Cuadernos de la Guardia Civil

Revista de Seguridad Pública

Núm. 50-2015

GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR
GUARDIA CIVIL
DIRECCIÓN GENERAL

CUADERNOS DE LA GUARDIA CIVIL

REVISTA DE SEGURIDAD PÚBLICA

3ª ÉPOCA

SECRETARÍA:

Centro de Análisis y Prospectiva

Centro de Análisis y Prospectiva de la Guardia Civil
Guzmán el Bueno, 110
28003 MADRID
Teléf. 91 514 29 56
E-mail: CAP-cuadernos@guardiacivil.org

AUTORA Y PROPIETARIA

Dirección General de la Guardia Civil
ISSN: 2341-3263
NIPO: 126-14-006-3

EDITA

Ministerio del Interior
Secretaría General Técnica
Dirección General de la Guardia Civil
Centro Universitario de la Guardia Civil

Página oficial de Cuadernos de la Guardia Civil
http://bit.ly/1Fdw213

Lista de los números en KOBLI
http://bibliotecasgc.bage.es/cgi-bin/koha/opac-shelves.pl?viewshelf=59&sortfield=

Catálogo general de publicaciones oficiales
http://publicacionesoficiales.boe.es/

A lo largo de los años, la Guardia Civil ha venido haciendo una gran labor divulgativa con la publicación de la Revista de Estudios Históricos, lo que ha contribuido a la comprensión de su carácter, su tiempo, sus actividades y funciones.

Desde 1989 este esfuerzo en difusión de cultura de seguridad ha desembocado en la elaboración de los "Cuadernos de la Guardia Civil".

Se trata de una publicación académico profesional, de contenidos originales y periodicidad semestral, con contenidos relevantes sobre seguridad nacional, seguridad pública, técnica policial, riesgos y amenazas, en todas sus dimensiones (histórica, jurídica, estratégica, táctica, etc.). Los géneros documentales admitidos son los artículos de investigación, los artículos profesionales, y la reseña de libros. Los destinatarios son expertos en seguridad, académicos y profesionales, tanto del sector público y privado, estudiantes, así como cualquier ciudadano interesado en la materia.

Cuadernos de la Guardia Civil está abierta a cualquier autor, a cuyos efectos se establecen dos periodos para la recepción de artículos: el 1 de mayo y el 1 de noviembre. El primer número de cada año se publica durante el mes de enero, y el segundo durante el mes de julio. Se pueden publicar adicionalmente números especiales o suplementos. Los artículos propuestos serán enviados respetando las normas de publicación que figuran al final del número. Las propuestas se pueden enviar en formato electrónico a: CAP-cuadernos@guardiacivil.org

La evaluación y selección de los artículos se realiza previa evaluación mediante un sistema por pares, en el que intervienen evaluadores externos a la editorial, y posterior aprobación por el Consejo Editorial. Los artículos pueden ser escritos en español, inglés o francés.

La Revista Cuadernos de la Guardia Civil se compromete a mantener altos estándares éticos, y especialmente el "Code of conduct and best practices guidelines for journal editors" del Committee on Publication Ethics (COPE).

Los contenidos de la Revista Cuadernos de la Guardia Civil se encuentran referenciados en los siguientes recursos de información: LATINDEX, DICE (Difusión y Calidad Editorial de las Revistas Españolas de Humanidades y Ciencias Sociales y Jurídicas) y DIALNET.

Especial referencia merece su inclusión en el sistema bibliotecario de la Administración General del Estado, a través de la Plataforma KOBLI:

http://bibliotecasgc.bage.es/cgi-bin/koha/opac-shelves.pl?viewshelf=59&sortfield=

Este servicio permite consultar y realizar búsquedas por cualquier criterio bibliográfico (autor, tema, palabras clave…), generar listas. Permite la descarga en formatos PDF, Mobi y Epub. Adicionalmente es posible la suscripción a un sistema de alerta, cada vez que se publique un nuevo número, solicitándolo a la cuenta : CAP-cuadernos@guardiacivil.org.

ÍNDICE

DOSSIER: CRIMEN ORGANIZADO

ARTÍCULOS

RESEÑA DE LIBROS

¿POR QUÉ CRECEN LOS VÍNCULOS ENTRE TERRORISMO Y CRIMEN?

LUIS DE LA CORTE IBÁÑEZ

RESUMEN

Este artículo aborda las relaciones entre terrorismo y criminalidad común y organizada, también conocidas en la literatura especializada como “nexo terror-crimen”. Para ello se presta atención a las diversas percepciones al respecto, sus posibles modalidades y las principales actividades delictivas involucradas. A continuación se analizan las causas que posibilitan e inducen la implicación terrorista en actuaciones y relaciones delictivas, esbozando un modelo sobre las mismas y una revisión suplementaria sobre los factores endógenos y exógenos con capacidad para potenciar dicha implicación. Finalmente, se pasa revista a las consecuencias que pueden derivarse de la convergencia entre terrorismo y delincuencia común y organizada y se extraen conclusiones al respecto.

Palabras clave: Terrorismo, Crimen, Crimen organizado, Convergencia, Nexo Terror-Crimen

ABSTRACT

The present article review the relationship among terrorism and crime and organized crime. The so called Crime-Terror Nexus is approach taking in account the discrepancies about it, their different modalities and the mai criminal activity that the nexus involve. Then we outlining a theoretical model for explaining the involvement of terrorist actors in criminal activities. We also review the endogenous and exogenous drivers that increases the chances of the convergence between terrorism and crime. Finally, some consequences of convergence between terrorism and organized crime are discussed and common conclusions were drawn.

Key words: Terrorism, Crime, Organized Crime, Crime-Terror Nexus

1. INTRODUCCIÓN

De acuerdo con el Real Decreto 873/2014, aprobado por el Consejo de Ministros el pasado 10 de octubre de 2014, el Ministerio del Interior creará una subdirección general de la Secretaría de Estado de Seguridad resultante de la integración de las estructuras del Centro Nacional de Coordinación Antiterrorista (CNCA) y el Centro de Inteligencia Contra el Crimen Organizado (CICO). Las funciones asignadas al nuevo Centro de Inteligencia contra el Terrorismo y el Crimen Organizado (CITCO) son las de impulsar y coordinar la integración y valoración de cuantas informaciones y análisis operativos dispongan las Fuerzas y Cuerpos de Seguridad del Estado en materia de terrorismo, crimen organizado y radicalismo violento, elaborar inteligencia criminal estratégica a ese respecto, establecer criterios de actuación y coordinación operativa entre organismos concurrentes y diseñar estrategias globales de lucha contra los fenómenos citados.

Junto a la preocupación por optimizar recursos y eliminar duplicidades administrativas, el Ministerio del Interior añade como justificación complementaria para crear el CITCO tanto la existencia de vínculos directos y objetivos entre actividades terroristas e individuos involucrados en otras labores delictivas como la advertencia de crecientes similitudes en diversos patrones de actuación desarrollados por grupos terroristas y otras organizaciones criminales. Teniendo en cuenta las implicaciones de lo anterior y la relevancia del cambio institucional y estratégico que supondrá la aparición del nuevo organismo, parece un momento oportuno para examinar el problema de las interacciones entre terrorismo (o fenómenos insurgentes asociados) y otras modalidades criminales, particularmente la delincuencia organizada. Este artículo aborda el nexo terror-crimen y las diversas percepciones que sobre él existen, sus posibles modalidades y las principales actividades delictivas involucradas. A continuación se presta especial atención a las causas que posibilitan e inducen la implicación terrorista en actuaciones y relaciones delictivas, esbozando un modelo sobre las mismas y una revisión suplementaria sobre los factores endógenos y exógenos con capacidad para potenciar dicha implicación. Finalmente, se pasa revista a las consecuencias que pueden derivarse de la convergencia entre terrorismo y delincuencia común y organizada y se extraen conclusiones al respecto.

2. UN NEXO POSIBLE Y CRECIENTE

Durante décadas la hipótesis sobre la existencia de vínculos sustantivos entre terrorismo y otras modalidades de actuación criminal, en concreto la delincuencia común u organizada, ha sido contemplada con escepticismo[1]. El reflejo más evidente de esa postura remite a la tradicional separación orgánica de los departamentos y unidades con atribuciones en materia antiterrorista e investigación criminal, así como el abordaje teórico y académico igualmente diferenciado de cada de una de las problemáticas aludidas. En aparente congruencia con tales planteamientos, y aun admitiendo la posibilidad de conexión entre ambos e incluir algunos indicios y pruebas ocasionales, los informes anuales de EUROPOL sobre terrorismo y crimen organizado no han logrado identificar ninguna tendencia definitiva al respecto.

Sin embargo, desde hace ya varios años esa separación conceptual y organizativa ha comenzado a ser cuestionada por un creciente número de investigadores y expertos. Por lo pronto, en una resolución (1373) aprobada pocos días después de producirse los atentados del 11 de septiembre de 2001 en Nueva York y Washington, el Consejo de Seguridad de Naciones Unidas apuntaba:

(El Consejo de Seguridad) observa con preocupación la estrecha conexión que existe entre el terrorismo internacional y la delincuencia organizada transnacional, las drogas ilícitas, el blanqueo de dinero, el tráfico ilícito de armas y la circulación ilícita de materiales nucleares, químicos, biológicos y otros materiales potencialmente letales, y a ese respecto pone de relieve la necesidad de promover la coordinación de las iniciativas en los planos nacional, subregional, regional e internacional, para reforzar la respuesta internacional a este grave problema y a esta gran amenaza a la seguridad internacional[2].

La misma clase de advertencias volverían a reproducirse en otros documentos

1 Sobre esta controversia véase Frank Bovenkerk y Bashir Abou Chakra, “Terrorism and Organized Crime”, Forum on Crime and Society, 4, 1-2, 3-16, 2004.

2 Consejo de Seguridad de Naciones Unidas, Resolución 1373 (2001), 28/9/2001. Disponible en: http://www.acnur.org/biblioteca/pdf/6078.pdf?view=1

estratégicos posteriores emitidos por Naciones Unidas, otros organismos internacionales y numerosos países. En esa línea, la Estrategia de Seguridad Nacional aprobada por el gobierno de España en 2013 apunta como la constatación de vínculos cada vez más estrechos entre grupos u organizaciones criminales y terroristas supone un incremento sustantivo de la peligrosidad de ambos fenómenos para la seguridad de España[3]. Tal afirmación resulta plenamente congruente con varias conclusiones reveladas un año antes en un informe específico encargado por el Parlamento Europeo. Los autores del mismo advierten haber encontrado amplia evidencia sobre la existencia de un cierto "matrimonio de conveniencia" entre grupos terroristas y de crimen organizado dentro de los países pertenecientes a la Unión Europea[4].

Entre los principales argumentos y evidencias que hoy apoyan una reevaluación de las relaciones entre terrorismo y otras formas criminales destacan los que se detallan a continuación.

1. La citada relación no es natural o necesaria pero tampoco imposible o contra natura. Así lo demuestran numerosos ejemplos pasados y presentes de actores terroristas (grandes organizaciones, pequeños grupos o redes, individuos) implicados en la comisión de otros delitos. Sin ir más lejos y según datos proporcionados por el Ministerio del Interior el 20% de los individuos encarcelados en España entre 2005 y 2011 por su presunta vinculación a elementos yihadistas pasaron previamente por prisión como consecuencia de su participación en otras actividades delictivas. Aunque menos numerosos tampoco faltan ejemplos de actores relacionados con la delincuencia organizada que hayan perpetrado ataques y campañas violentas propiamente terroristas[5].

2. Mientras las conexiones entre actores terroristas y diversas formas de delincuencia menor han sido relativamente frecuentes en distintos escenarios, la convergencia entre terrorismo y criminalidad organizada ha sido y continúa siendo mucho más frecuente y extendida en áreas ampliamente afectadas por problemas de fragilidad y/o inestabilidad institucional.

3. De acuerdo con un número creciente de expertos, la escasez de pruebas que avalen vínculos significativos entre terrorismo y delincuencia organizada en países desarrollados y estables podría no deberse a la inexistencia de dicha clase de vínculos sino más bien al tratamiento compartimentado que sus agencias de seguridad e inteligencia conceden a tales amenazas. A fin de cuentas, resulta bastante más complicado encontrar pruebas sobre la convergencia entre dos fenómenos delictivos cuando, de entrada, los departamentos respectivamente ocupados en investigarlos no consideran plausible la confluencia entre ambos ni tampoco han sido estimulados a colaborar y compartir información sobre tales asuntos[6].

3 Estrategia de Seguridad Nacional, 2013. Disponible en: http://www.lamoncloa.gob.es/documents/seguridad_1406connavegacionfinalaccesiblebpdf.pdf

4 Tamara Makarenko, Europe's Crime-Terror Nexus: Links between terrorist and organized crime groups in the European Union, Parlamento Europeo, Bruselas, 2012. Disponible en: http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/462503/IPOL-LIBE_ET(2012)462503_EN.pdf

5 Luis de la Corte Ibáñez y Andrea Giménez-Salinas, Crimen.org. Evolución y claves de la delincuencia organizada, Ariel, Barcelona, 2010.

6 Louis Shelley, Dirty Entanglements: Corruption, Crime and Terrorism, Cambridge University Press, Cambridge, 2014.

4. El análisis de algunos de los más importantes atentados terroristas cometidos en los últimos quince años en países occidentales, considerados como auténticas sorpresas estratégicas, han revelado contactos y conexiones con el crimen común y organizado que de haber sido tomadas en cuenta quizá podrían haber facilitado su prevención. Como ejemplo se puede citar los dos ataques terroristas más graves perpetrados en países occidentales en las últimas décadas, incluyendo el más letal de todos los tiempos. Varios de los secuestradores de los aviones estrellados en Nueva York, Washington y Pennsylvania obtuvieron visados de entrada a Estados Unidos y permisos de conducción que les fueron aportados por miembros de redes criminales dedicadas al tráfico y la falsificación de documentos[7]. Por su parte, varios de los perpetradores de los atentados del 11 de marzo de 2001 contaban con una carrera criminal previa a su etapa de radicalización y usaron sus contactos y experiencia delictivas para financiar la operación y obtener los explosivos con que llevarla a cabo[8].

3. TIPOS DE CONVERGENCIA Y ACTIVIDADES ILÍCITAS INVOLUCRADAS

La convergencia entre terrorismo y crimen puede introducir cambios en la naturaleza de las entidades o grupos que la protagonizan, así como en sus actividades. Además, esos cambios pueden adoptar formas y grados variados[9].

Una primera forma de interacción entre los fenómenos que comentamos supone la implicación directa e independiente de actores terroristas (cuya violencia suele responder a objetivos políticos o político-religiosos) en prácticas delictivas cuya comisión permite obtener insumos económicos u otros recursos materiales. O, viceversa, la comisión de atentados típicamente terroristas (es decir, orientados a atemorizar y coaccionar a amplias audiencias) por parte de grupos o estructuras criminales carentes de ideología. Como se ve, en ambos casos la convergencia consiste en la *apropiación* por parte de un actor de formas de actuación que son características del otro.

La *colaboración* entre actores terroristas y criminales es otra opción, no necesariamente incompatible con la primera. Tal cooperación puede responder a dos motivaciones diferentes. Las predominantes son de tipo práctico, conducentes al desarrollo de transacciones o acuerdos para el intercambio de bienes y/o servicios. Dentro de esta categoría entrarían la compra/venta de armas, explosivos, documentación o cualquier otro recurso buscado por los terroristas que pueda ser ofertado por elementos criminales. Además de suministrar bienes ilícitos, los clientes o socios procedentes del mundo criminal pueden facilitar a los terroristas el acceso a refugios o rutas que permiten su tránsito clandestino de unos países a otros o prestarles servicios relacionados con la transferencia y el blanqueo de fondos ilegales o el soborno a funcionarios públicos.

Viceversa, también los terroristas pueden vender y servicios a los criminales. En

7 Louise Shelley, Countering Terrorismin the U.S.: The Fallacy of Ignoring the Crimen-Terror Nexus, en R.W Orttung y A. Makarychev (eds.), National Counter-Terrorism Strategies (pp. 203–12), IOS Press, Amsterdam, 2006.

8 Fernando Reinares, Matadlos. Quién estuvo detrás del 11-M y por qué se atentó en España, Galaxia Gutemberg, Barcelona, 2014.

9 Thomas M. Sanderson, “Transnational Terror and Organized Crime: Blurring the Lines”, SAIS Review vol. 24, nº 1, 2004, pp. 49–61.

algunas operaciones de tráfico de armas, drogas o incluso personas los terroristas desempeñan el papel de vendedor, bien porque se estén transformando en meros actores criminales o porque utilicen esa clase de mercancías para intercambiarlas por algún otro recurso útil para el ejercicio del terrorismo, como cuando se cambian drogas por armas. Asimismo, los terroristas pueden alquilar su potencial de intimidación y violencia a otros elementos delictivos, por ejemplo para proteger cultivos de droga y mercancías ilícitas. No todas las transacciones entre terroristas y criminales son elegidas por estos últimos sino que en ocasiones constituyen una forma de extorsión abierta o sutil. Es el caso de algunas de las tasas que grupos extremistas imponen a traficantes ilegales como condición para atravesar un territorio bajo su control. La cooperación también puede implicar la participación conjunta en una o varias de las fases de una cadena de tráficos ilícitos o la subcontratación o encargo de servicios específicos (desde falsificación de documentos hasta operaciones de blanqueo). Asimismo pueden abarcar desde la realización de transacciones oportunistas planteadas a iniciativa de unos u otros actores (criminales o terroristas) hasta la forja de alianzas tácticas que supongan la colaboración conjunta en acciones o campañas violentas, ya sea por motivos de afinidad ideológica o por anticipar un beneficio común a extraer de dichas alianzas. En ocasiones, esas alianzas pueden acabar dando lugar a relaciones de larga duración de tipo parasitario o simbiótico.

Los dos anteriores tipos de convergencia pueden darse de forma puntual, esporádica, continuada o incluso permanente. Empero, los casos de implicación o colaboración duraderos y que sus protagonistas valoren como exitosos pueden acabar induciendo procesos de *transformación* parcial o total de las entidades implicadas y de su agenda de prioridades. Un grupo u organización terrorista puede acabar dando tanta importancia a la obtención de beneficios económicos como a la realización de sus objetivos políticos originales, convirtiéndose en una estructura híbrida a medio camino entre formación extremista y organización criminal. O incluso puede despolitizar totalmente los fines de su actividad real, aun cuando siga cultivando cierta fachada ideológica. Y, al menos teóricamente, una organización criminal también podría incorporar motivaciones políticas a su acción o acabar transformándose en un actor militante.

Las actividades ilegales en que se ha venido a concretar la confluencia entre terrorismo y crimen son numerosas. Entre ellas destacan los tráficos ilícitos de distinta naturaleza (drogas, armas, personas, recursos naturales y energéticos, piedras preciosas y mercancías diversas), robos y venta de bienes robados, secuestros, extorsión y servicios de protección de personas y productos, fraudes y estafas y el blanqueo de capitales (ver tabla 1).

Tráficos ilícitos	Drogas; Armas; Personas; Órganos; Recursos naturales (piedras preciosas, petróleo, madera, otros); Contrabando ilegal de diversos productos y mercancías (tabaco, combustible alimentos o bienes de primera necesidad, productos falsificados, robados o exportados/importados ilegalmente)
Otras	Robos y venta de bienes robados; Secuestros; Extorsión y chantaje; Servicios ilegales de protección de personas y mercancías; Fraudes y estafas; Explotación laboral o sexual; Piratería marítima; Delitos cibernéticos; Blanqueo de capitales

Tabla 1: Principales actividades delictivas relacionadas con el Crimen Organizado

Los actores terroristas pueden involucrase en esas actividades a través de las

diferentes modalidades de convergencia criminal anteriormente señaladas. Las que conectan con mercados ilícitos transnacionales, como el de drogas, armas y personas, hacen inevitable una cierta dosis de colaboración con actores puramente criminales. Otras, como las operaciones de robo destinadas a abastecerse de armas u otros recursos de utilidad logística, ciertas prácticas extorsivas, los secuestros o el blanqueo de dinero, pueden desarrollarse de forma independiente, si bien ello no excluye la opción de colaborar con individuos y estructuras delictivas especializadas a las que incluso se puede subcontratar. Por último la implicación (independiente o no) en aquellas actividades con capacidad para aportar ingresos máximos (principalmente el narcotráfico, otros tráficos ilícitos y la práctica sistemática de secuestros) son las más susceptibles de abrir paso a un proceso de criminalización/despolitización de actores terroristas que, como ya hemos visto, puede ser parcial (hibridación) o total (transformación)[10].

4. LA IMPLICACIÓN TERRORISTA EN ACTIVIDADES Y RELACIONES CRIMINALES: ESBOZO DE UN MODELO EXPLICATIVO

Puesto que la participación de un actor terrorista en actividades delictivas y/o relaciones criminales no es una constante sino solamente una opción resulta tan importante explicar ésta posibilidad como su contraria (es decir, explicar también los casos en que la implicación criminal no llega a tener lugar o se abandona). Como cualquier otra modalidad de acción, la probabilidad de que un actor terrorista convencional se involucre en actuaciones o alianzas delictivas, las abandone o se abstenga de ellas vendrá determinada, por factores de *capacidad, oportunidad* y *motivación*[11]. Podría decirse que los dos primeros (capacidad y oportunidad) son esencialmente objetivos mientras que el tercero (motivación) es más bien subjetivo. Para delinquir o entrar en tratos con elementos criminales hay que contar con ciertas capacidades y oportunidades que la hagan realizable en tanto que sin ellas la implicación criminal sería sencillamente imposible. Empero, con lo anterior no basta pues para consumarse la implicación criminal ha de ser previamente elegida, normalmente en función de su utilidad; en suma, ha de ser deseable y deseada por sus propios protagonistas. Pero examinemos la cuestión con mayor detalle.

4.1. CAPACIDADES Y OPORTUNIDADES

Algunas de las *capacidades* o competencias básicas asociadas a la actividad terrorista son aprovechables para la comisión de cierta clase delitos. La costumbre de operar en forma clandestina, el potencial de violencia y la falta de escrúpulos a la

10 Para más detalles y ejemplos específicos sobre las diferentes modalidades de convergencia puede verse Luis de la Corte Ibáñez y Andrea Giménez Salinas, Crimen.org. Evolución y claves de la delincuencia organizada, Ariel, Barcelona, 2010, pp. 319-340. Véase también Tamara Makarenko "The Crime-Terror Continuum: Tracing the Interplay between Transnational Organised Crime and Terrorism", Global Crime, vol. 6, nº 1, 2004, 129-145.

11 Aun siendo de elaboración propia, el modelo explicativo que se presenta a continuación está en deuda con el planteamiento ilustrado en Dipak K. Gupta, Understanding Terrorism and Political Violence. The life cycle of birth, growth, transformation, and demise, Nueva York, Routledge, 2008; y, asimismo, con el enfoque teórico general para el estudio de la acción humana propuesto en Jon Elster, La explicación del comportamiento social. Más tuercas y tornillos para las ciencias sociales, Gedisa, Barcelona, 2010, pp. 187-200.

hora de emplear la fuerza concede a los terroristas una evidente ventaja a la hora de acometer ciertas prácticas delictivas como extorsiones, robos, secuestros y de impedir que éstas trasciendan a la luz pública. En cambio, la posibilidad de involucrarse en actividades delictivas más complejas y sofisticadas o ajenas al uso de la fuerza queda supeditada a la disponibilidad de capacidades o habilidades específicas para su desarrollo. Algunas serán más accesibles a grupos terroristas que cuenten entre sus filas con individuos procedentes del mundo criminal y que mantengan contactos en dicho ámbito. Tales contactos, por ejemplo suelen resultar imprescindibles para introducirse en los mercados relacionados con tráficos ilícitos. Asimismo, las grandes estructuras terroristas, dotadas de una militancia heterogénea, potentes aparatos de captación y reclutamiento y amplias bases sociales de apoyo también tienen más opciones de incorporar personas con la experiencia o formación necesarias para realizar delictivas especializadas, ya sean la falsificación de documentos, la realización de estafas a través de internet o las operaciones financieras de blanqueo de capitales. No obstante, la ausencia de capacidades requeridas para el desarrollo independiente de algunas actividades ilícitas puede ser compensada mediante la cooperación con ciertos agentes criminales especializados: falsificadores, cultivadores y productores de droga, traficantes y contrabandistas, estafadores, ladrones, estafadores, hackers, etc.

Pero ya hemos dicho que la participación en actividades delictivas también es cuestión de *oportunidad*. A fin de cuentas, no todos los escenarios y circunstancias son igualmente propicias a la acción criminal y al establecimiento de colaboraciones o alianzas delictivas. Tal condicionamiento situacional explica en gran medida por qué la distribución geográfica de los casos de convergencia entre terror y crimen no es igualitaria y alcanza su máxima frecuencia e intensidad en países y regiones menos estables, como ya se apuntó en un apartado anterior. Las oportunidades de implicación criminal también pueden variar significativamente en función de otros elementos, como la eficacia de los sistemas de seguridad implantados en los escenarios donde los terroristas operan, el acceso a recursos naturales o bienes que puedan comercializarse en algún mercado ilegal o la presencia/proximidad de actores delictivos en esos mismos escenarios.

4.2. MOTIVACIONES (I): BENEFICIOS Y SERVICIOS

Como es natural, la implicación criminal únicamente tendrá lugar cuando exista una motivación directa a su favor. Podemos suponer que en cualquiera de los casos se tratará de una motivación instrumental, dependiente de la *utilidad* que los mismos actores terroristas atribuyan a su participación en actividades o relaciones delictivas. En concreto, la principal utilidad o función que puede rendir la comisión de acciones delictivas características de la delincuencia menor y organizada radica en la obtención de recursos económicos y/o materiales aprovechables para satisfacer las exigencias planteadas por la actividad terrorista. No sin razón, algunos economistas se hayan atrevido a definir el terrorismo como una especie de “guerra barata”[12]. Ciertamente, el coste de las actividades terroristas es relativamente modesto si se lo compara con el de otras formas de violencia política u organizada promovidas por milicias, guerrillas e insurgencias, ejércitos privados o estatales. Y lo mismo puede decirse de la

12 Mikel Buesa, ETA S.A. El dinero que mueve el terrorismo y los costes que genera, Planeta, Barcelona, 2011.

inversión requerida por la mayoría de las operaciones terroristas convencionales. Sin embargo, los grupos y organizaciones terroristas con voluntad de continuidad deben afrontar toda una amplia variedad de gastos. En primer lugar, esos costes incluyen los que se derivan de la preparación y ejecución de atentados y la adquisición de todos los medios y equipamientos necesarios para ello: armas y explosivos, vehículos, documentos, costes de traslado y viajes, dispositivos tecnológicos de comunicación, informáticos, etc. A ellos hay que agregar los gastos relacionados con la creación y el mantenimiento de las estructuras operativas (grupos, redes u organizaciones terroristas) y de apoyo. Aquí entran o pueden entrar los que se destinan al sustento de los propios militantes (alojamiento, manutención y otros gastos básicos), a labores de captación y reclutamiento de nuevos integrantes, de adiestramiento (a veces en campos que hay que construir, regentar o alquilar o trasladar) y propaganda, entre otros[13]. Como consecuencia de todo ello, algunas organizaciones terroristas, las más potentes y ambiciosas, desarrollan presupuestos que conllevan gastos anuales por cientos de millones de euros o dólares[14].

