está siendo objeto de inversión por parte de las grandes empresas europeas y estadounidenses. La capacidad de las empresas militares de adaptarse al mundo civil[24], de ampliar sus productos, exportar e innovar será clave para su supervivencia. Esta última, la capacidad innovadora, determinará no sólo las posibilidades de supervivencia de las empresas si no el devenir del propio mercado. La competencia durante los próximos años será terrible y las empresas deberán jugar entre la inevitable caída en la contratación y la imperante necesidad de aumentar su esfuerzo innovador. Posiblemente veremos fusiones, ventas y grandes esfuerzos de diversificación por parte de las empresas de seguridad – muy especialmente las que, como Lockheed Martin o BAE Systems, cuentan con una cuota de ventas de defensa muy alta.

Sin embargo, dentro de este estudio queda una incógnita que está fuera de las manos de cualquier empresa: ¿cómo reac-

24. En los trabajos de Acosta et al. (2011) y Acosta et al. (2013) tratan sobre esta cuestión. Utilizando exclusivamente tecnologías patentadas, los autores concluyen que un 25% de las patentes militares (*en el campo de armas y municiones*) fueron utilizadas como antecedentes para desarrollar otras invenciones patentadas en el ámbito civil.

cionarán los gobiernos ante la diversificación de las empresas tradicionales de defensa al mundo civil? ¿Cómo serán regulados los nuevos productos duales? La tecnología dual y las aplicaciones civiles tienen una regulación más laxa que la que sufren las empresas militares y sus productos específicos para dicho mercado. La entrada de las empresas en el mundo civil no sólo aumenta su cartera de productos, si no que facilita la exportación y venta de sus productos. La entrada de las empresas tradicionalmente militares y su tecnología en el mundo civil puede llegar a suponer un aumento de la regulación.

5. Conclusión

Para concluir el estudio, se debe volver a la pregunta original: ¿el aumento de la inversión I+D aumenta las ventas? Como se ha visto a lo largo de todo el trabajo, la respuesta a esta pregunta no se responde tan fácil con un sí o un no. La inversión innovadora es importante para las empresas, hasta tal punto que su viabilidad a largo plazo en el mercado depende de ello – sobre todo en los mercados de alta tecnología, como es el de la defensa.

Una inversión I+D que responde a las demandas del mercado[25] sitúa a la empresa en una posición de ventaja competitiva con respecto al resto. Si bien hay variables que actúan sobre esta competitividad: la dinámica en inversión I+D por parte de la empresa, su esfuerzo innovador histórico (posicionándose en una situación de entrada mejor o peor[26]), su capacidad de buscar oportunidades en el mercado, su estructura de costes y en el caso de la defensa, su país de origen también juega un papel muy importante debido a la soberanía nacional. Por este concepto de soberanía nacional, las empresas nacionales de los países se ven fuertemente favorecidas por la contratación pública en defensa y la manera que tiene una empresa extranjera de «robar» cuota de mercado de defensa a una empresa nacional es mediante la

25. Una inversión I+D es una decisión estratégica a largo plazo. Para que un proyecto I+D tenga sentido, la empresa debe tener un plan de a dónde quiere ir. Un ejemplo claro lo encontramos en cualquiera de las grandes empresas de defensa: Finmeccanica con su estrategia de tecnologías duales o Lockheed Martin ampliando su mercado a la ciberseguridad.

26. Cuanto peor sea la posición de entrada, mayor deberá ser el esfuerzo I+D.

competitividad de su propio producto. La competitividad es, por tanto, un elemento fundamental en la capacidad de contratación y venta de una empresa.

A lo largo del trabajo se han estudiado dos modelos de financiación I+D en el mercado de la defensa: por un lado tenemos el modelo estadounidense en el que el Estado realiza un gran esfuerzo innovador con proyectos y programas con un alto contenido en I+D. Las grandes beneficiadas de dichos programas son las empresas nacionales estadounidenses. Por otro lado, está el modelo europeo por el cual el esfuerzo innovador a través de programas y proyectos financiados por la administración es menor. De esta manera, la empresa debe compensar la falta de financiación estatal con un esfuerzo privado mayor[27]. En la actual situación de caída generalizada de presupuestos de defensa y aumento del apoyo a conceptos como el Pooling and Sharing, el modelo europeo está tomando una mayor relevancia. EEUU copa gran parte del mercado de defensa ya que su gasto militar está muy por encima del de sus aliados. Sin embargo, la dinámica del mercado y la profunda crisis financiera ha provocado una priorización del gasto a la reactivación de la economía y al gasto social – dejando a un lado el gasto en defensa. Aunque la aportación estadounidense al mercado de la defensa sigue siendo muy alta, las empresas estadounidenses —como Lockheed Martin— han comenzado a aumentar su esfuerzo innovador para compensar la caída de programas I+D. Este aumento del esfuerzo privado es un claro guiño al modelo europeo.

La caída de los presupuestos no sólo ha provocado un cambio de modelo en la gran potencia del gasto militar, sino que también ha incrementado la competencia del mercado en general: tanto en EEUU como en Europa[28]. La disminución de contratación pública provoca una caída de los márgenes en los programas y

27. Tal es el caso de todos los países europeos estudiados, excepto España y su empresa Indra que siguen un modelo americano con un presupuesto muy inferior al estadounidense.

28. James (2006) discute las diferencias entre la industria defensa de Estados Unidos y Europa, así como diferencias entre países europeos. Desde una perspectiva distinta, Molas-Gallart (2001) y James (2009) estudian los cambios políticos y estratégicos en la investigación en defensa en el Reino Unido, que está dirigida a incrementar la transferencia de conocimiento hacia aplicaciones no defensivas.

las licitaciones para las empresas[29], que tiene como consecuencia lógica la supervivencia del más fuerte: sólo las empresas más competitivas sobrevivirán en el cambiante mercado y es ahí, en la competencia, donde el I+D es clave. Un I+D que responde a las necesidades del cliente: mayores aplicaciones duales, capacidad de adaptación de soluciones militares a entornos civiles, la ciberseguridad… no sólo son nuevos mercados como puede ser Arabia Saudí y su carrera armamentística, si no nuevos clientes. La ciberseguridad, mercado emergente y con grandes márgenes, formará sin lugar a dudas parte importante del nuevo mercado de defensa. La grandes empresas de defensa ya invierten en él (Lockheed Martin, BAE Systems, Finmeccanica, Thales…) y los países – a la vista del ciberterrorismo y la cantidad de información que circula en la red, comienzan a demandar fuertemente la protección de su información de manera explícita.

El mercado de la defensa está cambiando, mutando hacia productos más flexibles y con múltiples usos. El declive de los presupuestos públicos destinados a la defensa está acelerando el cambio y aumentando la exigencia hacia las empresas; aquellas que deseen sobrevivir deberán ser más competitivas, más flexibles y más innovadoras, sólo así se pueden asegurar un puesto en el nuevo mercado.

A río revuelto, ganancia de pescadores, en los próximos años veremos quién es pescado y quién es pescador.

Bibliografía

Acosta, M., Coronado, D., Marín, R., (2011). Potential Dual-Use of Military Technology: Does Citing Patents Shed Light on this process? Defence and Peace Economics 22, 335-349.

Acosta, M., Coronado, D., Marín, R., Prats, P., (2013). Factors affecting the diffusion of patented military technology in the field of weapons and ammunition. Scientometrics 94, 1-22.

Alé-Ruiz, Rafael (2013). «Humanismo, nuevo paradigma empresarial», Editorial Académica Española, pág. 28.

Bonache, Jaime (1999). El estudio de casos como estrategia de construcción teórica: características, críticas y defensas. Cuadernos de economía y dirección de la empresa, núm. 3, 1999, págs. 123-140.

29. Las mismas empresas licitando por menos contratos. La concentración del mercado provoca la caída de los márgenes.

Cowan, R., Foray, D., (1995). Quandaries in the economics of dual technologies and spillovers from military to civilian research and development. Research Policy 24, 851-868.
De Carlos Izquierdo, Javier (2015). Las Estrategias de Seguridad Nacional de EEUU ¿Algo Nuevo? Instituto Español de Estudios Estratégicos. Publicado 10 de agosto.
Department of Defense (2012). Sustaining US Global Leadership: Priorities for 21st Century Defense. Enero 2012.
Estrategia Española de Seguridad (2011). Una Responsabilidad de Todos. Editado: Gobierno de España.
French National Digital Security Strategy (2015) First Minister. Publicado octubre.
Fuenta Cobo, Ignacio (2015). La Revisión de la Defensa Británica: Una Medida de su Ambición Estratégica. Instituto Español de Estudios Estratégicos. Publicado.
Global Competitiveness Report 2015. World Economic Forum.
James, A., (2009). Organisational change and innovation system dynamics: the reform of the UK government defence research establishments. J Technol Transf 34, 505-523.
James, A.D., (2006). The Transatlantic Defence R&D Gap: Causes, Consequences and Controversies. Defence and Peace Economics 17, 223-238.
Molas-Gallart, J., (2001). Government defence research establishments: the uncertain outcome of institutional change. Defence and Peace Economics, 12, 417–437.
Laborie Iglesias, Mario (2014). La Estrategia de Seguridad Nacional (mayo 2013). Instituto Español de Estudios Estratégicos. Publicado: 3 junio. Página 4.
Ley 36/2015, de 28 de septiembre, de Seguridad Nacional. Publicada finalmente el 29 de septiembre de 2015, BOE número 233, páginas 87106 a 87117.
Libro Amarillo (2016). Presentación del Proyecto de Presupuestos Generales del Estado 2016. Gobierno de España.
Marrone, Stefano Silvestri, Alessandro R. Ungaro (2015). The White Paper: A Strategy for Italy's Defence Policy. Instituto Affari Internazionali. Edición 2015. Publicado: 15 junio.
Parada, Pascual (2013). Análisis PESTEL, una herramienta de estudio del entorno. Publicado 10 de enero.
Research in Italy, land of «Hidden Gems». Italian Trade Commision. Publicado: NY, Enero 2010.
Sandler, T. and Hartley, K., 1995. The Economics of Defense. Cambridge: Cambridge University Press.
Stowsky, J., (2004). Secrets to shield or share? new dilemmas for military R&D policy in the digital age. Research Policy 33, 257-269.
Transferencia de Armas (2015), SIPRI, Base de Datos.

UNESCO Institute for Statistics, Editado: Banco Mundial. Varios años
Wen-Min Lu, Qian Long Kweh , Mohammad Nourani, Feng-Wen Huang (2016), Evaluating the efficiency of dual-use technology development programs from the R&D and socio-economic perspectives. Omega – The International Journal of Management Science. Núm. 62, pag 82-92.
White Paper Defense and National Security (2013). Ministerio de Defensa Francés.
World Economic Outlook Database (2015). Internatinal Monetary Fund, varios años.

MODELO DE GESTIÓN DEL CONOCIMIENTO ECONÓMICO BASADO EN EL MARCO INPUT OUTPUT. UN CASO DE ESTUDIO APLICADO AL SECTOR DE LA DEFENSA EN ESPAÑA

José Ramón Coz Fernández
Universidad Complutense de Madrid
Investigador del Departamento de Economía Aplicada VI

Resumen

En el escenario actual macro económico la toma de decisiones en materia económica de cualquier entidad pública debe de estar sustentada por una adecuada inteligencia económica. Es prioritario disponer de modelos, técnicas y herramientas que permitan garantizar un control adecuado en todas sus inversiones.
En la presente propuesta exponemos un modelo de gestión del conocimiento basado en el marco input output, que nos permite conocer el impacto económico de las inversiones realizadas. Este modelo está soportado por un sistema de información que coadyuvará a los analistas económicos para la toma de decisiones en el campo de las inversiones públicas.
El modelo y el sistema se han aplicado en el área de la Defensa al objeto de conocer el impacto económico de una serie de programas de inversión en el sector aeronáutico.

Palabras claves

Análisis Input-Output, Impacto Económico, Economía de la Defensa, Gestión del Conocimiento.

1. Introducción bibliográfica

Hemos tomado como referencia central de nuestro modelo el análisis input output, que tiene sus raíces en los trabajos de Leontief (1936, 1941, 1951) y en el desarrollo posterior del marco input output en Leontief (1986) y Leontief W., Carter y A., Petri P.A. (1977). Una de las primeras aplicaciones de esta metodología se encuentra en el trabajo de Herderson (1955) donde se utiliza el método Input-Output para analizar la economía italiana. En

el ámbito de algunos sectores como el transporte marítimo la literatura recoge innumerables trabajos como el de Hill (1975), que determinó el impacto del puerto de Baltimore (EEUU) , o incluso en el sector de las competiciones lúdico-deportivas, con Barker, M.; Page, S.J. y Meyer, D. (2002); Crompton, J.; Lee, S. y Shuster, T.J. (2001), y Kasimati, E. (2003).

También existen algunos estudios relevantes de impacto bajo el marco input output en España como el artículo de Llano, que analiza el impacto en la economía española a nivel interregional Llano, C. (2004), o el artículo de Goicolea A., Herce JA y De J. Lucio (1998) que estudian el crecimiento de la economía en España; en el artículo de Alcaide (1996) se propone un modelo simplificado de contabilidad a nivel regional y otro artículo revisado de la bibliografía con referencias al marco input output es el de Moreno R., López-Bazo E., Go E. y Artis M. (1999) que analizan los efectos externos en la producción, Fontela-Montes, E, y Rueda-Cantuche (2005) que ofrecen un modelo input-output mundial de contabilidad social (incluyendo aspectos medioambientales), y el análisis llevado a cabo por Soza-Amigo, S. y Ramos-Carvajal, R. (2011) que ofrece interesantes conclusiones sobre cómo influye la reducción de una tabla input-output en los multiplicadores y encadenamientos de las ramas que no se unen.

En lo que se refiere a su aplicación en los Sectores, destacaremos los estudios aplicados en el ámbito turístico en España, como los trabajos de (González, 2010) Puertas-Medina, R., Martí-Selva, L. y Calafat-Marzal, C. (2012) o Sánchez-Rivero M. (2012). Otro caso más específico analizado ha sido el estudio de Martí et ál. (2009), que recoge su aplicación a los distintos puertos de la Comunidad Valenciana.

La gestión del conocimiento, entendida a través de los trabajos de Koontz H. y Weihrich H. (1996), Laurence Prusak (1996) y Jozef Loermans, (2002) se sustenta en un proceso que permite localizar, filtrar, organizar y presentar información al objeto de mejorar el aprendizaje y la compresión de una específica área de interés; y lo realiza, según Malhotra, Y. (1998), a través de la búsqueda de una combinación sinérgica de datos e información, el uso de las tecnologías de la información y las capacidades de creatividad e innovación de las personas.

A la hora de afrontar un proyecto de Gestión del Conocimiento los autores Davenport T., De Long D. y Beers M. (1997)

proponen una gran variedad de formas para generar valor en base a los activos del conocimiento. Estas propuestas, no significan soluciones tecnológicas necesariamente, sino una combinación de factores de diferentes tipos, que mediante su relación estructuren la solución final.

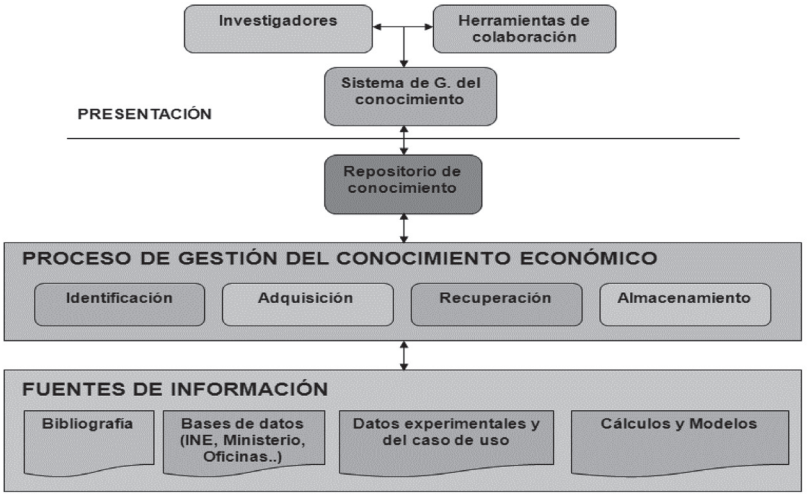
A partir de estas propuestas, las bases conceptuales y últimos avances en gestión del conocimiento, y aplicando las técnicas y procesos propuestos por el marco input output en las referencias mencionadas, nuestro trabajo se ha centrado en desarrollar un modelo de gestión del conocimiento sobre el impacto económico de las inversiones. Este modelo se aplicado en el sector de la Defensa, sobre varios programas aeronáuticos de gran alcance económico.

2. Modelo del conocimiento para el impacto económico (MOCIE)

Para llevar a cabo nuestro proyecto relacionado con la gestión del conocimiento construimos un modelo que incluye tres capas de gestión del conocimiento (la percepción de los componentes existentes en el entorno organizacional, la comprensión de su significado y la proyección de su estado en el futuro). Nuestra propuesta está soportada por un modelo que hemos denominado MOCIE (Modelo de Conocimiento para el Impacto Económico).

Este modelo nos permite relacionar las capas de la conciencia situacional con los niveles del proceso de fusión datos en términos de impacto económico de un programa de inversiones. En la figura siguiente mostramos un esquema simplificado de dicho modelo.

Figura 1: Estructura General de MOICE



Los sensores representados en la figura son dispositivos en el sistema que capturan la información de las fuentes y proporcionan dicha información a una serie de niveles. Ejemplos de estos sensores son los diferentes informes de las oficinas de los programas de inversión, la información del Instituto Nacional de Estadística que nos proporciona los datos nacionales input output o las bases de datos internacionales de datos input output.

En el nivel cero de nuestro modelo se integrarían los datos de los sensores procedentes de diversas fuentes mediante un proceso de fusión de datos, que permite abordar los problemas de adaptación (por ejemplo, los cambios de moneda, las actualizaciones de precios, la precisión de los datos) o las diferencias en la presentación de formatos de salida.

El nivel uno del modelo está soportado por un proceso de fusión de la información que combina estos datos para realizar diferentes cálculos y simulaciones, permitiendo obtener información estandarizada que pueda ser operada por un modelo matemático completo en el nivel 2.

A nivel dos se combinan todas las variables en un modelo para proporcionar como salida la perspectiva actual del estado de nuestras inversiones en términos de impacto económico. A nivel tres, el proceso proporciona una capacidad de predecir los estados futuros de nuestros sistemas de inversión (por ejemplo, si

invertimos más en ciertos sectores ¿cómo variaría nuestro impacto económico? o ¿cuánto tengo que invertir en cierto sector para obtener mayor empleo en sectores estratégicos?, ¿qué sectores son los que reciben un mayor impacto sí modifico mi esquema de inversión en ciertos proyectos?).

El nivel cuatro del modelo MOCIE aborda la capacidad del sistema para el mantenimiento de reglas y sensores. Por ejemplo, la actualización de datos input output a nivel nacional sería un ejemplo de capacidad básica del nivel cuatro.

Por último, el nivel cinco es la interfaz entre el analista económico y el sistema de fusión de datos. La visualización de la información juega aquí un papel muy relevante. En general, la visualización consiste en la representación de información de forma gráfica para poder transmitir un concepto de manera clara. Se trata de un componente esencial en la transmisión de la conciencia situacional y que permite una mayor rapidez en la toma de decisiones ya que la presentación de los datos de manera visual permite aprovechar la potencia del procesamiento del cerebro humano, junto con nuestra capacidad natural para detectar patrones, tendencias y cambios en las imágenes.

El análisis completo de la información económica seguirá necesitando de un gran componente humano, a pesar de todos los esfuerzos de automatización, aunque continuará siendo cada vez más exigente. Aquí los sistemas de visualización jugarán un papel esencial.

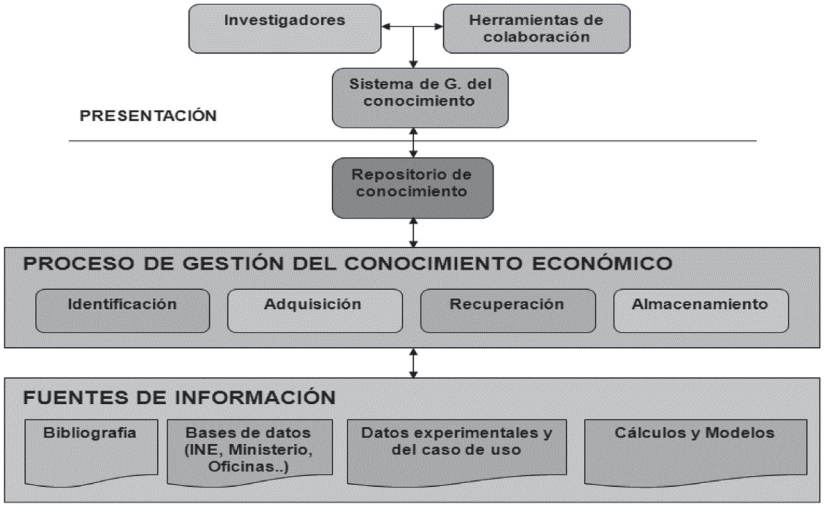
El flujo de datos ha de ser analizado tanto en tiempo real como sus datos históricos. Es por ello por lo que se hace necesario contar con sistemas de visualización que permitan reducir el tiempo de análisis sin producir una falta de datos al haberlos resumido en exceso y acorten el tiempo necesario para la toma de decisiones. Uno de nuestros objetivos para lograr este propósito fue desarrollar un sistema de información de soporte a este proceso.

2.1 *Sistema desarrollado de gestión del conocimiento*

La figura dos expone la arquitectura de nuestro sistema de gestión del conocimiento, de soporte al modelo MOCIE, formado por una capa de presentación, donde los investigadores puedan interactuar mediante una serie de herramientas de colaboración.

Esta capa está integrada con un repositorio del conocimiento, donde reside toda la información.

Figura 2: Esquema del Sistema de Información de soporte a MOCIE



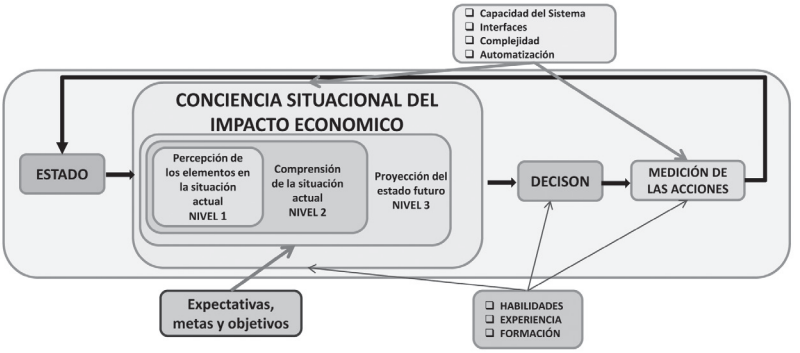
Para gestionar esta información proponemos un proceso que permita identificar, obtener, clasificar, transformar, recuperar y residir esta información. Las fuentes de datos forman parte de la bibliografía, los datos experimentales y de uso de nuestros casos prácticos, los cálculos y modelos y finalmente las diferentes bases de datos consultadas, que para nuestro caso de estudio serán fuentes del Instituto Nacional de Estadística de España (INE), del Ministerio de Defensa, de la Unión Europea y de las Oficinas de Programas, principalmente.