Huelga explicar que la cantidad de recursos económicos de los que disponga una organización terrorista determina su capacidad de actuación y, por tanto, su peligrosidad. Además, la obtención de fondos mediante desarrollo de actividades ilegales presenta ciertas ventajas frente a otras formas de financiación del terrorismo. Por ejemplo, la rapidez con la que algunas de esas actividades permiten acceder a los ingresos buscados o la independencia que aporta la autofinanciación en comparación con la dependencia a la que pueden estar sometidos los actores terroristas cuyos fondos provienen de alguna población de referencia o de un Estado patrocinador. A estos beneficios hay que sumar a veces ciertos efectos sociales y políticos útiles a la causa terrorista que pueden derivarse de las actividades delictivas desarrolladas. Como el control social que los terroristas pueden ejercer sobre las poblaciones o segmentos de población a los que extorsionen. Los golpes de efecto asociados a operaciones delictivas de cierta espectacularidad. O la escenificación de actos de coacción a un Estado a través de la realización de secuestros y episodios de toma de rehenes. Además, el involucramiento en determinados mercados ilegales puede proporcionar cierto capital social o político y apoyo social entre segmentos de población o comunidades cuya subsistencia, ingresos u oportunidades de inserción y ascenso social dependan de su participación en las economías y actividades ilícitas que los propios terroristas contribuyan a promocionar[15]. Por último, la participación en ciertos negocios y actividades ilícitas particularmente rentables puede permitir la acumulación de insumos económicos que superen con creces la cuantía necesaria para cubrir sus requerimientos operativos y organizativos, ofreciendo a los terroristas la oportunidad de convertir su actividad en un medio de vida y un lucrativo negocio.

Además de aportar ingresos, otras formas de implicación criminal también relacionadas con la financiación del terrorismo se orientan a mover o transferir fondos o

13 Luis de la Corte Ibáñez, La lógica del terrorismo, Alianza, Madrid, 2006.

14 Michael Freeman (2011): The Sources of Terrorist Financing: Theory and Typology, Studies in Conflict & Terrorism, 34:6, 461-475.

15 Para sendos análisis de situaciones y tendencias semejantes véase Valda Felbab-Brown, Shooting Up: Counterinsurgency an the War on Drugs, Brookings, Washington D.C, 2010; y también Mabel Gonzáles Bustelo, Narcotráfico y crimen organizado. ¿Hay alternativas?, Icaria, Barcelona, 2014.

blanquearlos (como ya se apuntó anteriormente) o incluso incrementarlos[16]. La transferencia de fondos es especialmente relevante en el caso del terrorismo internacional. Toda entidad terrorista cuyas actividades y/o estructuras se extiendan a más de un país necesitan mover su dinero a través de fronteras y hacerlo de forma clandestina. Y puesto que esta necesidad afecta a todo tipo de fondos algunas operaciones financieras ilegales realizadas por elementos terroristas suponen "ensuciar" dinero previamente obtenido por medios no ilícitos, como el que puede proceder de donaciones privadas o actividades económicas legales. Por su parte, la obtención de fondos por medios ilegales a veces aboca a los terroristas a implicarse en labores de blanqueo, especialmente si los ingresos obtenidos son sustanciosos. Para ello pueden recurrir a la realización de diferentes inversiones en la economía legal o la creación o participación en negocios o empresas "pantalla" o "tapadera". Para terminar, los terroristas también pueden involucrarse en negocios ilícitos con el propósito de aumentar el rendimiento de los excedentes previamente obtenidos mediante otras actividades de financiación, ya sean legales o ilegales, como cuando el dinero extraído de donaciones o secuestros se invierte en operaciones de narcotráfico.

Finalmente, hay que recordar que además de proporcionar dinero o beneficios económicos la implicación de elementos terroristas en actividades criminales puede rendir otros servicios, principalmente de tipo logístico y relacionados con la obtención de recursos materiales necesarios para el desarrollo de operaciones terroristas o el mantenimiento de estructuras. El robo de armas, vehículos y otras propiedades y la falsificación de documentos son los ejemplos más conspicuos de ello.

4.3. COSTES Y RIESGOS

La implicación criminal no sólo genera beneficios sino que además entraña riesgos y costes. Por ejemplo, las actuaciones ilícitas por parte de actores terroristas y sus contactos con actores criminales pueden facilitar su entrada en el radar de las agencias de seguridad e inteligencia, arriesgando con ello la detección de sus militantes, operaciones y estructuras. Asimismo, en caso de que su implicación criminal llegara a trascender los terroristas se exponen a proyectar una imagen de entidad marginal o "mafiosa" que podría hacerles perder apoyos sociales entre su comunidad de referencia. Los individuos procedentes del mundo criminal que entren en tratos con grupos u organizaciones terroristas o se incorporen a sus filas pueden ser susceptibles de convertirse en confidentes de las agencias de seguridad e inteligencia, ya sea porque caigan bajo control de sus agentes o porque se decidan a venderles información comprometedora. Finalmente, si resultan cuantiosos los beneficios económicos obtenidos por colaborar con delincuentes profesionales también pueden suponer un riesgo por su capacidad para corromper a algunos de sus militantes y erosionar su compromiso ideológico. Por su parte, al prestarse a cooperar con terroristas sus socios criminales no sólo arriesgan el descubrimiento de sus negocios ilegales sino también el control de los mismos (que podría llegar a pasar a manos de los extremistas con los que colaboran), además de afrontar un posible aumento de la presión judicial y policial sobre ellos impuesta y

16 La distinción entre actividades ilícitas destinadas a obtener fondos, transferirlos y almacenarnos ha sido convenientemente analizada en Jennifer L. Hesterman, The Terrorist-Criminal Nexus. An Alliance of International Drug Cartels, Organized Crime, and Terror Groups, CRC Press, Boca Ratón, 2013, pp.165-200.

castigos más severos a sus actividades. Por último, a lo anterior cabría añadir algunos costes en sentido estricto que se derivan de la implicación criminal. Como, por ejemplo, el tiempo, energía y recursos (humanos, materiales) que dicha implicación pueda consumir y que serán detraídos de su empleo en otras tareas directamente relacionadas con la actividad terrorista. Las expectativas sobre tales riesgos y costes explica por qué muchos actores terroristas que no encuentran alternativa a la implicación criminal para financiar su actividad se decanten por la comisión de delitos de pequeña escala y eviten entrar a colaborar o competir con otras estructuras criminales[17].

4.4. NECESIDAD O VENTAJA

Los cálculos que cualquier actor terrorista realice para determinar la conveniencia de implicarse (o continuar su participación) en actividades o relaciones criminales conllevarán una evaluación conjunta de beneficios/servicios, riesgos y costes. Dejando aparte los casos de plena despolitización/criminalización, los actores terroristas suelen estar menos dispuestos que otros agentes criminales a arriesgar su seguridad a cambio de mayores beneficios económicos. Por ese motivo, y dada la importancia de los riesgos y costes especificados, cabe suponer que un actor terrorista sólo estará suficiente motivado para implicarse en actividades o relaciones delictivas bajo las dos condiciones siguientes:

1. *De necesidad*: cuando la implicación criminal permita resolver una necesidad económica o logística que no pueda ser plenamente satisfecha de otra manera.
2. *De ventaja suficiente*: cuando aun pudiendo cubrir las exigencias materiales mínimas para desarrollar la propia actividad terrorista el actor anticipe que la implicación criminal podría depararle alguna ventaja sustantiva, sin exponerle a costes o riesgos que pudieran resultar inasumibles.

La distinción entre una motivación fundada en la necesidad y otra inspirada en las ventajas atribuidas a la implicación criminal es relevante porque tienen intensidades diferentes y varían en su relación con los factores de capacidad, oportunidad y riesgo antes examinados. Indudablemente la aparición de una necesidad estricta de involucrarse en actividades criminales para hacer posible la acción terrorista constituye un impulso mucho más poderoso que la mera búsqueda de ventajas. Así, cuando un actor terrorista no tenga más remedio que involucrarse en actuaciones o tratos criminales las capacidades y oportunidades que pudieran faltar para ello serán creadas y buscadas, partiendo además de una disposición al riesgo muy superior. En cambio, cuando la implicación criminal sea sólo una opción entre otras su elección estará seguramente mucho más condicionada por las capacidades disponibles, las oportunidades sobrevenidas (no necesariamente buscadas) y también por la magnitud de los riesgos y costes previsibles.

Recapitulando, la participación de un actor terrorista en actuaciones o relaciones criminales requiere una decisión cuya gestación vendrá condicionada por los factores de capacidad, oportunidad y motivación que acabamos de examinar, conforme a un proceso deliberativo cuya secuencia podría coincidir con la que se ilustra en la siguiente figura:

17 Brynjar Lia, Globalisation and the future of terrorism. Patterns and Predictions, Routledge, Nueva York, 2005, pp. 129.

Figura 1: La implicación terrorista en actividades y relaciones criminales

Con todo, una vez identificados en abstracto los factores generales que determinan la posibilidad de implicación criminal por actores terroristas conviene advertir que la expresión de cada uno de esos mismos factores carece de un valor fijo, único y equivalente para todos los casos sino que aquellos pueden variar significativamente en función del momento y las características de cada actor. De ahí que puedan detectarse diferencias relevantes en la proclividad terrorista al crimen.

5. POTENCIADORES DE LA ACTUAL CONVERGENCIA ENTRE TERRORISMO Y CRIMEN

Como ya señalamos al principio de este trabajo, aunque la implicación de elementos terroristas en actividades propias de la delincuencia común y organizada no sea una pauta nueva, cada vez son más abundantes las pruebas e indicios que apuntan a una progresión o incluso un salto cualitativo a ese respecto. Por consiguiente, todavía necesitamos identificar los factores capaces de alimentar esa tendencia, lo que podríamos llamar *potenciadores* de la convergencia entre terrorismo y crimen[18]. Sobre ellos convendría aclarar dos cuestiones: ¿cómo o por qué medios pueden ejercer dicha función? y ¿cuál es su naturaleza y origen específicos?, lo que en último término implica determinar cuántos y cuáles esos potenciadores.

En principio, cualquier cambio en las probabilidades de implicación criminal por parte de un actor terrorista debería reflejar una variación correspondiente en alguna o varias de las dimensiones explicativas incluidas en el modelo esbozado en el epígrafe anterior. Así, el incremento en frecuencia o grado de la participación terrorista en acciones criminales requiere que la propia implicación se vuelva:

18 Para una definición más amplia de la noción de potenciadores y su importancia en la explicación y previsión de riesgos y amenazas a la seguridad véase Luis de la Corte y José María Blanco, “Potenciadores del riesgo. Una visión ampliada para un mundo global”, en Luis de la Corte y José María Blanco (eds.) Seguridad Nacional. Amenazas y respuestas, Lid Editorial, Madrid, 201, pp. 55-78.

1. *M*ás *necesaria*, en la medida en que otras formas alternativas de cubrir las exigencias económicas, materiales o de cualquier otra índole queden anuladas.
2. *M*ás fácil, en tanto aumenten las capacidades y/o oportunidades requeridas para delinquir o entrar en trato con criminales.
3. *M*ás *ventajosa*, bien porque surjan oportunidades delictivas que permitan obtener recursos inaccesibles por otras vías (por ejemplo, cierta clase de armamento) o incrementar sus ingresos de forma sustantiva, lo que puede constituir una tentación difícil de resistir.
4. *Menos costosa y arriesgada*, como a menudo ocurre cuando se opera en ciertos escenarios o entornos caracterizados por un alto nivel de impunidad delictiva.

Los factores con capacidad para inducir cambios en cualquiera de los cuatro sentidos anteriores son múltiples y diversas. Algunos pueden responder a la propia evolución de las actividades terroristas y criminales involucradas, siendo por tanto de carácter *endógeno*. Por el contrario, otros serán *exógenos*, relativos a elementos y fuerzas externas proclives a influir en los modos y condiciones en que tales fenómenos se expresen y operen. De ellos nos ocupamos a continuación.

5.1. POTENCIADORES ENDÓGENOS, O CÓMO LA EVOLUCIÓN DEL TERRORISMO Y EL CRIMEN PROMUEVE SU CONEXIÓN

Hasta cierto punto la confluencia entre terrorismo y crimen (especialmente en sus modalidades de delincuencia organizada) es consecuencia de las variaciones que esos fenómenos puedan experimentar, tanto por causa de ciertos aspectos de su evolución general como por las evoluciones que uno o varios actores concretos (terroristas o criminales) puedan protagonizar en el devenir de sus actividades. Veamos cuáles son algunos de estos potenciadores endógenos.

Internacionalización del terrorismo y la criminalidad organizada. De todas las tendencias que han marcado la evolución de la delincuencia organizada su internacionalización ha sido seguramente la más decisiva[19]. Aunque no todo el crimen organizado sea transnacional si lo es en gran medida y en un grado creciente gracias a tres causas principales: el incremento sustantivo de la colaboración entre grupos y organizaciones criminales con diferente ubicación, la emergencia de auténticos mercados ilícitos mundiales cuyas fases de negocio se distribuyen en distintas regiones del mundo y la aparición de organizaciones criminales con presencia activa o implantación a escala internacional. Por su parte, sin llegar a las cotas alcanzadas por el crimen organizado también el terrorismo se ha ido internacionalizando de forma progresiva aunque no por igual en todas sus expresiones. Los grupos y organizaciones que operan dentro de la órbita de Al Qaida y el movimiento yihadista global destacan en ese sentido sobre todas las demás formas actuales, operando algunos de ellos como máximos exponentes de terrorismo internacional. La internacionalización de la delincuencia organizada y el terrorismo supone la ampliación transfronteriza, a través de países, regiones y continentes, de sus actividades, estructuras y objetivos. Varias de las consecuencias de ese proceso

19 United Nations Office on Drugs and Crimen, The globalization of crime. A transnational organized crime threat assessment, Viena, 2010. Disponible en: http://www.unodc.org/unodc/en/data-and-analysis/tocta-2010.html.

de internacionalización amplían incentivos y oportunidades de convergencia entre ambos fenómenos. Quizá la más importante de todas ellas sea la creación de diversos mercados ilícitos de escala internacional. Aunque las implicaciones económicas de todo ello merezcan un comentario aparte, resulta obvio que la configuración de un auténtico mercado mundial relacionado con el tráfico ilegal de armas facilita enormemente a los terroristas el acceso a tan imprescindible recurso y añade un interés muy especifico para entrar en contacto y realizar negocios con elementos criminales. Otro efecto relevante es la coincidencia de actores terroristas y criminales en un número creciente de países y escenarios, condición necesaria para posibles colaboraciones. Asimismo, la creciente necesidad de los terroristas de desplazarse a través de múltiples fronteras puede convertirles en clientes preferenciales de redes criminales dedicadas tanto a la falsificación de documentos de identidad como a facilitar el tránsito ilegal de migrantes en distintas partes del mundo. Por último, al tratar de desarrollar sus actividades y establecer estructuras propias en más de un país o región las organizaciones terroristas que adoptan una orientación internacional pueden verse en la necesidad de ampliar sus fondos y buscar nuevas formas de financiación, incluidas las de tipo ilegal.

Expansión de la economía criminal global. La interconexión progresiva entre actores y grupos relacionadas con el crimen organizado y la consiguiente emergencia de redes delictivas de alcance regional y global es responsable del formidable incremento constatado durante las últimas décadas en los beneficios procedentes de negocios ilícitas[20]. Según las últimas estimaciones aportadas por Naciones Unidas, con apoyo en datos de 2009, la criminalidad organizada podría estar generando ganancias cercanas a los 870 miles de millones de dólares anuales, cifra equivalente al 1,5% del PIB mundial, al 7% de los ingresos obtenidos cada año mediante la exportación mundial de mercancías y al PIB de un país como Holanda, cuya economía figura entre las veinte primeras del planeta[21]. Tal crecimiento en los beneficios no puede sino aumentar el atractivo que para los actores terroristas ofrece su posible introducción entrada en los circuitos de la economía criminal global, lo cual explica bien, por ejemplo, la progresiva conexión en ciertos escenarios entre terrorismo y narcotráfico en tonto que primera fuente de ingresos relacionados con la delincuencia organizada transnacional, calculados también por Naciones Unidas en torno a los 320 mil millones de dólares anuales. Otra consecuencia de la emergencia de una economía criminal global que debe ignorarse es su estrecha relación con la proliferación de paraísos y entidades fiscales y de técnicas de ingeniería financiera aplicadas al blanqueo de dinero ilícito cuyo aprovechamiento por parte de elementos criminales puede ser compartido con otros actores, incluidas organizaciones terroristas.

Descentralización y multiplicación de estructuras. En las dos últimas décadas los grupos criminales y terroristas han experimentado una evolución similar respecto a sus atributos organizativos. Han diversificación sus formas y han aumentado las diferencias entre ellas en términos de tamaño, o número de integrantes, y de estructuras. Del predominio de organizaciones con un tamaño considerable, una estructura jerárquica y un sistema de toma de decisiones altamente centralizado (cuasi militar en ciertos casos) se ha pasado a la combinación de aquella forma clásica con otros modelos organizativos y la proliferación de grupos de menor tamaño, más flexibles y

20 Moisén Naim, Ilícito. Como traficantes, contrabandistas y piratas están cambiando el mundo, Debate, Barcelona, 2006.

21 United Nations Office on Drugs and Crime http://www.unodc.org/unodc/index.html

dinámicos en su funcionamiento y estructuras más descentralizadas, incluyendo pequeñas redes prácticamente horizontales, algunas de ellas de gestación casi improvisada al objeto de llevar a cabo sólo una o unas pocas operaciones pero igualmente susceptibles de colaborar con otras estructuras de mayor entidad o acabar integrándose en ellas. Existen varias razones por las que la participación terrorista en actividades delictivas puede resultar más sencillo, y por tanto más probable, para grupos terroristas cuya estructura y atributos están próximos a esos nuevos modelos de organización más horizontales y de menor tamaño. De una parte, a mayor horizontalidad o equivalencia de estatus entre los miembros de un grupo terrorista mayor es también la libertad de elección de cada uno de ellos y menor el control ejercido por sus líderes. En tales condiciones se reducen también las posibilidades de prevenir las iniciativas particulares de implicación criminal aún cuando aquéllas puedan parecer peligrosas o desviadas a los ojos de otros miembros del propio grupo terrorista. De otro lado, la capacidad de un grupo para obtener fondos económicos suele ser directamente proporcional a su tamaño especialmente si dichos fondos se buscan por medios alternativos a la financiación criminal, como las aportaciones voluntarias de los propios terroristas y sus allegados, la captación de donaciones, el desarrollo de negocios legales o la búsqueda de patrocinios estatales. Por eso, los grupos terroristas con menor entidad serán menos resistentes a la tentación de involucrarse en negocios ilegales.

Células autónomas y terrorismo individual. Durante la década de 1980 algunos ideólogos del movimiento por la supremacía blanca en Estados Unidos propugnaron entre sus seguidores una forma de continuar sus actividades violentas de inspiración racista que rompiera con el modo de funcionamiento característico de los grupos y organizaciones terroristas tradicionales. Los defensores de la llamada estrategia de resistencia no dirigida o “sin líderes” propusieron aprovechar las nuevas funcionalidades ofrecidas por las tecnologías de la información y la comunicación para alentar y orientar a sus seguidores violentos para actuar por cuenta e iniciativa propia, evitando al mismo tiempo crear o mantener estructuras organizativas que ayudaran a las agencias de seguridad y autoridades judiciales a conectar unos con otros. Más recientemente, varias grandes organizaciones yihadistas (empezando por la propia Al Qaida) y algunos de sus estrategas más importantes decidieron contribuir a reproducir una pauta como la que se acaba de describir, instrumentalizando su gran potencial de comunicación y propaganda para incitar a sus simpatizantes a cometer atentados allí donde les fuera posible sin esperar a recibir ayudas o apoyos externos. La estrategia en cuestión explica tanto la actual proliferación de células autónomas y actores solitarios, responsables de un número creciente de tentativas terroristas en Europa y Norteamérica, así como la frecuente vinculación de esos actores con prácticas delictivas, tendencia nada sorprendente dado el reducido tamaño de estos actores carentes de cualquier fuente externa de financiación.

Relación con bases sociales y niveles de apoyo popular. La variabilidad de las posiciones asumidas por diferentes grupos terroristas acerca de la opción criminal, o por el mismo grupo en distintos momentos, puede estar fuertemente condicionada por las características de sus bases sociales y su comunidad de referencia. Los grupos que cuentan con amplio apoyo popular pueden llegar a financiarse por medio de las donaciones y aportaciones económicas recibidas de sus colectivos de apoyo lo cual elimina el principal incentivo que para muchos de esos grupos presenta la opción criminal.

Además, esta dependencia también puede funcionar como obstáculo a la implicación terrorista en actividades criminales en la medida en que ello provoque rechazo o decepción entre los simpatizantes que conforman el propio colectivo de referencia. Pero las cosas pueden funcionar de muy forma distinta si los negocios y actividades ilícitas a desarrollar también redundan en algún beneficio para el colectivo de referencia de los terroristas, como así ocurre con los negocios de narcotráfico en países o regiones donde gran parte de la población carece de otra alternativa para cubrir su propio sustento u obtener un sueldo mínimamente digno. Volviendo a un plano más general, los grupos terroristas que operen de espaldas a cualquier gran colectivo, que cuenten con un apoyo social exiguo o inexistente serán más libres para decidir con qué métodos cubrir sus necesidades económicas y logísticas o si conviene aprovechar unas u otras oportunidades de negocio, sean legales o no. Finalmente, un descenso drástico y repentino en el volumen de los fondos aportados a un grupo terrorista por sus simpatizantes puede estimular el salto a la actividad criminal.

Confluencias entre terrorismo, delincuencia organizada y conflictos armados. El terrorismo es una actividad que tiene cabida y expresión en múltiples escenarios, incluyendo coyunturas de guerra donde puede desempeñar una función auxiliar y combinarse con otras formas de violencia insurreccional y con modalidades de combate propias de la guerra de guerrilla o la guerra convencional. Tales combinaciones han ganado relevancia en los últimos años gracias a la interacción entre grupos yihadistas, algunos de ellos con capacidades y hechuras que los convierten en auténticas milicias o pequeños ejércitos privados, e insurgencias locales (islamistas, nacionalistas o laicas). Por su parte, la sustitución de la guerras interestatales por las conflictos armados internos como tendencia bélica predominante desde finales del siglo pasado ha otorgado a la criminalidad organizada un papel protagonista en muchas economías de guerra y una significativa influencia en evolución de los conflictos y en los escenarios de reconstrucción postconflicto[22]. Y la coexistencia de actores insurgentes/terroristas y criminales en contextos bélicos crea coyunturas particularmente propicias a la convergencia entre ambos fenómenos[23]. Este asunto ha sido tematizado a partir del concepto de las “guerras híbridas”, de empleo cada vez más frecuente en análisis estratégicos y militares[24]. Aparte de volver casi inevitable el contacto entre elementos criminales y terroristas su vinculación a la dinámica de los conflictos armados también estimula la convergencia entre ambos por otras vías. De una parte, las insurgencias que practican el terrorismo ven ampliadas las oportunidades de actividad criminal, como las que se les ofrecen cuando logran tomar el control de algún territorio o se introducen en los circuitos de contrabando que definen en buena medida las economías de guerra. De otro lado, las organizaciones criminales pueden extraer importantes beneficios de sus tratos con los terroristas/insurgentes, bien porque necesiten de su protección o porque los conviertan en clientes preferentes. En tercer lugar, ambos

22 Luis de la Corte, “Criminalidad organizada y conflictos armados”, Ejército, 838, 18-26, 2013.

23 La evolución de los conflictos y su creciente confusión con diferentes forma de violencia organizada y actividad criminal fue especialmente destacada y descrita en el Informe Mundial del Desarrollo publicado por el Banco Mundial para el año 2011. Disponible en: http://documents.worldbank.org/curated/en/2011/01/14282125/world-development-report-2011-conflict-security-development-overview-informe-sobre-el-desarrollo-mundial-2011-conflicto-seguridad-y-desarrollo.

24 Véanse Frank Hoffman, Conflict in the 21st Century: The rise of hybrid wars, Potomac Institute for Policy Studies, Arlington,2007; Fabián Sánchez, “El conflicto híbrido, ¿una nueva forma de guerra?”, en El enfoque multidisciplinar a los conflictos híbridos, CESEDEN, Madrid, 2012, pp. 11-24.

actores pueden disfrutar en tales escenarios de la impunidad que les es característica y que procede de la incapacidad del Estado amenazado o en guerra para perseguir eficazmente sus ocupaciones delictivas. Todo lo cual puede crear un interés específico de las organizaciones criminales por alimentar la continuación del conflicto a través de la colaboración y el apoyo explícito al bando terrorista/insurgente.

Otras vicisitudes de los grupos terroristas y de sus miembros. La participación terrorista en actividades criminales puede verse favorecida por factores relacionados con la vida interna y la evolución de los propios actores terroristas. Como ya se ha dicho antes, la existencia entre las filas de un grupo terrorista de uno o varios militantes con un pasado delictivo puede allanar el camino hacia la implicación del propio grupo en actividades ilícitas. Aunque no fuera una pauta desconocida en los últimos años se ha podido constatar un aumento de los casos de radicalización protagonizados por individuos procedentes del mundo delictivo, con particular incidencia en algunos países europeos incluido el nuestro. Pasando a otro asunto, a veces lo único que detiene a un grupo u organización terrorista de involucrarse en acciones criminales es la oposición ejercida a el respecto por un líder o por su estructura de mando. Por eso, una segunda circunstancia capaz de estimular la implicación criminal es la aparición de una crisis de liderazgo. Ésta puede sobrevenir tras la detención o eliminación algunos de sus dirigentes o como consecuencia de la gestación de un conflicto interno entre facciones con líderes enfrentados por uno u otro motivo y con actitudes enfrentadas respecto a la conveniencia atribuida a la opción de participar en operaciones puramente delictivas. Una última situación capaz de desencadenar dinámicas favorables a la implicación terrorista en actividades criminales es su entrada en una fase de declive, desmoralización o una vez consumada su derrota operativa. Lo normal es que a medida que los miembros de una organización terrorista comiencen a perder la fe en su causa orienten su vida hacia nuevos objetivos y aumenten las deserciones (lo que a su vez tienen a agravar la crisis de la organización). Carentes en no pocos casos de otras habilidades diferentes a las adquiridas en su etapa de militancia y con escasas oportunidades para volver a una vida legal y ordinaria, algunos de los desertores que no caigan bajo el poder de las autoridades pueden verse tentados a volcar su experiencia iniciando una carrera criminal. Intención parecida pueden albergar algunos de los terroristas que se resistan abandonar la militancia aún cuando hayan asumido ya la imposibilidad de alcanzar los objetivos políticos que inicialmente la motivaron. No es infrecuente por ello que durante la última fase de vida activa de determinados grupos terroristas e insurgentes (que a veces puede prologarse durante años) o tras su disolución oficial algún sector de tales fuerzas se criminalice y perviva como un simple grupo delictivo o como fuerza mercenaria.