El modelo de gestión del conocimiento proponemos que se aplique en un escenario de toma de decisiones, tal y como se presenta en la figura 3. Las decisiones y acciones que se llevan a cabo, y que son medidas a posteriori, varían en función del estado, que es analizado a través de diferentes niveles (percepción, compresión y proyección), tal y como se puede observar en la figura.

En función de las habilidades, la formación y la experiencia de los roles que participan en el flujo de decisión, éstos alimentan un bucle que es soportado por un sistema con diversidad de interfaces, un cierto grado de automatización y complejidad. La

principal entrada del modelo son las expectativas, metas y objetivos de las misiones encomendadas.

Figura 3: Toma de decisiones en el modelo MOCIE



En el caso de algunas organizaciones se podría hacer uso del concepto «sensemaking», que es el proceso por el cual un analista de inversiones podría, desde la conciencia situacional, dar sentido a la información que percibe sobre las inversiones, y desde ese nivel hacer fluir la información hasta las capas de toma de decisión, en el caso necesario y con un nivel de detalle adecuado.

Para conseguir este propósito, las organizaciones más avanzadas podrían hacer uso de modelos que permitieran relacionar todas las capas de información de la conciencia situacional en términos de impacto económico.

Las representaciones gráficas de los datos en nuestro caso se realizan utilizando el color, la forma, la posición, el tamaño o cualquier otra propiedad gráfica que pueda codificar la información. Ha de ser posible, partiendo de unos datos de un alto nivel de abstracción, moverse de manera interactiva hacia los datos de menor nivel en caso de que fuera necesario para poder comprender lo que se nos muestra.

Las técnicas de visualización son diseñadas o seleccionadas para alinearse con uno o más de las fases o niveles de la conciencia situacional: Percepción, Comprensión y Proyección.

Estas fases se refieren, respectivamente, a ser consciente de los datos actuales, tener un entendimiento necesario que permita obtener conclusiones sobre la situación en la que nos encontramos en relación con esos datos y, finalmente, intentar predecir

la situación futura en la que nos encontraremos en base a esa información.

Existen cinco usos estandarizados principales de la visualización en nuestro modelo, tal y como son mostrados en la figura siguiente:

—Monitorización, en la que se observa un fenómeno en curso en el que los datos pueden estar en continuo cambio, como pueda ser el caso de los valores de cambio de una moneda,
—Inspección, en la que el analista busca detalles específicos, solicita aclaraciones y encuentra datos que le permiten comprobar hipótesis,
—Exploración, donde se realiza un estudio concienzudo y libre de los datos, se investiga sin tener pistas previas, se combinan los datos de forma novedosa y se experimenta interactivamente con las vistas de los datos, encontrando regiones de interés para su análisis y se generan nuevas hipótesis,
—Predicción, en la que, o bien intentamos encontrar el estado futuro más probable suponiendo que la progresión actual continuará si no se interviene, o determinamos un estado futuro particular basado en planes de acción potenciales y
—Comunicación, en la que se presentan todos los datos a terceros, se realizan informes, o se presentan las actividades realizadas.

Figura 4: Conceptos de visualización en el modelo MOCIE

3. Aplicacion a un caso de estudio en el sector defensa

La Industria de Defensa tiene una importancia estratégica para el Estado. Las actividades de Defensa y asociadas representan el 1,9% del empleo total de la economía española y más de la mitad de la Demanda de Defensa se dirige hacia industrias de alta tecnología e intensivas en conocimiento. Los Programas de Defensa, y en concreto los Programas Especiales de Armamento (denominados PEAs), han supuesto una inversión muy importante en materia económica, en empleo, en investigación innovación y desarrollo en los últimos años, y han constituido un tractor de la industria nacional en multitud de sectores.

Nuestro caso de estudio nos permite analizar el impacto de una serie de programas de Defensa en la economía nacional: el impacto en materia de producción, en el empleo, en sectores estratégicos de la economía, etc. El uso de nuestro modelo MOCIE nos puede dar soporte a la denominada inteligencia económica del Ministerio de Defensa, permitiendo una mejora en la toma de decisiones.

Nuestro caso de estudio tiene un gran alcance: varios programas de mantenimiento del avión F-18. La adquisición y el mantenimiento de los F18 han constituido un referente tanto para el Ministerio de Defensa como para la Industria del Sector, desde que en mayo de 1983 el Consejo de Ministros decidiera la adquisición de los aviones al Gobierno de Estados Unidos.

Este hito constituye el inicio de una política industrial de Defensa ejemplar que dio lugar a la actual Política de Cooperación Industrial en materia de Defensa. Los programas de mantenimiento del F18 han tenido un gran impacto económico en la Industria de Defensa en España, incluyendo el desarrollo en el campo de la simulación, los bancos de pruebas automáticos, los subsistemas de aviónica, el desarrollo de componentes estructurales de aeronaves, la creación del Centro Logístico de Armamento y Experimentación (CLAEX), la cogeneración eléctrica con centrales térmicas, etc.

Para nuestro caso de estudio hemos tomado la información de diversos programas de mantenimiento de los aviones F18 entre los años 2005 y 2010, que incluyen programas de adquisición de equipamiento de guerra electrónica, la instalación de las comunicaciones de los aviones, la actualización de la media vida o los programas de mantenimiento mayor del sistema de armas.

El conjunto de programas bajo estudio conlleva una gran complejidad, pues se trata de adquisiciones que engloban asistencias técnicas, consultoría, producción de sistemas, apoyo logístico, formación, construcción de materiales, desarrollo de sistemas informáticos y de comunicaciones, desarrollo de equipamiento electrónico, gestiones financieras y un largo etcétera.

Con el objetivo de poder utilizar las herramientas de análisis proporcionadas por el marco input-output incorporadas en nuestro modelo, hemos reconstruido las Tablas Input Output de la economía española desde el nivel cero (que corresponde a las entradas, fuentes y sensores ligeramente modificados), para incorporar e individualizar el programa de inversiones bajo estudio.

La desvinculación se realiza en el nivel uno del sector Administraciones Públicas, ya que en nuestro caso este sector de la Defensa no está individualizado en las tablas que provienen de las fuentes del nivel cero, y que corresponden a la información del Instituto Nacional de Estadística.

El objetivo final en el nivel cinco (el que corresponde con los interfaces finales de salida para los analistas), es convertir el caso bajo estudio en un sector económico propio, que nos permitirá efectuar un análisis riguroso para medir la relación del programa con los demás sectores de la economía y la dependencia de éstos con respecto al programa. Nuestro modelo nos permite desde dicho nivel, no sólo medir el peso del programa de Defensa en la economía, sino también mostrar sus relaciones con los demás sectores a través de los intercambios con ellos. La tabla input output se modifica en el nivel 1 (que corresponde a los interfaces de nuestro sistema, los cálculos matriciales y las simulaciones).

Desde el nivel 2, podremos mostrar, por un lado, a qué sectores vende dicho programa y cuánto les vende, es decir, quiénes son sus clientes y qué importancia tiene cada uno. Y, por otro lado, a qué sectores compra y cuánto les compra, o quiénes son sus proveedores y con qué importancia. Esta información detallada nos permitiría calcular los efectos que tiene dicho programa, tanto de forma directa como indirecta, en otros sectores de la economía.

La tabla simétrica input-output del año 2005 de la economía española es la utilizada como fuente de datos inicial. En ella, la Defensa aparece agregada en el sector de servicios de la Administración Pública. Por lo tanto, para incluir un programa como un

sector más de la economía, será necesario realizar esta desagregación en el nivel 1. La imputación de las ventas del Programa no será necesaria, ya que, al tratarse de un sector de servicios públicos, éstas no existen como tales y por tanto esa capa en nuestro caso no se utiliza. En el caso de los inputs o consumos intermedios del Programa se utilizarán los datos de sus compras de bienes y servicios.

Partiendo del conocimiento de los procesos productivos de cada sector y sus relaciones, es decir, de la TIO modificada en el nivel 1, el análisis que se lleva a cabo con el modelo consiste en calcular toda la cadena de efectos que produce la actividad de un sector o empresa. De este modo, se puede traducir la actividad económica de una empresa (o sector de la economía) en una mayor oferta y en aumentos de demanda de diversos sectores. Éstos, a su vez, demandan más bienes y servicios a todos los demás, mientras que los receptores de la oferta incrementan su producción, produciéndose así toda una sucesión de efectos intersectoriales que pueden ser medidos combinando la información input-output con el álgebra matricial, que es implementado en detalle en el nivel dos. Desde este nivel, nuestro sistema nos permite llegar a una expresión que calcula el efecto total y que además se puede descomponer en los efectos directos, indirectos e inducidos que se describen a continuación.

En el caso concreto que nos ocupa, el efecto directo consiste en la inyección de recursos que los programas de Defensa bajo estudio aportan a la economía nacional. Esta cuantía es la que se utiliza para el cálculo de los denominados efectos intersectoriales (la suma del efecto indirecto y el efecto inducido), que también se realizan en el nivel dos. El efecto indirecto se compone de diversas cuantías derivadas de las relaciones entre los sectores productivos.

Por un lado, se cuantifica el efecto que la actividad del programa tiene en los sectores de la economía española con los que se relaciona directamente, en lo que se denomina efecto indirecto dependiente. Es decir, trata de medir la producción en otros sectores que se destina a satisfacer la demanda de bienes y servicios del programa bajo estudio.

Por otro lado, los sectores directamente beneficiados por la actividad (compras y ventas) del programa generan, a su vez, una serie de efectos indirectos. Por el lado de los proveedores, para

producir lo que se les demanda, compran más a sus proveedores que, a su vez, también generan nuevas demandas en la economía. Y por el lado de los clientes; el aumento de oferta de bienes y servicios beneficiaría a todos los sectores que compran a estos clientes y así sucesivamente.

El resultado final de estas rondas de efectos en la producción de los sectores es el llamado efecto indirecto independiente. El impacto sobre la producción al final se agota porque en cada sucesiva ronda de gasto los efectos indirectos son cada vez menores hasta desaparecer.

El efecto suma de los anteriores todavía tiene efectos adicionales. El aumento en la producción genera un mayor empleo y esto significa aumento en las rentas del trabajo que se traduce a consumo en función de la propensión a consumir de los hogares. El incremento en consumo produce toda una nueva cadena de efectos como los descritos anteriormente, cuya suma se conoce como efecto inducido.

Uno de nuestros primeros objetivos fue obtener tanto el efecto directo como el efecto indirecto de nuestro caso de estudio para hacerlo visible en el nivel cinco de nuestro modelo a los analistas. El efecto directo consistirá en la producción generada por el programa en la economía española.

El efecto indirecto será el producido por los gastos necesarios para llevar a cabo las actividades de los sectores directamente afectados, y por los gastos necesarios en el resto de sectores económicos generados por las reacciones en cadena que origina el programa. Estas reacciones provienen de las interrelaciones económicas entre los sectores originariamente afectados y el resto de sectores económicos.

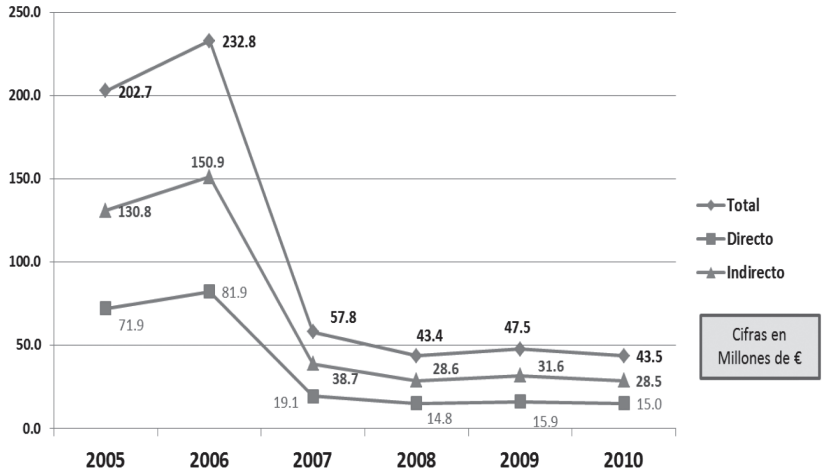
Junto a estos efectos, existe uno más: el efecto inducido, que es el ocasionado por el aumento de consumo que produce el crecimiento en el empleo ocasionado.

Con ayuda del modelo planteado obtenemos en el nivel cinco que el impacto más alto en la producción se produce en los años 2005 y 2006, donde se realizaron grandes inversiones, principalmente en el grupo de programas de actualización de media vida, alcanzando cifras de más de cien millones de euros, tal y como se puede observar en el gráfico 1.

En términos globales, incluyendo el impacto en la producción de todos los años considerados en nuestro caso de estudio y de

todos los programas, el impacto total en la producción ha sido de 627,56 Millones de Euros.

Gráfico 1: Impacto en la Producción del Caso de Estudio

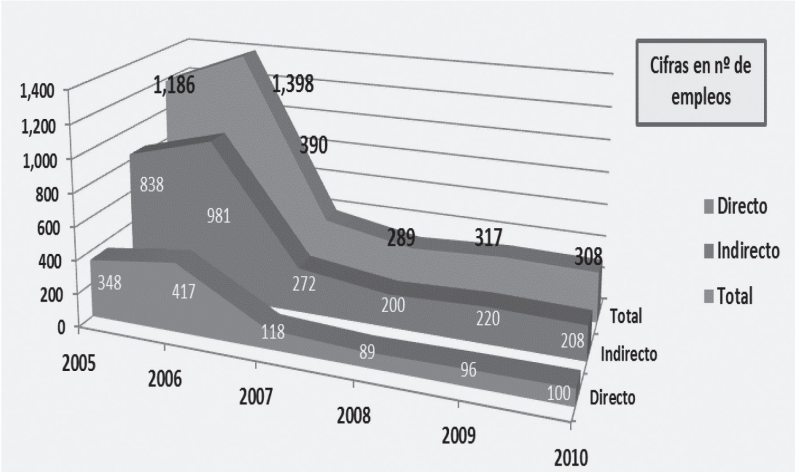


Fuente: elaboración propia, desde el nivel cinco del modelo MOCIE

Además, el segundo de los objetivos de la aplicación de nuestro modelo al caso bajo estudio, ha sido la obtención desde el nivel dos de los datos correspondiente al empleo obtenido, tanto de forma directa como indirecta. El nivel cinco nos permite obtener las gráficas correspondientes, tal y como se muestran en el gráfico 2.

Como se puede observar desde los datos obtenidos en el nivel cinco, en términos globales, incluyendo el impacto en el empleo de todos los años considerados en nuestro caso de estudio y de todos los programas, el impacto total ha sido de 3.887 empleos, correspondiendo 1.167 al impacto directo y 2.720 al impacto indirecto.

Gráfico 2: Impacto en el Empleo del Caso de Estudio



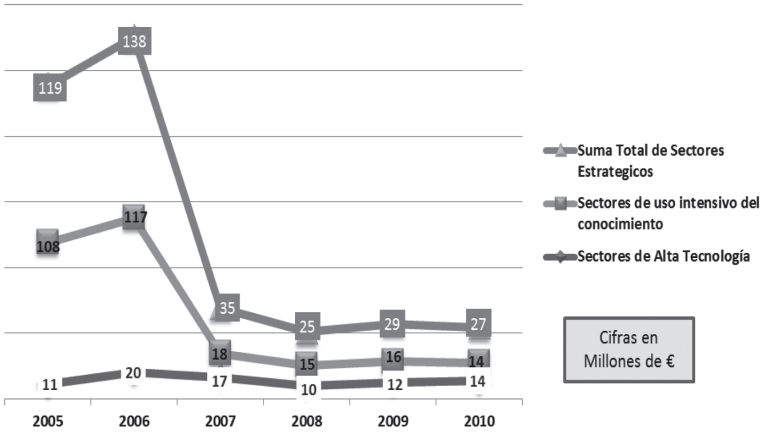
Fuente: elaboración propia, desde el nivel cinco del modelo MOCIE.

Otro aspecto analizado con nuestro modelo ha sido la importancia de la demanda final dirigida, tanto a industrias de alta tecnología, como a sectores intensivos en el uso del conocimiento, según la definición de la Organización para la Cooperación y el Desarrollo Económico (OCDE).

A partir de esta información, en nuestro nivel 1 realizamos una asociación de los sectores correspondientes en nuestra tabla input output y en el nivel dos realizamos los cálculos necesarios para obtener este impacto, haciendo uso del álgebra matricial. El nivel cinco nos permite obtener las correspondientes Gráficas 3 y 4.

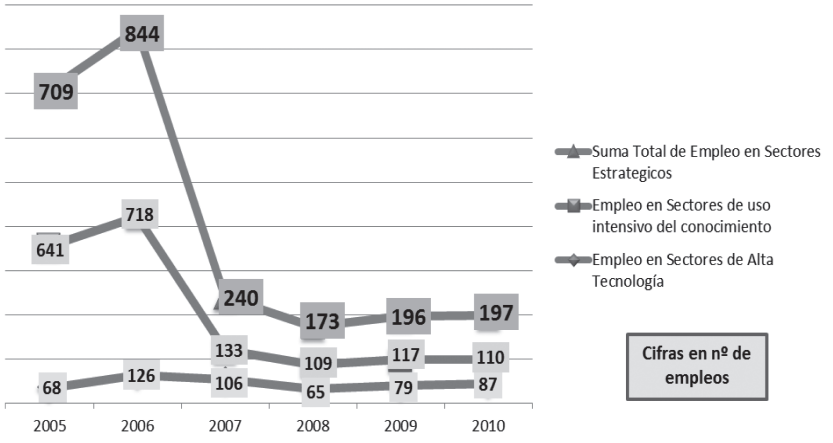
Tal y como se puede observar, el impacto total en estos sectores estratégicos, de alta tecnología y uso intensivo del conocimiento ha sido de 372,89 Millones de Euros y de 1.553 empleos lo cual nos indica la importancia estratégica de este tipo de programas.

Gráfico 3: impacto en la producción en sectores estratégicos



Fuente: elaboración propia, desde el nivel cinco del modelo mocie.

Gráfico 4: impacto en el empleo en sectores estratégicos



Fuente: elaboración propia, desde el nivel cinco del modelo mocie.

Para hacer uso de nuestro modelo hemos partido de diversas hipótesis que han permitido un desarrollo básico de los niveles 3 y 4 del modelo (los modelos predictivos y los mecanismos de actualización y mantenimiento de los sensores), ya que, pese a que el alcance del estudio incluye los datos correspondientes a varias anualidades, únicamente hemos utilizado como uso comparativo las tablas input output del año 2005.

Todos los cálculos se realizan en base este año 2005, que ha sido el año de referencia para nuestro caso de estudio. Un aspecto también importante a considerar es que todos los cálculos para obtener el impacto económico se realizan en el nivel dos sobre el gasto ejecutado en los programas y no sobre el gasto presupuestado, al objeto de obtener el impacto económico más real de los programas bajo estudio. Esta parte es considerada en el modelo MOCIE dentro del nivel 3, lo que nos permite poder hacer predicciones de impacto económico en base al presupuesto y poder realizar comparativas con respecto a las ejecuciones reales de dichas inversiones.

SIMOCIE incluye los interfaces de nuestro sistema de información de soporte al modelo MOCIE, donde podemos observar las diferentes funcionalidades desde un interfaz gráfico común que permite a los analistas interactuar con los diferentes niveles del modelo. En el nivel 0 el analista puede obtener los datos de los diferentes programas de inversiones específicos del caso de estudio y los datos fuente del Instituto Nacional de Estadística, con la información correspondiente al marco input output.

El sistema tiene un interfaz que permite el acceso y la edición de esta información. En el nivel 1 se obtienen datos técnicos como los coeficientes técnicos o las entradas agregadas por cada ano de inversión. En el nivel 2 se pueden visualizar datos obtenidos desde la aplicación específica del marco input output y el modelo matemático simulado en este nivel 2 como los multiplicadores o los vectores de demanda. El interfaz de soporte al nivel obtiene todos los datos de forma gráfica y amigable para el analista. Se ha incluido, en cada uno de los interfaces, el nivel correspondiente al modelo MOCIE, al objeto de facilitar el entendimiento del proceso global para los usuarios del sistema.

Conclusiones

Al objeto de disponer de mejores herramientas para la gestión económica de una entidad pública, el artículo propone un modelo de gestión del conocimiento denominado MOCIE, que permite obtener el impacto económico de las inversiones públicas. Este modelo está basado en las últimas tendencias de gestión del conocimiento y en el marco input output. Como complemento necesario a este modelo, en el artículo se describe el desarrollo de

un sistema de información que da soporte a este modelo a través de una arquitectura que permite interactuar desde las diferentes fuentes de información, obtener los impactos de las inversiones y realizar ciertas predicciones económicas. A través de la integración de este modelo con un esquema de toma de decisiones que se presenta en este artículo, las organizaciones pueden hacer uso de estas técnicas y herramientas para conocer el estado de sus inversiones y sus impactos económicos.

Como caso de estudio particular se ha utilizado el modelo en el sector de la defensa. Las conclusiones de este estudio destacan que las inversiones en el campo de la Defensa tienen un impacto económico de gran relevancia y se focalizan sobre sectores clave de la economía. El conjunto de programas conlleva una gran complejidad, pues se trata de adquisiciones que engloban asistencias técnicas, consultoría, producción de sistemas, apoyo logístico, formación, construcción de materiales, desarrollo de sistemas informáticos y de comunicaciones, desarrollo de equipamiento electrónico, gestiones financieras y un largo etcétera. Nuestro modelo ha permitido realizar un análisis en profundidad de dichas inversiones, como la obtención tanto el efecto directo como el efecto indirecto de los programas bajo estudio y su impacto en sectores clave de la economía y en el empleo.

Tanto el modelo desarrollado como el sistema de información, aunque han sido utilizados en un caso particular del sector de la Defensa, pueden ser extrapolados a otras problemáticas de gestión del conocimiento económico de cualquier entidad. Todas estas conclusiones obtenidas nos han permitido no solamente la puesta en práctica de nuestro modelo, sino también ofrecer datos de gran interés en la toma de decisiones dentro del paraguas de la gestión de los programas públicos.

Agradecimientos

Quisiera agradecer a la Catedrática Aurelia Valiño Castro sus estudios e investigaciones en la materia, sus conocimientos y amplia experiencia. También quisiera agradecer al Ejército del Aire de España, haciendo una mención muy especial al General José Jiménez Lorenzo Bastida y al Coronel José Antonio Manzanares. El soporte documental, las tertulias de economía y su amplia experiencia y conocimientos han sido muy enriquecedores. Por

último, quisiera mencionar al Doctor Néstor Duch, al Almirante Beltrán y los ex Vicepresidentes de Isdefe Maurici Lucena e Ignasi Nieto, por su gran profesionalidad durante la Catedra de Economía con el Instituto de Economía de Barcelona para la Secretaría de Estado de Defensa.

Referencias bibliográficas

Barker, M.; Page, S.J. y Meyer, D. (2002): «Evaluating the Impact of the 2000 America's Cup on Auckland, New Zealand», Event Management, 7, 2, 79-92.

Crompton, J.; Lee, S. y Shuster, T.J. (2001): «A Guide for Undertaking Economic Impact Studies: The Springfest Example», Journal of Travel Resarch, 40, 79-87.

Davenport T., De Long D. y Beers M. (1997) «Building Successful Knowledge Management Projects». Managing the Knowledge of the Organization. *1997 Ernst & Young LLP.*

Fonfría and Correa-Burrows, (2010). «Effects Of Military Spending On The Profitability Of Spanish Defence Contractors», Defence and Peace Economics, 21: 2, 177-192.