5.2. POTENCIADORES EXÓGENOS Y CONTEXTOS PROPICIOS

Tanto el terrorismo como el crimen (en particular la delincuencia organizada), han demostrado una gran capacidad para adaptarse a los cambios operados en sus entornos de actuación y las nuevas oportunidades de actividad y negocio sobrevenidas a raíz de la evolución de las sociedades contemporáneas y de la sucesión de acontecimientos y coyunturas políticas y económicas. La influencia de varios de esos factores en la convergencia entre terrorismo y crimen ya ha sido consignada en el apartado anterior, dedicado a identificar unos potenciadores endógenos que en última instancia, traen causa de otros fenómenos externos o exógenos.

Descenso del patrocino estatal. Durante las últimas décadas de la Guerra Fría el terrorismo y otras formas de violencia de orientación subversiva funcionó hasta cierto punto como una herramienta al servicio de la política exterior de diferentes países. Ello fue posible gracias al patrocinio económico y otras formas de apoyo que los Estados de esos países prestados a una variedad de actores terroristas: grupos terroristas y milicias armadas de extrema izquierda, nacionalistas, islamistas, de extrema derecha, etc. Sin embargo, principalmente la caída del Muro de Berlín y después los atentados del 11 de septiembre de 2001 acabaron con el recurso generalizado al patrocinio estatal, en parte por razón de los cambios geopolíticos sobrevenidos y en parte por el crecimiento del rechazo de las opiniones públicas frente al terrorismo. Existe un amplio acuerdo en considerar esta tendencia como un inductor principal del incremento de la participación terrorista en actividades delictivas, asumidas como alternativa a la financiación y el respaldo logístico previamente obtenido de unos u otros Estados.

Respuesta al terrorismo y sus medios de financiación. Como es bien sabido, otra las consecuencias relevantes de los atentados del 11-S fue la puesta en marcha de una ofensiva antiterrorista global, liderada en sus inicios por las autoridades estadounidenses pero a la que de inmediato sumaron iniciativas y programas de respuesta específicos planteados por diversos organismos internacionales y una larga lista de países. La ya mencionada resolución 1373 del Consejo de Seguridad de Naciones Unidas (2001) instaría a los Estados miembros a adoptar nuevas y más potentes medidas para prevenir y reprimir la financiación del terrorismo. En concreto, se solicitaba la tipificación como delito la provisión o recaudación intencionales de fondos destinados a su empleo en la preparación de actos de terrorismo, la congelación inmediata de fondos y demás activos financieros o recursos económicos de toda persona vinculada a actividades terroristas, la denegación de cobijo a quienes las financian. Y asimismo se alentaba a aplicar las normas internacionales generales enunciadas en las cuarenta recomendaciones sobre el blanqueo de capitales y las nueve recomendaciones especiales sobre financiación del terrorismo del Grupo de Acción Financiera (GAFI). A partir de estas directrices, que asimismo incluían una condena explícita de las prácticas de patrocinio estatal, la lucha contra la financiación del terrorismo se convertiría en una de las dimensiones fundamentales de la actividad contraterrorista. Podría afirmarse, no obstante, que aún resultando necesarias y efectivas las acciones emprendidas en ese sentido éstas han tenido efectos contrapuestos sobre la relación entre terrorismo y crimen. De una parte, la orientación a detectar posibles conexiones entre los flujos de la economía legal y grupos y organizaciones terroristas ha reducido las opciones de obtener fondos procedentes de patrocinadores estatales y de poderosos donantes privados, cuyo almacenamiento y recepción puede requerir la colaboración con entidades e intermediarios financieros poco escrupulosos. Sin embargo, al cegar esas vías de financiación se ha añadido un nuevo y potente incentivo para buscar dinero a través de la participación en operaciones delictivas y negocios ilícitos de diversa índole[25].

Tendencias desestabilizadoras, conflictos armados y procesos de transición. La consideración del terrorismo como un factor de desestabilización para los países y sociedades que lo padecen no requiere explicación pues, de hecho, ese efecto defi-

25 Louis Shelley, Dirty Entanglements: Corruption, Crime and Terrorism, Cambridge University Press, Cambridge, 2014.

ne los objetivos inherentes a las tácticas que pueden denominarse terroristas[26]. Aunque no sea su propósito principal, la capacidad del crimen organizado para introducir inestabilidad también es conocida y se hace particularmente evidente cuando grupos criminales se involucran en intensas campañas de violencia (en ocasiones puramente terroristas) dirigidas contra sus competidores o contra las autoridades y el Estado[27]. Pero no siempre se percibe con igual claridad la dirección inversa de la relación entre terrorismo y crimen organizado, por un lado, y por otro dinámicas de desestabilización como las que pueden desatarse a partir de movimientos masivos de protesta y revueltas populares o tensiones comunitarias con capacidad para inducir procesos de cambio político, desembocar en violencia organizada o auténticas guerras civiles e incluso hacer colapsar a un Estado. La cuestión ya ha sido advertida al hablar de la creciente tendencia de actores armados no estatales a emplear el terrorismo en coyunturas de guerra y gestionar su economía implicándose en diversos mercados ilícitos e interactuando con redes u organizaciones puramente criminales. Sin embargo, no es ocioso volver a recordarlo aquí para advertir cómo la naturaleza intrínsecamente desestabilizadora del terrorismo y de ciertas expresiones del crimen organizado traen causa de tendencias e iniciativas de desestabilización previas y externas. Por otro lado, las ventajas específicas que los conflictos armados ofrecen a la interacción entre terrorismo y crimen son hasta cierto punto semejantes a las que rigen durante las fases iniciales de determinados procesos de transición política, violentos o pacíficos. Todas esas situaciones alimentan algún grado de desorden y pueden llegar a socavar el funcionamiento ordinario de los servicios del Estado o incluso anularlo en los casos más extremos, lo que sin duda juega a favor de sus adversarios[28].

Acceso a (micro) entornos propicios a la actividad y la colaboración criminal. No todos los espacios son igualmente favorables a la convergencia entre terrorismo y crimen. Ni todos ofrecen las mismas oportunidades e incentivos ni tampoco todos son equivalentes en cuanto a los riesgos y costes que conlleva. Por efecto de sus características físicas, políticas, sociales y humanas, algunos escenarios son especialmente propicios al desarrollo de actividades criminales. Asimismo, cuando adopte la forma de una colaboración directa con actores procedentes del mundo criminal (individuos o grupos) la confluencia entre terrorismo y delincuencia estará fuertemente condicionada por factores de índole contextual. Después de todo, tal clase de cooperación exige la coincidencia y el encuentro entre los actores llamados a cooperar, el reconocimiento de intereses compartidos y el establecimiento de una cierta relación de confianza entre dichos agentes. Algunos entornos donde tales contactos son más frecuentes o incluso habituales son:

- *Prisiones*, sobre todo las que carecen de regímenes de internamiento separados

26 Para más detalles en ese sentido volvemos a remitir a: Luis de la Corte Ibáñez, La lógica del terrorismo, Alianza, Madrid, 2006.

27 United Nations Office on Drugs and Crime, Crime and instability. Case studies of transnational threats, Viena, 2010. Disponible en: http://www.unodc.org/documents/data-and-analysis/Studies/Crime_and_instability_2010_final_26march.pdf

28 En esta línea incide también la reciente Resolución 2195 aprobada del Consejo de Seguridad de Naciones Unidas del 19 de diciembre de 2014. En ella se hace explícita la creciente preocupación de los estados miembro por la capacidad de que los grupos terroristas que se benefician de la delincuencia organizada para debilitar a los Estados afectados por sus acciones, tanto en su seguridad como su estabilidad, gobernanza y desarrollo social y económico. Véase en: http://www.un.org/es/comun/docs/?symbol=S/RES/2195(2014)

para terroristas y que pueden funcionar como ámbitos favorables a la radicalización de los internos y su captación por parte de reclutadores extremistas.

- *Barrios marginales,* como los que existen en numerosas capitales y grandes ciudades, afectados por una escasa presencia institucional, altas tasas de delincuencia y una arraigada subcultura criminal, a la que a menudo se suma una alta concentración de población inmigrante o de representantes de minorías.
- *Localidades o* áreas *transfronterizas* en las que intersecten distintas jurisdicciones nacionales y que funcionen simultáneamente como punto de tránsito para uno o varios tráficos ilícitos internacionales y para terroristas.

Escenarios de riesgo y críticos. La probabilidad de convergencia entre terrorismo y crimen también tiende a variar de unos países y regiones a otras, con clara ventaja para aquellos en los que la presencia de actores terroristas coincide con una o más de las siguientes condiciones de riesgo (entre las que se incluyen varias que ya han sido comentadas):

- Disponibilidad de zonas de cultivo vinculadas a la producción de drogas o de recursos naturales susceptibles de explotación ilegal.
- Inclusión en las rutas de uno o varios tráficos ilícitos como puntos de conexión entre países productores o emisores y países consumidores o receptores.
- Conflictividad armada.
- Procesos de transición política.
- Fragilidad o colapso estatal (ausencia del Estado y de servicios sociales).
- Subdesarrollo económico y social.
- Corrupción elevada y alto grado de economía irregular o sumergida.
- Fronteras amplias y porosas.

Por último, cuando por causas históricas, políticas, económicas, geográficas, sociales u otras varias de estas condiciones coinciden en un mismo país o grupo de países estos se convierten en *escenarios críticos* donde la convergencia entre terrorismo y crimen puede volverse extrema y endémica. Vale la pena advertir que más de la mitad de los atentados terroristas perpetrados en 2013 (último año para el que existen registros completos al respecto) tuvieron lugar en sólo tres países, Irak, Pakistán y Afganistán[29], exponentes ejemplares todos ellos de los escenarios críticos que acabamos de reseñar y en los que la convergencia entre terrorismo y crimen alcanza también sus máximas cotas[30]. La franja occidental del Sahel[31] y Libia, tan relevantes para la

29 National Consortium for the Study of Terrorism and Responses to Terrorism, "Majority of 2013 terrorist attacks occurred in just a few countries", Universidad de Maryland, Diciembre de 2014. Disponible en: http://www.start.umd.edu/news/majority-2013-terrorist-attacks-occurred-just-few-countries

30 Sobre la noción de escenarios críticos y su empleo para analizar los vínculos entre terrorismo, insurgencia y criminalidad organizada en Afganistán, Pakistán, Irak y el Sahel véase Luis de la Corte, "¿Hasta qué punto convergen el terrorismo global y la criminalidad organizada? Parámetros generales y escenarios críticos", Revista del Instituto Español de Estudios Estratégicos, 1, 353-380, 2013.

31 Nos hemos ocupado del caso del Sahel en Boukara Houcine, Messaoud Fenouche, Touatit Lofti,

seguridad en el conjunto de los países situados en la ribera sur del Mediterráneo y tan cercanos a las costas españolas, constituyen otros dos magníficos ejemplos de escenarios críticos para la convergencia entre terrorismo y crimen, igual que Siria, estrechamente ligada al escenario iraquí, Somalia y Nigeria (ambos incluidos en la lista de los diez países más afectados por terrorismo en 2013).

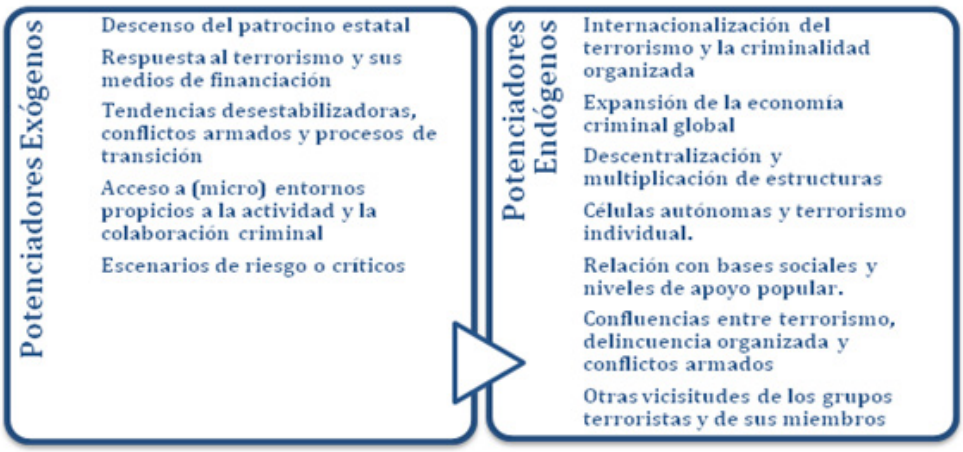


Figura 2: Potenciadores de la implicación terrorista

6. CONSECUENCIAS Y CONCLUSIONES

A juzgar por las evidencias acumuladas en los últimos años la convergencia entre terrorismo y crimen no es una relación por demostrar ni una simple anécdota. El asunto al que hemos dedicado una atención preferente en este trabajo, la participación de actores terroristas (individuos, grupos, organizaciones) en modalidades delictivas orientadas por una motivación esencialmente económica, se ha demostrado frecuente y progresiva. Esta pauta ha adquirido especial significación en algunos escenarios críticos coincidentes con países o regiones que concentran la mayor parte de los incidentes terroristas que ocurren en el mundo.

La creciente convergencia entre terrorismo y delincuencia (sobre todo en su dimensión organizada) tiene amplísimas repercusiones a diferentes niveles. Los ingresos extraídos por grupos criminales gracias a su colaboración con terroristas aportan un estímulo específico al desarrollo de economías ilícitas, eleva los costes por seguridad de los negocios legales existentes, disminuye las iniciativas a crear otros nuevos y por esa vía frena toda opción de crecimiento y desarrollo económico. Al surtirles de fondos y otros recursos, la implicación de actores terroristas en prácticas delictivas posibilita la perduración de su actividad violenta y sus estructuras, contribuyendo así a deteriorar las condiciones de seguridad y exponer a las poblaciones afectadas al riesgo de atentados, agresiones, secuestros, amenazas y prácticas extorsivas, robos,

Benhadj Karima, José María Blanco y Luis de la Corte Ibáñez, “Terrorismo y tráfico de drogas en África subsahariana”, Madrid, Instituto Español de Estudios Estratégicos e Instituto Militar de Documentación, Evaluación y Prospectiva de Argelia. Documento de Trabajo del Instituto español de Estudios Estratégicos, 13/3/2013. Disponible en: http://www.ieee.es/Galerias/fichero/docs_trabajo/2013/DIEEET01-2013_IEEE-IMDEP.pdf. También sobre el Sahel Wolfram Larcher, “Organized Crime and Conflict in the Sahel-Sahara Region”. Carnegie Endowment for International Peace, September 2012. Disponible en: http://www.carnegieendowment.org/files/sahel_sahara.pdf;

etc. Además, la incorporación de una finalidad de lucro a la agenda de algunos grupos y organizaciones terroristas permite que éstos se mantengan en activo aun cuando las circunstancias objetivas hayan anulado ya toda posibilidad de éxito político, prolongando de ese modo todos los perjuicios derivados de su actividad. El potencial de desestabilización que se deriva de la convergencia entre terrorismo y crimen en aquellos países donde ese vínculo alcanza su máxima expresión contribuye a ahondar los problemas de gobernabilidad e ineficiencia represiva previamente existentes y genera una dinámica viciosa en la que una y otra amenaza conviven y se retroalimenta. Por otra parte, el hecho de que tales formas extremas de convergencia ocurran lejos de los países occidentales no impide que sus efectos se prolonguen más allá de sus fronteras. Al contrario, la intensa confluencia constatada en los denominados "escenarios críticos", algunos de los cuales operan como verdaderos epicentros de un terrorismo con pretensiones de expansión mundial (Afganistán, Pakistán, Irak, Siria, Sahel, etc.), también amenaza la paz y la seguridad internacional. De un lado, porque los beneficios de origen ilícito allí acumulados por elementos terroristas contribuyen a la continuación de conflictos armados que requieren la implicación de la comunidad internacional. Y de otro lado, porque al financiar y facilitar la afluencia de voluntarios extranjeros radicalizados se crea también el riesgo de acabar irradiando terrorismo a otras naciones próximas o lejanas (España y los países europeos incluidos) mediante acciones y campañas violentas protagonizadas por los combatientes que retornen de tales escenarios.

Deliberadamente, este estudio también ha incluido en sus consideraciones a la delincuencia común y organizada de baja escala. La financiación de los atentados perpetrados en Madrid el 11 de marzo de 2004 a base del dinero obtenido mediante unas pocas y humildes operaciones delictivas realizadas por un puñado de delincuentes comunes demostró que subestimar el peso de esa clase de vínculos criminales de menor entidad puede tener consecuencias dramáticas.

En definitiva, la preocupación por la posibilidad de que terrorismo y crimen confluyan en una o más formas está ampliamente justificada, máxime cuando todo apunta a que ambas amenazas seguirán con nosotros por mucho tiempo. En ese sentido, la generación de mecanismos de coordinación y cooperación entre departamentos de seguridad e inteligencia con responsabilidades en materia de investigación criminal y antiterrorismo abre nuevas oportunidades de avance.

Fecha de recepción: 04/11/2014. Fecha de aceptación: 17/12/2014

HERRAMIENTAS DE APOYO A LA INFRAESTRUCTURA TECNOLÓGICA DE LOS GRUPOS ORGANIZADOS QUE OPERAN EN LA RED

FÉLIX BREZO Y YAIZA RUBIO

RESUMEN

Las soluciones tecnológicas disponibles en la red son utilizadas con éxito por grupos organizados para satisfacer sus estrategias de comunicación. Sin embargo, las necesidades de cada grupo y el contexto en el que operan son los que marcan los requisitos técnicos de estas aplicaciones. En algunos casos, las alternativas comerciales no son opciones válidas para estos grupos debido a la preocupación por los programas de vigilancia gubernamentales y a la presión que se pueda ejercer sobre las grandes corporaciones para lograr acceso a la información de sus usuarios. En este contexto, la elección de herramientas libres permite a las organizaciones un mayor control sobre su información con una capa adicional de anonimato a un coste razonable. En este artículo se identifican las aplicaciones utilizadas por diferentes grupos organizados para satisfacer sus necesidades de difusión de información, comunicación interna y financiación a través de la red.

Palabras clave: internet profundo, tor, internet de superficie, dinero electrónico.

ABSTRACT

Organized groups successfully use technological solutions available in the network in order to meet their communication strategies. However, each group's needs and the context in which they operate are the factors that determine the technical requirements of these applications. In some cases, commercial alternatives are not a valid option for these groups because of concerns regarding government surveillance programs and the pressure that may be exercised on major corporations to access information on their users. In this context, choosing free software tools enables organisations to have a major control over their information with a larger level of anonymity at a reasonable price. In this article we identify the applications used by different organized groups in order to meet their information dissemination, internal communication, and funding through the network.

Key words: dark internet, surface, deep web, tor, electronic money.

1. INTRODUCCIÓN

La utilización de las nuevas tecnologías no ha pasado desapercibida para los grupos organizados que encuentran en ellas herramientas que mejoran sus procesos de funcionamiento interno. Sin embargo, la preocupación por los programas de vigilancia en internet y por la presión que puedan ejercer los gobiernos sobre plataformas como Facebook y Google para que compartan información sobre sus usuarios ha reforzado

el interés de algunos grupos por proteger su anonimato. Algunos de ellos ya han desplegado infraestructuras tecnológicas que les permiten proteger la integridad de sus comunicaciones.

El objetivo de este artículo es identificar las herramientas utilizadas por diferentes grupos organizados en función de su actividad, desde la difusión de sus acciones y la captación de nuevos miembros, hasta los mecanismos de comunicación interna y las alternativas de financiación que ofrecen estas tecnologías.

En consecuencia, este documento está estructurado como sigue: la sección 2 recoge definiciones y conceptos generales. La sección 3 analiza la disposición de herramientas empleadas para dar soporte a las actividades de distintos grupos y organizaciones que operan en la red. Por último, en la sección 4 se recogen las conclusiones a extraer de este trabajo.

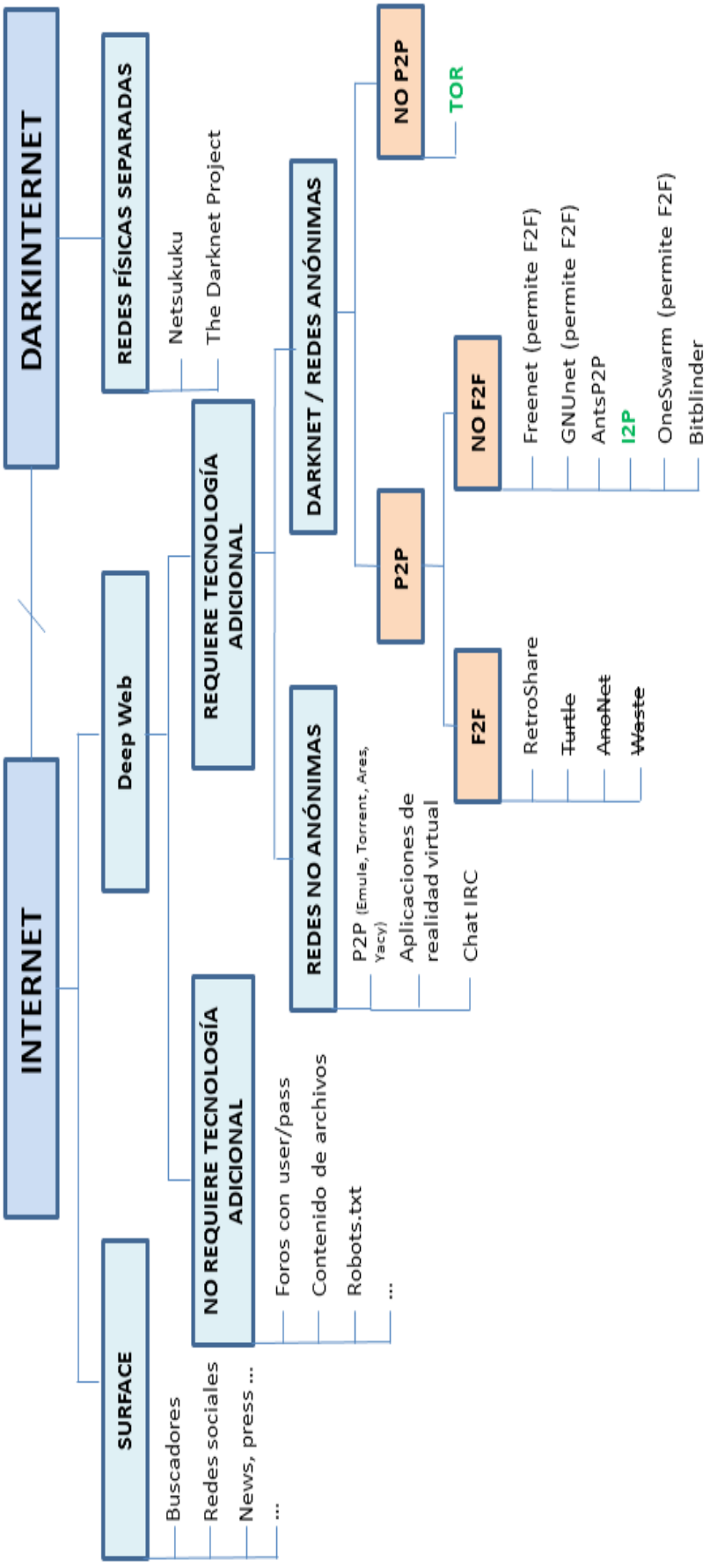
2. CONCEPTOS GENERALES

Las características propias de una investigación en el ámbito de internet y las comunicaciones obligan a la definición de los elementos que componen su arquitectura para afrontar con garantías el proceso de investigación. A continuación, se enumeran una serie de conceptos generales que, aplicados a las redes de ordenadores y a la evolución observada más recientemente de los mecanismos de financiación que proliferan en la red, servirán para comprender los casos de estudio recogidos en este documento.

2.1. CONCEPTOS GENERALES APLICADOS A REDES DE COMUNICACIÓN

En este apartado se va a proceder a detallar parte de la terminología relativa a la estructura de los contenidos de la red en función de la forma en que estos pueden ser consultados. En la Figura 1 se recoge la clasificación propuesta por los autores atendiendo a la naturaleza de las conexiones. En general, se puede hablar de la existencia de dos grandes familias:

- **Internet**. Es un conjunto de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP, lo cual hace que las redes físicas heterogéneas que la componen funcionen como una red única.
- **Dark internet**. Se consideran dentro de esta categoría todas aquellas redes físicas separadas de internet que hacen uso de infraestructuras físicas al margen del internet convencional. Actualmente, este tipo de redes son utilizadas por distintos tipos de organizaciones para evitar el control gubernamental, como ocurre con la red Guifi (1), proyectos patrocinados por el Departamento de Estado de los EEUU (2) como Commotion Wireless (3) del Open Technology Institute o aplicaciones de comunicación que utilizan el *wireless* de los dispositivos móviles como Firechat (4). Tienen la particularidad de que su estudio requiere acceso físico a dichas redes, lo que dificulta su monitorización si estas están muy localizadas o son administradas por grupos muy reducidos de personas.


INTERNET
SURFACE
Buscadores
Redes sociales
News, press ...
...
Deep Web
NO REQUIERE TECNOLOGÍA ADICIONAL
Foros con user/pass
Contenido de archivos
Robots.txt
...
REQUIERE TECNOLOGÍA ADICIONAL
REDES NO ANÓNIMAS
P2P (Emule, Torrent, Ares, Yacy)
Aplicaciones de realidad virtual
Chat IRC
DARKNET / REDES ANÓNIMAS
P2P
F2F
RetroShare
Turtle
AneNet
Waste
NO F2F
Freenet (permite F2F)
GNUnet (permite F2F)
AntsP2P
I2P
OneSwarm (permite F2F)
Bitblinder
NO P2P
TOR
DARKINTERNET
REDES FÍSICAS SEPARADAS
Netsukuku
The Darknet Project

En cualquier caso, en este trabajo se va a hacer referencia a diversas fuentes de internet. Es habitual diferenciar entre internet de superficie (o *surface*) e internet profunda (o *deep*).