Fontela-Montes, E, y Rueda-Cantuche, L. (2005*)* «Linking cross-impact probabilistic scenarios to input-output models.» *Revista de economía mundial*, 13, 2005, 99-112. ISSN 1576-0162.

Goicolea A., Herce JA y De J. Lucio (1998) «Regional integration and growth: The Spanish case». Documento de trabajo 98-14. FEDEA.

González, M. (2010): «Impacto económico de los hoteles: Aplicación a la ciudad de Sevilla», PASOS. *Revista de Turismo y Patrimonio Cultural*, 2, 319-338

Herderson, P.H. (1955): «El método del factor-producto: Una aplicación del mismo a la economía italiana», *Moneda y Crédito*, 54, 3-25.

Hill, J. (1975): «The Economic Impact of the Port of Baltimore and Maryland. Division of Transport, Business and Public Policy», College of Business and Management, University of Maryland.

Jozef Loermans, (2002) «Synergizing the learning organization and knowledge management», Journal of Knowledge Management, Vol. 6 Iss: 3, pp.285 - 294

Kasimati, E. (2003): «Economic Aspects and the Summer Olympics: A Review of Related Research», International Journal of Tourist Research», 5(6), 433-444.

Koontz H. y Weihrich H. (1996) «Administración, una perspectiva global». Mc Graw Hill -10ª edición-1996

Laurence Prusak (1996) «Knowledge in Organizations». Business management Knowledge Reader Series. Resources for the knowledge-based economy. Editor Elsevier, 1997. ISBN 9780750697187.

Leontief, W. (1936): «Quantitative Input and Output Relations in the Economic Systems of the United States». The Review of Economic Statistics, 18(3), 105-125.

Leontief, W. (1941): «The Structure of American Economy, 1919-1929: An Empirical Application of Equilibrium Analysis», Harvard University Press.

Leontief, W. (1951): «The Structure of American Economy, 1919-1939». Oxford University Press, Nueva York.

Leontief, W. (1974): «Structure of the World Economy: Outline of a Simple Input-Output Formulation». American Economic Review 64, no.6 (December 1974) :823-34.

Leontief, W. (1986) «Input-Output Economics»; Oxford University Press: New York, 1986.

Leontief, W., Carter A., Petri P.A. (1977): «The Future of the World Economy.» New York: Oxford University Press.

Llano, C. (2004) «The Interregional Trade in the Context of a Multirregional Input-Output Model for Spain». *Estudios de economía aplicada* Vol. 22 - 3, 2 0 0 4. P Á G S . 539-576

Malhotra, Y. (1998) Knowledge Management, Knowledge Organizations & Knowledge Workers: A View from the Front Lines [WWW document]. URL: http://www.brint.com/interview/maeil.htm

Martí, ML., Puertas, R. y Fernández, J.I. (2009): «Metodología para el análisis de impacto portuario: Aplicación a los puertos de Gandía», Sagunto y Valencia, Fundación Valenciaport.

Puertas-Medina, R. , Martí-Selva, L.y Calafat-Marzal, C. (2012). «Tourist spending economic impact: low cost versus traditional companies». *Revista de economía mundial*, 32, 2012, 51-71. ISSN 1576-0162.

Sánchez-Rivero M. (2012*)*. «Quantitative analysis of the economic impact of competitiveness on international tourism destinations». *Revista de economía mundial*, 32, 2012, 103-125. ISSN 1576-0162.

Soza-Amigo, S. y Ramos-Carvajal, R. (2011*)* «The aggregation in the input-output model: a review from the perspective of the branches that do not join». *Revista de economía mundial*, 28, 2011, 247-276. ISSN 1576-0162.

BLOQUE VI

ENSEÑANZA, FORMACIÓN Y CONOCIMIENTO DE LAS FFAA

BOLOGNE PROCESS FOR A MUTUAL TRUST TOP-NOTCH EDUCATION

Antonio Martínez de Baños Carrillo
*Academia General Militar**
mdb@et.mde.es

Abstract

Our nations are facing numerous challenges within the new strategic security environment. There are new risks and threats that are interconnected and their level of danger is maximized by globalization. It is an obvious reality for present armies to join forces and collaborate in many different international missions. The Bologna declaration is suggested for the European armies to ensure comparability in the military and defense standards and quality of higher education in close conjunction with a shared understanding engendered through cooperative education based upon mutual trust in the NATO frame.

Keywords

Higher Education, academy, security, globalization, officership.

1. Introduction

Western countries are in constant evolution in defense and security affairs. Although the countries are responsible for their armies, a common route in education should be increasing in their educational programs. There are four parts that make sense to this essay which are within the frame of the Bologna Process to confluence to a shared NATO foundation: «The Security concept», «Technical, scientific and humanistic expertise», «Education in values and leadership» and «New technologies applied to the academic scope».

This paper is to provide the European Union and NATO countries with an academic route able to have an educational reference.

2. Educational pathways

Education is a very wide concept in the Bologne Process. I will try to hammer out and clarify all the necessary concepts so as to be more transparent and trail-blazing to better understand our educational pathways that will lead us straightforward to our bull's-eye —NATO mutual trust— to foster our international partnership.

The Charter of the United Nations determines that:

> The Parties to this Treaty reaffirm their faith in the purposes and principles of the Charter of the United Nations and their desire to live in peace with all peoples and all governments.

Based on this principle the focus of this piece of work will be the education in the armies to achieve peace.

Prior to the signing the Bologna declaration, the *Magna Charta Universitatum* was proposed by the University of Bologna in 1986; it was signed by 755 universities from 80 countries to celebrate the university traditions and encourage bonds amongst European universities. It also served as a universal inspiration open to universities throughout the world.

Afterwards the Bologna Process came up with the signing the Bologna declaration by Education Ministers from 29 european countries in 1999. It is a series of ministerial meetings and agreements between European countries designed to ensure comparability in the standards and quality of higher education qualifications. Through the Bologna Accords, the process created the European Higher Education Area (EHEA), meant to ensure more comparable, compatible and coherent systems of higher education in Europe with the Budapest-Vienna Declaration of March 2010.

The basic framework adopted is of three cycles of higher education qualifications. It was adopted by the ministers at their meeting in Bergen in 2005 and defines the qualifications in terms of learning outcomes. In describing the cycles the framework makes use of the European Credit Transfer and Accumulation System (ECTS):

Within the NATO frame, and based on these Bologna premises, two interesting points can be found at the manual of the year 2013: ALLIED JOINT DOCTRINE FOR CIVIL-MILITARY COOPERATION:

a) The importance of a shared understanding engendered through cooperative working, liaison, education and a common language, and
b) The value of collaborative working based upon mutual trust.

With this regard, the Spanish National Defense Directive is very clear by pointing out that Spain must have good and reliable allies, and must also behave as a loyal and supportive actor within the collective security environment.

One of the main Spanish objectives with our allies is to promote the multinational cadets' education and training, by improving cooperative exchanging programs, sharing knowledge, and debating opinions with regard to military academic development. The idea is to build a network of international partners in order to exchange programs and initiatives related to military education, also in values. I am sure this will also be a key aspect in order to study the interoperability between our education models and to explore the possibility for cadet exchanges in the future.

To this regard the proposed common NATO countries program could be split up in four sections:

2.1. *The first section to be fleshed out is known as «Security» in our Academies*

The intensification and effects of the globalization concept have contributed to the proliferation and spread of unbounded threats in a relatively short time. This has been greatly facilitated by both a remarkable communications development and an easy access to information.

Without neglecting traditional hazards ultimately resurfacing, new risks and new players are showing up such as cyber threats and cyber espionage, organized crime, drug trafficking and narco-terrorism, immigration, energy vulnerability, as well as heavy dependence on services and essential infrastructures. Of course, the constant growth of terrorism due to religious causes, not only limited to the various jihadist groups, but also highlighted by the continuous appearance of isolated threats such as the famous «lone wolves». To this regard terrorists consider that every person is the frontier of a country. In such a case, a terrorist attack against a person is against the country.

However, the novelty of these new threats is its trans-nationalization, world-wide nature, interconnections and magnitude. These factors make the impact of their actions look greatly enhanced and the difficulty of coping with such perils is growing exponentially.

2.2. *The second section will lead us to «Technical, scientific and humanistic expertise»*

In Spain, following the example of other friendly countries, the military syllabus has recently been integrated into the general educational system. Thus, our young officers can obtain a university degree, in our case the Industrial Management Engineering. It implies to provide them with the technical, scientific and humanistic basis. These skills will allow them to acquire the analysis and synthesis capacity, improving at the same time, their capabilities for human team conduction and technological process management. The humanistic, scientific and technical areas are combined accordingly to train our officer-cadets on a comprehensive formation.

The Academia General Militar officer-cadets, coming from the university public entrance exam of the general education system, receive high education in the first four years thanks to the creation of the University Center for Defense, an institution belonging to the Ministry of Defense but under the standards and rules established by the University of Zaragoza through institutional agreements.

However, the new officership training program is not only based on the knowledge acquainted at the University Center for Defense but also in the military formation focused more consistently on the Academia General Militar, taking into consideration present and varied conflicts or those new ones to be foreseen. Together with the specific military subjects, a plan to empower the Values and Leadership permits the cadets to get their knowledge and to be able to apply their moral duties, carrying out their obligations with integrity and honorability.

In their last fifth year, the cadets complete their military education at their respective arms academies; but in this case, following a strictly military syllabus.

The Internal Promotion has been also boosted to enable Non-Commissioned Officers and enlisted personnel, with a scien-

tific university degree, to enter our Academy. In order to become officers, they need to study a 2-year military program, the first one at the Academia General Militar and the second at the arms academies. This model is also offered to other armies.

2.3. *The third section is about «Education in values and leadership»*

Leadership, moral and military values are the cornerstone in the training of our Officers. Leadership, as a primary pillar, is based on Ethics. The Ethics of an organization will be reflected in its values which are concepts that individuals either in teams or isolated consider being the ideal way to behave. Values that have to be put into practice in the military daily routine and achieved by means of a socialization process.

The values consider are: the values enshrined in the Spanish Constitution; the military education own values; those military values included in the Royal Ordinances; ethical principles in the behavioral rules shown in the Cadet Decalogue of the Spanish Military Academies, anthems, etc., as well as the precepts gathered in the Land Forces Doctrine, NATO included. Taking into consideration these factors, some general values were selected and grouped in three which encompass all the other ones: Patriotism, Honor and Exemplariness. The demand of the new designed Plan of Studies inserted in the Bologna Process in a NATO environment, forces us to take full advantage of the military values and leadership training based on role-modeling.

A Leadership Plan that organizes and prioritizes many of the traditional activities has been designed. This new Leadership Plan has as objective for the Army members to internalize, mature and put into action the proposed military values. Its lines of action are briefly as follows:

Training Military Values whose objective is that the Army members assume the essence of military the profession.

A Tutorial Action Plan has the objective of individual guidance by both tutor-teachers and the Departments of Educational Guidance.

Finally, the Plan for Reading Development and Military Cultural Education is an exhortation for reading and / or movie viewing military topics.

2.4. *The fourth and last section deals with «New technologies applied to the academic scope»*

The new information and communication technologies in our societies have led to a profound change in economy, politics, military, society and culture, which has deeply changed the wealth concept, the social interaction, the identification of identities and the knowledge sharing.

It is also clear that our Armed Forces are increasingly using sophisticated and complex armament and means which are more difficult to maintain and operate. They demand users with a higher level of technological knowledge.

However, this training is exclusively theoretical and in our formation, knowledge is not enough for us. Our cadets, future officers, need to learn the 'knowhow'. The use of new technologies in teaching has re-known advantages since they facilitate the most basic instruction such as hand weapons and shoulder weapons shooting, the training in combat simulations from team and squad unit to brigade-sized units conduction in complex constructive simulators. The Academia General Militar counts on a simulation room of Spanish origin for small weapons, the VICTRIX that is highly used by cadets.

The economic cost of training combat and transportation of military vehicles has decreased by using the simulator. Although virtual skills have substituted for real practices, this training is still necessary.

Conclusión

To conclude I would like to sum up my words. Warfare remains fundamentally a human contest and a clash of wills, that´s why the human element will always be our most valuable and agile resource. New complex and demanding scenarios require well trained and equipped units. These scenarios require outstanding leaders able to make quick and sound decisions that can have impact not only at tactical level, but also at operational or strategic levels.

To achieve these leaders we must provide our cadets with a high level training in technical, scientific, physical and humanistic aspects. However, the most important pillar of our leaders' comprehensive education will always be the education in values.

In this complex environment the best way to face issues affecting peace, security and international stability is through multinational cooperation. That is why our forces are now working together on the field in a lot of multinational operations all over the world, and that is why we are here today sharing knowledge and expertise, and providing the basis for future cooperation and exchange on subjects of mutual interest.

The Academia General Militar has the responsibility for getting the goals to have the best and the most appropriate brand new officers able to cope with the NATO missions.

Eventually, the aim is to train vocational officers, instilled with moral values, able to lead their men and women, and with the professional competence which guarantees the successful accomplishment of any mission they might be assigned.

Acknowledgement

To the Commandant of the Academia General Militar.

References

Chan I-Harn, A. La gama completa del modelo de liderazgo y su aplicación a las Fuerzas Armadas de Singapur. [s. n.] [En línea] [24/10/10] http://www.mindef.gov.sg/safti/pointer/back/journals/2001/Vol27_3/5.htm.

Ibrahim, F. Imam; Wnek, J. eds. *Proceedings of the First International Workshop on Intelligent Adaptive Systems (IAS-95)*, 1995, pp. 38-51, Florida. [En línea] [20/11/10] http://www.google.es/search?hl=es&q=Constructive+Induction-based+Learning+Agents&btnG=Buscar&aq=f&aqi=&aql=&oq=&gs_rfai.

España. Ministerio de Defensa. International Isodoma Meeting Conclusion. *Leadership*. 2015, Academia General Militar, Zaragoza.

España. Ministerio de Defensa. ME7-007, Mando de adiestramiento y doctrina. *Manual de enseñanza. El mando como líder. Ejército de tierra*, 1998, Granada.

Marcano Lárez, B. «Estimulación emocional de los videojuegos: efectos en el aprendizaje». En García Carrasco, Joaquín (Coord.) *Estudio de los comportamientos emocionales en la red* [monográfico en línea]. Revista electrónica, Teoría de la Educación: Educación y Cultura en la sociedad de la información. Vol. 7, 2006, nº 2. Universidad de Salamanca. [En línea] [13/12/10] http://www.usal.es/~teoriaeducacion/rev_numero_07_02/n7_02_beatriz_marcano.pdf .

España. Ministerio de Defensa. North Atlantic Treaty Organization. *Allied Joint Doctrine For Civil-Military Cooperation,* (2013), Edition A

Version 1, Published by the Nato Standardization Agency (NSA). Brussels.

Pérez Cañado, M. L. ed. *Competency-based Language Teaching in Higher Education*, 2013, Amsterdam: *Springer*.

Pérez Cañado, M. L. «The Transformation of Teacher and Student Roles in the European Higher Education Area». *Journal of Language Teaching and Research*, Vol. 1, March 2010, núm. 2, pp. 103-110, Finland.

España. Ministerio de Defensa, Reales Ordenanzas para las Fuerzas Armadas, (2009). [En línea] [19/09/10] http.//www.mde.es.

Ricks S. F. *Distributed Learning: A leadership Multiplier*. Army Management Staff College-Perspectives on leadership, 2009, pp. 97-105. Leavenworth.

Stringer, K. «¿Cómo Educar al Soldado Estratégico? Un cambio de paradigma». Military Review. (Enero-Febrero 2010), Leavenworth. [En línea] [09/11/10] http://usacac.army.mil/CAC2/MilitaryReview/Archives/Spanish/MilitaryReview_20100228_art007SPA.pdf.

Italia. The Bologna Declaration (19th June, 1999). Joint declaration of the European Ministers of Education. [En línea] [10/10/13] http://www.eees.es/pdf/Declaracion_Bolonia.pdf.

Estados Unidos. US. ARMY FM 3-0 OPERATIONS (2001). [En línea] [04/12/10] http://www.globalsecurity.org/military/library/policy/army/fm/3-0/ch2.htm.

Estados Unidos. US Army, Fm 7-0 Training For Full Spectrum Operations (2008). [En línea] [06/11/10] http://usacac.army.mil/cac2/Repository/FM70/FM7-0.pdf.

Estados Unidos. US Army, FM 100-5, (1993), *Operations*. Department Of The Army United States Marine Corps.

Estados Unidos. US Army, FM 101-5-1, MCRP 5-2A, (2014) *Operational Terms And Graphics Headquarters*, Department Of The Army United States Marine Corps. [En línea] [03/10/16] http://www1.udel.edu/armyrotc/current_cadets/cadet_resources/manuals_regulations_files/FM%201-02%20-%20Operational%20Terms%20&%20Graphics.pdf.

Valero-García, M.; Navarro, J. «Diez metáforas para entender (y explicar) el nuevo modelo docente para el EEES». Revista d'innovació educativa, No. 1, 2008, Universitat de València. [en línea] [14/11/10]) http://bioinfo.uib.es/~joemiro/semdoc/diezMetaforas.pdf.

PROYECTO SOBRE GESTIÓN DEL CONOCIMIENTO EN LA DIRECCIÓN DE INVESTIGACIÓN, DOCTRINA, ORGÁNICA Y MATERIALES (DIDOM)

Manuel Sáiz-Pardo Lizaso

Dirección de Investigación, Doctrina, Orgánica y Materiales (DIDOM) del Mando de Adiestramiento y Doctrina (MADOC), Ejército de Tierra (ET), Ministerio de Defensa

Resumen

Los sistemas de gestión del conocimiento mejoran la eficiencia de las organizaciones, obteniéndose una ventaja competitiva.
La mejora de la gestión del conocimiento implica acciones impulsadas por el mando, dedicando recursos humanos, materiales y procedimientos. Todo ello atendiendo a principios de eficiencia, economía de medios y adaptabilidad a los requisitos.
La DIDOM desarrolla un proyecto con la UGR (con la colaboración del CEMIX) para sentar las bases (recomendaciones, buenas prácticas) para definir un concepto de gestión del conocimiento, un plan de implantación y su puesta en práctica en la Dirección, así como la posible extrapolación de estos elementos a otras Direcciones del MADOC y del ET.

Palabras clave

Sistema de gestión del conocimiento, organizaciones, eficiencia.

1. Prólogo

En este trabajo se analizan aspectos generales sobre la base conceptual en que se ha de basar la Gestión del Conocimiento (GC) en el Ejército de Tierra, exponiendo también la metodología y los principales resultados del proyecto de Gestión del Conocimiento que se lleva a cabo en la DIDOM.

El creciente desarrollo de las tecnologías de la información y las comunicaciones y la importancia de adaptarse a la aceleración del ciclo de innovación tecnológica, está convirtiendo al conocimiento en el activo más importante de una organización.

La continua innovación en este campo podría ocasionar que el Ejército quedara desfasado en sus posibilidades de llevar a cabo sus misiones fundamentales, o bien, siguiera haciéndolo pero de forma poco eficaz.
Aceptado que el conocimiento aporta una de las mayores ventajas competitivas, es necesario que el Ejército realice un esfuerzo significativo en mejorar la eficiencia del sistema de GC de la organización, en particular:

—creando una cultura del conocimiento;
—dotándose de las herramientas adecuadas de gestión de la información y del conocimiento;
—creando un mapa de conocimiento estructurado en áreas;
—articulando mecanismos de generación de conocimiento (foros de expertos, etc.);
—estableciendo canales de difusión del conocimiento;
—nombrando gestores de un sistema de GC y definiendo sus responsabilidades, etc.

En este trabajo se pretende dar un enfoque generalista y conceptual, y presentar los resultados del proyecto de gestión del conocimiento en marcha en la DIDOM. Esta comunicación se complementa con otro proyecto también presentado en este congreso sobre «Visión, implementación y explotación del motor de búsqueda de contenidos web en redes Intranet. El caso de la Intranet de Defensa» (Ruiz Carrasco, 2016).

2. Introducción

a) Aspectos conceptuales de la gestión del conocimiento

Los **datos** son observaciones sencillas de fácil estructuración, cuantificables y transferibles, que se pueden capturar con máquinas. La información se obtiene a partir del análisis y del consenso de los datos en su contexto. Aplicado a una organización, si se añaden experiencia y reflexión se obtiene conocimiento. Así, se puede definir que el conocimiento es la información combinada con la experiencia, el contexto, la interpretación y la reflexión (Arredondo y Sáiz-Pardo, 2014).

La frontera entre dato, información y conocimiento es difusa; a medida que aumentamos el grado de participación humana

añadimos valor y dificultamos la estructuración, la captura por máquinas, la transferencia y la cuantificación del mismo.

El conocimiento se origina en la mente del individuo (conocimiento tácito), el cual puede escribir lo que sabe en un documento (conocimiento explícito), que se guarda en un repositorio. Otras personas pueden leer ese documento y mejorarlo. El autor inicial ve los cambios y los asimila, cerrando así el «ciclo del conocimiento»[1].

También se puede reunir un grupo de expertos y hablar sobre un tema, sin mediar documentos, elevándose el valor del conocimiento tácito de todos ellos. De esta manera, el valor añadido se genera más rápidamente y con menor ambigüedad. Los grupos de expertos suponen la forma más eficiente para generar el mejor conocimiento explícito organizacional. Después, el resultado debe ser difundido a los interesados y puesto en un repositorio fácilmente accesible.

Aunque todas las personas y organizaciones, de alguna manera, siempre han gestionado el conocimiento, el desarrollo de las tecnologías de la información y las comunicaciones exige una reflexión y adaptación para el cumplimiento eficiente de los objetivos. De hecho, la organización que no gestione su conocimiento de una forma eficiente perderá competitividad, decaerá su eficacia y quedara desfasada. Lo contrario redundará de forma transversal en el beneficio de los demás procesos fundamentales de la organización.

La finalidad de la GC es poner el conocimiento pertinente a disposición de los responsables en la toma de decisiones, analistas o investigadores. Y esto implica gestionar de manera eficiente los procesos de generación, almacenamiento y difusión del conocimiento.

Por tanto, la GC busca mejorar de forma sistemática el rendimiento del activo intelectual, en este caso de la DIDOM, aprovechando la experiencia y conocimiento tácito de las personas, grupos de trabajo y unidades, poniéndolo a disposición de todos los usuarios interesados.

1. Distinguimos el conocimiento tácito y el explícito, como lo hacen también autores como Nonaka y Takeuchi (Nonaka y Takeuchi, 1995).

b) *Antecedentes del proyecto de Gestión del conocimiento en la DIDOM*

El Ejército creó en 2013 la Sección de Gestión del Conocimiento (SEGECON) de la Dirección de Investigación, Doctrina, Orgánica y Materiales (DIDOM) del MADOC (DIDOM, 2013), con la finalidad de reunificar y buscar la sinergia de todas las herramientas existentes en la Dirección relacionadas con la gestión del conocimiento: Milit@rpedia, Biblioteca Virtual, Servicio de Documentación, correo electrónico múltiple selectivo, grupos de trabajo en red, entre otras.

Tras este importante hito, se plantea la necesidad de definir un concepto de gestión del conocimiento en el Ejército y de un plan para su implantación, entre otras propuestas.