- ***Surface.*** Se considera *surface* a aquel contenido indexado por los buscadores convencionales, por lo que se encuentran en esta categoría las redes sociales (exceptuando los perfiles privados), los foros (exceptuando aquellas partes que establezcan mecanismos de protección como usuario y contraseña) y las plataformas de *pastes* (exceptuando aquellos que se hayan borrado previamente a la indexación por parte de los buscadores)[1].

- ***Deep.*** Es aquel contenido al que no se puede acceder a través de un buscador convencional. La ausencia de contenidos indexados en dichos buscadores puede venir motivada por la necesidad de autenticar el acceso mediante un usuario y contraseña o por el uso de una tecnología adicional entre otras razones. En esta última categoría se encuentran las redes no anónimas y las redes anónimas.

Las redes anónimas se utilizan para compartir información y contenidos digitales entre distintos nodos. En ellas se toman medidas para preservar el anonimato de las identidades de quienes intercambian información. Este tipo de redes pueden dividirse en redes P2P, aquellas en las que las relaciones entre todos sus miembros son de igual a igual, y no P2P.

El caso de Tor (5) es el de una red de comunicaciones distribuida de baja latencia y superpuesta sobre internet en la que el encaminamiento de los mensajes que viajan por ella está concebido para proteger la identidad de los usuarios, la integridad de la información y la confidencialidad de la misma. En la red Tor se cifra la información en los nodos de entrada y se descifra en los nodos de salida, momento en el que un atacante podría acceder a la información que circula por ellos si no se emplea un protocolo de cifrado a nivel de aplicación como SSL.

Por su parte, las redes P2P se pueden dividir en *friend-to-friend* (F2F), aquellas redes P2P anónimas en donde los nodos tienen la capacidad de conectarse únicamente con nodos *amigos* conocidos, limitando la exposición de los mismos, y redes no *friend-to-friend* (no F2F). Las primeras presentan grandes inconvenientes para su monitorización, dada la necesidad de que ambos nodos consensuen la comunicación. A continuación se enumeran algunos ejemplos existentes de este tipo de redes.

- **Retroshare** (6). Por su arquitectura, es una red P2P que únicamente funciona como F2F. Se trata de un tipo de red en el que la gente se conecta directamente con sus amigos, por lo que se necesitarían otro tipo de capacidades no técnicas para tener acceso al contenido.

- **I2P** (Invisible Internet Project) (7). Es una red de capa anónima pensada para el envío de mensajes punto a punto preservando el anonimato. Está concebida para alojar cualquier servicio de internet tradicional como servidores de correo, canales de chat IRC, servidores HTTP, así como otras aplicaciones distribuidas. Sin embargo, a diferencia de Tor, no está concebida para acceder a la *surface* de forma anónima.

1 Las excepciones señaladas se encuentran dentro de la categoría de deep web como contenido que no requiere una tecnología adicional para acceder.

- **Freenet**. Es una red P2P destinada a la distribución de información anónimamente entre los usuarios que la conforman (8) y que ponen a disposición de la red parte de su ancho de banda y de su capacidad de almacenamiento. Tiene la característica de que se puede configurar para funcionar como una red F2F.

Además, existen otras tecnologías que ofrecen diferentes soluciones de conectividad como las plataformas de compartición de archivos GNUnet (9), OneSwarm (10), Bitblinder (11) y AntsP2P (12) o los proyectos ya descontinuados Turtle, Anonet (13) y Waste (14).

2.2. CONCEPTOS GENERALES DE LA ECONOMÍA EN LA RED

El dinero convencional y los métodos de pago han encontrado diferentes formas de evolucionar y adaptarse a las nuevas tecnologías. El efectivo ha dado paso al dinero electrónico y este a la aparición de métodos de pago alternativos cuyo control escapa a organismos centralizados. En este sentido, tomaremos como referencia la definición de dinero electrónico procedente de la Directiva 2009/110/CE (15) sobre el acceso a la actividad de las entidades de dinero electrónico cuyo proceso de trasposición en España se culminó con la Ley 21/2011 sobre dinero electrónico (16):

- **Dinero electrónico.** «Todo valor monetario almacenado por medios electrónicos o magnéticos que representa un crédito sobre el emisor, se emite al recibo de fondos con el propósito de efectuar operaciones de pago, según se definen en el artículo 4, punto 5, de la Directiva 2007/64/CE, y que es aceptado por una persona física o jurídica distinta del emisor de dinero electrónico».

Otro punto de vista es el sostenido por un informe del Departamento del Tesoro de los EEUU enfocado al análisis de las monedas virtuales convertibles (17), es decir, aquellas que tienen un valor equivalente en divisas virtuales. Los conceptos de divisa convencional y divisa virtual son definidos como sigue:

- **Divisa convencional**. «La moneda o papel moneda de los EEUU o de cualquier otro país que ha sido designada como de curso legal y que circula y es utilizada y aceptada como medio de intercambio en el país emisor».
- **Divisa virtual**. «La divisa utilizada como medio de intercambio que funciona como tal en determinados entornos, pero que no posee todos los atributos de las monedas convencionales. En particular, las divisas virtuales no tienen estatus de curso legal en ninguna jurisdicción».

En base a estas definiciones y a la tipología de las entidades de gestión de las divisas virtuales, estas se pueden clasificar de dos formas:

- **Centralizadas**. Se entiende por divisas centralizadas todas aquellas cuya gestión corre a cargo de un organismo central, que las expide y se hace responsable de ellas. Ejemplos de este tipo de plataformas son Paypal (18), Skrill (19), Webmoney (20), CashU o Ven (21). En otro ámbito, existen plataformas virtuales que también permiten la compraventa de bienes digitales dentro de las distintas comunidades virtuales que las utilizan, como los Linden Dollars de Second Life (22) o las divisas utilizadas en plataformas de compraventa de

exploits[2] y servicios de *hacking* y *cracking* como 1337day.com[3] (23). Estas divisas no necesariamente han sido concebidas originalmente para el comercio electrónico pero sí entran en la definición de *convertibles* del Financial Crimes Enforcement Network (17) que recogíamos en la definición de divisas virtuales.

- **P2P**. A semejanza del funcionamiento de las redes P2P en otros ámbitos, esta arquitectura también funciona para la gestión de los pagos realizados con *criptodivisas* de forma que son los nodos de la red los que mantienen la integridad de las transacciones de la moneda. La *criptodivisa* más utilizada es Bitcoin, que acapara el 84% de la capitalización total del mercado (24). Se trata de un protocolo público que implementa una divisa virtual basada en una arquitectura *peer-to-peer* (P2P) en la que no existen servidores centrales (25). Su mantenimiento recae en la capacidad computacional de la red de usuarios en sí misma aplicando un modelo de *proof-of-work*[4] para la validación de las monedas. El hecho de que se trate de un proyecto de *software* libre ha permitido la proliferación de monedas derivadas como Litecoin, Peercoin y Namecoin. Pese a la hegemonía de las *criptodivisas* basadas en Bitcoin, Ripple, Nxt y BitSharesX son ejemplo que, aun no compartiendo el código fuente, heredan su filosofía.

3. HERRAMIENTAS UTILIZADAS POR LOS GRUPOS ORGANIZADOS EN LA RED

Los grupos organizados se sirven de soluciones existentes en la red para mejorar la efectividad de sus campañas de difusión, agilizar los procesos de toma de decisiones mejorando sus estructuras de comunicación interna y explotar nuevas vías de financiación al margen de los sistemas convencionales. En consecuencia, en esta sección se recogen las opciones que tienen a su alcance cuatro tipos de entidades de diferente naturaleza que comparten la utilización de la red para como instrumento organizativo.

3.1. ORGANIZACIONES ACTIVISTAS Y MOVIMIENTOS SOCIALES

Tanto las organizaciones internacionales como los movimientos sociales que defienden causas sectoriales hacen uso de las nuevas tecnologías para multiplicar su capacidad de convocatoria, aumentar la presión sobre los organismos e instituciones con poder de decisión o eludir las limitaciones interpuestas por los gobiernos para materializar sus objetivos.

2 Un exploit es un fragmento de software utilizado con el objetivo de explotar una vulnerabilidad de seguridad dentro de un sistema informático para conseguir que este se comporte de una forma en la que no fue concebido siendo explotado por el atacante.

3 En 1337day.com, la moneda de intercambio es el Gold (1 Gold = 1USD al cambio) y permiten el depósito y el retiro empleando criptodivisas o Webmoney entre otros. Cuenta con un modelo de negocio que acapara un 20% de comisión en las retiradas de dinero.

4 Estos sistemas se caracterizan por hacer que los nodos de una red resuelvan una serie de operaciones matemáticas (a menudo hashes) antes de poder ejecutar una acción sobre la misma (en el caso de Bitcoin, añadir un nuevo bloque) de modo que se previenen ataques de denegación de servicio o abusos contra ella dado que se puede ir ajustando la dificultad de los problemas matemáticos solicitados. En el caso de Bitcoin, estos modelos hacen que la posibilidad de recibir la autorización de la red para añadir un nuevo bloque sea directamente proporcional al porcentaje de la capacidad de cómputo total que representa un nodo con respecto al resto de la red.

3.1.1. Mecanismos de difusión

Una parte importante de las acciones activistas es la promoción de sus actividades para la difusión del mensaje. Una de las estrategias de comunicación consiste en aparecer en los medios de comunicación convencionales con protestas mediáticas como las llevadas a cabo por colectivos como Femen (26) (27) (28) o Greenpeace (29). Antes de la democratización del uso de internet, estas prácticas constituían el eje central de sus campañas para alcanzar a un público más amplio.

Hoy en día, estos grupos también encuentran en la red un medio propicio para la difusión de sus acciones y motivaciones, así como para la publicación de decálogos que ya venían siendo difundidos en el pasado mediante cadenas de correo o sitios Web 1.0. En este sentido, las redes sociales y las plataformas de recogidas de firmas se conforman como medios de difusión que permiten poner a disposición de cualquiera vídeos y materiales de manera inmediata e independiente a grupos de presión y con mayor capacidad de viralización para la identificación de perfiles afines.

3.1.2. Mecanismos de comunicación interna

Históricamente, las salas de chat IRC y las listas de correo han sido utilizadas como mecanismos de comunicación interna. De hecho, la plataforma activista Riseup todavía mantiene una colección de listas de correo en la que se alojan más de 17 000 agrupadas por temáticas (30). Sin embargo, este tipo de soluciones presentan problemas para clasificar contenidos, realizar el seguimiento de una determinada temática y abrir hilos en paralelo dada la gran cantidad de conversaciones simultáneas existentes.

Actualmente, se utilizan herramientas de edición colaborativa de documentos como Google Docs, cuyo anonimato depende de la confianza depositada en la compañía que ofrece el servicio. Existen alternativas libres como Loomio[5] (31) o Etherpad-lite[6] (32) que permiten su despliegue en servidores privados o, si el objetivo es reforzar el anonimato, en los *hidden services* de Tor o de Freenet. En este sentido, plataformas como Riseup ofrecen a los diferentes grupos activistas la posibilidad de utilizar la solución de Etherpad a través de una versión pública desplegada en sus propios servidores (33).

El uso de herramientas para evadir el control que ejercen sobre internet los gobiernos en los que se limita la libertad de expresión o de reunión es de gran utilidad para los grupos activistas. Existen soluciones que apuestan por evitar la utilización de la infraestructura cableada de los proveedores de servicios de Internet y que se apoyan en arquitecturas físicas creadas *ex professo* por los activistas para mantener la conectividad interna. Por ejemplo, Firechat, que fue utilizada con éxito por los manifestantes en las protestas de Hong Kong de otoño de 2014 (34) (35) (36), explota el concepto de topologías de red en malla o *mesh networks*[7] para crear redes P2P interconectadas

5 Loomio es un proyecto de software libre distribuido bajo licencia AGPL que permite la toma de decisiones, el trabajo colaborativo y la votación de propuestas a través de una interfaz web. El código fuente del proyecto está disponible en Github (83).

6 Etherpad es un proyecto de The Etherpad Foundation que mantiene una solución para la edición de documentos de forma colaborativa y en tiempo real liberada bajo la licencia Apache 2.0. El código fuente del proyecto está disponible en Github (90).

7 Las topologías de red en malla no requieren de un nodo central que las gestione permitiendo que

haciendo uso de la conexión Wifi de los dispositivos y eludir la presión que pudiera aplicarse sobre los proveedores de servicio.

Para agilizar el proceso de toma de decisiones, existen aplicaciones para la administración de los procesos de votación[8]:

- Appgree (37) es una plataforma centrada en la formulación de procesos de votación multipropuesta de forma ágil mediante la creación de tantos subgrupos de población elegidos al azar como propuestas iniciales se hayan planteado en las que cada uno de estos subgrupos será consultado sobre un número limitado de propuestas de forma representativa.
- Agora Voting (38) es un proyecto de Wadobo Labs que presenta una plataforma web distribuida bajo licencia AGPL[9] concebida para la administración de procesos de votación basados en el concepto de democracia líquida, es decir, procesos en los que el participante puede optar por delegar el voto en personas de su confianza.

3.1.3. Mecanismos de financiación

Pese a que tradicionalmente la financiación de las actividades de organizaciones activistas se ha mantenido a costa de las cuotas de sus abonados y suscriptores, la red ofrece hoy en día otras soluciones complementarias:

- Donaciones voluntarias enviadas a través de plataformas como Paypal, Google Wallet o similares.
- Proyectos específicos financiados a través de sitios como Kickstarter (39), Peerbackers (40) y Goteo (41). Se trata de plataformas en las que organizaciones y particulares proponen proyectos que son financiados por la comunidad a cambio de determinados beneficios y que se llevan a cabo cuando una determinada cifra es alcanzada.
- *Merchandising* y venta de productos por internet que incluyan lemas o mensajes asociados al movimiento como camisetas, tazas, llaveros y otros productos similares (42).

En cualquier caso, no es habitual que estas plataformas empleen *banners* de publicidad de productos de terceros para aumentar sus ingresos, ya que predomina el interés por mantener su independencia.

3.2. GRUPOS *HACKTIVISTAS*

La actividad de los grupos *hacktivistas* se ha incrementado en las últimas décadas aprovechando el descontento social para identificarse con otras causas activistas (43).

los mensajes circulen por los nodos que pertenecen a la red y agregando tolerancia a fallos en el caso de que un nodo se desconecte o falle.

8 Organizaciones como la Electronic Frontier Foundation (89) o GNU (87) e incluso activistas del software libre como Richard Stallman (92) ya han manifestado en el pasado dudas en relación a los problemas que entraña para la privacidad de los votantes la utilización de dispositivos electrónicos.

9 El código fuente del proyecto está disponible en Github (95).

Se erigen como defensores de la libertad de expresión y de los derechos humanos y denuncian de la actividad de los gobiernos y corporaciones a partir de la utilización de herramientas digitales para la filtración de documentos, la ejecución de DDoS[10], la ingeniería social[11] o la realización de otros ataques más sofisticados técnicamente como inyecciones SQL[12] o ataques de *cross-site-scripting*[13] entre otros.

3.2.1. Mecanismos de difusión

Los grupos *hacktivistas*, al igual que las organizaciones activistas, tienen su propia estrategia de comunicación, esencialmente a través de internet. Utilizan las redes sociales para difundir tanto sus próximas actuaciones, denominadas *operaciones*, como la información obtenida a partir de sus ataques. Por este motivo, muchos de estos grupos han visto cancelados en algún momento sus perfiles en distintas plataformas, como ocurriera con Anonymous en Facebook (44) o Youtube (45) por publicar información «privada y confidencial de otras personas». Para asegurarse de que dicha información no desaparezca de internet y sea visible desde cualquier buscador, suelen utilizar plataformas con términos y condiciones menos restrictivas en cuanto al tipo de información publicada como Pastebin (46).

Asimismo, es habitual que las identidades que colaboran con estos grupos reivindiquen la atribución de sus actos. Suelen utilizar páginas como Zone-H (47) en las que los atacantes dan a conocer las vulnerabilidades que han descubierto o publicar su logo o lema en aquellos *sites* que han sido objetivo de sus ataques. Sus actividades suelen tener consecuencias legales y, es por ello que en ocasiones utilizan pseudónimos para evitar ser relacionados con otras de sus identidades en la red o, por el contrario, que se refugien bajo otros movimientos *hacktivistas* como los de Anonymous, Lulzsec o Turkish Ajan.

3.2.2. Mecanismos de comunicación interna

La organización de los grupos *hacktivistas* es anárquica y a menudo difusa (48). Se caracterizan por tener una estructura flexible y por funcionar como redes P2P en las que la desaparición de una identidad no implica la pérdida de una funcionalidad estructural significativa. En cualquier caso, no es imprescindible que sus miembros posean altos conocimientos informáticos para colaborar en la ejecución de ataques ya que pueden utilizar programas denominados LOIC[14] (del inglés, Low Orbit Ion Cannon),

10 Un ataque de denegación de servicio distribuido tiene como objetivo la paralización intencional de una red informática inundándolo con datos enviados simultáneamente desde varios ordenadores.

11 La ingeniería social se define como el conjunto de técnicas psicológicas y habilidades sociales utilizadas de forma consciente y muchas veces premeditada para la obtención de información de terceros.

12 Una inyección SQL es un método de infiltración de código que se vale de una vulnerabilidad informática presente en el nivel de validación de entradas de una aplicación que realiza consultas a una base de datos.

13 Los ataques de cross-site-scripting o XSS son un tipo de inyección en el que el atacante se sirve de una vulnerabilidad en una aplicación web para enviar código malicioso al usuario final. Como el navegador del usuario no tiene forma de comprobar si es de confianza, ejecutará la secuencia maliciosa de comandos.

14 Low Orbit Ion Cannon (LOIC) es una herramienta de inundación utilizada para generar una gran cantidad de tráfico de red. Esta alta tasa de resultados de tráfico tiene el objetivo de degradar la disponibilidad de una plataforma y, potencialmente, provocar una interrupción del servicio.

diseñados para realizar denegaciones de servicio de forma sencilla y sin necesidad de compartir una localización geográfica.

Las vías de comunicación entre expertos de seguridad informática tienen en común la dificultad del rastreo de sus miembros y de la información que estos publican. Aún hoy en día, uno de los principales mecanismos de comunicación son las listas de distribución a partir del correo electrónico.

Este tipo de listas dieron paso a mecanismos de comunicación más interactivos. Los chats IRC[15] y las zonas privadas de los foros de seguridad son utilizados por los grupos *hacktivistas* para coordinar sus ofensivas contra objetivos planificados. En cambio, los foros habitualmente presentan dos zonas, una pública, que es utilizada a modo de agregador de noticias y consultas técnicas generales, y otra privada para la planificación de operaciones. A menudo, se utilizan medidas de seguridad adicionales para dificultar el acceso a las plataformas por parte de programas de monitorización automatizados. Las más utilizadas son las siguientes:

- Verificación del User-Agent del navegador para evitar el acceso de *crawlers* y recolectores de enlaces o correos.
- Ejecución de javascript que solicita *feedback* al usuario y que complica las tareas de automatización.
- Obligación de contar con una cuenta registrada y la necesidad de contar con permisos de acceso al recurso.
- Resolución de captchas[16] visuales o auditivos, así como de operaciones matemáticas u otras preguntas de verificación que dificultan accesos no deseados a la plataforma.
- Obligación de publicar un comentario para poder acceder a cierta información.

Por otra parte, las redes sociales funcionan de manera similar. Los grupos *hacktivistas* tienen la posibilidad de comunicarse a través de grupos privados con la salvedad de que la administración de la página es ajena a la organización. Esta circunstancia hace que sea susceptible de ser utilizada por las fuerzas de seguridad aprovechando las exigencias que se pueden requerir a los administradores de sitios como *Facebook*.

Con respecto a los correos electrónicos como herramienta de comunicación, se cuenta con la posibilidad de emplear servidores anonimizados a través de la red Tor como Mailtor (49) o el ahora desactivado Tormail (50). También se utilizan técnicas de cifrado PGP (51) en los proveedores de servicio convencionales para evitar que se pudiera acceder al contenido del correo electrónico, en el caso de que la información fuera requerida a los administradores del servicio de correo electrónico por mediación de una autorización judicial. Estas técnicas sólo pueden ser vulneradas cuando se

15 Algunos de los chats IRC más utilizados por grupos como Anonymous son los servidores irc.cyberguerrilla.org, irc.anonops.com, irc.anonibero.com e irc.anonnet.org.

16 Un captcha (del inglés, Completely Automated Public Turing test to tell Computers and Humans Apart) es un test automático controlado por una máquina conformado por una prueba en la que se pretende determinar si un usuario es un humano o un bot. Se utilizan desafíos que supuestamente solo sabrían solventar los usuarios humanos como la lectura de una imagen distorsionada o la respuesta concreta a preguntas complejas o enunciados de problemas sencillos.

carezca tanto de protección física del punto en el que se encuentra la clave privada utilizada como de protección lógica de las claves que dan acceso a ella.

3.3. GRUPOS DEDICADOS A ACTIVIDADES CRIMINALES EN INTERNET

La capa adicional de anonimato que ofrece operar detrás de un ordenador ha dado pie a la proliferación de grupos criminales que operan en la red. La existencia de dichos grupos depende del mantenimiento de un ecosistema que les permita continuar con sus actividades delictivas. Este caso de estudio tiene el objetivo de conocer el modo en el que los grupos dedicados al crimen en la red se organizan de tanto para la venta de contenidos (robo de credenciales o de tarjetas bancarias) o el ofrecimiento de servicios ilegales (alquiler de *botnets*, servicios de *hacking* y *exploits*) como para la compartición o distribución de contenido de pornografía infantil.

3.3.1. Mecanismos de difusión

Estos grupos evitan su exposición en la web de superficie. Suelen utilizar foros[17] con medidas de seguridad basadas en relaciones de confianza o en la publicación de *posts* para acceder a la información robada como mecanismo de prevención frente a *bots*. Asimismo, las salas de chat IRC también permiten poner en contacto a los interesados para concertar el formato de entrega de contenidos. Estos dos tipos de fuentes no garantizan, por definición, la anonimización de los delincuentes a no ser que hagan uso de VPN que protejan su identidad o realicen las conexiones a través de *proxies* alojados en distintos países para conectarse a dichas plataformas y dificultar el rastreo.

En cambio, uno de los grandes desafíos que se plantea a los organismos policiales es el seguimiento de grupos criminales a través de redes anónimas. El grado de anonimato que les otorgan estas redes ha conseguido que los delitos tradicionales del tráfico de drogas, órganos y armas hayan puesto especial interés sobre estos servicios ocultos. En concreto, a partir de Tor, la red anónima por excelencia, podemos encontrar mercados negros como Silk Road (52) (53) o Agora (54), servicios de email como los ya mencionados Tormail (50) o Mailtor (49) e, incluso, distintos tipos de redes sociales en las que poder ponerse en contacto con más usuarios como Torchat (55) y la extinta Torbook (56).

3.3.2. Mecanismos de comunicación interna

Los ciberdelincuentes son conscientes de que uno de los tipos de comunicación existentes en internet y que garantizan una mayor complejidad de rastreo es el proporcionado por aquellas redes P2P anónimas en donde sus nodos se conectan únicamente con sus «amigos». En este punto, se hace inviable una monitorización automatizada del contenido que circula por ellas y, llegado el caso, sería necesario otro tipo de capacidades como la infiltración en dicha red para tener acceso al contenido.

Adicionalmente, un informe del European Cybercrime Centre (57) reconoce que la dificultad de identificar la ubicación del material ilegal, especialmente cuando este es

17 Por ejemplo, los foros de leakforums.org (97) y lampeduza.so (98) están especializados en la venta de credenciales y tarjetas bancarias sustraídas.

borrado tras su visualización, y la de averiguar el momento exacto en el que se está reproduciendo un recurso en *streaming* son los principales retos a los que deben hacer frente los organismos policiales en relación con la detección de delitos asociados a los abusos contra la población infantil en internet.

3.3.3. Mecanismos de financiación

A continuación, se recogen algunas de las principales líneas de acción que pueden ser utilizadas por grupos dedicados al cibercrimen para monetizar sus actividades.

- Administración de *botnets*. Symantec (58) identifica diversas formas de monetizar una *botnet*. Pueden variar desde el ofrecimiento de servicios de denegación de servicio bajo demanda utilizando los nodos infectados, hasta el envío de *spam*, el ofrecimiento de servicios de *proxies* a través de los equipos comprometidos, el *click-frauding*[18], la venta de credenciales o incluso la minería encubierta de bitcoins en dichos equipos.
- Compra de seguidores. El auge de las redes sociales y la importancia de la imagen de marca en la red han motivado que algunas compañías opten por la compra de seguidores para ganar reputación con mayor rapidez, dando pie al desarrollo de un mercado *underground* de venta de seguidores y *likes* (59).
- Contratación de servicios ofensivos. En algunas plataformas como 1337day.com se ofrecen servicios de *hacking* bajo demanda. De hecho, la dirección de Bitcoin asociada a 1337day.com a finales de 2014 había aparecido en casi 150 transacciones habiendo recibido más de 234 bitcoins (60) (65 000 € al cambio[19]).
- *Ransomware*. Se trata de un tipo de aplicación maliciosa que extorsiona a los usuarios mediante el secuestro de documentos (habitualmente ofimáticos) de los equipos infectados cifrando dichos documentos con una clave aleatoria para solicitar posteriormente el pago de un rescate que permita a la víctima recuperar los ficheros. Aunque en el caso de algunas filtraciones de bases de datos corporativas se han solicitado rescates de gran importe (61), es habitual que se apueste por rescates de tamaño medio o bajo, pero siempre en órdenes de magnitud que el usuario infectado esté dispuesto a abonar (62).
- *Phishing*. Utilizando técnicas de ingeniería social, los delincuentes pueden obtener credenciales bancarias y nombres de usuario y contraseñas de acceso a servicios sensibles para venderlos posteriormente.
- Contratación de servicios no autorizados. La proliferación de los *smartphones* da paso a la difusión de aplicaciones que pueden formalizar la contratación de servicios Premium sin conocimiento del usuario.

Además, las características propias de las *criptodivisas* dificultan la atribución de las transacciones y la identificación de los responsables frente a la monitorización de las divisas convencionales. Esta realidad, propicia un escenario en el que la sustracción

18 El click-frauding es un tipo de abuso perpetrado contra las plataformas de anunciantes que se basa en la realización de peticiones automáticas para visualizar anuncios controlados por el atacante generando tráfico artificial no humano.

19 Tasa de cambio estimada por blockchain.info a fecha 11 de diciembre de 2014 (88).

de monederos virtuales acapare un interés creciente para los grupos dedicados al cibercrimen ya que en ellos se almacenan monedas virtuales de más fácil sustracción que el dinero electrónico convencional.

3.4. GRUPOS TERRORISTAS

Las redes terroristas utilizan internet para satisfacer tres objetivos estratégicos de comunicación que, según Corman y Schiefelbein (63), son la legitimización de su causa, la propagación de su movimiento y la intimidación de sus oponentes. Dependiendo del propósito que deseen satisfacer, se situarán en una zona de internet u otra.

3.4.1. Mecanismos de difusión

Grupos terroristas como el Ejército Islámico de Irak y el Levante (ISIS) han desarrollado una sofisticada estrategia a través de redes sociales como medida de promoción de sus acciones ante el mundo. Por medio de estos canales, publican todo hecho en el que se destaque su fuerza militar y sus avances territoriales, llegando a realizar vídeos promocionales como la *Campaña de los mil millones* en la que se instaba la población musulmana a que colgara vídeos en Youtube e Instagram apoyando la causa (64). Con el objetivo de inundar las redes, crearon la aplicación The Dawn of Glad Tidings que publicaba *tweets* automáticamente en las cuentas de aquellos que se la hubieran descargado (65).

En vista de que la estrategia de comunicación de ISIS está siendo muy efectiva de cara al reclutamiento de combatientes extranjeros, el gobierno iraquí bloqueó el 13 de junio de 2014 el acceso a Facebook y a Twitter, lo que motivó la utilización de la aplicación Whisper (66) que permite la publicación de comentarios de forma anónima y que ha cobrado protagonismo en Iraq incluso entre militares desplegados en la zona (67) (68). Asimismo, también se ha incrementado el uso de Tor y de Psiphon que da la posibilidad a los usuarios de utilizar su dispositivo como *proxy* para permitir que terceros puedan acceder a internet a través de ellos (69).

3.4.2. Mecanismos de comunicación interna

Hace tiempo que los grupos terroristas son conscientes de las implicaciones que tendrían para su organización las fugas de información derivadas de la incautación de sus equipos. La banda terrorista ETA ya utilizaba como medida de protección de su información en el año 2003 el sistema de cifrado PGP (70) y en 2010 el proyecto de TrueCrypt[20] (71).

Por su parte, Al-Qaeda utiliza desde 2007 (72) una aplicación de cifrado para Windows denominada Asrar Al-Mujahideen (*secretos muyahidines* en español) que permite el intercambio de mensajes y archivos cifrados ya sea a través de foros o de buzones de correo electrónico. Adaptándose a los nuevos tiempos, en 2013, The Global Islamic Media Front hizo público el desarrollo de una aplicación de cifrado

20 El proyecto de Truecrypt fue descontinuado repentinamente por sus desarrolladores en mayo de 2014 (76) pese a sus funcionalidades multiplataforma y a que la propia comunidad había patrocinado un análisis forense de su código para verificar su robustez (77).

para dispositivos Android y Symbian que permite el cifrado de SMS, archivos y correo electrónico con criptografía asimétrica (73).

En el caso de aquellos grupos con una estructura localizada, las alternativas que crean una infraestructura de red paralela a la infraestructura telefónica convencional aportan una capa adicional de seguridad al resto de elementos de seguridad de la red, dado que las comunicaciones tienen lugar al margen de la red instalada por los proveedores de servicios de comunicaciones. Este es el caso de The Darknet Project, una red que habría permitido a Los Zetas mantener su estructura de comunicación sin depender de la red telefónica convencional (74).

3.4.3. Mecanismos de financiación

Las *criptodivisas* ofrecen nuevas posibilidades de financiación complementarias a los métodos tradicionales. Sin embargo, los grupos terroristas tienen que enfrentarse al insuficiente número de pasarelas de intercambio que permitan la realización de transacciones de dinero en efectivo por bitcoins de una forma anónima. Solamente la proliferación de comercios que acepten esta *criptodivisa* como medio de pago o la utilización de cajeros automáticos que los expendan permitirían superar las barreras de seguridad interpuestas por estas plataformas.

Sin embargo, atendiendo a los datos recogidos en el proyecto de coinmap.org[21] (75), el número de establecimientos físicos que aceptan bitcoins o litecoins como medio de pago apenas supera los 6000 en todo el mundo. La realidad es que la adquisición de grandes cantidades de bitcoins es compleja si no se cuenta con una red de un tamaño suficiente como para asimilar el volumen de transacciones a realizar. En el caso particular de los grupos asociados al Estado Islámico, a las dificultades tecnológicas que conlleva la implantación de estos sistemas en puntos de venta físicos, se suma la inexistencia de comunidades activas en los países limítrofes lo que limita su margen de maniobra en esta región.

4. CONCLUSIONES

Las soluciones tecnológicas disponibles en la red están siendo utilizadas con éxito por grupos organizados para satisfacer sus objetivos de manera más eficiente, pero serán las necesidades concretas de cada grupo las que marquen el tipo de aplicaciones a utilizar. En este sentido, las organizaciones que centran sus esfuerzos en acciones de presión harán uso de la web de superficie (redes sociales, blogs, plataformas de recogida de firmas, etc.) para garantizar la difusión de su mensaje hacia un público más amplio. Por el contrario, aquellos grupos criminales o aquellas organizaciones que lleven a cabo actividades perseguidas por los estados optarán por soluciones que provean una capa de anonimato más robusta (Tor, I2P, Freenet, etc.) para dificultar las labores de investigación de las agencias de seguridad.

De la misma manera, las soluciones comerciales dedicadas a proteger los activos tecnológicos de empresas y organizaciones pueden ser percibidas como una amenaza para aquellos grupos que vean en ellas una puerta a intrusiones de los organismos

21 Su código fuente es distribuido como software libre bajo licencia AGPL (76).

de seguridad. Por ello, estos grupos suelen optar por soluciones de *software* libre y de código abierto que permitan mantener el control teórico sobre los sistemas ejecutados con unos costes de despliegue razonables. De todas formas, la elección de este tipo de soluciones no está exenta de riesgos de seguridad como puso de manifiesto la repentina clausura del proyecto de Truecrypt y los esfuerzos dedicados por su comunidad para auditar su código.

Por último, las *criptodivisas* ofrecen nuevas posibilidades de financiación complementarias a los métodos tradicionales. Las dificultades adicionales que conlleva el rastreo de las transacciones y el acceso a mercados de compraventa presentes en la *deep web* son elementos que podrían incentivar su uso de forma sumergida. Pese a ello, su utilización sistemática dependerá de la capacidad de los mercados para absorber el capital ingresado y de la preocupación de los actores involucrados para preservar su anonimato.

BIBLIOGRAFÍA

1. Lluis Dalmau. ¿Qué es guifi? | guifi.net. [En línea] 20 de marzo de 2009. [Citado el: 13 de diciembre de 2014.] https://guifi.net/es/trespasos.

2. Glanz, James. U.S. Underwrites Internet Detour Around Censors. [En línea] The New York Times, 12 de junio de 2011. [Citado el: 13 de diciembre de 2014.] http://www.nytimes.com/2011/06/12/world/12internet.html?_r=2&.

3. Open Technology Institute. About Commotion | Commotion Wireless. [En línea] 2012. [Citado el: 13 de diciembre de 2014.] https://commotionwireless.net/about/.

4. Open Garden. Open Garden | /firechat. opengarden.com. [En línea] [Citado el: 9 de octubre de 2014.] https://opengarden.com/firechat.

5. Tor Project: Anonymity Online. torproject.org. [En línea] [Citado el: 9 de octubre de 2014.]

6. RetroShare. sourceforge.net. [En línea] [Citado el: 9 de octubre de 2014.] http://retroshare.sourceforge.net/.

7. Red anónima I2P. geti2p.net. [En línea] [Citado el: 9 de octubre de 2014.] https://geti2p.net/es/.

8. The Freenet Project. freenetproject.org. [En línea] [Citado el: 9 de octubre de 2014.] https://freenetproject.org/?language=es.

9. GNUnet | GNU's Framework for Secure Peer-to-Peer Networking. gnunet.org. [En línea] [Citado el: 9 de octubre de 2014.] https://gnunet.org/.

10. OneSwarm - Private P2P Data Sharing. oneswarm.org. [En línea] [Citado el: 9 de octubre de 2014.] http://www.oneswarm.org/.

11. BitBlinder. uptodown.com. [En línea] [Citado el: 9 de octubre de 2014.] http://bitblinder.en.uptodown.com/.

12. ANts P2P. sourceforge.net. [En línea] [Citado el: 9 de octubre de 2014.] http://antsp2p.sourceforge.net/.

13. Anonet Wiki. anonet2.biz. [En línea] [Citado el: 9 de octubre de 2014.] http://anonet2.biz/.

14. Waste. sourceforge.net. [En línea] [Citado el: 9 de octubre de 2014.] http://waste.sourceforge.net/.

15. Diario Oficial de la Unión Europea. Directiva sobre el acceso a la actividad de las entidades de dinero electrónico y su ejercicio, así como la supervisión prudencial de dichas entidades. 2009.

16. Boletín Oficial del Estado. Ley 21/2011, de 26 de julio, de dinero electrónico. Núm. 179, Sec. I. Pág. 84235, Madrid : s.n., 2011.

17. Financial Crimes Enforcement Network. Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies . Washington : Department of the Treasury (USA), 2013. Guidance. FIN-2013-G001.

18. Paypal. Comprar, vender y transferir dinero por internet - Paypal España. paypal.com. [En línea] [Citado el: 09 de octubre de 2014.] https://www.paypal.com/.

19. Skrill. What is Skrill? | Skrill. skrill.com. [En línea] [Citado el: 10 de octubre de 2014.] https://www.skrill.com/en/about-us/.

20. Webmoney. Webmoney -- Universal Payment System. wmtransfer.com. [En línea] [Citado el: 10 de octubre de 2014.] http://www.wmtransfer.com/eng/information/short/index.shtml.

21. Hub Culture. Hub Culture | About us. hubculture.com. [En línea] [Citado el: 9 de octubre de 2014.] https://hubculture.com/groups/hub/projects/62/wiki/.

22. Second Life Community. Second Life Wiki. [En línea] [Citado el: 10 de octubre de 2014.] http://wiki.secondlife.com/wiki/Getting_Linden_Dollars_FAQ.

23. 1337day. FAQ | 1337day Inj3ct0r Base de datos de exploits : vulnerabilidades : 0day : Nuevos exploits : shellcode por equipo Inj3ct0r. 1337day.con. [En línea] [Citado el: 10 de octubre de 2014.] http://es.1337day.com/faq/buy_gold#buy_gold.

24. CoinMarketCup. Crypto-Currency Market Capitalizations. [En línea] 15 de diciembre de 2014. [Citado el: 15 de diciembre de 2014.] https://coinmarketcap.com/all/views/all/.

25. Nakamoto, Satoshi. Bitcoin: A Peer-to-Peer Electronic Cash System. [Documento] s.l. : Bitcoin.org, 2008.

26. FEMEN. FEMEN. femen.org. [En línea] [Citado el: 9 de noviembre de 2014.] http://femen.org/gallery?attempt=1.

27. Díez, Anabel. Activistas de Femen irrumpen en el Congreso: "El aborto es sagrado". elpais.com. [En línea] 9 de octubre de 2013. [Citado el: 9 de noviembre de 2014.] http://politica.elpais.com/politica/2013/10/09/actualidad/1381304240_913874.html.

28. EFE. Activistas de Femen protestan ante Rouco por la reforma del aborto. elpais.com. [En línea] 3 de febrero de 2014. [Citado el: 9 de noviembre de 2014.] http://sociedad.elpais.com/sociedad/2014/02/02/actualidad/1391372833_430221.html.

29. EFE/AP. Ecologistas franceses entran a planta nuclear en paracaídas. terra.com. [En línea] 5 de febrero de 2012. [Citado el: 9 de noviembre de 2014.] http://noticias.terra.com/mundo/ecologistas-franceses-entran-a-planta-nuclear-en-paracaidas,6540c6cef6e07310VgnVCM5000009ccceb0aRCRD.html.

30. Colectivo Riseup. lists.riseup.net. riseup.net. [En línea] [Citado el: 9 de noviembre de 2014.] https://lists.riseup.net/www/.

31. Loomio. Loomio | Toma de decisiones colectiva. loomio.org. [En línea] [Citado el: 8 de diciembre de 2014.] https://www.loomio.org/?locale=es.

32. The Etherpad Foundation. Etherpad. [En línea] [Citado el: 8 de diciembre de 2014.] http://etherpad.org.

33. Riseup.net. pad.riseup.net. [En línea] [Citado el: 8 de diciembre de 2014.] https://pad.riseup.net/.

34. Cohen, Noam. Hong Kong Protests Propel FireChat Phone-to-Phone App. nytimes.com. [En línea] 5 de octubre de 2014. [Citado el: 9 de noviembre de 2014.] http://www.nytimes.com/2014/10/06/technology/hong-kong-protests-propel-a-phone-to-phone-app-.html?_r=0.

35. Shadbolt, Peter. FireChat in Hong Kong: How an app tapped its way into the protests. cnn.com. [En línea] 16 de octubre de 2014. [Citado el: 9 de noviembre de 2014.] http://edition.cnn.com/2014/10/16/tech/mobile/tomorrow-transformed-firechat/.

36. BBC Mundo. La app con la que los manifestantes de Hong Kong burlan la censura china. bbc.co.uk. [En línea] 30 de septiembre de 2014. [Citado el: 8 de diciembre de 2014.] http://www.bbc.co.uk/mundo/noticias/2014/09/140930_tecnologia_hong_kong_app_protestas_ig.

37. Appgree. Appgree: Now we are talking. appgree.com. [En línea] [Citado el: 8 de diciembre de 2014.] http://www.appgree.com/.

38. Wadobo Labs. Agora Voting. agoravoting.com. [En línea] [Citado el: 8 de diciembre de 2014.] https://agora.agoravoting.com/.

39. Kickstarter Inc. Kickstarter. [En línea] [Citado el: 8 de diciembre de 2014.] https://www.kickstarter.com/.

40. Peerbackers llc. peerbackers - Your Path To Capital - Crowdfunding Consulting. peerbackers.com. [En línea] [Citado el: 8 de diciembre de 2014.] http://peerbackers.com/index.html.

41. Goteo.org. Goteo.org - Crowdfunding the commons. goteo.org. [En línea] Fundación Fuentes Abiertas. [Citado el: 9 de noviembre de 2014.] https://goteo.org.

42. FEMEN. FEMEN official store. femenshop.com. [En línea] [Citado el: 9 de noviembre de 2014.] http://femenshop.com/.

43. Paget, François. El ciberespacio: nuevo medio de difusión de ideas políticas. [En línea] [Citado el: 23 de octubre de 2014.] http://www.mcafee.com/es/resources/white-papers/wp-hacktivism.pdf.

44. El País. elpais.com. [En línea] 9 de diciembre de 2010. [Citado el: 2014 de di-

ciembre de 8.] http://internacional.elpais.com/internacional/2010/12/09/actualidad/1291849211_850215.html#EnlaceComentarios.

45. abc.es. abc.es. [En línea] 21 de diciembre de 2012. [Citado el: 8 de diciembre de 2014.] http://www.abc.es/medios-redes/20121219/abci-twitter-cierra-cuenta-anonymous-201212192044.html.

46. Pastebin. Privacy Policy for pastebin.com . [En línea] [Citado el: 8 de diciembre de 2014.] http://pastebin.com/privacy.

47. Zone-h. Zone-H.org - Unrestricted information. [En línea] [Citado el: 10 de diciembre de 2014.] http://www.zone-h.org/?zh=1.

48. Samuel, Alexandra. Hacktivism and the Future of Political Participation. Cambridge, Massachusetts : Harvard University, 2004.

49. Mailtor. Mailtor is a free anonymous email service provider. mailtor.net. [En línea] [Citado el: 8 de diciembre de 2014.] http://www.mailtor.net/.

50. Hawes, John. Freedom Hosting arrest and takedown linked to Tor privacy compromise. sophos.com. [En línea] 5 de agosto de 2014. [Citado el: 8 de diciembre de 2014.] https://nakedsecurity.sophos.com/2013/08/05/freedom-hosting-arrest-and-takedown-linked-to-tor-privacy-compromise/.

51. Callas, J., y otros, y otros. OpenPGP Message Format. IETF. [En línea] noviembre de 1998. [Citado el: 15 de diciembre de 2014.] https://www.ietf.org/rfc/rfc2440.txt.

52. Silk road: eBay for drugs. Barratt, Monica J. 3, s.l. : Addiction, 2012, Vol. 107.

53. Silk Road. Silk Road - We rise again. silkroad6ownowfk.onion. [En línea] [Citado el: 30 de septiembre de 2014.] http://silkroad6ownowfk.onion.

54. Agora Market. Agora Market. [En línea] 2014. [Citado el: 14 de diciembre de 2014.] https://agorahooawayyfoe.onion/.

55. 7bit@arcor.de. Decentralized anonymous instant messenger on top of Tor Hidden Services. github.com. [En línea] 28 de junio de 2012. [Citado el: 15 de diciembre de 2014.] https://github.com/prof7bit/TorChat.

56. TorBook. Torbook. [En línea] mayo de 2014. [Citado el: 15 de diciembre de 2014.] http://torbookdjwhjnju4.onion.

57. European Cybercrime Centre. The Internet Organized Crime Threat Assessment. s.l. : Europol, 2014.

58. G., Tim. Renting a Zombie Farm: Botnets and the Hacker Economy. [En línea] 8 de octubre de 2014. [Citado el: 11 de diciembre de 2014.] http://www.symantec.com/connect/blogs/renting-zombie-farm-botnets-and-hacker-economy.

59. Poultry markets: on the underground economy of twitter followers. Stringhini, Gianluca, y otros, y otros. [ed.] ACM. New York : s.n., 2012. Proceedings of the 2012 ACM workshop on Workshop on online social networks. ISBN: 978-1-4503-1480-0.

60. Blockchain.info. Dirección de Bitcoin 1AWqYR4CCP5j9GEqMNk8b3ZNPPfG5Jniu1. [En línea] [Citado el: 11 de diciembre de 2014.] https://blockchain.info/address/1

AWqYR4CCP5j9GEqMNk8b3ZNPPfG5Jniu1?currency=EUR.

61. Kumar, Mohit. Hacker threatens to sell data of 3.7 Million Israeli Bank Customers, demands extortion money in Bitcoin. thehackernews.com. [En línea] 21 de diciembre de 2013. [Citado el: 11 de noviembre de 2014.] http://thehackernews.com/2013/12/hacker-Israeli-Bank-botnet-malware-extortion-bitcoin.html.

62. Wei, Wang. CryptoLocker Ransomware demands $300 or Two Bitcoins to decrypt your files. thehackernews.com. [En línea] 13 de octubre de 2013. [Citado el: 11 de noviembre de 2014.] http://thehackernews.com/2013/10/cryptolocker-ransomware-demands-300-to.html.

63. Corman, Steven R. y Schiefelbein, Jill S. Communication and Media Strategy in the Jihadi War of Ideas. Arizona State University. Arizona : Consortium for Strategic Communication, 2006. Report #0601 .

64. Mundo, BBC. bbc.co.uk. [En línea] 20 de junio de 2014. [Citado el: 13 de diciembre de 2014.] http://www.bbc.co.uk/mundo/noticias/2014/06/140620_internacional_irak_isis_redes_sociales_amv.

65. Report, ITV. itv.com. [En línea] 17 de junio de 2014. [Citado el: 13 de diciembre de 2014.] http://www.itv.com/news/2014-06-17/isiss-official-app-available-to-download-on-google-play/.

66. WhisperText LLC. Whisper - Comparte y Conoce. [En línea] 9 de diciembre de 2014. [Citado el: 13 de diciembre de 2014.] https://play.google.com/store/apps/details?id=sh.whisper.

67. Segall, Laurie. cnn.com. [En línea] 16 de junio de 2014. [Citado el: 13 de diciembre de 2014.] http://money.cnn.com/2014/06/16/technology/social/whisper-app-iraq/.

68. The Guardian. Whispers, regrets and re-deployment: 10 Iraq war veterans on the Isis effect. [En línea] 17 de junio de 2014. [Citado el: 13 de diciembre de 2014.] http://www.theguardian.com/commentisfree/2014/jun/17/iraq-war-veterans-isis-stories.

69. Makuch, Ben. vice.com. [En línea] 24 de junio de 2014. [Citado el: 13 de diciembre de 2014.] http://motherboard.vice.com/en_uk/read/iraqs-isis-targeting-internet-bans-have-caused-a-huge-surge-in-tor-usage.

70. El Confidencial. elconfidencialdigital.com. [En línea] 4 de abril de 2014. [Citado el: 13 de diciembre de 2014.] http://www.elconfidencialdigital.com/seguridad/Guardia-Civil-TrueCrypt-ETA-Seguridad_0_1372662745.html.

71. El confidencial digital. Así descifra la Guardia Civil el 'TrueCrypt', el nuevo sistema de encriptación de ETA: se ha pedido ayuda a la agencia de Seguridad de Obama. [En línea] 7 de abril de 2010. [Citado el: 13 de diciembre de 2014.] http://www.elconfidencialdigital.com/seguridad/Guardia-Civil-TrueCrypt-ETA-Seguridad_0_1372662745.html.

72. Qaeda Plot Leak Has Undermined U.S. Intelligence. [En línea] http://www.nytimes.com/2013/09/30/us/qaeda-plot-leak-has-undermined-us-intelligence.html?pagewanted=2&_r=0.

73. al-'Amil, Sheikh Abu Saad. Mobile Encryption for Android (V 1.1) and Symbian.

[En línea] 2013. [Citado el: 13 de diciembre de 2014.] http://gimfmedia.com/tech/en/download-mobile-encryption/.

74. Jusino, Eric. die-less. [En línea] 2012. [Citado el: 8 de octubre de 2014.] http://die-less.com/2012/01/06/zetas-offgrid-darknet/.

75. Coinmap.org. CoinMap. [En línea] 2014. [Citado el: 13 de diciembre de 2014.] http://coinmap.org/.

76. Prusnak. Coinmap: Map showing places where you can use Bitcoin and Litecoin. [En línea] 2014. [Citado el: 13 de diciembre de 2014.] https://github.com/prusnak/coin-map.

77. Larimer, Daniel, Hoskinson, Charles y Larimer, Stan. A Peer-to-Peer Polymorphic Digital Asset Exchange. [Digital] 2013.

78. Junestam, Andreas y Guigo, Nicolas. TrueCrypt: Security Assessment (Final Report). s.l. : iSEC Partners, Open Crypto Audit Project, 2014. Security Assessment.

79. Irrera, Anna. Q&A with LMAX CEO on Ven Virtual Currency. eFinancialNews Limited. Financial News.

80. Linden dollar and virtual monetary policy. Ernstenberger, P. s.l. : Macroeconomics, Departmen of Economics, Economics I, Bayreuth University, 2009.

81. Truecrypt Development Team. WARNING: Using TrueCrypt is not secure as it may contain unfixed security issues. [En línea] mayo de 2014. [Citado el: 13 de diciembre de 2014.] http://truecrypt.sourceforge.net/.

82. blockchain.info. Número de direcciones Bitcoin únicas utilizadas. [En línea] 17 de noviembre de 2014. [Citado el: 17 de noviembre de 2014.] https://blockchain.info/es/charts/n-unique-addresses?timespan=all&showDataPoints=false&daysAverageString=1&show_header=true&scale=0&address=.

83. Loomio. Loomio is an open-source web application that helps groups make better decisions together. github.com. [En línea] [Citado el: 8 de diciembre de 2014.] https://github.com/loomio/loomio.

84. Boletín Oficial del Estado. Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo. Núm. 103, Sec. I, Pág. 37458, Madrid : s.n., 2010.

85. Webmoney. Guarantors in the WebMoney Transfer System. wmtransfer.com. [En línea] [Citado el: 10 de octubre de 2014.] http://www.wmtransfer.com/eng/subjects/guarantors/index.shtml.

86. Free Software Foundation. GNU Affero General Public License - GNU Project. gnu.org. [En línea] 3, 19 de noviembre de 2007. [Citado el: 29 de septiembre de 2014.] https://www.gnu.org/licenses/agpl.html.

87. GNU.FREE project. FREE project policy change... gnu.net. [En línea] 25 de octubre de 2002. [Citado el: 8 de diciembre de 2014.] http://www.gnu.org/software/free/.

88. Blockchain.info. Exchange Rates API: Market Prices and exchanges rates api. [En línea] 2014. [Citado el: 11 de diciembre de 2014.] https://blockchain.info/es/ticker.

89. Electronic Frontier Foundation. E-Voting Rights. eff.org. [En línea] [Citado el: 8 de diciembre de 2014.] https://www.eff.org/es/issues/e-voting.

90. The Etherpad Foundation. Etherpad: Really real-time collaborative document editing. github.com. [En línea] [Citado el: 8 de diciembre de 2014.] https://github.com/ether/etherpad-lite.

91. EMule-Project.net - Sitio Oficial de eMule. Descargas, ayudas, documentación, novedades, ... emule-project.net. [En línea] [Citado el: 9 de octubre de 2014.] http://www.emule-project.net/home/perl/general.cgi?l=17.

92. FSF France. Electronic voting and Free Software. fsffrance.org. [En línea] 17 de octubre de 2004. [Citado el: 8 de diciembre de 2014.] http://fsffrance.org/voting/voting.en.html.

93. Parlamento Europeo y el Consejo. Directiva 2009/110/CE del Parlamento Europeo y del Consejo, de 16 de septiembre de 2009 , sobre el acceso a la actividad de las entidades de dinero electrónico y su ejercicio, así como sobre la supervisión prudencial de dichas entidades, por la que se mod. DO L 267 de 10.10.2009, p. 7/17 , Directiva 2009/110/CE . s.l. : Diario Oficial de la Unión Europea, 2009.

94. Ares | Descarga gratis el mejor programa P2P. ares.com.es. [En línea] [Citado el: 9 de octubre de 2014.] http://www.ares.com.es/.

95. Wadobo Labs. A Liquid Voting system made with python and django. github.com. [En línea] [Citado el: 8 de diciembre de 2014.] https://github.com/agoravoting/agora-ciudadana.

96. Elistas. elistas.net. [En línea] [Citado el: 15 de diciembre de 2014.] http://www.elistas.net/grupos/Informatica/Seguridad.