Para apoyar esta necesidad, en marzo de 2105 el Centro Mixto UGR-MADOC aprueba el proyecto de investigación (PIN) «Estudio piloto de Gestión de Conocimiento en la DIDOM», con la colaboración de la empresa consultora Zahareña Conocimiento[2] S.L (http://www.zahareña.com), que pretende sentar las bases (recomendaciones, buenas prácticas) para definir un concepto de GC, un plan estratégico de implantación de un sistema de GC y su puesta en práctica, en plan experimental, en la DIDOM y su posible extrapolación a otras Direcciones del MADOC y del ET. Contempla y supera la auditoría de la información, estudia los procesos de control y diagnóstico global del conocimiento, que permitirán reducir información irrelevante, evitar duplicidades y fomentar el intercambio y la participación.

El momento actual parece adecuado para avanzar en el sistema de GC en la DIDOM. Para ello es necesario:

—Avanzar en el campo de la GC estableciendo un punto de situación interno en colaboración con el mundo académico y el empresarial, por supuesto aprovechando el desarrollo del Proyecto del CEMIX.

2. Zahareña Conocimiento S.L (http://www.zahareña.com) es una empresa consultora especializada en la gestión del conocimiento implantando sistemas en organizaciones, siendo clave su participación en el proyecto al servir de nexo entre el equipo investigador y la experiencia práctica. Se subcontrató a dicha empresa para la elaboración del trabajo de campo y recopilación de la información necesaria para su análisis, y en la elaboración del informe principal.

—Definir un concepto de GC en la DIDOM para el ET, evitando disfunciones y desviaciones en la interpretación e implementación de la GC.
—Estudiar el modelo interno de GC como un primer paso.
—Difundir internamente las herramientas de GC del MADOC.
—Impulsar y potenciar los grupos de trabajo de analistas (la mejor herramienta para la creación de conocimiento), potenciando el empleo de las herramientas disponibles (SharePoint, Servicio de documentación, Biblioteca Virtual, Milit@rpedia, etc.).
—Estudiar la forma de utilizar con eficiencia el conjunto de herramientas disponibles, acabando su desarrollo y continuando con la investigación de otras.

3. El proyecto de investigación sobre gestión del conocimiento

a) *Justificación del proyecto del CEMIX*

La información que posee la DIDOM (en papel, digital o en la mente de su capital humano) puede ser transformada en conocimiento y aplicada para la consecución de objetivos estratégicos.

Para ello se necesitan identificar los recursos que permiten hacer esa información accesible a las personas, que convertirán en conocimiento toda aquella información identificada; el modo en que se va a dar uso a esa información en la consecución de objetivos; a las personas que utilizarán la información; las herramientas necesarias para instrumentalizarla; y los criterios que se usarán para evaluar costes y valor de la información.

El proyecto trata de poner en valor el conocimiento organizacional que ya se posee así como la forma en que se crea, almacena, usa, mantiene, transfiere, etc., y proporcionar orientaciones y buenas prácticas para hacer efectivo el sistema de gestión del conocimiento de la DIDOM.

El identificar y fortalecer el conocimiento que se genera permite:

—Realizar cambios y modificaciones con un menor número de errores, perdiendo menos recursos en los procesos;
—Mejorar los procesos de comunicación a partir de los marco de referencia compartidos entre las secciones de la DIDOM;

—Construir nuevos espacios de participación, de productos y servicios en las secciones;
—Mejorar la forma en que se hacen las cosas;
—Manejar eficientemente un gran volumen de datos e información;
—Generar nuevos conocimientos sobre la realidad en que se actúa.

Entre las distintas operaciones, necesarias para generar conocimiento, destacamos:

—la comparación de datos y nueva información, con las categorías ya almacenadas;
—la identificación de consecuencias por medio de tramos basados en la experiencia y conocimientos adquiridos en otros contextos;
—la nueva conectividad que se le ha dado a los datos y a la información;
—las diversas conexiones que se visualizan entre el nuevo conocimiento y los que se encuentran en repositorios;
—la opinión que nos dan otros sobre los datos y la información que se maneja.

La velocidad en que se realicen este tipo de operaciones determinará la eficiencia del sistema en responder a las demandas de conocimiento.

Este proyecto pretende ser el primer paso, en el diseño del mapa de ruta, que permita reducir el riesgo en la implementación de procesos de Gestión del Conocimiento en la DIDOM y que facilite la identificación de los instrumentos que capturan, estructuran y difunden conocimiento.

Será el instrumento que facilite, a las personas que producen contenidos y conocimiento, el que puedan ponerlo en común desde que éste es creado, plasmado en un documento físico u electrónico, para su valoración y traspaso a un archivo corporativo. Y que las necesidades de información en la organización sean satisfechas de manera precisa permitiendo búsquedas eficaces, efectivas y pertinentes.

4. Investigación

a) *Metodología*

A partir de 3 reuniones de trabajo con la Sección Gestión del Conocimiento de la SUBDIVA para la recogida de información del funcionamiento de la DIDOM[3], se identificaron las principales variables sobre las que trabajar para la recogida de información sensible para el proyecto.

Estas reuniones sirvieron para elaborar un cuestionario de recogida de información con el objetivo de:

—Identificar el conocimiento que se trabaja, dónde se encuentra, si está clasificado, quién lo genera, y qué se espera de él.
—Identificar las fuentes de conocimiento más utilizadas por la DIDOM.

Este cuestionario se estructuró según 3 campos para la recogida de información sobre la que iniciar la construcción del mapa de conocimiento:

—Primera: Conocimiento individual: adquisición, uso, valoración y creación de procedimientos para su aplicación.
—Segunda: Fuentes y limitaciones, recursos propios y de la organización, sistemas de colaboración/compartición y autoría del conocimiento, y documentación gris (aquella que es generada a lo largo de la vida de cualquier proyecto o trabajo).
—Tercera: Producto final y su alcance, canales de difusión y utilidad de las herramientas de la DIDOM para la gestión de conocimiento (Milit@rpedia, Biblioteca Virtual, Buscador, correo electrónico de multidifusión, etc.).

Identificados los mandos colaboradores con el proyecto, se enviaron los cuestionarios por correo electrónico a una muestra

3. La Dirección de Investigación, Doctrina, Orgánica y Materiales (DIDOM) se organiza en Secretaría Técnica (SETEC); Subdirección de Investigación, Lecciones Aprendidas y Gestión del Conocimiento (SUBDIVA); Subdirección de Doctrina, Orgánica y Materiales (SUBDOM); y diversas Jefaturas de Adiestramiento y Doctrina (JAD).

amplia de 47 analistas, identificados por la Sección de Gestión del Conocimiento. Los cuestionarios aportan al estudio perspectivas sensibles de análisis desde todas las secciones y jefaturas de la DIDOM, según la siguiente representación del número de cuestionarios:

—Sc. DDOCTRINA: 8
—Sc. LLAA: 4
—Sc. INVESTIGACIÓN: 4
—Sc. MATERIALES: 3
—Jefaturas de Adiestramiento y Doctrina (JAD): 22
—Total (incorporando en esta apartado también el personal de SETEC, Sc. ORGÁNICA y Sc. GESTIÓN DEL CONOCIMIENTO): 47

La recepción de cuestionarios finalizó el 3 de septiembre de 2015.

Tras el primer análisis de las respuestas obtenidas se elaboró un plan de entrevistas en profundidad que, siempre partiendo de datos clave volcados en el cuestionario, permitieron profundizar en los indicadores que facilitaran la identificación de la matriz del conocimiento necesario, utilizado y generado en la DIDOM, y las líneas de actuación prioritarias para la elaboración del mapa de conocimiento y sus flujos entre su capital intelectual.

Las entrevistas las realizaron un total de 14 profesionales (1 mando de SETEC, 4 de SUBDIVA, 5 de SUBDOM, y 4 de las JAD) que, partiendo de sus respuestas al cuestionario, ampliaron y desarrollaron información cualitativa, mediante la metodología de entrevista, que ha sido definitiva para la articulación de las variables del mapa de conocimiento del MADOC.

Las entrevistas iniciaron el 3 de noviembre y finalizaron el 17 de diciembre de 2015.

Este análisis, por la naturaleza de la organización y por ser la principal fuente de información para este proyecto, se ha prolongado hasta el mes 9 del proyecto, pero permite dibujar las principales líneas de actuación de las siguientes fases, el diseño del mapa del conocimiento y sus flujos entre su capital intelectual (Humano, Estructural, Relacional) al proporcionar información sobre:

—Los recursos de información y conocimiento necesarios y utilizados;

—Los procesos organizativos en los que se genera conocimiento;
—Los canales de coordinación que existen entre las distintas estructuras que generan, almacenan, o distribuyen conocimiento;
—Los recursos que permiten convertir información en conocimiento;
—El análisis del modo en que se usa la información para la consecución de objetivos estratégicos;
—La selección de herramientas;
—Y la definición de criterios para evaluar costes y valor de la información.

b) *Análisis de los Procesos de Creación del Conocimiento*

i. *Adquisición del conocimiento: experiencia y formación para el puesto de trabajo*

El propósito de este punto de análisis es valorar el peso que se le da a la experiencia y formación como generadora de conocimiento transferible al puesto de trabajo del analista, que se ha adquirido tanto dentro del Ejército como fuera de él. Cómo se ve en el gráfico el peso de la experiencia es compartido por todas las áreas analizadas, confluyendo la valoración más alta en la experiencia en destino.

En las entrevistas se ha evidenciado cómo se producen los procesos de aprendizaje. El aprendizaje es individual y no está estructurado, la adquisición de competencias es autodidacta y al tiene los siguientes ingredientes: conocimiento, habilidades, destrezas, capacidad de toma de decisión basada en la experiencia. Cuando se produce un nuevo relevo el proceso comienza desde el principio, y se inicia un nuevo ciclo en el siguiente destino. Por los cambios de destino, la especialización se hace difícil de mantener en el tiempo.

Con respecto a la formación destaca la alta valoración que se da a la formación especializada en metodología de la investigación, y la importancia de documentar y justificar las fuentes de conocimiento de la que se extraen los datos e informaciones a las que se hace referencia en los documentos.

Las competencias lingüísticas, sobre todo en inglés, aunque también el francés, son muy valoradas por las personas que las tienen y aquellas que las necesitan para poder trabajar diariamente

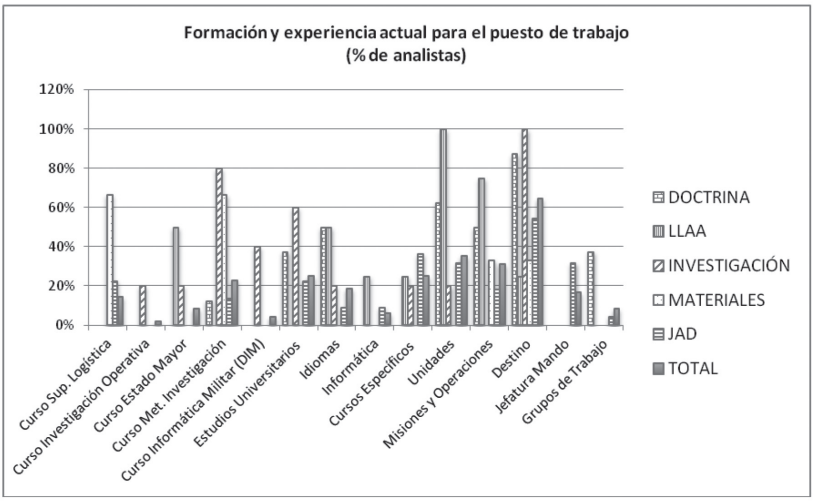
con documentación de referencia en esos idiomas, cada día más extensa. Además de su dominio en reuniones internacionales y participación en grupos OTAN.

Se han identificado formaciones de especialización en gestión de conocimiento, lecciones aprendidas y estrategias logísticas, estas últimas compartidas en valoración por las JAD.

Hay una alta sensibilidad hacia la formación y la adquisición de competencias técnicas y trasversales en todas las áreas estudiadas. En resumen, se valoran:

—Experiencia en el destino (65% de los analistas han valorado este punto)
—Experiencia en otros destinos, unidades (35%)
—Experiencias en misiones y operaciones (31%)
—Curso de Metodología de la Investigación (23%)
—Cursos de especialización (25%): Curso Superior de Logística (15%), Diploma de Estado Mayor (8%), Diploma de Informática Militar (4%), Curso de Investigación Operativa (2%), curso de Gestión del Conocimiento del INAP, lecciones aprendidas, estrategias logísticas
—Estudios universitarios (25%)
—Idiomas (inglés, francés) (19%)
—Jefatura, mando (17%)
—Experiencia en grupos de trabajo (8%)
—Conocimientos en informática (6%)

En la información representada en el gráfico de abajo, el eje vertical mide el porcentaje de analistas que han considerado cada respuesta. El «Total» es una media aritmética de las respuestas de todos los analistas. Se han agrupado respuestas similares, dado que no se habían predefinido los elementos a valorar, dejando su propuesta libremente a los analistas. Dado que es una aproximación cualitativa, el gráfico se ha incluido para ilustrar la explicación, pero sin ánimo de ser muy exhaustivo, por lo que debe interpretarse con la debida precaución.



ii. *Formación y experiencia ideal para el puesto de trabajo*

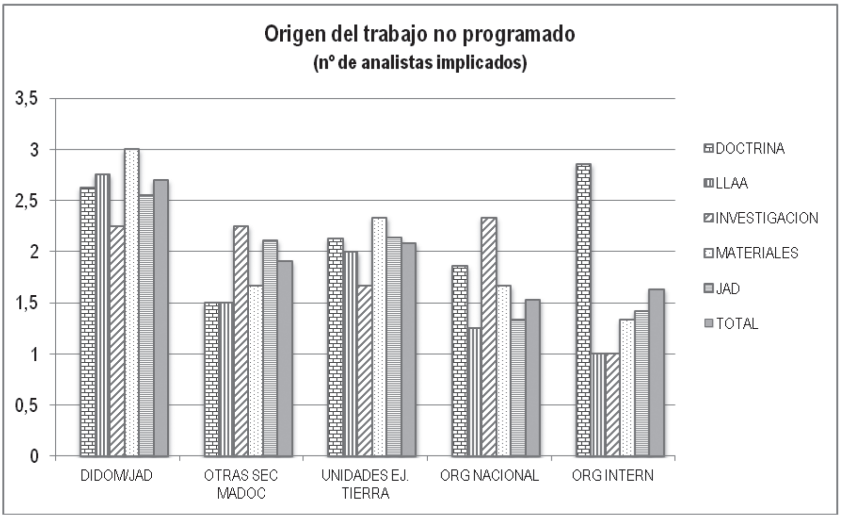
Por la naturaleza de las funciones desarrolladas por los analistas en los distintos destinos en los que están adscritos, se les ha pedido que identifiquen qué tipo de competencias sería necesario requerir a sus futuros relevos para garantizar que la rotación en los puestos de trabajo fuese lo más flexible y efectiva posible.

De este análisis, sobre todo, destacan la valoración de la experiencia profesional en destinos y en el MADOC, las competencias lingüísticas, la formación especializada en metodología de la investigación, y las misiones y operaciones y grupos de trabajo internacionales, aparte de los aspectos que ya se habían reseñado en el apartado anterior (cursos específicos, etc.), y que completarían la lista de requisitos.

iii. *Origen del trabajo no programado*

Preguntamos por la carga en tiempo de tareas que, no estando programadas, acometen los analistas.

Analizamos las interactuaciones y flujos de colaboración entre áreas, tras preguntar a los analistas sobre el origen del trabajo no programado que realizan y el volumen que supone. Como se puede ver en el gráfico todas las secciones interactúan, en mayor o menor medida, con las 5 estructuras identificadas.



iv. *Procedimientos de producción de documentos*

Se ha pedido a los analistas que describan brevemente el procedimiento de elaboración de los documentos que producen. En este punto se han analizado las respuestas de cada sección individualmente. La búsqueda y análisis de información y la redacción de documentos son aspectos que están altamente valorados en todas las secciones.

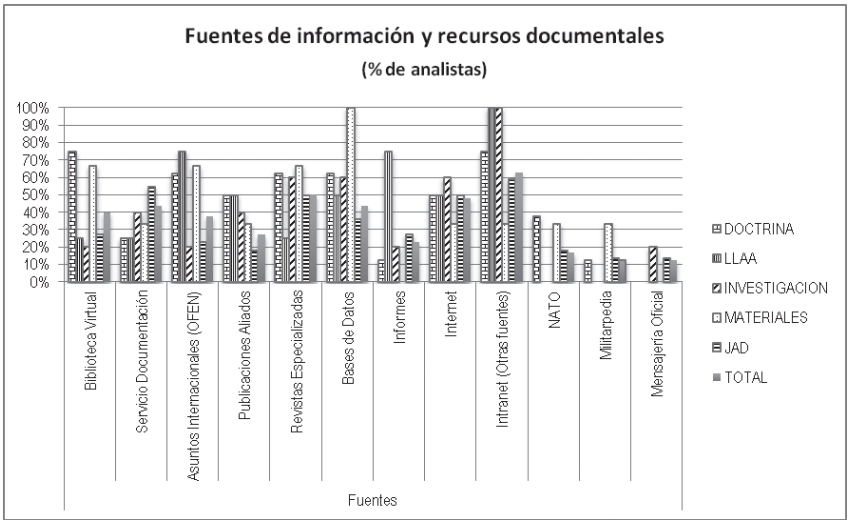
Cada analista, aparte de su propia experiencia, tiene identificadas unas fuentes explícitas individuales (informes personales, documentos, artículos, referencias, casos en los que ha participado anteriormente, etc.) que están almacenadas en su ordenador (con su propia metodología de almacenaje y recuperación) y de los que se abastecen a nivel individual para documentarse, investigar y analizar la información sobre la que construir conocimiento nuevo. Esta fuente de recursos la reconocen como conocimiento experto propio, de hecho todos ellos guardan con celo profesional el contenido de sus ordenadores. Pero no como fuente de recursos compartida, al carecer de metodología estratégica para la compartición de espacios de trabajo y documentación de referencia seleccionada y validada por cada uno de ellos en sus distintos trabajos de análisis y producción documental. En general, tampoco existe un repositorio de conocimiento experto corporativo.

Como actividades identificadas por los analistas para la producción documental están: identificación de la necesidad, búsqueda de información, análisis, grupo de trabajo, reflexión y experiencia, redacción, recogida de propuestas, supervisión y aprobación y difusión.

v. *Fuentes de información*

Se ha pedido a los analistas que enumeren las fuentes de información que utilizan para su trabajo (revistas, repositorios, bases de datos, páginas web, PMET, publicaciones de países aliados, etc.).

En el gráfico se han identificado las fuentes más utilizadas por los analistas, señalándose en el eje vertical el porcentaje de analistas que han considerado cada respuesta.



Destacar en este punto, extraído de las entrevistas en profundidad, las limitaciones que los analistas tienen en sus puestos de trabajo para acceder a informaciones de referencia para la elaboración de sus trabajos documentales.

La mayor parte de la adquisición de información se obtiene a través de la Biblioteca Virtual, el Servicio de Documentación e Internet, siendo este último un recurso que todos valoran como necesario para el trabajo diario, pero por las limitaciones de

seguridad de la Intranet hacen que acceden a Internet fuera de horario laboral desde sus domicilios, al poder trabajar con ella de forma más efectiva, con mejor acceso y rentabilidad de tiempos y eficacia.

Este dato llama también la atención sobre la extensión de la jornada laboral de los analistas, que además de las horas de trabajo en sus puestos, suman las que desarrollan fuera de horario laboral, siempre para alcanzar los objetivos de los que son responsables.

Por otra parte debido a la gran cantidad de documentación que periódicamente se envía a través del correo electrónico corporativo y Mesincet, están saturados de información, infoxificados, y almacenan los documentos recibidos hasta poder encontrar el «tiempo» necesario para poder valorarlos. El envío se hace de forma masiva con documentación adjunta. Los analistas recomiendan que se haga una breve descripción del contenido enviado y se motive el uso de documentación aportada, y cómo esta puede ayudar y enriquecer el trabajo que desarrolla el analista.

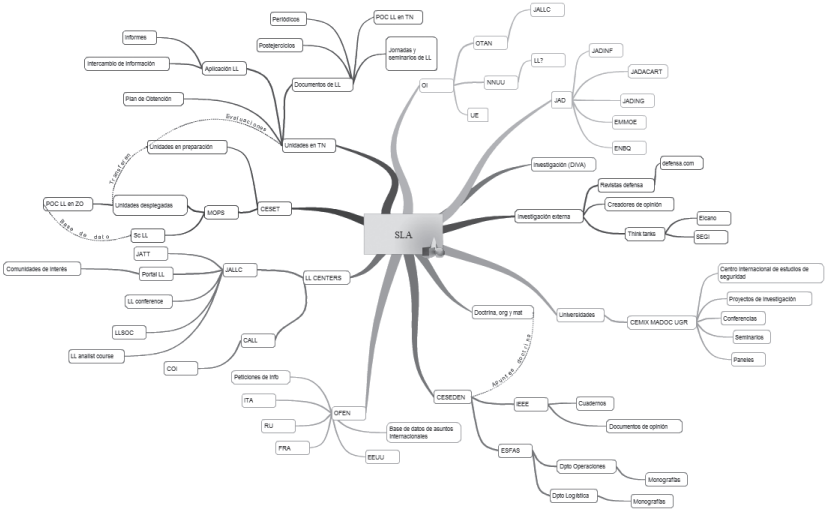
En la DIDOM existen tantas bibliotecas virtuales como puestos de analistas hay. Todos almacenan en sus discos duros la información que se les envía, buscan, capturan, elaboran y procesan. Existe recelo a perder información de valor documental para su futura utilización, y se almacena en cada ordenador siguiendo metodologías distintas en función del analista: se archivan los documentos o bien por carpetas en función de áreas de interés o conocimiento y en ellas se crean subcarpetas por fechas, o al contrario. La nomenclatura difiere en cada caso, unos por años-mes-día, otros por día-mes-año, sección-tema-doc, etc.

Con una metodología de organización documental compartida en un único repositorio se facilitaría no sólo el acceso a información de calidad y validez, sino que se reducirían espacios tanto en el servidor como en los propios ordenadores de los analistas que a la fecha los tienen saturados de información, muchos de ellos en históricos sin identificar o clasificar.

Se deben jerarquizar las fuentes de información y temas validados para su reutilización del conocimiento.

Un ejemplo de cómo cada analista estructura de forma individual sus fuentes documentales y recursos de para la adquisición de información, es el mapa que se aporta en uno de los cuestionarios «El siguiente mapa ofrece una idea de la diversidad de

fuentes a las que habitualmente es necesario acudir para elaborar algunos de los documentos que se elaboran en la Sección de Lecciones Aprendidas de DIDOM».



vi. *Limitaciones de acceso a la información*

Se ha preguntado a los analistas que enumeren las limitaciones que encuentran respecto a las fuentes de información que utilizan o les gustaría utilizar.

Entre los indicadores volcados en los cuestionarios destacar la limitación para acceder a información clasificada. En unos casos por el tiempo que se necesita invertir para poder llegar a ella, otros por desconocimiento del proceso a seguir para su acceso, y otros por la limitación de los puestos que tiene habilitado el acceso a estas fuentes. Hacen referencia a los permisos para acceder a información clasificada, a que, en ocasiones, es más fácil acceder a documentación desde Internet que desde Intranet

También aluden a la imposibilidad de poder acceder a herramientas de Intranet desde Internet.