97. LeakForums. LeakForums. [En línea] [Citado el: 15 de diciembre de 2014.] http://leakforums.org/?c=1.

98. The Republic of Lampeduza. The Republic of Lampeduza - Carding Forum, Dumps & Credit Cards Security. [En línea] [Citado el: 15 de diciembre de 2014.] http://lampeduza.so/.

99. Europol. The Internet Organized Crime Threat Assessment. s.l. : European Cybercrime Centre, 2014.

Fecha de recepción: 20/11/2014. Fecha de aceptación: 17/12/2014

BLANQUEO DE CAPITALES Y FINANCIACIÓN DEL TERRORISMO

LAS RECOMENDACIONES COMO NUEVA FORMA DE EJERCER INFLUENCIA EN UN CONTEXTO INTERNACIONAL MARCADO POR LA DESCOMPOSICIÓN DE LAS RELACIONES DE PODER

CONCHITA CORNEJO GARCÍA

RESUMEN

Este artículo realiza un breve recorrido sobre la historia de la prevención del blanqueo de capitales, explicando los principales medios normativos e institucionales que se han creado para combatirlo. En particular, analiza la peculiar naturaleza del GAFI y sus Recomendaciones, que se han revelado como un medio exitoso de regular la amenaza del blanqueo de capitales y de la financiación del terrorismo aun sin tener poder coercitivo para imponer sus estándares. También aborda el tema de la recomposición de las relaciones de poder en el mundo actual y considera que mecanismos de poder blando, como el instaurado por el Grupo de Acción Financiera (GAFI), pueden anunciar el camino que se seguirá en el contexto de unas relaciones internacionales marcadas por unos organismos que se han revelado poco eficaces para imponer sus normas en un mundo cada vez más global.

Palabras clave: blanqueo de capitales, dinero negro, gris y blanco, lavado de dinero, expoliar, GAFI, poder blando.

ABSTRACT

This article focuses on the history of money-laundering prevention. It explains the principal normative and institutional means that have been created in order to fight it. It focuses, particularly, on the analysis of the peculiar nature of GAFI[1] and its Recommendations, which have proven to be a successful mechanism for the regularization of money-laundering and for terrorism financing. Nevertheless, it does not have any kind of binding power for imposing standards. It also addresses the rearrangement of power relations in the current world and considers that soft power mechanisms, like the one installed by GAFI , can show the direction to be followed in the context of international relations under the leading of the inefficient organisms that have failed at imposing its rules in a evolving global world.

Key words: money laundering; dirty, grey and white money; sack; GAFI, solf power.

1. INTRODUCCIÓN

La aproximación a cualquier fenómeno suele partir, como es lógico, de la definición de aquello que se pretende abordar.

En nuestro caso, podemos definir el blanqueo de capitales como el conjunto de mecanismos y procedimientos, variados y complejos, que tienden a dar apariencia de legalidad a bienes que tienen su origen en un delito, y que dan lugar a lo que

1 GAFI, in spanish, is “Grupo de Acción Financiera”. In english: Financial Action Group.

vulgarmente se conoce como dinero negro. Otras veces, en cambio, la ilicitud de los fondos deriva de que sus propietarios los extrajeron del círculo de bienes conocidos por las autoridades. En este caso, hay autores que prefieren hablar de dinero gris, por ser fondos procedentes de actividades legítimas -"dinero blanco"- que adquiere tintes oscuros al ser sustraído al control de la Administración.

Para designar a este fenómeno, aunque se han sugerido los términos 'regularización', 'reconversión' o 'legalización', en España ha acabado imponiéndose la traducción literal del francés ("blanchiment") y no la anglosajona "laundering" o lavado, que ha tenido más éxito en Latinoamérica.

2. ORÍGENES REMOTOS

A juzgar por las fechas en que se aprueban las primeras normativas sobre el blanqueo de capitales, pudiera parecer que estamos ante una materia extraordinariamente novedosa, pues no es hasta los años 80 cuando empiezan a ver la luz los primeros textos legales sobre el blanqueo de capitales como realidad autónoma, dotada de entidad propia.

Sin embargo, la ocultación de determinados productos o bienes y su posterior afloramiento con apariencia de legalidad no es en absoluto un hecho nuevo ni propio de sociedades desarrolladas. En todas las épocas los delincuentes han intuido los beneficios de ocultar los frutos de sus acciones delictivas, basándose en el lógico razonamiento de que estos no son sino las pistas que llevarían a las autoridades a descubrir los delitos que los generaron.

Como ejemplo de ello, podemos citar el Medievo, cuando la usura fue declarada delito y mercaderes y prestamistas se las ingeniaban para burlar las leyes que la castigaban, encubriéndola bajo diversos mecanismos. También los piratas y corsarios se convirtieron en expertos en el arte de esconder los frutos de sus asaltos, recibiendo en ocasiones el amparo de los herederos de la tradición templar, de los banqueros de origen judío, o hasta de la propia reina de Inglaterra[2]. Las guaridas que acogían los tesoros acumulados se convirtieron en la primitiva versión de los actuales refugios financieros, que tanto entonces como ahora constituyen el último eslabón en el proceso de ocultar muchas de las operaciones dudosas o manifiestamente fraudulentas que se llevan a cabo.

Tomando alguna referencia cultural, también nos sirve para ilustrar la antigüedad del fenómeno un revelador pasaje del capítulo 54 de nuestra obra literaria más universal, El Quijote, que expresa en estos términos las prácticas de los peregrinos:

"Juntéme con estos peregrinos, que tenían por costumbre de venir a España muchos dellos cada año, a visitar los santuarios della, que los tienen por sus Indias, y por certísima granjería y conocida ganancia. Ándala casi toda, y no hay pueblo ninguno de donde no salgan comidos y bebidos, como suele decirse, y con un real, por lo menos, en dineros, y al cabo de su viaje, salen con más de cien escudos de sobre trocados en oro, o ya en el hueco de los bordones, o entre los remiendos de las esclavinas, o con la industria que ellos pueden, los sacan del reino y los pasan a sus tierras, a pesar de las guardas de los puestos y puertos donde se registran".

2 Fue el caso de del pirata inglés Francis Drake, quien fue armado caballero en su nave por la propia reina Isabel I de Inglaterra, como recompensa por sus exitosos asaltos a puertos y barcos españoles. En 1612, Inglaterra ofreció a los piratas que abandonaran su actividad un perdón incondicional y el derecho a conservar el producto de sus felonías.

3. EL BLANQUEO DE CAPITALES EN LA MODERNIDAD

Tras siglos de blanqueo de capitales bajo unos esquemas más o menos precarios, los años 70 marcan un cambio sustancial en las dimensiones que adquiere el blanqueo de capitales, debido principalmente al extraordinario crecimiento de determinadas actividades delictivas y, muy en especial, del tráfico de drogas. Sin embargo, la Guerra Fría y su política de bloques marcaba un escenario de necesaria contención en el que el Muro de Berlín era, para bien y para mal, una enorme presa que retenía el desbordamiento de las estructuras y organizaciones delictivas que, años después, permitieron organizar la producción, distribución y comercialización de la droga y sus frutos económicos a escala mundial.

La caída del Muro de Berlín y, con él, la de los frenos existentes en los resortes que contenían la actividad delictiva transnacional, marcó un antes y un después en la política de lucha contra el blanqueo de capitales. De hecho, no es casualidad que el GAFI naciera precisamente en 1989, año en que Europa se vio por fin despojada de su vergonzoso Telón de Acero.

El fin de la política de bloques, y el consiguiente nacimiento de la globalización económica, tomaron la forma de un extraordinario crecimiento de los intercambios comerciales, de desarrollo de los transportes internacionales de mercancías, de liberalización del comercio internacional y de las restricciones arancelarias asociadas a ellos y, paralelamente, de una internacionalización del sistema financiero mundial. Los problemas, antaño nacionales, se hicieron globales y los países encargados de resolverlos pronto llegaron a la obvia conclusión de que hacía falta una arquitectura institucional transnacional para poder acabar con ellos.

La Administración Reagan se apresuró en tomar las riendas para dar cauce a esta demanda de soluciones globales, iniciando una aproximación internacional contra el tráfico de drogas que derivó, entre otras, en una clara conclusión: la lucha integral contra el narcotráfico debía incluir como uno de sus aspectos principales el impedir que los ingresos procedentes de la venta de drogas ingresaran en los cauces económicos ordinarios. Había nacido la lucha contra el blanqueo de capitales como fenómeno autónomo.

Una vez delimitada la parcela a combatir, faltaba identificar los frentes por los que atajarlo. Surgieron así dos vías, distintas y complementarias en cuanto a medios y fines:

1. La vía de la prevención: mediante esta vía se intenta evitar, básicamente, que el blanqueo de capitales llegue a producirse. Como en tantos otros sectores de la realidad (accidentes de tráfico, enfermedades coronarias, etc.), el dicho popular “más vale prevenir, que curar” toma forma en esta parcela de la realidad y se identifica una serie de medidas que resultarían idóneas para impedir que el blanqueo de capitales pueda tener lugar.

2. La vía de la represión o vía penal: entra en juego cuando los mecanismos preventivos han fracasado, los delincuentes logran ingresar el dinero negro en los cauces económicos ordinarios y el blanqueo de capitales se convierte así en una realidad. La actividad de las autoridades se centra entonces en el castigo de esta conducta.

3.1. LA VÍA DE LA PREVENCIÓN

El estudio de las actividades de los blanqueadores de dinero enseguida reveló que éste se producía principalmente a través del sistema financiero, cuyo crecimiento en volumen y complejidad durante la etapa de la globalización económica había resultado extraordinario.

La lógica consecuencia de esta constatación fue la imposición de determinadas obligaciones a quienes ejercían una actividad bancaria, en el entendimiento de que, al ser ellos quienes tenían un contacto directo con el cliente, debían colaborar con la administración a la hora de proporcionar determinada información de relevancia para el interés público.

La imposición a las entidades financieras de determinadas obligaciones que trascienden el ámbito propio de su actividad no es más que una constatación de las limitaciones de la Administración Pública, quien, para acceder a datos que por sus propios medios es incapaz de obtener, se ve en la necesidad de convertir a determinados sectores de la realidad económica en sujetos obligados por la legislación de blanqueo de capitales. Desde ese momento, las obligaciones de prevención del blanqueo de capitales se configuran como un requisito más para poder ejercer una determinada actividad (en este caso, inicialmente, sólo la financiera), entrando dentro de lo que se conoce en la terminología anglosajona como “the cost of doing business”.

Inicialmente, el sector financiero fue el destinatario principal de los primeros textos sobre prevención del blanqueo de capitales. Así se observa, por ejemplo, en:

- La Declaración de Basilea de 1988, adoptada por los representantes de los bancos centrales del Grupo de los Diez.
- Los informes del GAFI de principios de la década de los 90[3]
- La Primera Directiva 91/308/CEE de la Unión Europea sobre la materia, de 10 de junio de 1991, cuyo título es precisamente “Directiva relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales”.

En España, la transposición de esta Directiva se produjo mediante la Ley 19/1993, de 28 de diciembre, sobre determinadas medidas de prevención del blanqueo de capitales (hoy derogada por la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo). Conviene destacar aquí que nuestra ley fue pionera en no circunscribir el elenco de sus sujetos obligados a las entidades financieras, extendiendo notablemente su ámbito de aplicación a otros sectores (casinos, inmobiliarias, auditores, contables, asesores fiscales, notarios, abogados, etc.). Así, nuestra ley resultó ser claramente premonitoria de la imparable tendencia que se siguió en los años posteriores en toda la comunidad internacional y que se concreta en:

- el extraordinario incremento de los sectores que se convierten en sujetos obligados por la normativa de prevención del blanqueo de capitales, debido principalmente a que el cerco establecido sobre el sector financiero hizo que los blanqueadores buscaran otros cauces menos vigilados por las autoridades para disimular el origen de sus actividades

3 GAFI, La lutte contre le blanchiment de capitaux. Paris, 1990, p.16

- y el aumento del número de delitos que pueden dar lugar al blanqueo de capitales, pues si bien inicialmente sólo el narcotráfico tenía la condición de delito subyacente, pronto la comunidad internacional extendió esta consideración a cualquier tipo de delito.

3.2. LA VÍA DE LA REPRESIÓN O VÍA PENAL

A través de este cauce, los esfuerzos de la comunidad internacional se centraron en penalizar el blanqueo de capitales, tipificándolo como un delito en sí, autónomo e independiente de la actividad delictiva que producía el dinero que se intenta blanquear.

En este marco se inscribe la Convención de Viena de 1988 ("Convención de las Naciones Unidas contra el tráfico ilícito de estupefacientes y sustancias psicotrópicas"), que da un paso muy significativo al plasmar por primera vez en un texto internacional una clara definición del blanqueo de capitales, todavía vinculada exclusivamente al tráfico de drogas, en los siguientes términos: "conversión o transferencia de bienes a sabiendas de que procedieran de un delito de tráfico de drogas, la ocultación de su origen ilícito, o la ayuda al autor del delito para eludir las consecuencias jurídicas de sus acciones".

La Convención de Viena exigía a los países firmantes tomar medidas para tipificar en sus respectivos países el blanqueo de capitales, lo que supuso un espaldarazo definitivo en la lucha contra esta lacra. Más de 160 estados ratificaron el texto, haciéndolo el Estado español el 30 de julio de 1990.

El posterior Convenio de Estrasburgo de noviembre de 1990 y la Primera Directiva comunitaria de 1991, ya mencionada, siguen la misma senda, arrastrando tras de sí a la inmensa mayoría de los países occidentales, quienes se fueron sumando a la tipificación del delito de blanqueo de capitales. Como novedad con respecto a la Convención de Viena cabe destacar la extensión del concepto de blanqueo de capitales, que deja de estar referido únicamente a los fondos procedentes del narcotráfico para generalizarlo a los que tienen su origen en cualesquiera de las actividades delictivas.

En nuestro caso, el Código Penal Español de 1995 recoge la conducta del blanqueo de capitales en sus artículos 301 a 304, aunque sin utilizar este nombre específico que sí recogía el Proyecto de Código Penal de 1992.

4. EL BLANQUEO DE CAPITALES TRAS LA CAÍDA DEL MURO DE BERLÍN

Como señalábamos, a comienzos de la década de los 90 la comunidad internacional adquiere conciencia clara de los problemas que lleva aparejados el blanqueo de capitales. Dos son, en síntesis, los grandes bloques de amenazas:

- El favorecimiento de la actividad criminal subyacente.

  La dificultad para blanquear los beneficios es un factor que disuade o complica la actividad ilegal subyacente. Desde esta perspectiva, la mayor facilidad para legitimar los beneficios de actividades delictivas contribuye indirectamente a potenciar esas actividades y, muy especialmente, en los delitos que se desarrollan a escala internacional, como el tráfico de drogas.

- La desestabilización del incipiente sistema financiero internacional.

  Para explicar este riesgo es preciso no perder de vista que el objetivo de todo sistema financiero es canalizar el ahorro hacia la inversión. A partir del binomio riesgo/rentabilidad de los activos, se produce la asignación eficiente de los recursos. Pues bien, cuando el dinero ha sido ilícitamente obtenido se asigna o se invierte frecuentemente atendiendo a otro tipo de razones distintas de la rentabilidad/riesgo de los activos, ya que en estos casos predomina la inversión por razones de opacidad o de falta de transparencia en la identificación de los titulares.

  En un contexto cada vez más globalizado, estos riesgos no resultaban fáciles de prever y no atajarlos podía contribuir a generar movimientos desestabilizadores cuyo alcance resultaba complicado de evaluar.

  Por otra parte, la integridad y la credibilidad de las instituciones financieras y de los mercados de capitales dependían en buena medida de la percepción generalizada de funcionar conforme a estándares legales, profesionales y éticos adecuados. La sospecha o evidencia de actitudes de complicidad, involuntaria o no, con estas actividades podía producir un riesgo de daño serio en la credibilidad de las instituciones y, en último término, del propio sistema financiero.

  En consecuencia, vemos cómo junto al interés de los estados de luchar contra toda forma de delincuencia aparece la necesidad de alejar o de prevenir la utilización del sistema financiero como instrumento para el blanqueo, tratando de evitar las consecuencias de desestabilización y descrédito del sistema en su conjunto. Esto justifica de alguna manera la intervención del regulador económico mediante el establecimiento de normas administrativas de vigilancia y de prevención del uso del sistema financiero en la posible legitimación de beneficios ilícitamente obtenidos.

Paralelamente a la toma de conciencia sobre sus riesgos, el blanqueo de capitales se vio favorecido por diversos **factores y cambios en las políticas gubernamentales que tuvieron lugar durante la década de 1990**.

En primer lugar la mayor parte de países abandonaron el control de divisas, por lo que dejó de ser necesario obtener la autorización del gobierno para convertir moneda local en moneda extranjera, o viceversa. Ello disparó el volumen diario global de intercambio de divisas, que pasó de 590.000 millones de dólares en 1989 a 1,88 billones en 2004.

A ello hay que unir, en el ámbito de la Unión Europea, que unos cuantos países fusionaron sus monedas adoptando el euro, al tiempo que otros adoptaron el dólar o el euro prácticamente como segunda moneda oficial.

Estos factores ampliaron increíblemente el ámbito de actuación de los blanqueadores, quienes ganaron en oportunidades y ampliaron su radio de acción.

Como consecuencia lógica de esa libre conversión de divisas, tuvo lugar la apertura al extranjero de un número creciente de mercados de capitales que hasta ese momento habían sido locales. Así, en un breve lapso de tiempo, pasó de prohibirse la propiedad extranjera de bancos locales a convertirse en una práctica común, incluso

alentada por las propias autoridades, que impulsaban la inversión en el país. (Por dar un dato, la inversión directa extranjera anual pasó de 209.000 millones de dólares en 1990 a 560.000 millones en 2003).

Todo ello se tradujo en nuevas oportunidades para los blanqueadores, que vieron favorecido su objetivo de reintegrar el dinero blanqueado en la economía global.

Otro elemento catalizador del blanqueo de capitales fue la competencia por el capital. La necesidad de captar fondos favoreció enormemente a los blanqueadores, conocedores de que siempre habrá quien se salte los estándares internacionales y evite investigar acerca del origen del dinero con el objetivo de incrementar la cuenta de resultados de su compañía.

Pero la revolución de la información fue, sin duda, el factor más decisivo para potenciar las transacciones internacionales y, paralelamente, el blanqueo de capitales, permitiendo que transacciones instantáneas puedan realizarse –para bien y para mal - desde cualquier lugar del mundo.

Asimismo, la enorme demanda de servicios financieros ilícitos favoreció sin duda el blanqueo de capitales. Cada vez que una actividad comercial ilícita crece, crece también con ella la necesidad de blanquear sus frutos. De modo que el blanqueo de capitales no es sólo una actividad delictiva en sí misma, sino una necesidad imprescindible para los delitos subyacentes de los cuales trae causa.

Se calcula que en la actualidad el blanqueo de dinero representa entre el 2 y el 5 por ciento del PIB mundial; es decir, entre 800.000 millones y dos billones de dólares. Algunas estimaciones incluso lo sitúan en el 10 por ciento del PIB global. Si a ello le añadimos la evasión fiscal y los diversos tipos de fraude concluiremos que existen pocos negocios que disfruten de una demanda tan ingente como éste.

Gracias a ello, ha surgido una nueva clase de profesionales dedicada a canalizar el dinero hacia los lugares más apetecibles desde el punto de vista del riesgo y necesidades del cliente. Entre ellos puede citarse a los blanqueadores de dinero profesionales, que se encargan de realizar todas las operaciones necesarias, a cambio de una comisión, y que incluso actúan como gestores de activos de las ganancias blanqueadas. Este tipo de profesiones empieza a ser objeto de persecución por parte de las Recomendaciones del GAFI y las disposiciones nacionales que incorporan sus contenidos al Derecho patrio.

Los terroristas y los traficantes constituyen también dos grupos de usuarios de servicios financieros ilícitos. Pero existe otro constituido por los individuos corruptos. Nos referimos a personas cuya vida es aparentemente normal y cuyo perfil no encaja en el concepto clásico del delincuente que el cine norteamericano nos acostumbra a imaginar. Se trata de evasores de impuestos, políticos, jefes de estado corruptos o altos cargos de la administración pública, que desean ocultar el dinero expoliado a su país en cuentas secretas de bancos extranjeros.

Y es que hay delitos, como el narcotráfico, cuya ilicitud salta a la vista. Sin embargo otros, como la evasión fiscal, se sitúan en una línea fronteriza que hace más difícil separar lo lícito de lo ilícito. Y ello es así porque, en la mayor parte de los casos, la evasión de impuestos constituye una práctica casi legal que utiliza servicios financieros extranjeros para reducir las responsabilidades fiscales, cometiendo un fraude de

ley que cumple, aunque sólo en apariencia, con la literalidad de las normas.

Como vemos, libres de la burocracia y macroestructuras de los gobiernos e instituciones internacionales, los blanqueadores de dinero se situaron en una posición inmejorable para descubrir antes que nadie las infinitas posibilidades que ofrecía la globalización financiera para poseer, trasladar y utilizar fondos ilegales.

5. LA PECULIAR NATURALEZA DEL GAFI

Éste es el contexto en el que, en 1989, surge el GAFI, con el único objetivo inicial de combatir el blanqueo de capitales procedente del narcotráfico.

La principal peculiaridad del GAFI estriba en que se trata de un organismo que carece de capacidad legislativa o autoridad para la investigación de patrimonios, por lo que sus decisiones no tienen capacidad normativa, sino que actúan sólo como meras recomendaciones. Sin embargo, es llamativo cómo la fuerza de estas meras recomendaciones ha impulsado el cumplimiento voluntario de sus postulados. Los países buscan la adhesión a sus principios y adecúan sus normas nacionales a sus estándares internacionales, ya que el ser admitido como miembro supone que el país candidato debe tener importancia estratégica, lo que supone un reconocimiento público de gozar de una posición relevante. Es así como las recomendaciones del GAFI pueden encuadrarse dentro del concepto de poder blando o “soft power” que definiremos después.

Por otro lado, los futuros miembros deben también aportar un compromiso escrito con respaldo político en el que se comprometan con los principios y objetivos de la organización, con la aplicación de las recomendaciones y con el sometimiento a los procesos de evaluación mutua. Además, su candidatura debe contribuir a un equilibrio geográfico del conjunto.

Por su parte, cada Estado miembro del GAFI debe legislar sobre esta materia adaptándose a los objetivos de las recomendaciones, pero haciéndolo cada uno de conformidad con su propio sistema normativo y judicial. De algún modo, el GAFI funciona con un mecanismo similar al de las directivas comunitarias, que exigen unos objetivos que se deben cumplir pero dejan libertad a los estados en la elección de los instrumentos y medios para conseguirlo.

6. EL MUNDO TRAS EL 11 DE SEPTIEMBRE DE 2001

El repentino final de la Guerra Fría y la victoria ideológica que representó, junto con el crecimiento económico de Estados Unidos y el auge de las comunicaciones y la tecnología en los años noventa, parecían anunciar un mundo unipolar, en el que Estados Unidos, la superpotencia victoriosa, podría frustrar las ambiciones hegemónicas de otros posibles rivales.

Desde 1945, y hasta ese fatídico 11 de septiembre en que Estados Unidos se vio sacudido por un brutal atentado terrorista en su propio suelo, el mundo estaba en orden. Es cierto, sí, que se produjeron numerosos conflictos regionales causantes de dolor y destrucción, pero ninguno de ellos degeneró en una guerra mundial. Si indagamos acerca de la causa de tan perdurable paz, debemos encontrarla en la “Teoría de la estabilidad hegemónica”, desarrollada en los años setenta por el catedrático del Mit

Charles Kindleberger. Según ésta, una potencia dominante que tenga la capacidad y el interés de garantizar el orden mundial es el mejor antídoto contra un caro y peligroso caos internacional. Si no hay una potencia hegemónica, la única forma de asegurar la paz y la estabilidad es la adopción de un sistema de reglas basado en normas, leyes e instituciones que todos los países se comprometan a obedecer a cambio de los beneficios de esa paz y esa estabilidad.

El hecho de que el poder hegemónico norteamericano lograra dotar al mundo de un período inusitado de paz contribuyó a revelar dos nuevas tendencias que influyeron sobre el uso y los límites del poder en el sistema internacional. Una de ellas fue el poder blando, esa idea conforme a la cual el poder de un estado podía expresarse mediante el atractivo de su cultura, valores e ideas. La otra fue la extraordinaria proliferación de organizaciones, tratados, leyes internacionales y convenios a los que se fueron adhiriendo cada vez más países en la segunda mitad del S. XX.

Este poder blando como medio para triunfar en la política internacional resultó fascinante. Ya en tiempos remotos, la llamada “mission civilisatrice” de cualquiera de los imperios antiguos (romano, francés, español…) pretendía adoctrinar a los súbditos coloniales sobre las glorias de la civilización recurriendo a los atractivos del lujo o la creación de estructuras educativas, sociales y culturales.

En su versión moderna, como señala el politólogo Joseph Nye en su libro “La paradoja del poder norteamericano”, el poder blando es un tipo de poder difícil de medir pero fácil de detectar: el poder de la reputación y la estima, la buena consideración de las instituciones, una economía en la que resulta deseable trabajar o comerciar, una cultura seductora. O, en lo que a nosotros nos interesa, un sistema financiero confiable, acorde a los estándares internacionales, y menos proclive de ser malutilizado para el blanqueo de capitales.

Esta forma de poder puede ser menos cuantificable que el número de aviones de combate, divisiones de infantería o barriles de crudo, pero su impacto es indiscutible. Resulta obvio que Silicon Valley y Hollywood contribuyen al poder blando de Estados Unidos impulsando la innovación tecnológica mundial y difundiendo productos del mundo del espectáculo llenos de cultura americana y, en ese tipo de poder, aunque no pueda hablarse de total monopolio, su dominio era aplastante.

El mundo disfrutaba entonces del grado de cooperación internacional más alto de la historia. A partir de la creación de Naciones Unidas en 1945, los gobiernos confían en cada vez más instrumentos de cooperación, siendo las Recomendaciones del GAFI un caso particular de esos medios colaborativos que surgen en un contexto de ausencia de poder coercitivo internacional.

Así pues, esa acertada combinación de hegemonía y normas internacionales trajo consigo innumerables beneficios para la estabilidad mundial. Los teóricos de la estabilidad hegemónica parecían estar en lo cierto al afirmar que el poder duro de las armas y el dinero, el poder blando de la cultura y las ideas y los tratados que vinculaban a países e instituciones multilaterales garantizarían un largo periodo de paz sin amenazas.