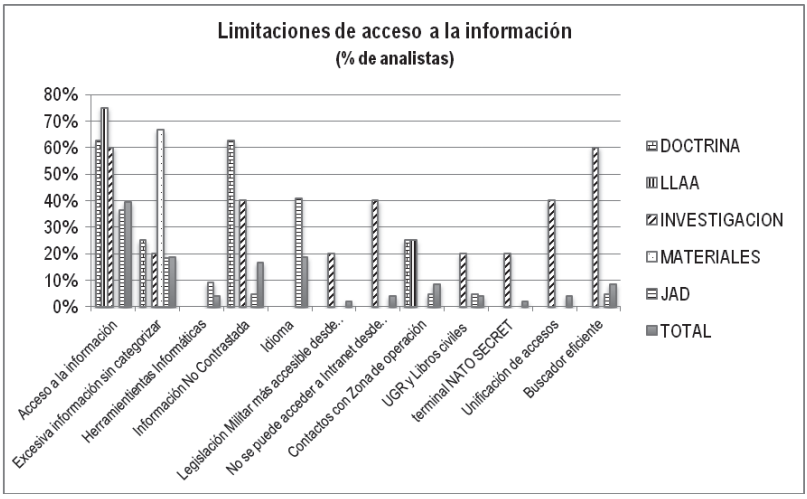
Le sigue, en valoración de dificultad, el idioma, es decir, se necesitan competencias lingüísticas avanzadas, principalmente en inglés, para poder trabajar con documentación de referencia. Cada vez son más los documentos en inglés a los que se recurre.

El desconocimiento de todas las fuentes documentales a las que recurrir para buscar información, de manera ágil y en fun-

ción de necesidades de estudio e investigación, también limita el trabajo de los analistas, haciendo referencia a esta dificultad como el «no saber dónde buscar».

El acceso a los profesionales que están en zona de operaciones, saber quiénes son, que misión están desarrollando, como poder acudir a ellos como fuente de información, también destaca en las limitaciones señaladas.

Igualan en puntuación los hitos relacionados con la lentitud de los procesos internos, aplicaciones informáticas, la existencia de una gran cantidad de BBDD (no siempre conocidas por todos, y que muchas de ellas están desorganizadas, sin actualizar, y no se conocen criterios para la búsqueda de información en ellas), e información que dicen no utilizar, como material de referencia, al no tener la seguridad de que esté contrastada y sea oficial. En este punto suele hablarse de Milit@rpedia, que aunque se valora como herramienta altamente recomendable, existe reticencia a su uso para la búsqueda de información para el desarrollo de las investigaciones de los analistas al considerar que puede contener información no oficial. Este hecho está directamente relacionado con la difusión, el conocimiento de la herramienta Milit@rpedia y su potencial. Actualmente se puede consultar información oficial y abierta, está claramente identificada y separada.



vii. *Colaboraciones*

Medimos el grado de colaboración con otros analistas, expertos o profesionales para diversas colaboraciones: búsqueda de contactos, de publicaciones doctrinales, de información específica; solicitud de información a oficiales de enlace, sobre temas específicos, corrección de los documentos; consultas sobre instalaciones, campos de maniobras, simulación, planes de estudio, cursos, etc.

Este punto se ha trabajado también en las entrevistas desde la perspectiva de la búsqueda y localización de expertos para el desarrollo de las investigaciones, y las relaciones de trabajo colaborativo existentes en DIDOM.

La gráfica, se ha elaborado por cada una de las secciones estudiadas, con la finalidad de identificar los canales de comunicación existentes en cada una de ellas, y que deben tenerse en cuenta a la hora de la implementación de herramientas de trabajo colaborativo y estrategias para la gestión del conocimiento en DIDOM.

Se ha preguntado por la colaboración con las siguientes entidades: analistas de la misma sección o JAD, analistas de DIDOM, analistas de MADOC, personal del Ejército, organismos nacionales, organismos internacionales, personal de otros ejércitos, expertos civiles. Notar que cuando se menciona una entidad, no incluye las entidades subordinadas o menores. Por ejemplo, al decir «analistas de MADOC» se exceptúan los «analistas de DIDOM» incluidos en la opción anterior.

Entre los canales de colaboración, se pueden destacar:

—Todas las secciones y JAD colaboran sobre todo con personal de la misma sección o JAD.
—La Sc. de DOCTRINA colabora «a menudo» con personal del Ejército y «alguna vez» con analistas de: DIDOM, otros ejércitos y organismos internacionales.
—La Sc. de LLAA colabora «a menudo» con personal del Ejército (JUFAS, DIVOPE, FUTER, etc.); y «alguna vez» con analistas de DIDOM.
—La Sc. de INVESTIGACIÓN colabora «alguna vez» con analistas de: DIDOM y MADOC; y «rara vez» con personal del Ejército (JUFAS, DIVOPE, FUTER, etc.).
—La Sc. de MATERIALES colabora «a menudo» con: personal del Ejército (JUFAS, DIVOPE, FUTER, etc.), analistas de DI-

DOM y de MADOC, organismos nacionales, otros ejércitos, organismos internacionales, y expertos civiles.

—Las JAD colaboran «a menudo» con: analistas de DIDOM, personal del Ejército (JUFAS, DIVOPE, FUTER, etc.); y «alguna vez» con: analistas de MADOC, organismos nacionales e internacionales civiles. Algunas JAD también colaboran con otros ejércitos y expertos civiles.

viii. *Recursos*

Este apartado se ha trabajado en profundidad en las entrevistas.

Destacar que los mandos echan en falta, o ya utilizan en sus puestos de trabajo pero no es conocido por el resto de compañero, y consideran necesarios: programas informáticos, plantillas y bases de datos, aplicaciones informáticas, canales de acceso a distintas plataformas y buscadores, recursos de trabajo colaborativo, y mejoras en la organización. Listamos las aportaciones que se hace en cada uno de ellos:

Recursos y redes:

—Buscador eficiente para la Intranet.
—Ordenadores personales más potentes y con dos pantallas.
—Terminal *Nato Secret* en el puesto de LLAA.
—Mejorar el Sistema de gestión de mensajería (no solo de mensajes Mesincet).
—Red con acceso directo a documentación clasificada, aparte de la ya existente de propósito general.
—Acceso a Intranet desde Internet (en particular para Milit@ rpedia, Biblioteca Virtual, etc.).
—Acceso a Internet desde la Intranet con permisos más amplios.

Aplicaciones Informáticas:

—Programas de edición de video y sonido;
—Traductor con léxico militar.
—Aplicaciones para soportes móviles (apps).
—Software para reducir el tamaño de los archivos (i.e. *Nx powerlite* reduce las presentaciones de *Power Point*).

—Programa de reconocimiento de voz para escritura automática para redacción de publicaciones (i.e. *Dragon naturally speaking*).
—Programa para incluir fácilmente fotos militares en las publicaciones que se confeccionan.
—Gestor de proyectos (Project).

Recursos colaborativos:

—Herramienta de trabajo colaborativo fácil e intuitiva, que permita la elaboración colaborativa de un texto por un grupo cerrado de trabajo. Por ejemplo, Sharepoint (en servicio en otros organismos como EMACON, Armada, JCISAT, MALE) permite la edición concurrente y permita el archivado y difusión de archivos (como las páginas *Wise*), entre otras funcionalidades. La plataforma colaborativa debería permitir, en resumen.
—Grupos de trabajo con parte privada y pública.
—Edición concurrente de textos.
—Chat.
—Multiconferencia.
—Suscripción individual voluntaria a temas de discusión, con aviso automático por email.
—Creación por iniciativa individual de temas de discusión.
—Repositorio de documentación «intermedia» (también llamada «documentación gris») o trabajada relativa a diferentes temas (FINABLE, REM, propuestas CALPE, histórico de *stanag*, fichas de *stanag*, comentarios a publicaciones, expertos, etc.), a disposición de los analistas, para que haya documentación histórica de referencia a la hora de afrontar un tema. El «esqueleto y procedimiento de uso de este sistema debe estar concienzudamente pensado, planeado y ser flexible».
—Aumentar las reuniones presenciales de un grupo de trabajo para mejorar el producto final (publicaciones doctrinales, manuales de instrucción, requisitos de estado mayor, etc.).

Repositorios y plantillas:

—Repositorio de fotografías en Intranet.
—Acceso a repositorios civiles a los que no se puede acceder desde la conexión de intranet al estar limitado su acceso.

—Acceso a repositorios de la UGR.
—Boletín de noticias con los aspectos más novedosos que pueden afectar al ámbito de las competencias del MADOC.
—Plantilla de publicaciones con tipos de letra, márgenes, tamaño, etc., en el que solo se necesitase rellenar el contenido.
—Plantillas de informes.

Mejoras:

—Mejorar la categorización de los repositorios digitales.
—Procedimiento para nombrar o codificar la información, archivos y documentos.
—Normativa para concienciar y mejorar la difusión del trabajo de los analistas (Milit@rpedia, Biblioteca Virtual, difusión por correo, etc.).

Recursos Humanos:

—Personal experto necesario.
—Más analistas.
—Aumentar el servicio de traducción de inglés (facilitaría la difusión del «pensamiento» nacional).
—Más tiempo para estudio y lectura de documentación (normalmente se usan ratos libres en casa y los viajes en tren o avión) y disminuir el dedicado a tareas burocráticas.
—Gabinete «informático» que diese solución a los problemas técnicos de software.
—Recursos humanos para Milit@rpedia (tutores de área).

Documentación Gris:

El personal auxiliar de las secciones guardaba una carpeta con toda la «documentación gris» (informes intermedios, actas de reuniones, aportaciones de los participantes en el equipo, búsquedas avanzadas de contenidos, etc.) previa a la redacción de la publicación final. La falta de personal hace que estos puestos estén desapareciendo. Además, hay que aprovechar que las nuevas tecnologías permiten métodos eficientes para la gestión de esta información.

El registro de esta «documentación gris» está valorado como posible recurso de utilidad para como documentación válida y se-

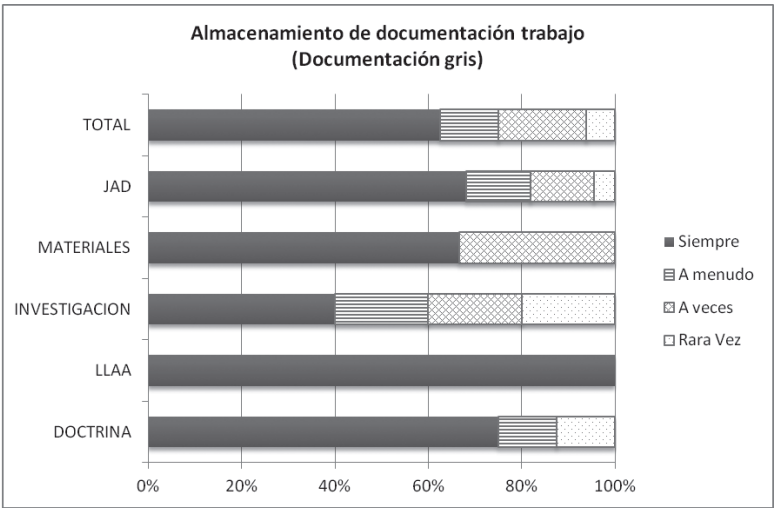
leccionada, en ocasiones comentada y valorada, que puede volver a utilizarse en futuras publicaciones de la misma o de otras áreas, aparte de facilitar la identificación de fuentes y de expertos.

Existen temáticas que se repiten todos los años para los que la recuperación de la documentación gris serviría para ahorrar tiempos y velar por la continuidad y fundamentación de las publicaciones.

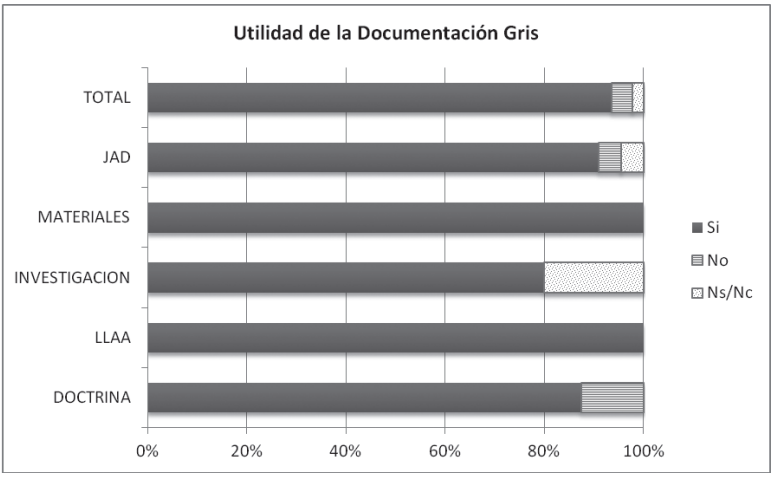
Habría que articular un procedimiento para regular o facilitar el archivado y recuperación de la documentación gris. Las soluciones en red pueden ser varias, como:

—Creación de un depósito único categorizado por secciones y grupos de trabajo en Sharepoint y recursos en red;
—Archivos comunes en red de uso compartido;

Como se puede ver en el gráfico, el 63% del total de los analistas consultados almacenan «siempre» en sus ordenadores documentos de referencia usados en la elaboración de informes, alcanzando los analistas de la Sección de Doctrina el 72%.



El 90% considera que es información útil, validada, contrastada y recuperable para su uso y aplicación en futuros trabajos. En el caso de Lecciones Aprendidas la utilidad la valoran con un 100%.



5. Mapa del conocimiento

La propuesta final de Mapa del Conocimiento de la DIDOM se ha decidido realizar de manera conjunta, y relacionada también con aquellas otras personas y estructuras que se relacionan con el sistema de conocimiento interno.

De esta manera se pretende poner en evidencia las interrelaciones que pueden favorecer la adopción de estrategias que favorezcan el crecimiento de la organización, al poner en relación los tres ámbitos de Capital Intelectual, el humano, el estructural y el relacional.

El mapa propuesto contiene:

—Capital Intelectual: Personas (clientes, usuarios internos o externos; y suministradores o proveedores de información y conocimiento).
—El momento del ciclo de transformación del conocimiento en que actúan, expresado en 5 fases, con dos actividades concretas cada una:
—Creación:
- Descubrimiento
- Transformación

—Almacenamiento:
- Sistematización
- Organización

—Apropiación:
- Uso

- Mantenimiento

—Transferencia:
- Distribución
- Generalización

—Evaluación:
- Validación
- Planificación

—Las Inputs o Fuentes utilizadas (input)

—Las Herramientas y Repositorios con el que se trabaja ese conocimiento, diferenciando en este primer nivel de análisis:
- Cuáles son Formales, es decir, puestas a disposición de manera consciente y organizada por la DIDOM o por el Ejército de Tierra.
- Cuáles son No Formales, al utilizarlas las personas de manera autónoma, ya sea por una iniciativa personal o de un grupo de personas.

—Los Conocimientos Clave que están en posesión o sobre los que trabajan las personas.

—Los Procedimientos utilizados en ese proceso de transformación del conocimiento.

—Los Outputs o Productos finales donde queda recogido el Conocimiento.

Algunos de estos campos se mostrarán en gris, tratando de poner en evidencia elementos que, durante la presente investigación, se han identificado como necesarios, pero que en la actualidad no existen en el Sistema de Gestión del Conocimiento.

A su vez, la ordenación de la información permite identificar de manera rápida los tres Capitales antes mencionados, capital humano, capital estructural y capital relacional.

Esta primera definición del Mapa surge del análisis documental de funcionamiento de la DIDOM y de los cuestionarios y entrevistas realizadas a su personal.

Sin embargo, no debe considerarse exhaustivo, sino más bien como una propuesta organizada y sencilla de representar y hacer un seguimiento al Conocimiento que genera la DIDOM. Por tanto, está sujeto a revisiones, puntualizaciones y ajustes.

En este documento se presenta como imagen, que aconsejamos imprimir en formato A3. Se adjuntará un archivo en Excel para facilitar trabajar con él.

Ubicación	Capital Intelectual	Ciclo del Conocimiento: Creación – Descubrimiento	Creación – Transformación	Almacenamiento – Sistematización	Almacenamiento – Organización	Apropiación – Uso	Apropiación – Mantenimiento	Transferencia – Distribución	Transferencia – Generalización	Evaluación – Validación	Evaluación – Planificación	Input (Fuente)	Repositorios / Herramientas – Formales	Repositorios / Herramientas – No formales	Contenido/Experiencia	Procedimientos	Output (Producto)
FFAA Alcalde / FFAA / MADOC / DIDOM	*Analista de Orgánica*	✔	✔		✔		✔	✔				Internet, Oficiales enlace, Biblioteca virtual, Normativa ET, Revistas, Militarpedia, Mesinet	MESINCET, Militarpedia, Outlook		Módulos de Planeamiento	Procedimiento Abreviado	Productos de Nivel 1
															Plantillas Orgánicas	Ciclo de Revisión Doctrinal	Publicaciones Niveles 2 al 4
	Analista de Doctrina	✔	✔		✔		✔	✔				BBDD, OFEN MADOC, OTAN, NSO, PMET (DIDOM), Artículos Revistas, Publicaciones aliadas, Biblioteca Virtual	BBDD, PMET (DIDOM), Biblioteca Virtual, Outlook	Videoconferencia, NX powerlite, Dragon naturally speaking, Background, Sharepoint	Operaciones y Funciones de Combate	Ciclo de Revisión Doctrinal	Publicaciones Niveles 1 al 4
															Aprovechamiento Experiencia en ZO	Procedimiento Abreviado	PMET Operaciones
	Analista de Materiales	✔	✔		✔		✔	✔				Biblioteca Virtual, BBDD grupos y asuntos Internacionales, Janes, Servicio de Documentación, OSE, DGAM, OTAM, NSA, Foro de Materiales, Militarpedia, OFEN	Biblioteca Virtual, BBDD, Foro de Materiales, Militarpedia, Outlook		Obtención de Recursos	Ciclo de Revisión Doctrinal	Publicaciones Niveles 1 al 4
															Detección de Carencias	Ciclo de Revisión Doctrinal	Publicaciones Niveles 1 al 4
															Logística Internacional	Ciclo de Revisión Doctrinal	Publicaciones Niveles 1 al 4
															Experimentación Materiales Especiales	Ciclo de Revisión Doctrinal	Publicaciones Niveles 1 al 4
	Analista de Investigación	✔	✔		✔		✔	✔				BBDD, Internet, Informes Oficiales de Enlace, Revistas ET, Publicaciones IEEE y CESEDEN, OTAN, FINABEL, MESINCET, Servicio Documentación, BBDD UGR	BBDD, Internet, MESINCET, Servicio Documentación, Outlook		Evolución y experimentación teórica del Combate	CALPE	PINV, CALPE
																Orden JEME a propuesta GEMADOC	Tendencias, Test E.F., Documento
	Analista de LL.AA.	✔	✔	✔	✔					✔	✔	BBPP, LLII y LLAA, Oficiales Enlace, Equipos LLAA en OZ, Informes ZO, Informes Fin de Misión, Entrevistas, POC en ZO, Reuniones	BBDD, Videoconferencias, Redes Seguras, Outlook	Mendeley,iMindMap,Sharepoint	Aprovechamiento Experiencia en ZO	Sistema de Lecciones Aprendidas	PMET Operaciones
															Todo tipo		8 tipos de Informes
	Analista de Gestión del Conocimiento			✔	✔		✔	✔				Militarpedia, Biblioteca Virtual, Web, BBDD	Militarpedia, Biblioteca Virtual, Web, BBDD, MESINCET, SIGEPLAN, Outlook	Motor de Búsquedas	TICS, NNTT, Difusión del Conocimiento, Comunicación y Marketing	Publicación, Traducción, Documentación	Respuesta a Solicitudes, Publicación Periódica, Subscripciones, Asesoramiento
	JAD	✔	✔			✔	✔	✔	✔	✔		Servicio Documentación, Internet, NSO y portal ID de OTAN, Biblioteca virtual, BBDD Internacionales, Revistas, SATANAG OTAN DIDOM, FINABEL, Publicaciones doctrinales, Normativa ET, Oficiales de enlace, PMT DIDOM, EEEI	Internet, Intranet, Biblioteca virtual, BBDD, SIGEPLAN, SIPERDEF, Militarpedia, Outlook	Programas de edición de video, cámaras, de video	A requerimiento	Grupos de Trabajo	Publicaciones Niveles 1 al 4
															Según Destino	Ciclo de Revisión Doctrinal	
	Secretaría SUBDOM			✔	✔			✔			✔	Biblioteca Virtual, OFEN, Militarpedia, Biblioteca virtual, Revistas especializadas	Biblioteca Virtual, Militarpedia, Biblioteca virtual, Outlook				
	Secretaría SUBDIVA			✔	✔			✔			✔	Biblioteca Virtual, OFEN, Militarpedia, Biblioteca virtual, Revistas especializadas	Biblioteca Virtual, Militarpedia, Biblioteca virtual, Outlook				
	Necesidades comunes	***Expresadas en la Investigación***										Terminal Nato Secret, BBDD UGR	Apps para móviles, BBDD Fotografías, **Sharepoint**, Wise DIDOM/MADOC, Traductor con léxico militar, NX powerlite, Dragon Naturally Speaking, Sistema Acceso Seguro a Intranet desde Internet, MS Project, Acceso a Militarpedia y Biblioteca Virtual desde Internet			Plantillas de Documentos	
		Propuestas por el Proyecto										Registro de Expertos, Comunidades de Expertos, Explotación Motor de Búsqueda, Carpeta Brigada en Red (CBR)	Indicadores de satisfacción (estrellas) y comentarios, Protocolo Bienvenida Analistas, Repositorio Recursos Formativos, Tesauro		Sistema de Trazabilidad del Conocimiento	Libro de Estilo, Procedimiento Estandarizado de Investigación Documental, Carpeta Brigada en Red (CBR)	Sistema de Gestión del Conocimiento Estandarizado
	Secretaría General / GEMADOC			✔	✔			✔			✔						
	DIEN						✔	✔	✔	✔					Ver las distintas academias y centros de formación y sus especialidades	Planes Formativos	Material Didáctico, Publicaciones Oficiales
	Expertos ET Ajenos DIDOM	✔	✔			✔			✔	✔		Grupo de Trabajo			Aprovechamiento Experiencia en ZO	Procedimiento Abreviado	PMET Operaciones
												Grupo de Trabajo			Aprovechamiento Conocimiento previo como Analistas	Carpeta del Brigada en Red, Sistema de Trazabilidad del Conocimiento	
	Estado Mayor - JEME	✔									✔	MADOC	MESINCET		Estructura del ET	Ciclo de Revisión Doctrinal	Directrices
	UCO - Unidades	✔				✔	✔		✔	✔		Solicitudes de Analistas	Biblioteca Virtual, Canales de Difusión, Militarpedia, Solicitudes a Documentación, MESINCET		Propios del trabajo en ZO	Determinado por quien pide información	Informes a Analistas
												Publicaciones del MADOC				Indicadores de satisfacción (estrellas) y comentarios	Comentarios
	Oficiales de Enlace	✔				✔		✔		✔		Solicitudes de Analistas	Biblioteca Virtual, Canales de Difusión, Militarpedia, Solicitudes a Documentación, MESINCET				
	JUPROAM	✔				✔		✔		✔			Biblioteca Virtual, Canales de Difusión, Militarpedia, Solicitudes a Documentación, MESINCET		Materiales	Solicitudes a Materiales	
	Personal del ET en General	✔				✔			✔	✔			Biblioteca Virtual, Canales de Difusión, Militarpedia, Solicitudes a Documentación, MESINCET		Temas relacionados con su destino y empleo	Indicadores de satisfacción (estrellas) y comentarios	Comentarios
	UTRAFAS	✔	✔	✔	✔			✔	✔	✔			Documentos intecambiados en Grupos de Trabajo		Temas varios 3 niveles	Grupos de Trabajo	Doctrina Conjunta - Combinada
	JUFAS	✔	✔	✔	✔			✔	✔	✔			Documentos intecambiados en Grupos de Trabajo		Temas varios 3 niveles	Grupos de Trabajo	Doctrina Conjunta - Combinada
OTAN		✔	✔	✔	✔	✔	✔	✔	✔	✔	✔		Documentos intecambiados en Grupos de Trabajo		Temas amplios	Distintos Grupos	Doctrina Internacional / Interoperable
Otros Ejercitos UE		✔	✔	✔	✔	✔	✔	✔	✔	✔	✔		Documentos intecambiados en Reuniones Bilaterales / Grupos de Trabajo		Desarrollo de Fuerza, Conocimiento, Compromiso, Memoria	FINABEL / Reuniones Bilaterales	Doctrina Internacional / Interoperable
Otros Ejercitos Internacionales		✔	✔	✔	✔	✔	✔	✔	✔	✔	✔		Documentos intecambiados en Reuniones Bilaterales		Temas concretos	Reuniones Bilaterales	Doctrina Internacional / Interoperable
Entorno Civil	*Expertos Externos UGR - CEMIX*	✔	✔					✔		✔		Grupos de Trabajo	BB.DD. Resultados de Proyecto		Definidos por Experience Acreditada		
	Otros Expertos Civiles	✔	✔							✔					Definidos por Experience Acreditada		
	Población Civil	✔						✔		✔		Publicaciones digitales	Web ET		Temas públicos de Funcionamiento y Difusión	Indicadores de satisfacción (estrellas) y comentarios	Comentarios

6. Líneas de actuación

Un Sistema de Gestión del Conocimiento es el conjunto organizado de personas, procedimientos y herramientas (software, repositorios, etc.), que facilitan la creación, almacenaje, compartición, transferencia y uso del conocimiento y la experiencia de la organización.