Pero no fue así. El 11 de septiembre hizo añicos la fantasía de que Estados Unidos tenía el control sobre el mundo y sus ciudadanos eran inmunes a ataques dentro de sus fronteras. Las guerras de Irak y Afganistán revelaron las insuficiencias de su

poderío militar. Y, más tarde, la crisis financiera y la recesión económica mostraron la fragilidad de su economía.

Y al tiempo que se debilita la influencia militar y económica de las grandes potencias, se diluye también su poder blando, ese que hace atractiva su cultura, sus marcas, su sistema político y sus valores. Hoy Hollywood compite con Bollywood, con las telenovelas latinoamericanas, los "reality shows" de Sudáfrica y los videojuegos y estrellas de música pop de Corea del Sur, quien también se va situando a la cabeza en la difusión mundial de marcas de consumo tales como Samsung, Hyundai, Kia y LG.

Las relaciones de poder cambian. Las superpotencias ya no actúan como venían haciéndolo en el pasado. Se estrecha su margen de maniobra y la capacidad de las pequeñas potencias para ponerles obstáculos, sortearlas o sencillamente ignorarlas comienza a crecer. La búsqueda de una superpotencia hegemónica que imponga el orden y la estabilidad, o de un pequeño grupo de naciones que dirija el mundo, resulta vana en un mundo lleno de actores multilaterales que afrontan nuevas amenazas difusas.

La manera en la que se redefine el poder obliga a buscar variaciones en los antiguos métodos para seguir garantizando la estabilidad mundial y la ausencia de conflictos. Y la financiación del terrorismo salta a la escena internacional como la principal amenaza a combatir, sin que los llamados a hacerlo contaran con las estructuras apropiadas para ello.

En ese contexto, la tendencia anterior de alcanzar acuerdos cada vez más globales se hace menos frecuente, mientras que se hace necesario buscar nuevas formas de coordinación internacional. Es entonces cuando la institución del GAFI y su sistema de recomendaciones se revela idóneo para afrontar esta lucha sin precedentes. Por ello, con carácter urgente, en el año 2001 el GAFI extiende su mandato a la lucha contra la financiación del terrorismo y se aprueban ocho (luego nueve) recomendaciones especiales dirigidas a este fin, que se suman a las 40 ya existentes para prevenir el blanqueo de capitales.

En 2003 las recomendaciones del GAFI se revisaron y junto con las recomendaciones especiales fueron avaladas con carácter voluntario por más de 180 países; y son reconocidas universalmente como el estándar internacional contra el lavado de activos y el financiamiento del terrorismo.

Frente a los grandes acuerdos globales a los que se aspiraba antaño, hoy considerados mayoritariamente utópicos, autores como Moises Naim apuestan por el llamado "minilateralismo", que consiste en reunir el menor número posible de países necesario para tener el mayor impacto en un problema global cuya solución escapa a la acción individual de un solo país. La idea es que intentar la búsqueda de acuerdos -y la actuación conjunta- entre un número pequeño de países tiene más posibilidades de tener un efecto significativo que intentar la coordinación de casi 200.

Ésta es la idea que subyace tras la creación de los organismos regionales hermanos de GAFI, que se dedican a la prevención y al combate del lavado de activos y financiamiento del terrorismo en sus respectivas áreas territoriales. Ante el éxito de GAFI, al que la mayoría de países quería pertenecer, surgieron estos organismos regionales que, con idénticos propósitos y métodos, llevaban a cabo sus funciones

en áreas más delimitadas, lo que traía consigo la ventaja de un mejor manejo de sus funciones, así como una identificación de tipologías comunes de lavado por zonas geográficas que facilitaba su combate en los respectivos territorios.

Bajo estos esquemas, basándose en GAFI, nacieron los siguientes organismos regionales:

- APG (Grupo Asia-Pacífico)
- GAFIC-CFATF (región del Caribe)
- MONEYVAL (países del Este pertenecientes al Consejo de Europa)
- EAG (Grupo Euroasiático)
- ESAAMLG (Grupo de África del Sur y del Este)
- GAFISUD (América del Sur)
- GIABA (Grupo intergubernamental del África Occidental)
- GAFIMENA (Grupo de Oriente Medio y Norte de África)

7. LAS TRANSFORMACIONES DEL PODER Y LAS NUEVAS AMENAZAS PARA LA COMUNIDAD INTERNACIONAL

La difusión del poder fomenta también la aparición de infinidad de grupos criminales o terroristas que atentan contra la seguridad ciudadana, llegando a erosionar la estabilidad internacional. Para ellos, las fronteras son irrelevantes y los gobiernos un obstáculo cada vez más ineficaz al que atacar o ignorar. Esta tendencia ha facilitado el auge de grupos políticos extremistas -separatistas, xenófobos o anarquistas- tanto en las democracias establecidas como en las incipientes.

Contar en el escenario internacional con un grupo de actores más variado e incluyente que antaño, y reducir el número de decisiones que unos cuantos poderosos imponen arbitrariamente al resto del mundo, tiene muchas ventajas. Pero ello conlleva también inconvenientes, puesto que lograr resultados en este contexto se ha convertido en una tarea mucho más complicada. Sin embargo, la protección de los bienes públicos globales como la seguridad internacional, la prevención del blanqueo de capitales, la represión del terrorismo internacional o la no proliferación de armas de destrucción masiva son metas que, de alcanzarse, beneficiarían a toda la humanidad y a las que no se puede en ningún caso renunciar.

Estas dificultades en la gobernabilidad se han hecho muy visibles en Estados Unidos, donde se están empezando a sentir los efectos de un sistema cargado de pesos y contrapesos. Como señala Francis Fukuyama “los norteamericanos se enorgullecen mucho de una Constitución que limita el poder ejecutivo mediante una serie de controles y contrapesos. Pero esos controles han sufrido una metástasis. Y Estados Unidos se ha convertido en una vetocracia. Cuando este sistema se une a unos partidos ideologizados su resultado es la parálisis”.

O en palabras del economista Peter Orszag: “si queremos salir de nuestra parálisis actual, necesitamos no solo un liderazgo fuerte, sino también cambios en las normas

institucionales (…) necesitamos hacer frente al hecho de que una administración polarizada y paralizada está causando verdadero daño a nuestro país. Y tenemos que encontrar alguna forma de salir de esa situación".

La multiplicidad de actores en un mundo global puede llevar a lo que MOISES NAÎM denomina "competencia ruinosa", como metáfora que designa los problemas que pueden surgir con la dispersión del poder y su consiguiente deterioro. El reparto del poder -ya lo decía Montesquieu- evita su abuso. Pero cuando el poder es más difícil de usar y conservar, y se reparte entre un grupo cada vez mayor y cambiante de pequeños actores, hay más probabilidades de que aparezcan formas de competencia e interacción perjudiciales para el bien social que amenazan la salud de las economías, la estabilidad de las naciones e incluso la paz mundial.

En filosofía política la idea análoga la representa el contraste clásico entre dos extremos: la tiranía y la anarquía. Cuando el poder está demasiado concentrado engendra tiranía. En el extremo opuesto, cuando más fragmentado y diluido está el poder mayor es el riesgo de anarquía, un estado en el que no existe orden. Ambos extremos son improbables. Pero lo esencial es que la dilución excesiva del poder y la incapacidad de los principales actores de ejercer el liderazgo son tan peligrosas como la concentración del poder en unas pocas manos. La degradación excesiva del poder, que hace que todos los actores importantes puedan vetar las iniciativas de los demás, pero ninguno de ellos pueda imponer su voluntad, constituye un peligro para cualquier comunidad, ya sea una familia, una escuela, un país o para el sistema de naciones. Cuando el poder tiene tantas restricciones, se crea un terreno muy fértil para la parálisis en la toma de decisiones. Y en esos casos la estabilidad, la previsibilidad y la seguridad resultan perjudicadas.

La aparición de nuevas amenazas en el panorama mundial no ha producido todavía sus propias respuestas institucionales: aún no han aparecido innovaciones en la organización de los problemas globales que mantengan a raya los innumerables peligros que genera el poder hiperdifuso.

La conclusión a la que nos llevan las transformaciones del poder es que sus múltiples beneficios chocan con la falta de alternativas de gobernabilidad que sustituyan a los esquemas antiguos. Acaso la forma en que la comunidad internacional afrontó la prevención del blanqueo de capitales y, más tarde, la lucha contra la financiación del terrorismo nos dé algunas pistas sobre el modo de afrontar problemas globales en un futuro próximo.

Durante el siglo XX la idea de cómo responder a problemas que ningún país puede solventar por sí solo fue crear organizaciones internacionales como Naciones Unidas, y todos sus organismos especializados, el Banco Mundial, el Fondo Monetario Internacional y grupos regionales. Por desgracia el número y la complejidad de estos problemas globales han crecido mucho, mientras que la capacidad de estas organizaciones para atenderlos con eficacia ha aumentado más lentamente. Pero los resultados conseguidos por GAFI y sus organismos regionales revelan un cumplimiento voluntario de estándares de conducta mutuamente aceptados que puede calificarse de altamente satisfactorio.

Otra de las claves de su éxito es que los estándares del GAFI están en constante adaptación. Así, después de concluida la tercera ronda de Evaluaciones Mutuas de

sus miembros, el GAFI revisó y actualizó sus Recomendaciones en cooperación con los Organismos Regionales estilo GAFI y los organismos observadores, incluyendo el Fondo Monetario Internacional, el Banco Mundial y las Naciones Unidas. Las revisiones contemplan nuevas amenazas emergentes (incluyendo la proliferación de armas de destrucción masiva) y clarifican y fortalecen muchas de las obligaciones existentes, manteniendo la estabilidad necesaria y el rigor de las recomendaciones.

Los estándares de GAFI han sido también revisados y se fortalecieron los requisitos para las situaciones de mayor riesgo a fin de permitir que todos los países se focalicen más en aquellas áreas de alto riesgo o donde se podría mejorar la implementación. Los países deben primero identificar, evaluar y entender los riesgos del lavado de activos y el financiamiento del terrorismo que enfrentan y, luego, adoptar las medidas adecuadas para mitigar los riesgos. El enfoque basado en riesgo permite que los países adopten medidas más flexibles para orientar los recursos de manera más efectiva y aplicar medidas preventivas acordes con la naturaleza de los riesgos, para focalizar sus esfuerzos de manera más efectiva, optimizándolos.

8. LOS NUEVOS PARAÍSOS FISCALES

Decíamos anteriormente que las guaridas que acogían los tesoros acumulados de piratas y corsarios se convirtieron en la primitiva versión de los actuales refugios financieros, que tanto entonces como ahora constituyen el último eslabón en el proceso de ocultar muchas de las operaciones dudosas o manifiestamente fraudulentas que se llevan a cabo.

Desde entonces, hasta hace no mucho, los llamados paraísos fiscales representaban algo bastante tangible, un conjunto de lugares que podían localizarse en un mapa. Su término se popularizó porque inicialmente muchos de los territorios eran paradisíacas islas en las que se combinaban a la perfección estos servicios financieros privilegiados con la oferta turística más atractiva. Ejemplo de ello son las islas Bermudas o las Caimán, cuya proximidad geográfica con Miami o Nueva York favorece sus actividades. Las cifras son elocuentes. El estado de Nauru, en el Pacífico, con una población de 12.000 habitantes, es sede de 40.000 empresas registradas, incluido un número estimado de 400 bancos fantasma que en la práctica se reducen a un pequeño despacho con una placa en la puerta. Las islas Caimán, cuya población es de unos 43.000 habitantes, cuentan con cerca de 600 bancos, entre los que se encuentran 47 de los 50 más importantes del mundo.

En la actualidad, sin embargo, no resulta tan fácil identificar los “refugios” de capital ilícito. Aunque perduran los paraísos clásicos, existen hoy muchos más sitios donde blanquear dinero y hacer negocios ilícitos sin levantar las sospechas asociadas a las paradisíacas islas. Son lugares estratégicos, situados al filo de la ley, pero más útiles aún para el anonimato que demanda este tipo de actividades. Lo que los define es la existencia de regulaciones débiles, gobiernos permisivos y fuerzas policiales fácilmente sobornables.

Ejemplo de ello es el contrabando que se da en la triple frontera de Ciudad del Este, lugar de canalización de la cocaína procedente de los países andinos. O también el que se produce en Transdniéster (en las proximidades del mar Negro) o en la provincia afgana de Badajshán.

Los nuevos “paraísos” ganan atractivo por su capacidad de convertir en dinero efectivo mercancías valiosas fácilmente transportables. Dubai, por ejemplo, ofrece a los blanqueadores una poderosa combinación, al ser al mismo tiempo un centro de transporte internacional, una plaza bancaria off-shore y uno de los principales mercados de oro del mundo.

Además, Internet es una poderosa maquinaria de crear negocios que pueden funcionar como tapadera para el blanqueo de dinero, al hacer muy sencillo mantener el anonimato y no existir una jurisdicción claramente responsable a la que atribuir los delitos.

Asimismo, las llamadas “cajas chinas” o “matrioskas” aluden a las empresas tapaderas de Europa oriental que son filiales unas de otras en una cadena interminable que resulta muy difícil desenmascarar.

9. UNA NUEVA NORMATIVA PARA UN TIEMPO NUEVO

Las 40+9 Recomendaciones del GAFI se revisaron en 2012, dando lugar a un documento único denominado “Estándares internacionales contra el Lavado de Dinero y la Financiación del Terrorismo y la Proliferación: Las Recomendaciones del FATF-GAFI” (International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: the FATF Recommendations).

Sus principales diferencias con las anteriores están en que el documento actual no maneja recomendaciones diferenciadas, en función del tipo de amenaza que se propone combatir, y en el hecho de que ahora se recoge, de modo expreso, la materia de la proliferación de armas de destrucción masiva, que se situó bajo el paraguas de GAFI a partir del año 2008.

Las Recomendaciones se agrupan en torno a las siguientes áreas temáticas:

Las Recomendaciones 1 y 2 versan sobre la evaluación de los riesgos existentes bajo el llamado enfoque basado en el riesgo (risk-based approach) y la coordinación y cooperación nacional de las distintas autoridades, tales como la unidad de inteligencia financiera, las autoridades de política económica y legislativa o las fuerzas de seguridad.

Las Recomendaciones 3 y 4 tratan acerca de la tipificación del delito de blanqueo de capitales y los aspectos relacionados con la confiscación y las medidas provisionales.

Los aspectos centrados en la tipificación de los delitos de financiación del terrorismo, de financiación de la proliferación, en las sanciones financieras sobre ambos y las organizaciones sin fines de lucro se abordan en las Recomendaciones 5 a 8.

En cuarto lugar, en las Recomendaciones 9 a 23, se especifica el grueso de las medidas preventivas a tomar por entidades financieras y por las actividades y profesiones no financieras designadas, para impedir el lavado de activos y la financiación del terrorismo y la proliferación, tales como: secreto bancario, medidas de debida diligencia con el cliente, mantenimiento de registros actualizados, medidas para personas expuestas políticamente, banca de corresponsales, servicios de transferencia de dinero, etc.

Las Recomendaciones 24 y 25 se refieren a la adopción de las medidas necesarias para que las personas jurídicas y otras estructuras análogas sean transparentes, impidiendo su utilización ilícita.

En sexto lugar se tratan las responsabilidades de las autoridades competentes, con facultades de supervisión y sanción, y exigiendo la creación de una unidad de inteligencia financiera en cada país (Recomendaciones 26 a 35).

Los aspectos relacionados con la cooperación internacional se abordan en las Recomendaciones 36 a 40, donde se presta especial atención a asuntos tales como los sistemas de asistencia legal mutua y la extradición.

La aplicación de estas Recomendaciones merece también ser objeto de atención, ya que se lleva cabo por el GAFI y sus organismos regionales mediante un proceso de revisión multilateral. Su nombre inglés, Multilateral Peer Review, es un claro reflejo del carácter paritario que preside este sistema que ha desarrollado claros mecanismos cooperativos ante la ausencia de un poder coactivo capaz de exigir, bajo la amenaza de sanción, los estándares internacionales que promueve.

Los mecanismos del GAFI se basan, pues, en el estímulo dado a los países para que promuevan los estándares internacionales más elevados en materia de prevención del blanqueo de capitales y financiación del terrorismo. El aparecer ante la comunidad internacional como un estado saneado y confiable en cuanto a los estándares de prevención de estas lacras es motivo suficiente para que estos, sin necesidad de estar movidos por ninguna sanción de tipo pecuniario o coercitivo, deseen cumplir con las recomendaciones. De no ser así, la única sanción que recibe el país es su inclusión en una lista que, en función del riesgo, puede calificarse como:

- jurisdicciones de alto riesgo y no cooperativas;
- jurisdicciones con deficiencias estratégicas en política AML/CFT, que no han avanzado suficientemente en su resolución o no se han comprometido en un plan de acción desarrollado con el GAFI para su resolución;
- jurisdicciones que hacen avances significativos en el cumplimiento de los estándares AML/CFT en el seno de un plan de acción desarrollado con el GAFI sobre la base de un compromiso escrito político de alto nivel;
- jurisdicciones que no hacen suficientes avances.

Además, el GAFI completa su labor con programas de asistencia técnica y difusión de publicaciones sobre buenas prácticas en la materia. Asimismo, promueve el intercambio de información entre actores, especialmente con el sector privado.

Llama la atención este modelo de administración internacional cooperativa, que contrasta con las administraciones nacionales, más proclives al dictado de normas y al ejercicio tasado de su poder sancionador. Acaso el GAFI, sus recomendaciones y su modelo de revisiones mutuas sea el precursor de una nueva forma de ejercer el poder en un contexto internacional en el que éste está cada vez más difuminado.

Bajo estos esquemas de funcionamiento, las recomendaciones han sido ya adoptadas por más de 180 países y, gracias ellas, en un contexto ausente de organizaciones globales con poder coercitivo, ha sido posible aumentar la transparencia del sistema financiero, facilitando la posibilidad de detectar las actividades delictivas y de dotar a los países de la capacidad de actuar eficazmente. Como dijimos, carecen de fuerza legal. Pero, sin embargo, su incumplimiento por parte de alguna jurisdicción trae como consecuencia que los restantes países vean con recelo las relaciones comerciales y

financieras con los países y territorios no cooperantes. Y eso, en el contexto actual, puede ser mucho más disuasorio que cualquier penalización directa que se pudiera imponer sobre ellos.

Del mismo modo, cuando un país revela a la comunidad internacional un elevado cumplimiento de estos estándares, los beneficios se hacen sentir en unos sistemas financieros más transparentes, estables y atractivos para los inversores extranjeros. Y ello potencia el cumplimiento voluntario de estas recomendaciones.

10. LA NORMATIVA ESPAÑOLA

En España la Ley 19/93, de 28 de diciembre, sobre Determinadas Medidas de Prevención del Blanqueo de Capitales, quedaba derogada desde la entrada en vigor de la actual Ley 10/2010, de 28 de abril, de Prevención del Blanqueo de Capitales y de la Financiación del Terrorismo.

La aprobación de la Ley 10/2010, de 28 de abril, de Prevención del Blanqueo de Capitales y de la Financiación del Terrorismo, supone un marco más específico, fruto de la transposición de la Tercera Directiva (Directiva 2005/60/CE del Parlamento Europeo y del Consejo, de 26 de octubre de 2005, relativa a la Prevención de la Utilización del Sistema Financiero al Blanqueo de Capitales y para la Financiación del Terrorismo), que a su vez incorporaba las 40 Recomendaciones del GAFI sobre prevención del blanqueo de capitales, más las nueve sobre financiación del terrorismo al acervo comunitario.

En dicha Ley se unifica el tratamiento jurídico de la prevención del blanqueo de capitales y de la financiación del terrorismo estableciendo, sin embargo, una diferenciación orgánica para ambos fenómenos. Así, lo relativo a la financiación del terrorismo queda bajo la competencia del Ministerio del Interior, mientras que la prevención del blanqueo de capitales es responsabilidad del Ministerio de Economía, a través de la Comisión de Prevención del Blanqueo de Capitales, encuadrada en la Secretaría de Estado de Economía.

Nuestra Unidad de Inteligencia Financiera (SEPBLAC) depende, sin embargo, del Banco de España, si bien se constituye como uno de los órganos de apoyo de la mencionada Comisión de Prevención del Blanqueo de Capitales.

Es importante destacar que el nuevo Reglamento de la Ley 10/2010, aprobado por Real Decreto 304/2014, de 5 de mayo, profundiza en el enfoque basado en el riesgo que impulsó GAFI. Ello implica dejar más autonomía a los sujetos obligados en la valoración de los peligros en que incurren para, desde ahí, adoptar las medidas que estimen más adecuadas en su lucha contra estas amenazas. La nueva normativa abandona así el carácter más paternalista que inspiraba los primeros textos, para confiar en el buen criterio del sujeto obligado, a quien se le exige llevar a cabo un exhaustivo y documentado análisis con el que justificar, ante las autoridades, sus decisiones de mayor o menor laxitud en los controles que adoptan. Ello es aplaudido por algunos y criticado por otros, quienes rechazan la inseguridad jurídica y la discrecionalidad que permite a la administración adoptar este enfoque menos tasado.

Fecha de recepción: 06/11/2014. Fecha de aceptación: 17/12/2014

LA EVOLUCIÓN DEL COMPONENTE POLICIAL EN LAS OPERACIONES DE MANTENIMIENTO DE LA PAZ

JOSÉ ALBERTO RAMÍREZ VÁZQUEZ

RESUMEN

El presente trabajo se centra en la evolución del componente policial en las operaciones de mantenimiento de la paz. Para poder estudiar dicha evolución se parte de un estudio estadístico que nos sirve para poner en contexto histórico a las operaciones de paz en su conjunto y posteriormente se estudian los datos de participación de los diferentes componentes de las operaciones para valorar su evolución y específicamente la del componente policial en relación con el resto de elementos presentes en las operaciones.

Tras el estudio estadístico se analizan los mandatos y las doctrinas de utilización del contingente policial desde un punto de vista histórico.

Finalmente se hacen dos estudios particulares que se consideran que son de especial interés para entender las operaciones de paz y, en particular, su componente policial, como son el papel de las unidades policiales reunidas y las operaciones puestas en marcha por la Unión Europea.

La principal conclusión del estudio realizado es que el componente policial ha sufrido una importante evolución, tanto numérica como doctrinal, convirtiéndose en un elemento esencial de la acción internacional, siendo sin duda el más versátil.

Palabras clave: operaciones de paz, policía civil, concepto SMART, integración, misiones ejecutivas.

ABSTRACT

The present essay is focused in the evolution of police component in peacekeeping operations. The first part is a statistical analysis in order to establish the historical context of peace operations and specifically the evolution of policing related with the rest of peace operations components.

After the statistical study, the mandates and doctrines of the police are analyzed from a historical approach.

Finally two specific topics are studied as they are considered to be of special interest to understand peace operations. Such topics are the role of the Integrated Police Units and of European Union in the field.

The study main conclusion is that the police component has suffered a relevant evolution, both in numbers and in doctrine, becoming an important element for international action, and no doubt the most versatile.

Key words: peace operations, civilian police, SMART concept, integration, executive missions.

1. INTRODUCCIÓN

Las operaciones de paz han sido, desde la creación de las Naciones Unidas, una herramienta fundamental de esta organización y de la acción internacional para mantener el orden y la paz internacionales. Pese a no estar específicamente recogidas en la Carta de las Naciones Unidas, y pese a que su adscripción a un capítulo concreto no es siempre clara, la praxis ha hecho que ocupen un lugar destacado entre el resto de actividades realizadas por los diferentes actores internacionales para evitar los conflictos y las guerras.

Esta falta de sujeción normativa, que podría suponer un lastre para la puesta en práctica de acciones multilaterales, ha demostrado ser una ventaja que ha permitido que su actuación se adapte a la cambiante situación del contexto internacional.

Este estudio parte de la hipótesis de que las operaciones de paz han evolucionado y de que su componente policial ha ido cobrando importancia de forma gradual.

Otros aspectos que se resaltarán en el estudio son el papel de las unidades policiales reunidas y la importancia de las actividades de la Unión Europea en el campo de las operaciones de paz.

En cuanto a la metodología utilizada para el artículo, en primer lugar se ha procedido a compilar la mayor cantidad posible de datos sobre misiones de paz, tanto de las Naciones Unidas como de la Unión Europea. Una vez obtenidos los datos se han realizado varios gráficos comparativos para conseguir tener una idea sobre su evolución, con especial atención al componente policial.

A continuación se ha elaborado un estudio de los mandatos de las diferentes operaciones y de las circunstancias históricas que dieron lugar a la intervención internacional, tratando de poner en relación la situación internacional con la ubicación y características de las operaciones establecidas.

El siguiente objetivo del estudio, centrado en la función policial, ha sido la situación actual de la doctrina que sustenta dicha función, para lo que se han utilizado fundamentalmente documentos elaborados por las Naciones Unidas.

Finalmente se ha realizado un estudio sobre las misiones policiales de la Unión Europea, para lo que tras una introducción normativa se ha realizado un estudio cronológico de dichas misiones.

2. ESTUDIO ESTADÍSTICO. LA EVOLUCIÓN DE LAS OPERACIONES DE PAZ DE LAS NACIONES UNIDAS

Las primeras operaciones de paz de las Naciones Unidas se regían por el Capítulo VI de la Carta de las Naciones Unidas y se pusieron en marcha poco después de la creación de la ONU. Estos contingentes, constituidos por tropas, sólo podían usar la fuerza para la propia defensa y su despliegue requería el consentimiento del gobierno anfitrión y un acuerdo de alto el fuego[1].

Este tipo de despliegue era el normal en conflictos entre estados, en los que se

1 www.un.org

precisaba una fuerza neutral para vigilar el cumplimiento de un acuerdo y, en muchos casos, al no atajar el conflicto, motivaba que la presencia internacional se debiera mantener en el tiempo, en ocasiones desde finales de los años 40 hasta hoy.

Para comprender la evolución que han sufrido las operaciones de paz de las Naciones Unidas en su más de medio siglo de historia, resulta necesario analizar los datos relativos a las fechas y lugares de realización, a su duración, a los efectivos empleados y a su composición.