El Sistema de Gestión del Conocimiento de la DIDOM, como espacio vivo, comprende: expertos identificados (con su formación y experiencia), orientaciones sobre cómo generar conocimiento, «metodología de la investigación y análisis», grupos de trabajo, cómo almacenarlo, difundirlo, con qué recursos trabajar en cada momento y con qué herramientas colaborativas, el protocolo de bienvenida para los relevos, normativa, etc.

Dicho sistema, necesita de un procedimiento escrito y aprobado, en base a un plan articulado de implementación en función de los siguientes objetivos:

Almacenamiento-recuperación-acceso

—Recuperar información de los repositorios corporativos de forma rápida y fácil, sin necesidad de tener información duplicada.
—Disponer de un buscador de contenidos web eficiente, que busque en los repositorios de interés.
—Definir un procedimiento de almacenamiento de la documentación gris en la red organizacional.
—Definir un procedimiento de codificación o etiquetado de la información
—Definir un procedimiento para organizar los metadatos de la documentación, que incluya resumen, valoración, utilidad, temas, participantes
—Definir un procedimiento para organizar los metadatos de las publicaciones web

Creación

—Impulsar el trabajo en red de los grupos.
—Impulsar herramientas que permitan el trabajo en red de forma eficiente (Sharepoint, Project, foros, repositorios, etc.) y la explotación del repositorio organizacional.
—Impulsar comunidades de expertos con objeto de mantener la especialización conseguida a lo largo de los ciclos

de aprendizaje obtenidos en los distintos destinos, para su perduración, mantenimiento, y crecimiento de la carrera profesional.
—Definir un procedimiento de registro de expertos participantes en los trabajos, de forma que se reconozca la autoría de alguna forma.
—Definir un procedimiento de recompensas o gratificaciones para fomentar al personal más participativo.
—Impulsar un foro posibilite la creación de temas de debate
—Impulsar un procedimiento para explicitar el conocimiento de las personas que abandonan el destino o pasan a la reserva
—Detectar carencias de conocimiento (temas de investigación, propuestas de analistas, estadísticas de términos buscados, etc)
—Impulsar un procedimiento que permita mejoras e innovaciones, a partir de las propuestas de los analistas, y de las prácticas en funcionamiento individualmente, valoradas en común por los demás analistas.

Mantenimiento

—Definir un procedimiento para el mantenimiento de la información en los distintos repositorios y listas de distribución. En particular en Milit@rpedia, conviene tener designados tutores o responsables por áreas de conocimiento.

Difusión

—Impulsar un procedimiento sobre la forma de difundir cada producto, usando los repositorios (Biblioteca Virtual, Milit@rpedia, etc.) y herramientas disponibles (Mesincet, correo electrónico corporativo, correo electrónico de difusión selectiva, etc.).
—Disponer de un buscador de contenidos web eficiente.
—Impulsar el servicio de documentación de la DIDOM.
—Impulsar el servicio de traducción de la DIDOM.
—Disponer de una herramienta de difusión selectiva por correo electrónico.

Sistema de GC

—Impulsar un concepto de gestión del conocimiento para la DIDOM.
—Orientar la implantación del sistema de gestión del conocimiento por objetivos y por proyectos piloto. El concepto anterior sería la base que permita ir mejorando los elementos de gestión del conocimiento e ir introduciendo otros nuevos según las necesidades y las herramientas disponibles
—Respaldar a los analistas de SEGECON para acometer los pasos necesarios, observados desde la propia estructura de la DIDOM, definiendo sus competencias respecto al sistema de gestión del conocimiento de la DIDOM.

Concienciación

—Concienciar que la gestión del conocimiento se basa en la implicación de los recursos humanos, y en que tras el trabajo realizado, está el registro, la difusión, validación y reutilización.
—Impulsar una cultura de la gestión del conocimiento.

Formación

—Definir la formación de los analistas para su puesto en DIDOM (metodología de la investigación y análisis, herramientas disponibles, inglés, cursos específicos, etc.
—Elaborar un protocolo para los relevos, en el que se proporcione documentos necesarios que se deben conocer para su incorporación. El «paquete de bienvenida» de analistas debe contener: presentación sobre la sección, tareas del puesto de trabajo, relaciones habituales, normativa y directrices; herramientas disponibles (repositorios de trabajo de la sección o grupos; servicio de documentación: acceso a recursos documentales, Biblioteca Virtual, Milit@rpedia, etc.), acceso a documentación clasificada, cursos, etc.
—Se puede transformar en recurso didáctico, sistematizado en fichas y presentaciones, estructurado y almacenado en el repositorio común para que sea fácil su recuperación y uso cuando se necesite.

Es necesaria la creación de un sistema de trabajo colaborativo centralizado que descargue la gestión de los analistas, permita crear productos y acceder a proyectos anteriores. La Sección GC puede:

—articular el sistema integral que identifique el flujo de la información y sus canales (quien, que, cómo, cuándo, dónde y para qué),
—disponer el sistema de almacenamiento de información útil y transferible,
—promover metodologías y herramientas que faciliten el trabajo colaborativo y en red, y
—registrar a los expertos que han participado en los grupos de trabajo para futuras colaboraciones o recomendaciones.
—recuperar la «carpeta del auxiliar» y ponerla a disposición de todos en red.

Para ello se deberá diseñar y aprobar un procedimiento sistematizado que aúne:

—Las normas de funcionamiento interno bajo la premisa de la búsqueda continua de la eficacia de los procedimientos de los analistas.
—El objetivo de la Dirección, la producción de documentos de manera sistemática y periódica.
—Los expertos, identificarlos y que se posibilite su colaboración de manera transversal en función de su área de conocimiento.
—La validación de la calidad y utilidad de la documentación compartida. Vigilancia de la actualización de la información, valoración de la contribución del experto y de los distintos repositorios identificados:
  - Sharepoint / directorios en red / otros para el trabajo en grupo (información gris intermedia e información de trabajo que no se quiera que salga del ámbito de la dirección o del grupo de trabajo)
  - Milit@rpedia / Biblioteca Virtual / difusión por correo y servicio de documentación (información que se decide hacer pública fuera de la Dirección)
—La identificación de los mandos que trabajan con herramientas colaborativas para que transfieran su conocimien-

to al resto de los analistas. Algunas de las herramientas existentes en la DIDOM, pero no conocidas por todos los analistas, que facilitan el trabajo colaborativo son:

- Project (gestor de proyectos)
- Foro de Materiales
- Imindmap
- Sharepoint
- *Wise* DIDOM/MADOC
- *Nx powerlite*: software para reducir el «peso» de las presentaciones de *power point*.
- *Dragon naturally speaking* (programa de reconocimiento de voz para escritura automática).

Referencias bibliográficas

Arredondo Gonzalo, Pablo y Sáiz-Pardo Lizaso, Manuel; «Visión general de la gestión del conocimiento en el Ejército», Comunicación del I Congreso Internacional de Estudios Militares, 2014.

Castro Castro, Carlos, «Auditoría del conocimiento en el MADOC. Análisis preliminar para la implantación de Sistemas de Gestión del Conocimiento en el Ejército Español». Memoria de proyecto de investigación del CEMIX UGR-MADOC, 2015.

DIDOM, «Seguimiento del estudio piloto de gestión del conocimiento en la DIDOM». Memoria de proyecto de investigación, 2016.

DIDOM. Norma 04/13: Organización de la Sección de Gestión del Conocimiento y Nuevas Tecnologías. Dirección de Investigación, Doctrina, Orgánica y Materiales (DIDOM) del Mando de Adiestramiento y Doctrina (MADOC) del Ejército. 2013.

Nonaka, Ikujiro; Takeuchi, Hirotaka. *The knowledge-creating company: how Japanese companies create the dynamics of innovation*. 1995.

Ruiz Carrasco, Alejandro; «Visión, implementación y explotación del motor de búsqueda de contenidos web en redes Intranet. El caso de la Intranet de Defensa». Comunicación en el II Congreso Internacional de Estudios Militares Granada, 18-20 de octubre de 2016.

VISIÓN, IMPLEMENTACIÓN Y EXPLOTACIÓN DEL MOTOR DE BÚSQUEDA DE CONTENIDOS WEB EN REDES INTRANET. EL CASO DE LA INTRANET DE DEFENSA

Alejandro Ruiz Carrasco
DIDOM-MADOC
aruicar@et.mde.es

Resumen

La demanda de información por parte de los usuarios de una Intranet creciente, y la dificultad de encontrar lo buscado en un tiempo razonable, nos lleva a pensar en la necesidad que tienen dichos usuarios de disponer de un servicio de búsqueda de contenidos web sobre la misma Intranet, que sea capaz de indexar contenidos web de diferente naturaleza: hipertexto, documentos PDF, Word, Excel, powerpoint, multimedia … y procedentes de distintas aplicaciones, repositorios y servidores web. Una clara referencia de este proyecto es el buscador «Google Search» de Internet. El proyecto planteado tiene particularidades en cuánto al ámbito de aplicación y limitaciones, pero también cuenta con pequeñas ventajas añadidas adaptadas a cada Intranet en virtud de su propia distribución de la información.

Palabras claves

«Búsqueda», «Buscador», «Intranet», «Información», «Web»

1. Antecedentes

Este trabajo es una continuación fundamental del proyecto presentado en el primer congreso Internacional de Estudios Militares, denominado «*Casuística derivada de la posible explotación de un motor de búsqueda de contenidos web en una red Intranet organizacional. La red Intranet de Defensa*», donde se expusieron las bases teóricas de un proyecto que actualmente se encuentra en fase de desarrollo y pruebas, y del que se pueden extraer las conclusiones que se resumen en los siguientes cuatro puntos:

1.1. *Exposición del problema*

Muchas organizaciones se ven en la necesidad de compartir sus activos de información y conocimiento entre su propio personal y desde distintas sedes, pero simultáneamente surgen otras necesidades, las más destacadas son:

—Privacidad de la información: los activos de información no deben ser públicos para el resto del mundo.
—Reducción de amenazas: evitar la exposición a posibles ciberataques desde el espacio de Internet cuya desastrosa conclusión pueda significar la pérdida o el saboteo de sus activos de información.

Conscientes de esta realidad, muchas organizaciones han tomado como solución tecnológica predominante la instauración de redes Intranet, lo cual les confiere una de las mejores garantías para difundir sus datos dentro del ámbito de su Intranet sin que esta sea accesible o vulnerable desde Internet o desde una Intranet ajena.

No obstante, en la cara negativa de la instauración de las redes Intranet, cabe señalar que de manera predeterminada una Intranet no dispone de los potentes motores de búsqueda de Internet tales como Google, Bing, Altavista o Yahoo; de forma que se puedan satisfacer algunas de las demandas de información procedentes de la propia Intranet organizacional.

¿Dónde está la relevancia de este hecho?, probablemente encontremos una respuesta si nos preguntamos cuan a menudo y por qué motivo utilizamos los buscadores de Internet como Google Search, el cual, según el ranking de *Alexa Internet, Inc.*, es el sitio web de Internet más visitado a escala mundial.

En el caso de una red Intranet, siempre que su volumen de información sea lo suficientemente significativo, es probable que la naturaleza predominante de los activos información sea de carácter corporativo, lo que no se considera motivo suficiente para obviar la posible necesidad de un motor búsqueda en servicio sobre la Intranet corporativa.

1.2 *¿Cómo debe ser la solución al problema?*

Si una organización optara por explotar un motor de búsqueda sobre su propia Intranet, casi con total seguridad le exigirá a

este sistema, la satisfacción de una serie de máximas organizacionales contempladas en forma de restricciones de distinta naturaleza, y que son determinantes en la búsqueda y elección de este sistema. Algunas de estas restricciones podrían encuadrarse en las siguientes áreas:

—*(RG1) Restricciones de seguridad de la información*
La información es uno de los activos más importantes de cualquier organización, este sistema será acaparador de gran cantidad de datos públicos en la Intranet de la organización.

—*(RG2) Restricciones operativas*
Son restricciones orientadas al mantenimiento permanente del sistema, donde es importante mantener un ritmo de actualizaciones constante, de conformidad con la evolución tecnológica y el área de la seguridad informática.

—*(RG3) Restricciones económicas*
Se trata de disminuir costes de adquisición y mantenimiento.

—*(RG4) Restricciones legales derivadas de la propiedad y licenciamiento*
Si la organización desarrollara este sistema, podría ser su propietaria y no existirían restricciones derivadas de la propiedad intelectual o de los derechos de uso, explotación o de posibles licenciamientos por parte del sistema desarrollado.

—*(RG5) Restricciones técnicas organizacionales*
El sistema deberá satisfacer las exigencias técnicas de la organización, en el caso de la Intranet de Defensa están expresadas en la arquitectura técnica unificada (ATU). Dicho documento recoge explícitamente las condiciones de explotación de sistemas gestores de base de datos, lenguajes de programación y otros entornos y sistemas que puedan intervenir en cualquier software utilizado por la organización. Este punto suele ser especialmente restrictivo con el software libre.

—*(RG6) Restricciones técnicas de infraestructura*
El sistema debe ser soportado por la infraestructura de red de la organización, así como por otros elementos intervinientes, como es el caso de las máquinas servidor y cliente dentro del marco hardware y software.

Además, podrían surgir también intereses organizacionales que impliquen cambios en el funcionamiento del motor de búsqueda respecto al funcionamiento de los tradicionales motores de búsqueda de Internet. Algunos de estos cambios podrían encuadrarse en las siguientes áreas:

—Integración con el dominio corporativo.
—Registro automático de las búsquedas ejecutadas por los usuarios de la Intranet y estadísticas de explotación.
—Posibilidad por parte de los usuarios, de denunciar contenidos web no lícitos o contrarios a la organización.
—Posibilidad de trabajar con un tesauro específico de la organización, que pueda mejorar la calidad de la búsqueda.
—Otros, etc.

1.3. *Presentación de alternativas y viabilidad*

En el trabajo anterior se procedió a realizar un estudio sobre aplicación de las restricciones, que comúnmente, pueden ser exigidas por una organización y que por supuesto, pueden ser de aplicación para el caso de la Intranet de Defensa, del mismo modo, el estudio se amplió con el análisis de funcionalidades que podrían ser de posible interés. Frente a esto, se plantearon algunas alternativas de solución existentes en octubre de 2014, con objeto de intentar dar una respuesta apropiada a la necesidad desde tres áreas bien diferenciadas:

—Software libre
—Software propietario
—Desarrollos a medida

1.4. *Evaluación y selección*

En la que se exponen las justificaciones por las que se estima o desestima cada una de las alternativas propuestas en el punto anterior, en el caso particular de la Intranet de Defensa únicamente se estima la solución representada por la tecnología de Microsoft. NET, debido principalmente al peso de las restricciones impuestas, especialmente en lo relativo a la seguridad de la información.

2. Implementación del motor de búsqueda

Fruto del trabajo anterior y de su análisis, se concluyó que la solución elegida en el ámbito de la Intranet de Defensa sería un desarrollo a medida, que cumpla los requisitos exigidos de carácter más crítico, y que incluya en lo posible, nuevas funcionalidades que se adapten a los intereses de la organización. La solución tecnológica seleccionada sobre el que implementar este sistema ha sido el entorno Microsoft .NET.

2.1. *Principios destacados de la implementación*

Existe un conjunto de bases teóricas sobre las que implementar el motor de búsqueda, qué de no estar presentes de antemano, complicarían sin duda el proceso de implementación en toda su magnitud.

2.1.1. *Arquitectura común*

Desde el punto de vista de la implementación, cabe decir que existe una gran multitud de alternativas para implementar un sistema de estas características con la solución tecnológica seleccionada basada en Microsoft.NET, pero si simplificáramos todas ellas, nos encontraríamos que independientemente de la solución tecnológica adoptada, todas convergen a una misma *arquitectura común* que todo sistema de estas características debe implementar, y que básicamente se puede dividir en componentes, módulos o subsistemas independientes bien diferenciados que interaccionan con un repositorio de información:

—Repositorio de información
Donde se almacenan los datos del sistema, y que podría estar constituido por una o varias bases de datos de distinta naturaleza: simples, federadas, distribuidas…

—Subsistema Web Crawler + Indexador
El web crawler se encarga de rastrear la web en búsqueda de nuevos contenidos, mientras que el indexador, tiene por misión indexar o grabar en el repositorio de información una serie de datos seleccionados de los contenidos web rastreados por el web crawler.

—Subsistema de Búsquedas (Search)
Obtiene las consultas procedentes de las demandas de información de los usuarios, y tras realizar en cada caso las

correspondientes consultas contra el repositorio de información, obtiene un conjunto de resultados de búsqueda.

Es a partir de esta arquitectura común, donde divergen las distintas soluciones de implementación para el motor de búsqueda de contenidos web. Cada implementación puede especificar aún más cada uno de los módulos descritos, así como agregar otros nuevos para satisfacción de los objetivos de cada sistema en particular.

2.1.2. *Contexto de Intranet*

En el contexto donde se implementará el motor de búsqueda, existen aspectos relacionados con la Intranet que podrían ser cruciales en la concepción del motor de búsqueda:

—*Problema de la abundancia*
«Gran parte de la información publicada en una Intranet, no es revisada en el momento de su publicación, y puede estar duplicada total o parcialmente. El motor de búsqueda debe tratar con el gran tamaño y la tasa de cambio de la web».

—*Intranet profunda*
«Es la parte web de la Intranet no indexada por el motor de búsqueda, compuesta de los contenidos web no deseados para su indexación, que tienen dificultad para ser rastreados o indexados, que son privados o protegidos por contraseñas».

2.1.3. *Metodología de desarrollo*

En el proceso de desarrollo de un sistema de alta complejidad, es cuanto menos recomendable, llevar a cabo una serie de buenas prácticas contemplados por la ingeniería del software:

—*Ciclo de vida incremental*
Consiste en ejecutar el desarrollo por etapas u objetivos parciales, para posteriormente, integrarlas en la misma solución. Esto se podría interpretar como el proceso por el que se desarrollan distintos módulos o subsistemas lo más encapsulados e independientes entre sí (bajo acoplamiento), de forma que cada módulo se dedique a realizar en

exclusividad la tarea para la que fue concebido (alta cohesión). Otra interpretación, sería la de expandir con nuevas funcionalidades un módulo o subsistema determinado.

—*Ciclo de vida iterativo*

Consiste en ejecutar la implementación por iteraciones, de manera que en cada ciclo o iteración se revisa y se mejora el sistema o algunos de sus componentes seleccionados. Cada iteración, tiende a mejorar la calidad de lo implementado.

2.1.4. *Construcción de URL´s*

Una URL, una sigla del inglés correspondiente a *Uniform Resource Locator'*, es una secuencia de caracteres de conformidad con un estándar, que permite apuntar contenidos web para que puedan ser referenciados y direccionados.

Los contenidos web, son la empresa fundamental de un sistema de estas características, y cada uno de ellos es único en una Intranet en cuanto a su direccionamiento URL. La construcción de una URL no contiene partes aleatorias, y combina cuatro partes esenciales.

1. El protocolo, forma en la que se establece la comunicación para el intercambio de datos.
2. El servidor web o host, desde el que se publica en Intranet el contenido web. Si el servidor está integrado en un dominio, el nombre del dominio podría estar incluido en el nombre del servidor web o host.
3. El puerto del servidor, desde el que se establece la conexión.
4. La ruta relativa, que tiene el contenido web en su correspondiente servidor o host.
   Ejemplo de URL: http://servidorMBCW.dominius.es:80/motor_de_busqueda/principal.aspx
5. http es el protocolo.
6. servidorMBCW.dominius.es es el servidor web o host, el cual está integrado en el dominio dominius.es.
7. 80 es el puerto en el servidor
8. /motor_de_busqueda/principal.aspx es la ruta relativa en el servidor.

En la mayoría de los navegadores web no es requisito ingresar el protocolo «http://» para apuntar a una página web, ya que

HTTP es el protocolo más usado por los navegadores web. Del mismo modo, 80 es el puerto por defecto del protocolo HTTP, y tampoco es requisito su especificación en las URL. Si el navegador web funciona en una máquina integrada en el mismo dominio que el servidor web o host, tampoco suele ser necesario ingresar el dominio.

Una vez el sistema entre en funcionamiento e interaccione con los usuarios, estará constantemente sirviendo resultados de búsqueda, para cada uno de estos, se construirá una dirección URL de forma que el contenido web referenciado pueda ser accedido directamente por el usuario.

2.2. *Subsistemas del proceso actual de implementación*

El desarrollo del motor de búsqueda de contenidos web sobre la Intranet de Defensa, surge de una necesidad real y que se enmarca entre los proyectos de la Dirección de Investigación, Doctrina, Orgánica y Materiales (DIDOM) del Ejército de Tierra. En la actualidad, este proyecto se encuentra en fase de desarrollo y pruebas.

Se definirán los distintos subsistemas construidos para satisfacción de los requisitos, los que se contemplan en la citada comunicación al primer Congreso Internacional de Estudios Militares: *Casuística derivada de la posible explotación de un motor de búsqueda de contenidos web en una red Intranet organizacional. La red Intranet de Defensa.* El objetivo mínimo es recoger en estos subsistemas las exigencias impuestas por los requisitos «críticos», que son aquellos que nacen de la misma concepción del sistema.

2.2.1. *Subsistema de servidores*

Registrará servidores web de la Intranet, lo que supondrá la primera criba a la hora de indexar contenidos web, de forma qué, si un contenido web rastreado de Intranet, no fuera publicado explícitamente por uno de los servidores web aquí registrados, el contenido web no será indexado, no pudiendo ser en ningún caso, objeto de próximas búsquedas procedentes de los usuarios.

Esta criba viene a resolver, en parte, el citado *problema de la abundancia (concepto de 2.1.2),* dado que en ninguna Intranet se conoce de antemano una aproximación de cuantos contenidos web existen en ella, no obstante, lo natural es visionar un gran

volumen. También nos permitirá controlar una parte sustancial y deliberada que pasará a formar parte de la *Intranet profunda (concepto de 2.1.2).*

Otro factor de la concepción de este subsistema, es que es determinante para averiguar de cualquier URL, cuál es su servidor web o host de procedencia *(elemento de 2.1.4),* del mismo modo, es determinante para construir URL´s por cuánto estas integran la parte del servidor web o host.

Los datos que se registran de un servidor son:

—*Dirección IP,* en la mayoría de servidores se asume es estática, aunque es editable.
Ejemplo: «10.167.13.21»

—*Dominio,* solo en el caso que el servidor esté integrado en un dominio, se registrará el nombre de dicho dominio.
Ejemplo: «dominius.es»

—*Alias DNS,* solo en el caso que el servidor esté integrado en dominio, se registrarán múltiples valores, uno por cada Alias DNS que tenga el servidor en dicho dominio.
Ejemplo: el servidor «10.167.13.21» está integrado en el dominio «dominius.es», en el que tiene dos alias DNS: «ServidorMBCW» y «SRVMotor».

2.2.2. *Subsistema de aplicaciones*

El registro de aplicaciones permitirá categorizar ciertos contenidos web según el sistema de información, repositorio o base de procedencia dentro de la Intranet. Una misma aplicación puede estar compuesta de distintas trazas, cada una de ellas, referencia a:

—Un protocolo. *(elemento de 2.1.4)*
—Un servidor web o host. *(elemento de 2.1.4)*
—Un puerto en este servidor. *(elemento de 2.1.4)*
—Una ruta relativa en este servidor. *(elemento de 2.1.4)*
—Opcionalmente, una ampliación de la ruta relativa del punto anterior, que serviría para apuntar a uno de los portales web de la aplicación.

En estos campos existe una clara dependencia con el subsistema de servidores. Si una URL de un contenido web se divide en partes descritas (*2.1.4),* y existieran las siguientes coincidencias con alguna de las trazas de una aplicación:

—protocolo de traza = protocolo de contenido web
Ejemplo: (http = http)
—ip de servidor web de traza = ip de servidor web del contenido web
Ejemplo: (10.167.13.21 = 10.167.13.21)
—puerto de traza = puerto del contenido web
Ejemplo: (80 = 80)
—ruta relativa de traza está contenida por la izquierda en la ruta relativa del contenido web
Ejemplo: ('bibliotecas/vbd' es parte por la izquierda de 'bibliotecas/vbd/ejemplos/1')

Se confirmaría entonces que el contenido web pertenece a la misma aplicación que la traza correspondida. En una Intranet, es especialmente relevante el hecho de conocer las posibles aplicaciones de procedencia de los contenidos web por los siguientes motivos:

—Las aplicaciones podrán ser priorizadas para indexación de sus contenidos web.
—Sus contenidos web podrán ser ponderados favorable o desfavorablemente en el proceso de ordenamiento de los resultados de una búsqueda efectuada por un usuario.
—El usuario podrá realizar búsquedas avanzadas por aplicación de procedencia.
—En el momento de la presentación de los resultados de una búsqueda, el usuario podrá conocer de antemano, la aplicación de procedencia de cada resultado de búsqueda.

2.2.3. *Subsistema de web crawler*

Este subsistema es una especificación del subsistema de web crawler descrito en la arquitectura común del motor de búsqueda *(2.1.1)*, hasta ahora se sabe que es dependiente al subsistema de servidores por cuanto indexa únicamente los contenidos web publicados por los servidores registrados en el sistema, y qué en el momento de vincular los contenidos web con las distintas aplicaciones registradas en el sistema, establece una conexión con el subsistema de aplicaciones.

El objetivo principal de este subsistema es alimentar de forma controlada al repositorio de información vinculado al sistema,

para lo que indexará constantemente contenidos web de la Intranet, además en este asunto, deberá tratar también con la tasa de cambio de la web según se cita en el *problema de la abundancia*. Para afrontar esta tarea, se han creado dos tipos de procesos, complementarios e independientes entre sí:

—*Proceso de carga de contenidos web*

De forma abreviada, es el proceso del web crawler que tiene por misión indexar los contenidos web que NO han sido indexados, este proceso puede indexar por primera vez un contenido web si responde de manera apropiada a las siguientes cuestiones:

1. ¿Procede de un servidor web o host registrado en el sistema?

Respuesta válida: SÍ

2. ¿Ha sido alguna vez indexado?

Respuesta válida: NO

—*Proceso de actualización de contenidos web*

De forma abreviada, al contrario que el proceso anterior, es el proceso del web crawler que tiene por misión indexar los contenidos web que SÍ han sido antes indexados, este proceso puede actualizar o volver a indexar un contenido web previamente indexado, siempre que este responda afirmativamente a las siguientes cuestiones:

1. ¿Procede de un servidor web o host registrado en el sistema?

Respuesta válida: SÍ

2. ¿Ha sido alguna vez indexado?

Respuesta válida: SÍ

3. ¿Ha cambiado el contenido web desde la última vez que fue indexado?

Respuesta válida: SÍ

El proceso de actualización no tomará aleatoriamente los contenidos web a la hora de actualizarlos, para ello, se ha implementado un algoritmo de priorización de la actualización que actualmente funciona sobre los textos e hipertextos.

Factor	Descripción	Hipertexto	Texto
Factor 1 Formato	Bonifica según el tipo de contenido web.	+2	+0
Factor 2 Títulos vacíos	Si el título de un hipertexto es vacío o nulo, se penalizará. Del mismo modo sucede con los textos con nombre de archivo en blanco.	-50	
Factor 3 Por aplicación	Los contenidos web de en una aplicación, podrán ser bonificados o penalizados según la puntuación de esa aplicación.	(** Según aplicación)	
Factor 4 Hits	Cuantas más visitas tenga un contenido web, más bonificado será.	+1 por hit	
Factor 5 Más antiguos sin leer, primero	Cuantas más visitas tenga un contenido web, más bonificado será.	+ 5 x (días sin actualizarse)	
Factor 6 Los que más se actualizan, primero	Contra más reciente es un contenido web, más se le bonificará.	+ 5 x (*** rating de actualización)	

** Cada aplicación registrada, tendrá su propia puntuación.

** Cada contenido web tiene su propio rating de actualización, el cual es variable según se actualice:

Su valor mínimo e inicial es 0.

Si en una actualización, se detecta que SI ha sido modificado, su rating incrementará en 5.

Si en una actualización, se detecta que NO ha sido modificado, su rating decrementará en 1.

¿Qué tipo de contenidos serán indexados por el web crawler?

Para el web crawler, la totalidad de lo que se indexa son contenidos web, ahora bien, según la naturaleza del contenido web, este se categorizará como hipertexto, texto, imágenes, audio o video. Si un contenido web no se encuentra entre los formatos admitidos en su categoría, este no será indexado, en caso contrario, se indexarán los campos de su categoría o tipo de contenido, a los que en todo caso, se sumarán los campos que como contenido web también debe registrar.

Relación de herencia

Tipo de contenido	Formatos admitidos	Campos de indexación
Contenido web	Los admitidos por los tipos de contenido: hipertexto, texto, imagen, audio y video.	- Nombre y formato. - Fechas de creación, modificación, lectura. - Elementos de URL *(véase 2.1.4)* - Variables de estado.
Hipertexto	- Páginas web estáticas - Páginas web generadas dinámicamente.	- Título de la página web (<Title>) - Texto contenido
Texto	.pdf .doc / .docx .xls / .xlsx .ppt / .pptx Formatos de libre office.	- Texto contenido
Imagen	.jpg .png .gif	- Píxeles de altura - Píxeles de anchura
Audio	.mp3	- Duración
Video	.mp4 .flv	- Duración

¿Dónde se indexa lo rastreado por el web crawler?

En el repositorio de información o base de datos del sistema, existen dos almacenes de contenidos web que permiten este proceso:

—*Almacén de pre-contenidos web,* es un *almacén intermedio* de indexaciones que son previas a la indexación en el siguiente almacén de contenidos web.

Requisitos de entrada, se incluirá en este almacén todo aquello que rastree el web crawler, siempre que:
–Su procedencia sea de un servidor web registrado en el sistema.
–No se encuentre previamente registrado en este almacén.
–El formato debe encontrarse entre los admitidos según su naturaleza.

Composición, se compone de tres tipos de registros:

–Registros que están pendientes de ser evaluados exclusivamente por el «*proceso de carga de contenidos web*», con objeto de registrarlos o no, en el almacén final de contenidos web, tras su evaluación.
–Registros que fueron evaluados con éxito, y que tienen su reflejo en el almacén intermedio para que no se vuelvan a indexarse.
–Registros que fueron evaluados sin éxito, y que persisten en el almacén intermedio para que no se vuelvan a indexarse.

—Almacén de contenidos web, es un almacén final cuyos registros serán el alimento de las búsquedas generadas por los usuarios del sistema.

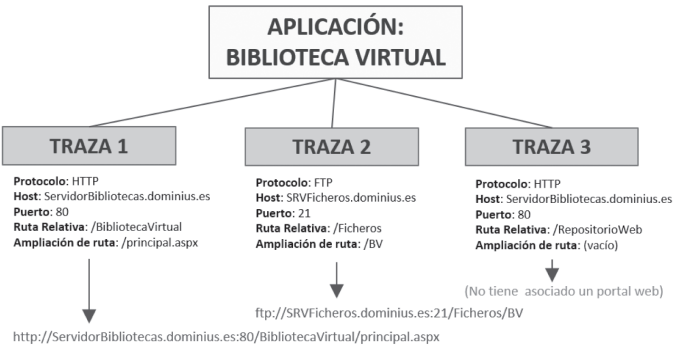
¿Cuándo se incluyen registros en el almacén intermedio de pre-contenidos web?

Existe la posibilidad en los siguientes tres casos:

1. Cuando las aplicaciones tengan registradas trazas que apunten a portales web, por registrar «*ampliaciones de la ruta relativa*» del subsistema de aplicaciones.
2. Tras la entrada de un registro en el almacén final de contenidos web, tras ser convenientemente evaluado por el «*proceso de carga de contenidos web*».
3. Tras una ejecutarse por el «*proceso de actualización de contenidos web*», una actualización de un registro del almacén final de contenidos web.

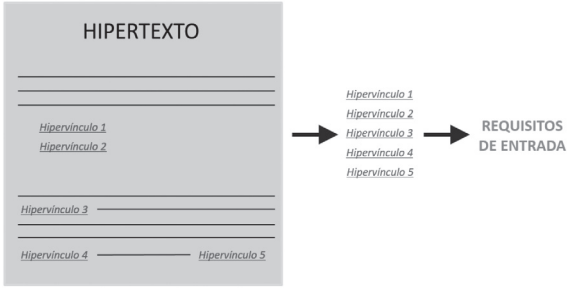
—En el caso 1, deben estar incluidos todos los registros procedentes de las aplicaciones registradas que apunten a

portales web, y que cumplan los «*requisitos de entrada*» del almacén intermedio de pre-contenidos web.



Ejemplo del caso 1: Las URL en verde se incluirán si cumplen los requisitos de entrada

—En los casos 2 y 3, si el registro es de tipo hipertexto, el subsistema recopilará todos los hipervínculos que contiene dicho hipertexto, y comprobará uno a uno, si cada una de las URL apuntadas por estos hipervínculos cumple con los «*requisitos de entrada*» del almacén de pre-contenidos web, en cuyo caso, las incluirá como nuevos registros.



Ejemplo del caso 2 y 3: Las URL en verde se incluirán si cumplen los requisitos de entrada

¿Cuándo se incluye un registro en el almacén final de contenidos web?

Cuando el «proceso de carga de contenidos web» evalúe adecuadamente un registro del almacén intermedio de pre-contenidos web, para lo que se debe satisfacer lo siguiente:

—Los componentes de la URL son válidos, y la URL responde adecuadamente.

—En el caso de los registros de texto e hipertexto, no existe en el almacén final de contenidos web un registro con título y contenido textual similares.

2.2.4. *Subsistema de búsquedas (search)*

Al igual que el subsistema de web crawler, este subsistema es una especificación del subsistema de búsquedas descrito en la arquitectura común del motor de búsqueda *(2.1.1)*. Tiene por misión atender las peticiones de información procedentes de los usuarios, a continuación, realizar las consultas internas correspondientes sobre el repositorio de información del sistema, y devolver finalmente un conjunto ordenado de resultados de búsqueda. Para su adecuado funcionamiento, ha sido imprescindible especificar en la implementación los siguientes aspectos destacados:

Tipos de búsqueda básicos

—Búsqueda predeterminada, es la búsqueda más pesada ya que busca en el título y contenido de hipertextos y textos que se encuentren indexados en el sistema. Adicionalmente, realizará una búsqueda de imágenes, e incluirá, si lo hubiera, un pequeño subconjunto de las imágenes resultantes en el cómputo total de resultados de búsqueda.
—Búsqueda de imágenes, es un tipo de búsqueda multimedia que buscará en los nombres de archivo y ruta relativa de las imágenes indexadas en el sistema.
—Búsqueda de audio, es un tipo de búsqueda multimedia que buscará en los nombres de archivo y ruta relativa de los audios indexados en el sistema.
—Búsqueda de video, es un tipo de búsqueda multimedia que buscará en los nombres de archivo y ruta relativa de los videos indexados en el sistema.

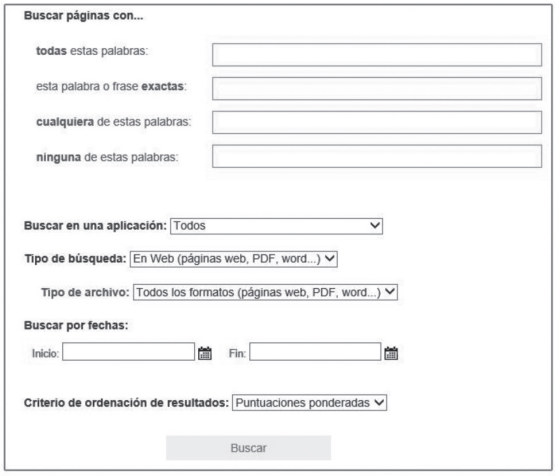
Coincidencias completas

El sistema encontrará el máximo número posible de coincidencias de explícita conformidad con los términos de búsqueda introducidos por el usuario, de forma qué de la totalidad de contenidos web indexados en el repositorio de información del sistema, se devuelvan aquellos donde exista al menos una coincidencia plena con los términos de búsqueda. El sistema no devol-

verá aquellos contenidos web que solo alcancen una coincidencia parcial con respecto a los términos de búsqueda.

Búsqueda avanzada

Al igual que la mayoría de los motores de búsqueda, existirá un tipo de búsqueda predeterminada, que se caracterizará por su simplicidad y sencillez de uso por parte de los usuarios con escasos conocimientos sobre este sistema. No obstante, en las redes Intranet por su naturaleza corporativa, es de gran importancia la implementación de buscadores avanzados que permitan a sus usuarios la posibilidad de realizar búsquedas más concretas con respecto a la búsqueda predeterminada; por este motivo, se ha seleccionado un conjunto de criterios de búsqueda de interés general, sobre lo que construir la búsqueda avanzada. Concretamente, y en sintonía con lo que pueda requerir el usuario en cada caso, el sistema realizará búsquedas avanzadas como producto de una combinación de los siguientes criterios:



Buscador avanzado con criterios por defecto sin cumplimentar

Desde el tipo de búsqueda predeterminada, también es posible realizar cierto tipo de búsqueda avanzada utilizando operadores de búsqueda; tomando como referencia el funcionamiento e importancia de estos operadores en los famosos motores de búsqueda de Internet, hasta ahora, se ha implementado un único operador de búsqueda:

Operador	Utilización
"	Al escribir en la búsqueda predeterminada una o varias palabras entre comillas, los resultados de búsqueda incluirán explícitamente aquellos contenidos web en los que aparecen esas palabras en el mismo orden. Ejemplo: "***trident juncture***"

Algoritmo de ordenación de resultados de búsqueda

Este algoritmo asigna una puntuación a cada resultado obtenido en una búsqueda, de forma que se presenten todos estos resultados en orden decreciente según su puntuación, con ello, se pretende que los primeros resultados de búsqueda sean los más relevantes de conformidad con la búsqueda inicial realizada por el usuario, además, cuanto mayor es el número de resultados de una búsqueda, mayor es la importancia de ordenarlos estratégicamente conforme a lo que el usuario espera encontrar.

La puntuación asignada a cada resultado de búsqueda es calculada en función de un conjunto de factores de ordenación, cada uno de estos factores tiene su propia puntuación que puede incluso ser negativa, de manera que la puntuación final de cada resultado de búsqueda coincide con la sumatoria de las puntuaciones ponderadas obtenidas por cada uno de los factores de ordenación que tenga asignado.

Hasta ahora se han implementado once factores de ordenación, a cada uno de ellos se le ha asignado uno o varios tipos de contenido web donde ejercer su influencia, el cálculo de puntuaciones por factor es orientativo.

Factor	Descripción
Factor 1 Repeticiones	Bonifica por coincidencias de una búsqueda en un contenido web. *Ejemplo: "trident juncture" aparece tres veces en un texto.*
Factor 2 Formato	Bonifica a distintos tipos de contenido web, es decir que hipertexto, texto, imágenes, audio y video pueden ser distintamente bonificados.
Factor 3 Títulos vacíos	Si el título de un hipertexto es vacío o nulo, se penalizará. Del mismo modo se penalizarán los textos con nombre de archivo en blanco.
Factor 4 Por aplicación	Los contenidos web categorizados en una aplicación, podrán ser bonificados o penalizados según la puntuación de esa aplicación.
Factor 5 Hits	Cuantas más visitas tenga un contenido web, más bonificado será.
Factor 6 Fecha de modificación	Contra más reciente es un contenido web, más se le bonificará.
Factor 7 Resolución	A mayor resolución tenga un contenido web (pixeles de altura x pixeles de anchura), más se le bonificará
Factor 8 Extensión	En un tipo de contenido web, se admiten distintos formatos, algunos bonifican más. *Ejemplo: los .pptx bonifican más que los .docx..*
Factor 9 Proximidad en título	Si una búsqueda coincide en el título o nombre de archivo, cuanto más próximos estén los términos de búsqueda, más se bonificará.
Factor 10 Proximidad en contenido	Si una búsqueda coincide en el texto contenido, cuanto más próximos estén los términos de búsqueda, más se bonificará.
Factor 11 Excedente en ruta relativa	Si un contenido web tiene una ruta relativa que se puede simplificar por otra ruta relativa más abreviada, se le penalizará.

Factor	Hipertexto	Texto	Imagen	Audio	Vídeo
Factor 1 Repeticiones	+3 por repetición				
Factor 2 Formato		+3			
Factor 3 Títulos vacíos	-100	-50			
Factor 4 Por aplicación	(** Según aplicación)				
Factor 5 Hits	+1 por hit				
Factor 6 Fecha de modificación		< 7 días, +30 < 30 días, +8			
Factor 7 Resolución			< 250000, +2 < 5000, +1		
Factor 8 Extensión			.png, +2 .jpg, +1		.mp4, +50 .flv, +58
Factor 9 Proximidad en título	(*L1) exacto, +150 (*L1) + 10 palabras, +50		(*L1), +150 (*L1+8), +60		
Factor 10 Proximidad en contenido	(*L1) exacto, +120 (*L1) + 10 palabras, +40				
Factor 11 Excedente en ruta relativa	-10				

** L1 es el nº de palabras que conforman una búsqueda.*
Ejemplo: «trident juncture»serían 2 palabras

*** Cada aplicación registrada, tendrá su propia puntuación*

—Módulo de sugerencias

En cada letra que introduce un usuario durante la construcción de sus términos de búsqueda, el sistema consultará rápidamente los títulos de los contenidos web indexados, e irá devolviendo aquellas sugerencias donde existan coincidencias con la búsqueda parcial del usuario. Para no sobrecargar al sistema, se requiere que el usuario ingrese al menos tres caracteres para entrar en funcionamiento. Las sugerencias orientan al usuario sobre algunos títulos que se encuentran indexados en el sistema, y que coinciden con su búsqueda en construcción.

2.2.5. *Subsistema de registros de búsqueda y hits*

Este subsistema tiene por objetivo llevar un registro de carácter estadístico de las búsquedas realizadas contra el sistema y de los hits, con el objeto de extraer una serie de conclusiones estadísticas que podrían resultar de alto valor para la organización propietaria de la Intranet. Como consecuencia de una masiva explotación del sistema por parte de los usuarios, podría generarse en este subsistema un importante volumen de datos a gran escala. Este subsistema es capaz de identificar a los usuarios contra el dominio de la organización, de forma qué tras ejecutarse la búsqueda de un usuario, el subsistema podría registrar algunos datos públicos que tiene este usuario en el dominio de la organización, es decir, que de una búsqueda efectuada por un usuario este subsistema podría registrar los siguientes datos:

—Términos de búsqueda introducidos
—Tipo de búsqueda utilizada
—Fecha/hora de la búsqueda
—Tiempo total de ejecución de la búsqueda

Actualmente, a pesar de su correcta implementación, este subsistema se encuentra pendiente de entrar en servicio; no solo es preciso revisar la Ley Orgánica de Protección de Datos (LOPD), también se deben concluir los trámites jurídicos correspondientes en el seno de la organización.

2.2.6. *Subsistema de etiquetas multimedia*

Cada contenido web de tipo multimedia (imágenes, audio y video) que se encuentre registrado en el sistema, tiene indexado un nombre de archivo y una ruta relativa (concepto de 2.1.2), los cuales son los únicos campos indexados por el web crawler sobre los que el subsistema de búsquedas (search) consultará las coincidencias de búsqueda, esto en ocasiones plantea problemas para que ciertos contenidos web de tipo multimedia puedan ser encontrados, ya que su verdadero contenido no se corresponde con el valor de ambos campos.

Ejemplo: Esta imagen que debería encontrarse buscando por «flor», «flora», «flores», «margarita», «margaritas» u otras relacionadas. No podrá encontrarse, ya que ni el nombre de archivo ni la ruta relativa guardan relación alguna con el contenido de la imagen. http://servidorMBCW.dominius.es:80/galeriaFotos/DSC03245_640x384.jpg

Este subsistema tiene por objetivo que sean los propios usuarios del sistema, los que asignen manualmente etiquetas a los contenidos web de tipo multimedia, de forma que el subsistema de búsquedas (search) pueda encontrar contenidos web de tipo multimedia, también por las posibles coincidencias de sus etiquetas con la búsqueda generada.

2.2.7. *Subsistema de configuración general*

Los usuarios que tengan el rol de administrador del sistema, en general, podrán establecer configuraciones, ejecutar procesos y realizar consultas de explotación.

—Ejecutar el proceso de carga, existen cuatro tipos:

- Normal, evalúa cualquier registro del *almacén intermedio*.
- Por servidor, evalúa registros del *almacén intermedio* que sean de un mismo host.
- Por aplicación, evalúa registros del *almacén intermedio* que sean de una aplicación.

- Evaluar una URL específica, si no se encuentra en el *almacén intermedio* se incluirá siempre que cumpla las reglas de entrada de dicho almacén.

—Ejecutar el proceso de actualización, existen cuatro tipos:
- Normal, actualiza cualquier registro del *almacén final*.
- Por servidor, actualiza registros del *almacén final* que sean de un mismo host.
- Por aplicación, actualiza registros del *almacén final* que sean de una aplicación.
- Actualizar una URL específica del *almacén final*

—Establecer modificaciones sobre las ponderaciones que ejercen los distintos factores de los siguientes algoritmos:
- Algoritmo de ordenación de resultados de búsqueda
- Algoritmo de priorización de la actualización

—Consultar estadísticas de explotación:
- Errores en los procesos de indexación
- Estadísticas de las consultas de los usuarios, como por ejemplo, los tiempos medios de ejecución de las respuestas.

—Crear, consultar, editar y eliminar registros de los siguientes subsistemas:
- Subsistema de servidores
- Subsistema de aplicaciones, incluyendo trazas de aplicación

—Desactivar contenidos web considerados ilícitos, para que el subsistema de búsqueda no los encuentre.

—Establecer configuraciones:
- Elementos por paginación de resultados de búsqueda.
- Número de sugerencias a mostrar.
- *timeout* en segundos para indexar un contenido web.
- Otros…

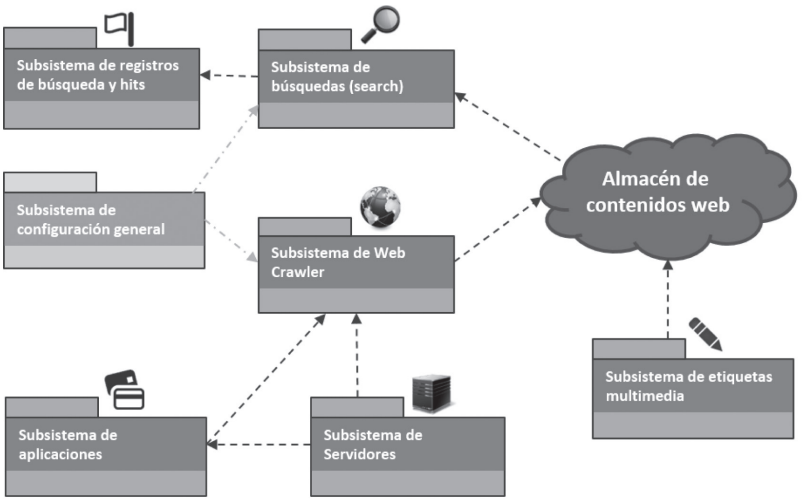


Diagrama de subsistemas y dependencias fuertes

2.3. *Posibles implementaciones pendientes*

—Big data. Una vez se alcancen importantes volúmenes de datos en:

- Contenidos web indexados.
- Registros de búsqueda y hits generados por interacción de usuarios contra el sistema.

Es momento de plantear un análisis de patrones sobre estos datos, que permita trabajar con modelos predictivos sobre los contenidos de la Intranet, así como de las tendencias de búsqueda de los usuarios. Su conocimiento aproximado, podría repercutir considerablemente en la calidad de este sistema, especialmente en la ponderación que ejercen todos los factores que intervienen en los algoritmos utilizados por el sistema.

—Base de datos distribuida. Otra de las consecuencias de alcanzar importantes volúmenes de datos, es que podría surgir la necesidad de implicar más de una unidad de disco donde almacenar los datos, e incluso ampliar el número de servidores de bases de datos con el mismo fin. Es determinante en estos casos, procurar un sistema fácilmente escalable, de forma que la integración de nuevas unidades de disco o servidores no genere problemas adicionales.

—Tesauro o diccionario. Se trata de obtener diccionarios de sinónimos y/o términos relacionados, con objeto de ampliar y mejorar las búsquedas de los usuarios. Llegado el caso, se podría plantear el uso de traductores externos que permitan recíprocamente las traducciones entre el español y distintos idiomas extranjeros.
—Carga concurrente. Para aumentar la tasa de rastreo e indexación del web crawler, es preciso aumentar el número de máquinas dedicadas exclusivamente a esta tarea, las cuales, estarán en constante interconexión con los servidores de base de datos.
—Software de reconocimiento de imágenes. Se trata de obtener un software capaz de interpretar imágenes generando etiquetas que identifiquen su contenido, de forma que el subsistema de etiquetas multimedia pueda funcionar autónomamente, con el objetivo de favorecer que un gran número de imágenes puedan ser encontradas.
—Algoritmo de priorización de la carga. Está por implementar un algoritmo de priorización de la carga, que regule el orden de prioridad en que se van indexando los contenidos web mediante este proceso.

Conclusión

En este tipo de sistemas, no solo basta con que las cosas funcionen, por supuesto, han de funcionar, pero la forma en que ha de ser, es probablemente la cuestión compleja, es aquí donde intervienen los grandes procesos de optimización de base de datos, donde se pone al límite las prestaciones del hardware de los servidores, y donde se exige el conocimiento de los últimos avances, por cuánto se procura el mejor rendimiento, y disminuir el elevado esfuerzo computacional que requiere un sistema de estas características, el cual está en continua expansión, y tiene que actualizarse conforme a la gran tasa de cambio de la web.

Este sistema está concebido para crecer poco a poco y de forma controlada, acotándose desde un principio el área de actuación del web crawler, y ampliándose el coto conforme se disponga de los recursos y tecnología que sean necesarios en cada etapa.

Agradecimientos

A la Sección de Gestión del Conocimiento de la Dirección de Investigación, Doctrina, Orgánica y Materiales, por entender el alcance de este proyecto, y por depositar su confianza en mi persona.

Referencias bibliográficas

Ruiz Carrasco, Alejandro; «Casuística derivada de la posible explotación de un motor de búsqueda de contenidos web en una red Intranet organizacional». Comunicación en el I Congreso Internacional de Estudios Militares Granada, 17-19 de septiembre de 2014.

Arredondo Gonzalo, Pablo y Sáiz-Pardo Lizaso, Manuel; «Visión general de la gestión del conocimiento en el Ejército», Comunicación del I Congreso Internacional de Estudios Militares, 2014.

«Especificaciones», GOOGLE INC. https://support.google.com/gsa/answer/4411411?hl=en&ref_topic=4564260

«Arquitectura», ORACLE, http://www.oracle.com/technetwork/es/database/317491-esa.pdf

«Esp. SQLServer», MICROSOFT, http://msdn.microsoft.com/es-es/library/ms143432(v=sql.100).aspx

«The Top 500 sites on the web», ALEXA (AN AMAZON COMPANY) http://www.alexa.com/topsites

NOTA BIOGRÁFICA DE LOS AUTORES

Marcos Gómez es actualmente jefe del Departamento de Defensa Nuclear de la EMDNBQ. Ha realizado, entre otros, el curso de Especialista en Defensa NBQ, el curso de Riesgos NBQ y el curso de empleo de armamento nuclear de la OTAN y Proliferación nuclear. Ha escrito e impartido conferencias sobre temas relacionados con la proliferación nuclear.

José Manuel Rodríguez-González es Doctor en Psicología. Profesor Titular de las facultades de Psicología y Derecho, Universidad de Sevilla. Profesor de la Escuela de Seguridad Pública de Andalucía: Consejería de Justicia e Interior. Responsable del Grupo de Investigación CTS 441 Intervención Psicológica: Promoción de la Salud y la Seguridad. Máster Universitario en Estudios Estratégicos y Seguridad Internacional, MADOC-Universidad de Granada. Título de Experto Universitario en Análisis del Terrorismo Yihadista, Insurgencias y Movimientos Radicales, Universidad Pablo de Olavide de Sevilla.

María del Pilar Ceballos-Becerril es Psicóloga. Miembro del Grupo de Investigación CTS 441 Intervención Psicológica: Promoción de la Salud y la Seguridad. Responsable del Dpto. de Educación para el Desarrollo en Fundación Tierra de hombres. Docente Colaboradora de la Escuela de Seguridad Pública de Andalucía: Consejería de Justicia e Interior. Máster Universitario Oficial en Psicología General Sanitaria. Universidad de Sevilla. Máster en Psicología Jurídica y Peritaje Psicológico Forense. Universitat de València. Máster Universitario Oficial en Psicología de la Salud. Universidad de Sevilla.

Pedro Álvarez Nieto es Teniente Coronel. Director del Departamento de Ciencias Jurídicas y Sociales de la Academia de Artillería. Analista experto en Relaciones Internacionales del Observatorio Permanente del Ejército de Tierra Español. Miembro del Grupo de Investigación CTS 441 Intervención Psicológica: Promoción de la Salud y la Seguridad. Experto en Relaciones Internacionales,

Univ. Rey Juan Carlos. Director y Coordinador de los cuatro Ciclos de Estudios Europeos (2010-2014) entre la Cátedra Jean Monnet (UE) de la IE University y la Academia de Artillería.

Pablo Rey García es Doctor en Comunicación. Profesor Encargado de Cátedra, Facultad de Comunicación, UPSA. Miembro del Grupo de Investigación CTS 441 Intervención Psicológica: Promoción de la Salud y la Seguridad. Máster en Paz, Seguridad y Defensa por el IU Gutiérrez Mellado-UNED. Diplomado en Estudios Avanzados en Historia Contemporánea, por la Universidad de Salamanca. Experto y Especialista en Resolución Pacífica de Conflictos y Mantenimiento de la Paz por el IU Gutiérrez Mellado-UNED. Especialista en Fundamentos de la Paz, la Seguridad y la Defensa, por la misma universidad.

Ana Belén Perianes Bermúdez es Doctora en Paz y Seguridad Internacional. Experta en Seguridad en el Mediterráneo, Próximo Oriente y Oriente Medio. Máster en Dirección de Recursos Humanos. Politóloga y especializada en asuntos exteriores; seguridad europea; mujer, paz y seguridad; ciberseguridad y política exterior estadounidense. Miembro de la Junta Directiva de la Asociación de Diplomados Españoles en Seguridad y Defensa. Coordinadora de *Spanish Women in International Security*.

José Antonio Restón Cantoy es oficial del Ejército de Tierra. Licenciado en Sociología. Especialista Universitario en Seguridad en el Mediterráneo, Próximo Oriente y Oriente Medio. Experto Universitario en Comunicación Pública y Defensa. Participación en distintas operaciones militares Bosnia y Herzegovina (1996), Kosovo (1999 y 2008), Iraq (2003) y Afganistán (2006).

Milton Meza Rivas es Abogado egresado en Venezuela. Doctorando en Derecho y Ciencia Política y Magister en Ciudadanía, Derechos Humanos, Ética y Política de la Universidad de Barcelona y Universidad de Girona. Observador de la reunión de expertos en la ONU sobre sistemas de armas autónomas letales. Ha sido Ministro Consejero ante la Corte Penal Internacional, Tribunal Especial para la Ex-Yugoslavia y la Corte Internacional de Justicia en La Haya; y delegado ante el Consejo de Derechos Humanos y la Conferencia de Desarme de la ONU-Ginebra (Suiza).

José Antonio Herráiz Reyes. Coronel de Infantería, Diplomado de Estado Mayor por España y Argentina. Doctor por la Universidad de León. Diplomado en Inteligencia Estratégica por la Escuela Superior de Guerra del Ejército Argentino. Diplomado superior de

seguridad por el Ejército de Tierra Español. Curso de información de la Guardia Civil. Diplomado en operaciones especiales y en el mando de unidades paracaidistas. Diploma de especialista en psicología militar. Premio extraordinario de la Escuela Superior de Guerra del Ejército Argentino.

Néstor Soiza Vázquez. Capitán de Transmisiones LXV promoción EO, destinado en el Regimiento de Transmisiones 21 BCTPCCE I/21. Graduado en Ingeniería de Telecomunicaciones por la Universidad Europea de Madrid. Participación en la instalación de la primera red certificada española en OTAN como jefe de instalación del proyecto en la red AMN (AFGAN MISSION NETWORK) en Herat y PSB «Ruy Gónzalez de Clavijo» en Qala-i-Naw (2012). Participación en misiones internacionales OP LH XV, ASPFOR XXX, OP LVXVII, Repliegue QiN ASPFOR XXIII, OP LH XXIV.

Pablo Lobato de Enciso es Teniente Psicólogo. Master Oficial en Intervención Psicológica en Contextos de Riesgos por la Universidad de Cádiz. Master en Psicología Clínica Legal y Forense por la Universidad Complutense de Madrid. Master en práctica Clínica en Salud Mental por la Asociación Española de Psicología Clínica Cognitivo Conductual. Especialista Universitario en Intervención Cognitivo Conductual en Niños y Adolescentes por la UNED. Experto Universitario en Estadística Aplicada en Ciencias de la Salud por la Fundación UNED.

Manuel J. Gazapo Lapayese es Director del International Security Observatory y miembro del Grupo de Investigación de Paisaje Cultural de la Universidad Politécnica de Madrid. PhD Candidate. Máster en Asuntos Internacionales por la Universidad Pontificia Comillas ICADE. Graduado en Relaciones Internacionales por la Universidad Complutense de Madrid. Diplomado en Economía, Seguridad y Política por Georgetown University.

Alejandra Hernández González es Abogada. Máster en Operaciones contra el Terrorismo Yihadista (CISDE). Parte del Grupo de Investigación Académica de Financiación Terrorista (CISDE). Especializaciones: DIH y Operaciones de Paz, Gestión Internacional de Crisis, Crimen Organizado Transnacional en IUGM. Con publicaciones en las Jornadas de Seguridad IUGM, IV Congreso de Seguridad y Defensa, I Congreso de Estudios Militares y, II Congreso de Terrorismo.

Luis Antonio Álvarez Álvarez es Doctor Ingeniero Industrial, Profesor Titular de Universidad en la ULPGC. Imparte docencia

en el Grado en Tecnología Industriales y en el Grado en Seguridad y Control de Riesgos, en el Máster de Investigación en Tecnologías Industriales y en el en el Programa de Doctorado de Tecnologías de la Información y sus Aplicaciones. Ha sido director de la ETSII y Vicerrector de Ordenación Académica y EEES de la ULPGC. En la actualidad es director del «Proyecto Open ULPGC» y miembro de la ANECA para la evaluación de los títulos de Grado de Ingeniería y Arquitectura.

Celso Perdomo González es Doctor en Tecnologías de la Información y sus Aplicaciones, ULPGC, Ingeniero Industrial. Profesor asociado a tiempo parcial de la ULPGC desde 2003 hasta la actualidad. Funcionario de carrera Inspector-Analista de Servicios en el Cabildo Insular de Gran Canaria desde el 2000 hasta la actualidad.

Ana Belén Valverde Cano es Licenciada en Derecho por la Universidad de Granada desde 2014 y en la actualidad es estudiante de Doctorado. Está realizando su investigación con el Proyecto I+D+I: «Formas contemporáneas de esclavitud y derechos humanos».

José Antonio Castillo Parrilla es Licenciado en Derecho por la Universidad de Granada desde 2013 y en la actualidad es estudiante de Doctorado. Está realizando su investigación a través de una beca de Formación del Profesorado Universitario desde el año 2014.

Ramón Orza Linares es Profesor del Departamento de Derecho Constitucional de la Universidad de Granada y Doctor en Derecho, desde 1989. Ha sido Secretario y Vicedecano de la Facultad de Derecho de la Universidad de Granada (1996-2004). Las líneas de investigación desarrolladas en los últimos años se centran en la influencia de las TIC's en el ejercicio de los derechos fundamentales y en el funcionamiento de la sociedad democrática.

Alejandro R. Mosteo es profesor del Centro Universitario de la Defensa de Zaragoza desde 2011. Obtuvo su doctorado en 2010 en la Universidad de Zaragoza, donde pertenece al grupo de Robótica, Percepción y Tiempo Real del Instituto de Investigación en Ingeniería de Aragón. Su investigación aborda los sistemas robóticos distribuidos: cooperación multi-robot, algoritmos descentralizados y comunicaciones escalables.

David Copé de los Mozos es actualmente el Jefe del Departamento de Informática de la Academia de Ingenieros y profesor, entre otras, de la asignatura de Seguridad de los Sistemas de

Información. Entre los cursos que ha realizado son de destacar, el Curso para la Obtención del DIM y el Curso de Especialidades Criptológicas. Durante su actual empleo de comandante ha estado destinado en la Academia de Ingenieros del Ejército de Tierra y en la Unidad Militar de Emergencias.

Marina Rojo Gallego-Burín, es Licenciada en Derecho. Máster Universitario en Derecho Internacional y Relaciones Internacionales de la Universidad de Granada. Matriculada en el Programa de Doctorado de Ciencias Jurídicas, dentro de la línea de investigación: Metodología e Historia del conocimiento y argumentación jurídica. Evaluación legislativa y aplicación del Derecho. Realiza su tesis doctoral bajo la dirección del Prof. Dr. D. José Antonio López Nevot, Catedrático de Historia del Derecho y de las Instituciones de la Universidad de Granada. Miembro del grupo de investigación: Justicia y Gobierno en la Historia del Derecho Español y Europeo.

Diego Becerril Ruiz es Profesor Titular de Universidad del Departamento de Sociología de la Universidad de Granada. Director del Grupo de investigación SEJ131 «Análisis de la Vida Social». Sus principales líneas de investigación: familia, juventud, estructura social, TIC y dependencia. Investigador en múltiples proyectos de I+D+I y profesor invitado en universidades internacionales (Harvard, Sorbona, Sapienza, La Habana).

José Manuel García Moreno es Profesor Ayudante Doctor en la Universidad de Granada. Doctor en Sociología por la Universidad de Granada. Master en Márketing y Gestión Comercial por ESIC (Madrid). Premio Nacional de Terminación de Estudios de Sociología en 2001. Miembro de la Red Internacional Homeshare International Research Advisory Group (HIRAG). Ha participado en proyectos de investigación I+D desde el año 2001 centrados tanto en Sociología de la Familia como en el ámbito de la Sociología del Trabajo y de las Organizaciones.

Mónica Luque Suárez es Licenciada en CC. Políticas y Sociología por la UNED. Doctora en Sociología por la UGR. Actualmente, Profesora Asociada desde 2010 en la Facultad de Educación y Humanidades de Melilla. Tutora del Centro Asociado-UNED de Melilla desde 2001. Socióloga y Coordinadora de Transnacionalidad en el Proyecto Europeo EQUAL 2005-2007. Directora del Centro de Menores de Melilla «Fuerte de la Purísima» (2001-2004)

Benigno Antonio Maújo Iglesias es miembro de la Asociación ARES de Reservistas Españoles (Asturias), Delegación de Defensa

en el Principado de Asturias. Abogado, MBA, Docente, Alférez Auditor (RV) Cuerpo Jurídico Militar.

Francisco Díaz de Otazú Guerri es miembro de la Asociación ARES de Reservistas Españoles (Asturias), Delegación de Defensa en el Principado de Asturias. Profesor de Enseñanza Secundaria, Historiador, Teniente (RV) de Infantería de Marina.

José Antonio López Díaz pertenece a la Asociación ARES de Reservistas Españoles (Asturias), Delegación de Defensa en el Principado de Asturias. Profesor de Enseñanza Secundaria, Ingeniero, Alférez de Fragata (RV).

Claudia Pérez Fornies es Directora de la Cátedra Paz, Seguridad y Defensa de la Universidad de Zaragoza y el Ministerio de Defensa. Profesora Titular del Departamento de Estructura e Historia Económica y Economía Pública de la Facultad de Economía y Empresa de dicha Universidad es Doctora en Economía de la Defensa y Diplomada en Altos Estudios de la Defensa por el CESEDEN. Ha publicado artículos y libros relacionados con actividades de seguridad y defensa en revistas nacionales e internacionales y de reconocido prestigio como Defence and Peace Economics.

Juan José Aizpuru Díaz de Terán Coronel de Intendencia del Ejército de Tierra (Reserva), diplomado en Estudios Económicos de Aplicación Militar, Master en Seguridad Global y Defensa por la Universidad de Zaragoza. Ha estado destinado en la Academia General Militar como profesor, en la Jefatura de Asuntos Económicos del Mando de Apoyo Logístico del Ejército como responsable de la gestión económica y como Jefe de la Jefatura de Administración Económica de la Inspección General de Sanidad de la Defensa. Ha participado en dos operaciones en el exterior: Afganistán.

Elia Breijo Pena. Licenciada en Administración y Dirección de Empresas por la Universidad Francisco de Vitoria y Máster en Logística y Gestión Económica de la Defensa (UCM y CESIA, Centro de Estudios Superiores de Intendencia de la Armada). Finalista en el premio Robin Cosgrove, Edición Iberoamericana 2012-2013 con el artículo «Sentido Común». Jefe de Proyectos en Thales España GRP SAU.

José Ignacio López Sánchez. Licenciado y Doctor en Ciencias Económicas y Empresariales Universidad Complutense de Madrid (UCM). Profesor de Organización de Empresas (Acreditado a Catedrático de Universidad) de la asignatura de Herramientas de

Apoyo a la Dirección del Máster en Logística y Gestión Económica de la Defensa (UCM y CESIA, Centro de Estudios Superiores de Intendencia de la Armada). Director de *Universia Business Review y Associate Editor del Journal of Globalization, Competitiveness and Governability (Georgetown University-Universia)*

José Ramón Coz es Doctor cum laude en Economía por la Universidad Complutense de Madrid y Doctor cum laude en Ingeniería Informática por la UNED. Además, es Licenciado en Ciencias Físicas por la Universidad de Cantabria y Grado Máster en Logística y Economía de la Defensa por la Universidad Complutense de Madrid. En la actualidad, trabaja como Auditor de proyectos de Ciberseguridad para la OTAN y es investigador en el Departamento de Economía Aplicada VI de la Universidad Complutense de Madrid.

Antonio Martínez de Baños Carrillo es Teniente Coronel, Director del Departamento de Idiomas de Academia General Militar. Es Doctor en Conflictos por la Universidad de Zaragoza. Posee el Máster en 'Seguridad y Defensa' por la Universidad a Distancia y el Instituto «General Gutiérrez Mellado». También el Máster en 'E-learning' por la Universidad de Salamanca. Ha sido BASE COMMANDER de la base internacional de SFOR in Mostar (Bosnia) EN 2004. Ha impartido clases en West Point, Estados Unidos.

Manuel Sáiz-Pardo es comandante del «Cuerpo de Ingenieros Politécnicos» del Ejército, es «Ingeniero Electrónico» por la Universidad de Granada; «Ingeniero de Armamento y Material» por la Escuela Politécnica Superior del Ejército; «Diploma de Estudios Avanzados» por dicha Escuela del Ejército; «Experto Universitario en Metodología de la Investigación y Análisis Prospectivo», título propio de la Universidad de Granada, entre otros. Actualmente está destinado en la Sección de Gestión del Conocimiento, en particular, como administrador de la Enciclopedia Militar Digital (Milit@rpedia).

Alejandro Ruiz es Teniente y obtuvo por la Universidad de Granada los títulos de Ingeniero en informática, Máster oficial en desarrollo del software, diplomado en Estadística y el CAP. Se ha especializado en la Ingeniería del software y en el desarrollo de software corporativo bajo los entornos IBM Notes y Microsoft .NET, y es conocedor de la gran importancia que tiene la formación y la constante actualización de conocimientos en estos campos.