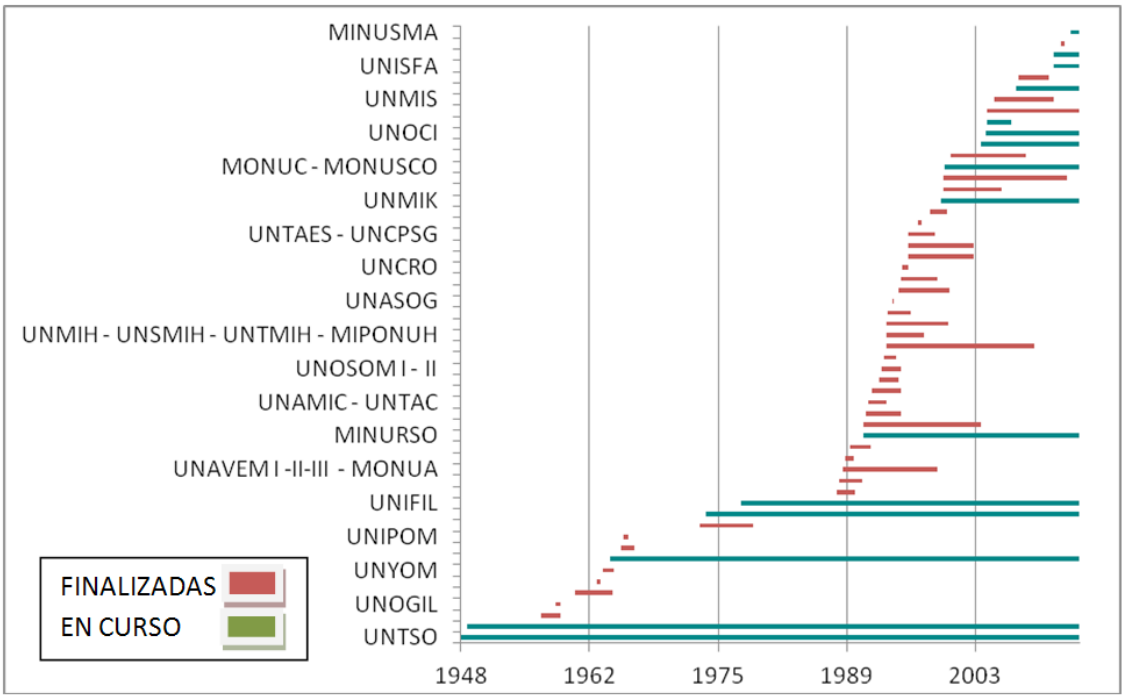


Ilustración 1 Inicio y duración de las operaciones de paz de las Naciones Unidas

Del análisis de las fechas de establecimiento de las operaciones y su duración se desprende una clara tendencia a una menor duración conforme avanzamos en el tiempo, aunque hasta este siglo se apreciaba una combinación de misiones de gran continuidad (de hecho varias de las primeras operaciones se mantienen en la actualidad) con otras de una corta duración (en ocasiones inferiores a un año); sin embargo, desde la primera década de este siglo, las operaciones muestran una mayor uniformidad en su duración que, salvo la excepción de la frustrada UNSMIS en Siria, no baja de tres años.

En lo que se refiere a su ubicación, para su estudio se ha efectuado una cierta agrupación de las operaciones, contando como una sola aquellas que se han desarrollado en el mismo país o territorio de forma consecutiva, al resultar más clarificador a estos efectos. Tras ello se observa que el 44% de las operaciones han tenido lugar en el continente africano, correspondiendo un 15% a cada una de las regiones de Asia, Oriente Medio y Europa y el 11% restante al continente americano, concretamente a Centroamérica y Caribe.

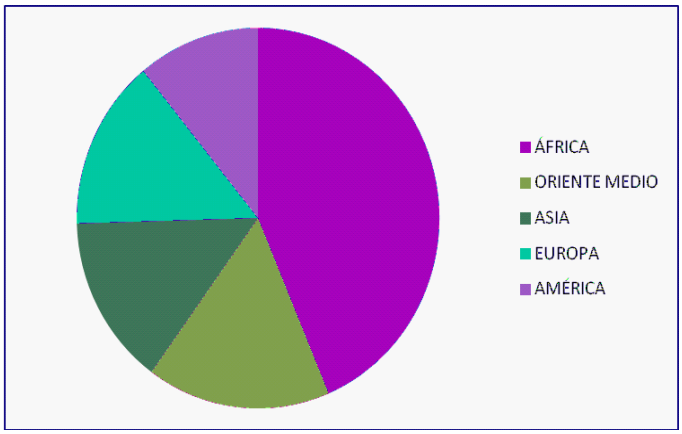


Ilustración 2 Distribución geográfica de las operaciones de paz

Esta agrupación geográfica no es uniforme a lo largo del tiempo, ya que en los años de inicio de las operaciones de paz, estas se concentraron en Oriente Medio, como resultado del conflicto árabe-israelí. Otro momento de concentración se dio a finales de los noventa en Europa como respuesta a los conflictos surgidos por la desintegración de Yugoslavia.

Las operaciones puestas en marcha en la última década se concentran en el continente africano.

Pasamos ahora a analizar la composición de las operaciones, encontrándonos con que los datos que se pueden recabar de la página web de Naciones Unidas no son lo suficientemente detallados para hacer un estudio en profundidad de la evolución en cuanto al número de personas implicadas en las operaciones en sus primeros años de historia; aunque las cifras encontradas indican claramente que, en general, las primeras actividades de mantenimiento de la paz contaron con una presencia de personal bastante reducida, en comparación con las operaciones emprendidas en los noventa y, sobre todo, en lo que va de siglo, con cierta reducción en esta tendencia de incremento a finales de los años noventa, para recuperarse después con motivo de la puesta en marcha de las ambiciosas operaciones en los Balcanes y África.

En este punto cabe resaltar que las dos grandes operaciones en los Balcanes citadas, la UNMBIH en Bosnia-Herzegovina y La UNMIK en Kosovo, carecían de personal militar armado, lo que la ONU denomina como “tropas”, ya que esta función fue desarrollada por los miembros de las operaciones de la OTAN en dichos territorios, y las consecutivas IFOR-SFOR y la KFOR, al actuar conforme a sendos mandatos de las Naciones Unidas, se pueden considerar las “tropas” de dichas operaciones, por lo que han sido contabilizadas como tal[2].

Un estudio más detallado sobre el personal empleado en operaciones de paz se puede realizar con datos relativos al año 1991 y siguientes, cuando nos encontramos con una mayor homogeneidad en los detalles facilitados por la página web de NN.UU. Conforme a los datos comprendidos entre 1991 y enero del presente año, se aprecia una clara tendencia al incremento del personal uniformado en operaciones de paz, con el bajón ya apuntado de finales de los años noventa.

2 Resoluciones 1035 del Consejo de Seguridad de las Naciones Unidas de 21 de diciembre de 1995 y 1244 de 10 de junio de 1999.

Ilustración 3 Personal uniformado en operaciones de Paz de las Naciones Unidas 1993-2014

Este análisis se ha realizado contabilizando los contingentes relativos a "tropas", "observadores militares" y "policía civil", resultando que, si bien el contingente de tropas supera en términos absolutos y claramente a los otros dos, el comportamiento del contingente de Observadores Militares se ha mantenido generalmente estable a lo largo del periodo. En cuanto al componente policial su importancia en términos relativos y en comparación con el resto de componentes uniformados ha ido ganando peso en la última década de forma continuada, con un descenso, si bien poco importante, en el año 2013, y una cierta recuperación el presente año. No obstante se puede restar importancia a esta reducción, ya que en ese mismo periodo se ha producido una reducción del resto del personal uniformado en las operaciones en marcha.

Ilustración 4 Porcentaje de personal policial sobre el total de personal uniformado en las operaciones de Paz de las Naciones Unidas 1993-2014

Este ascenso casi continuado indica un aumento de la importancia del contingente policial en las operaciones de paz, sobre todo con la generalización del uso de las Unidades Formadas de Policía, de las que hablaremos más adelante.

3. LA EVOLUCIÓN DE LA FUNCIÓN POLICIAL EN LAS OPERACIONES DE PAZ. ANÁLISIS DE LOS MANDATOS

Una vez realizado el estudio de los datos numéricos de participación de personal policial en las operaciones de paz, especialmente su comparación con el resto de componentes uniformados presentes, se hace necesario estudiar la correlación

entre esa evolución de cifras y las funciones que desarrollan los miembros del componente policial.

La primera operación de mantenimiento de la paz que contó con una presencia diferenciada de personal policial fue la UNFICYP, en Chipre, iniciada en 1964 y que se mantiene a día de hoy. Esta operación tiene un mandato clásico de interposición entre dos fuerzas enfrentadas, con el mantenimiento de una línea de separación custodiada por personal militar para evitar incidentes entre los contendientes. No obstante, al tener dicha línea una cierta permeabilidad, que además se ha incrementado con el tiempo, se pensó que la supervisión del control del cruce de personas entre ambas zonas se hiciera por parte de un contingente de policía civil[3].

En esta operación la función del personal policial era muy similar a la de los observadores militares cuya presencia venía siendo habitual en las operaciones desplegadas con anterioridad.

Hay que esperar hasta finales de la década de los ochenta para ver una nueva operación con presencia policial, que además fue significativa, tanto cuantitativa como cualitativamente: la UNTAG (United Nations Transition Assistance Group) que tuvo lugar en Namibia. En esta operación, que contó con un contingente militar de más de 4.000 efectivos, se autorizó la presencia de un contingente de policía civil de 1.500 miembros, para apoyar y supervisar las fuerzas policiales locales y la retirada de las fuerzas parapoliciales sudafricanas, especialmente de los elementos de la policía contra la insurgencia, la "*Koevoet*"[4].

La situación internacional en estos momentos, con la disolución del Pacto de Varsovia y la propia Unión Soviética, supone el inicio de un periodo de esplendor de las operaciones de mantenimiento de la paz durante la década de los noventa. Concretamente, entre los años 1991 y 2000 se ponen en marcha un total de 36 operaciones, un número muy elevado, sobre todo si tenemos en cuenta que hasta entonces sólo se habían desarrollado 18.

Pero la importancia de esta década no se limita al número de operaciones puestas en marcha; la situación internacional permite que estas sean mucho más intrusivas, sobre todo con la pérdida de fuerza de los partidarios a ultranza del principio de la no intervención en asuntos internos. Esto permite que las operaciones desarrolladas en Centroamérica, como ONUSAL en El Salvador, en África como ONUMOZ en Mozambique o en el Sudeste Asiático, como UNTAC en Camboya, cuenten con importantes contingentes militares y policiales y extensos mandatos, que además de la simple supervisión, incluyen la reforma de las fuerzas policiales existentes o la creación de nuevos cuerpos policiales. Esta última tarea que se suele llevar a efecto por entidades ajenas al propio Departamento de Operaciones de Mantenimiento de la Paz, como hizo, en el caso de Mozambique, el Programa de las Naciones Unidas para el Desarrollo (PNUD) que encargó la reforma a la Guardia Civil española[5].

Esta situación de hiperactividad del Consejo de Seguridad de las Naciones Unidas llega a su culmen a finales de la década, coincidiendo con la política intervencionista

3 Informe del Secretario General de las Naciones Unidas de 27 de mayo de 2003.
4 Informe del Secretario General de las Naciones Unidas de 23 de enero de 1989.
5 Hansen, Annika S. (2002): From Congo to Kosovo: Civilian Police in Peace Operations, New York, Routledge.

llevada a cabo por los Estados Unidos durante la Administración Clinton (1993-2001), facilitada por la disolución del bloque soviético y la situación aún de debilidad de la Federación Rusa.

Efectivamente, los Estados Unidos ejercen de única superpotencia mundial y cuando encuentran resistencia en las Naciones Unidas, utilizan la Organización del Tratado del Atlántico Norte (OTAN) para intervenir en un conflicto, el de los Balcanes, que había causado miles de muertos y atroces crímenes contra la población civil, televisados además a los hogares estadounidenses.

La desmembración de Yugoslavia había supuesto el inicio de duros conflictos armados en Croacia y Bosnia-Herzegovina, a los que respondió la comunidad internacional con la puesta en marcha de una importante operación de paz, la UNPROFOR que, tras actuar en Croacia con cierto éxito, se extendió a Macedonia y Bosnia-Herzegovina[6]. Si bien en este último territorio, pese a contar un amplio contingente de tropas, no fue capaz de evitar masacres como la de Srebenica, en las propias barbas de los cascos azules holandeses.

Este fracaso de la ONU en los Balcanes que motivó la actuación de la OTAN, se debió a la ausencia de un acuerdo de paz y a la limitación de su mandato, que se circunscribía al establecimiento de zonas protegidas, protección de corredores humanitarios y prohibición de sobrevuelo. Esta última tarea se realizó junto a la OTAN, en lo que fue la primera misión de esta organización militar y, sin duda, animó a esta organización militar a realizar una posterior intervención[7].

Esta actuación pasiva de las fuerzas internacionales cambió en 1995 y tras el lanzamiento de una granada de mortero en un mercado en Sarajevo, la OTAN argumentó que los serbobosnios habían vulnerado las resoluciones de las Naciones Unidas y se decidió a lanzar una campaña de ataques aéreos que puso fin al conflicto y coadyuvó a la firma de los acuerdos de Dayton entre los beligerantes[8].

Es importante destacar que durante la intervención aliada, se puso de manifiesto la debilidad del contingente militar de las Naciones Unidas, cuando varios observadores militares que se encontraban desarmados y sin protección fueron secuestrados por fuerzas locales y utilizados como escudos humanos para evitar la destrucción de diversas instalaciones por parte de la OTAN.

Como consecuencia de esta actuación militar, fue la OTAN la que llevó a cabo el mandato del Consejo de Seguridad de la ONU estableciendo dos misiones militares, en primer lugar la IFOR y un año después la SFOR, por lo que la Misión de las Naciones Unidas en Bosnia- Herzegovina (UNMIBH) que vino a sustituir a la UNPROFOR, carecía de componente militar, salvo un puñado de oficiales de enlace, pero tuvo un importante contingente policial, la International Police Task Force (IPTF), con más de 2.000 componentes, que estuvieron encargados de la supervisión de las actividades de las policías locales y su reforma[9].

Las funciones que desarrollaba el componente policial en este periodo se resumen

6 Resolución 743 de 21 de febrero de 1992 del Consejo de Seguridad de las Naciones Unidas.
7 Resolución 781 de 9 de octubre de 1992 del Consejo de Seguridad de las Naciones Unidas
8 www.nato.int
9 Resolución 1035 del Consejo de Seguridad de las Naciones Unidas de 21 de diciembre de 1995.

en el acrónimo inglés SMART: Support (Apoyo a los Derechos Humanos), Monitoring (Monitorización del comportamiento de las fuerzas de seguridad locales, prisiones, tribunales de justicia y el cumplimiento de los acuerdos), Advice (Asesoramiento a la policía local conforme a los estándares internacionales) Report (Informar de situaciones e incidentes) y Training (Formación de la policía local)[10].

El importante contingente de la SFOR contó, además de con numerosas tropas, con varias unidades de policía de carácter militar, que formaron la Multinational Specialized Unit (MSU), con misiones de seguridad en apoyo a las fuerzas militares, orden público y reserva y que será un nexo de unión entre las capacidades militares y civiles en operaciones de paz y servirá de antecedente a los siguientes despliegues[11].

La IPTF, por el número de componentes desplegados y sus amplios poderes de supervisión, es el antecedente directo de las posteriores misiones de carácter ejecutivo que supusieron la culminación del proceso intervencionista de la comunidad internacional y que contarían con elementos policiales internacionales haciendo cumplir la ley y dotados de armamento, pero si analizamos el proceso por el que las Naciones Unidas se hicieron cargo de la administración en Kosovo y Timor Oriental, únicos lugares hasta la fecha donde esto se ha hecho, se deduce que no se trató de un proceso planificado.

Para demostrar la anterior afirmación haremos una somera descripción cronológica del proceso de establecimiento de las misiones ejecutivas de las Naciones Unidas. Es nuevamente la OTAN la que, en marzo de 1999, interviene en el nuevo conflicto que se estaba desarrollado en los Balcanes, en este caso en Kosovo, parte de la propia Republica de Serbia, que aún mantenía un remanente de estado yugoslavo junto a Montenegro, que se independizaría posteriormente.

La comunidad internacional no quería una nueva escalada en el conflicto de Kosovo, con la repetición de las barbaridades cometidas en Bosnia-Herzegovina, por lo que la OTAN, sin contar esta vez con el mandato del Consejo de Seguridad de las Naciones Unidas, lanzó en marzo de 1999 la Operación fuerza Aliada que, en junio de ese año, obligó a las autoridades yugoslavas a firmar un Acuerdo Técnico Militar de retirada de sus fuerzas militares y de policía de Kosovo[12]. Ese acuerdo se refería a una resolución del Consejo de Seguridad de las Naciones Unidas, que no había sido aún aprobada, y autorizaba a la OTAN a constituir una fuerza para establecer y mantener un entorno seguro para todos los ciudadanos de Kosovo. El acuerdo no incluía la retirada de la Administración Civil yugoslava de Kosovo pero, ante la retirada del ejército y la policía del territorio, los funcionarios civiles decidieron marcharse junto a muchos ciudadanos de etnia serbia, dejando así Kosovo sin administración civil. Esta situación hizo que la comunidad internacional se encontrara un territorio que gobernar en todos los aspectos, debiendo la Resolución 1244/99 del Consejo de Seguridad de NNUU ir más allá de la mera supervisión de una situación de post conflicto, por lo que debió establecer una completa Administración Internacional transitoria, hasta que las nuevas autoridades que se constituyeran fueran capaces de administrar el territorio.

10 A trainer's Guide on Human Rights for CIVPOL monitors.
11 www.nato.int
12 Military Technical Agreement between KFOR and the governments of the Federal Republic of Yugoslavia and the Republic of Serbia (1999).

Una parte importante de esta administración civil internacional de transición, que constituyó la Misión de las Naciones Unidas en Kosovo (UNMIK), fue formada por un fuerte contingente policial que, en este caso, no realizaba funciones de supervisión o reforma, sino las mismas que en sus países de origen, velar por la seguridad ciudadana incluyendo desde el control del tráfico y la investigación de delitos comunes, a la custodia de prisiones.

Los primeros miembros de la UNMIK POLICE procedían de la IPTF de Bosnia-Herzegovina, por lo que tuvieron que recibir su armamento, necesario para la nueva misión precipitadamente y, en algunos casos como los británicos, debieron ser sustituidos por policías de dicho país que estuvieran duchos en el uso de armas o incluso abandonar la misión, como el contingente chileno a quienes su parlamento no permitió participar en una misión armada. Además estos policías se desplegaron siguiendo el modelo de IPTF, que hacía muy difícil su operatividad en estas circunstancias y carecían de un soporte en forma de normas de actuación.

Además de formar un cuerpo de policía regular, la UNMIK desplegó diversas unidades policiales reunidas, dotadas de capacidad de control de masas y con un armamento más potente, las Unidades Especiales de Policía (SPU). Esta unidad contó con el antecedente de una unidad similar desplegada en Haití durante la Misión de Policía Civil en dicho país (MIPONUH)[13].

Las SPU tuvieron también como modelo las MSU de la SFOR y coincidieron con una nueva MSU que la KFOR, la operación militar de la OTAN, desplegó en Kosovo.

El segundo, y último caso, en el que la policía civil de la ONU ejerció funciones ejecutivas se dio en Timor Oriental y tampoco parece que se hubiera programado así en el DPKO, no obstante hay que decir que el grado de confianza que la comunidad internacional había adquirido en esos momentos influyó también en que el vacío de poder en un territorio fuera cubierto de esta forma.

La UNAMET, que se estableció en Timor Oriental en junio de 1999 para preparar el referéndum de autodeterminación[14], debió ser parcialmente evacuada tras la celebración del plebiscito, por la actuación de las milicias favorables a la integración en Indonesia, lo que motivó la intervención de una fuerza militar internacional, liderada por Australia y con el acuerdo del propio gobierno indonesio, para pacificar el territorio, tras lo que se puso en marcha una nueva misión de administración temporal, la UNTAET, que contaba con un contingente militar de más de 6.000 soldados y una fuerza de policía civil armada de 1.200 miembros, incluyendo una Unidad Especial de Policía (SPU)[15].

Una vez más las Naciones unidas se ven obligadas a intervenir ante una situación no planificada, empleando esta vez toda su capacidad para hacerse cargo de un territorio falto de gobierno.

La puesta en marcha de estas dos misiones de carácter ejecutivo no supuso que a partir de entonces todas las operaciones de mantenimiento de la paz siguieran ese modelo, aunque es indudable que dotó a la comunidad internacional de unas posibilidades de actuación muy superiores a las que venía desempeñando. Las siguientes

13 Informe del Secretario General de las Naciones Unidas de 11 de noviembre de 1998.
14 Resolución 1246 del Consejo de Seguridad de las Naciones Unidas de 11 de junio de 1999.
15 Resolución 1272 del Consejo de Seguridad de las Naciones Unidas de 25 de octubre de 1999.

operaciones desplegadas en territorios y situaciones de gran complejidad como Sierra Leona, Liberia, República Democrática del Congo o Haití, siguieron el modelo tradicional, aunque los contingentes de policía civil que sufrieron una reducción en su número, en los primeros compases del siglo, han ido incrementándose de forma continuada hasta nuestros días, tanto en términos absolutos como relativos en comparación con el resto de contingentes uniformados.

Las operaciones puestas en marcha en lo que llevamos de siglo se han centrado en África, pese a que han surgido conflictos también en otros territorios como consecuencia de la actividad terrorista de corte integrista islámico y la reacción de los Estados Unidos tras los ataques sufridos el 11 de septiembre de 2001, pero la actividad internacional en Afganistán ha tenido un reflejo limitado en las Naciones Unidas, ya que junto a la misión de la OTAN, la ISAF, se ha establecido una misión de carácter político, la UNAMA[16], teniendo la actuación de la ONU en Irak, la UNAMI, también carácter de misión política y no de mantenimiento de la paz[17].

África concentra la actividad de mantenimiento de la paz de las Naciones Unidas en la actualidad. De las nueve operaciones puestas en marcha, desde el año 2005, sólo dos lo han sido fuera del continente africano y ambas han finalizado ya.

El modelo de operación de paz de las Naciones Unidas en la actualidad es el de una operación multidimensional, que incluye una gran diversidad de componentes y generalmente con una fuerte presencia armada, tanto militar como policial, con presencia de Unidades Formadas de Policía (FPU), un tipo de unidades que han venido a sustituir a las SPU y han consolidado el uso de esta importante herramienta. Los mandatos de estas operaciones son también generalmente muy amplios, incluyendo la protección de los civiles, la asistencia a los gobiernos locales para reformar su ejército, policía y sistema judicial y la asistencia para la celebración de referéndums (Darfur)[18] o elecciones (Mali)[19].

Otra característica de estas operaciones africanas es que muy frecuentemente se ejecutan junto a operaciones de otras organizaciones regionales, como la Unión Africana o la Unión Europea.

En las actuales operaciones de paz, el componente policial ejecuta una gran variedad de funciones, que van desde las tareas tipo SMART, ya citadas, a la reforma policial, la protección de personas e instalaciones, tanto de la ONU como locales, el apoyo operativo a las fuerzas locales o a las propias tropas de la ONU y la colaboración en el mantenimiento del orden público.

4. LA FUNCIÓN POLICIAL INTERNACIONAL. DOCTRINA ACTUAL

La actual doctrina en la que se basa la función policial internacional se fundamenta en la normativa que rige la propia actividad de las Naciones Unidas en el campo del mantenimiento de la paz y que ha ido evolucionando de forma lenta a lo largo de su ya dilatada historia.

16 Resolución 1401 del Consejo de Seguridad de las Naciones Unidas de 28 de marzo de 2002.
17 Resolución 1500 del Consejo de Seguridad de las Naciones Unidas de 14 de agosto de 2003.
18 Resolución 1769 del Consejo de Seguridad de las Naciones Unidas de 31 de julio de 2009.
19 Resolución 2100 del Consejo de Seguridad de las Naciones Unidas de 25 de abril de 2013.

Las primeras operaciones, aunque no figuraban expresamente en la Carta de las Naciones Unidas, se regían, como hemos dicho, por su Capítulo VI y siguiendo la corriente dominante en aquellos momentos de priorizar el principio de la no intervención, no se dirigían a solucionar el problema, sino a evitar el conflicto interponiéndose entre los contendientes, con lo que la situación de conflicto se alargaba, en muchos casos hasta nuestros días.

Tradicionalmente la función policial en las operaciones de paz se limitaba a monitorizar, observar e informar, hasta que desde comienzos de la década de los noventa se añadieron otras funciones como el asesoramiento, la tutoría y la formación de las fuerzas policiales existentes o creadas *ex novo*. Las operaciones de mantenimiento de la paz comenzaron a regirse por el Capítulo VII de la Carta de las Naciones Unidas, pudiendo sus componentes usar la fuerza para defenderse a si mismos, al mandato de la misión o a civiles en peligro inminente.

Este salto cualitativo fue posible gracias al informe del secretario general de la ONU Boutros Boutros-Ghali, que en su informe Agenda para la Paz de 1992 apostó porque las operaciones pasaran a regirse por el citado Capítulo VII[20].

La realización de estas funciones se llevó a cabo en ausencia de normas claras y específicas dirigidas a los miembros de los cuerpos policiales que, formando parte de los contingente de policía de la ONU, debían supervisar la actuación de sus colegas de territorios en situación de post-conflicto, no siendo hasta mediados de los años noventa cuando el Departamento de Operaciones para el Mantenimiento de la Paz no compila y publica las orientaciones y normas para llevar a cabo dichas tareas de monitorización.

En 1994 se publica *Estándares de Justicia Criminal para la Policía de las Naciones Unidas* y un año más tarde el *Manual de la Policía Civil de las Naciones Unidas,* con lo que se logra componer un marco normativo básico para guiar la actuación policial en operaciones de paz.

En cuanto a las tareas concretas realizadas para llevar a cabo las funciones citadas, estas se normalizan a partir de la UNTAG en Namibia y son el acompañamiento de las policías locales en el desempeño de su servicio, la recepción e investigación de denuncias sobre la actuación de la policía y la supervisión de las investigaciones realizadas por las unidades policiales locales.

Uno de los pasos fundamentales en la ampliación de funciones que se lleva a cabo durante el periodo esplendor de los años noventa es la implicación de las operaciones de paz en la reforma policial.

La década de los noventa, con su elevado número de operaciones, facilita la mejora de los procedimientos y tácticas que lleva a cabo la policía en operaciones de paz y permite que se genere una doctrina que procura abarcar todos los aspectos de la función policial en dichos ámbitos, con la puesta en marcha del denominado concepto SMART, y que se pondrá a prueba en misiones de gran importancia por el número de efectivos y amplitud del mandato, como la que se puso en funcionamiento en Bosnia i Herzegovina.

20 Un programa de paz. Informe del Secretario General de las Naciones Unidas presentado de conformidad con la declaración aprobada el 31de enero de 1992 en la Reunión de la Cumbre del Consejo de Seguridad.

La experiencia adquirida por las Naciones Unidas en esta década permite la puesta en marcha en el año 1999 de dos misiones extremadamente complejas en Kosovo y Timor Oriental en las que, como ya se ha indicado, se constituye una administración internacional que se hace cargo de la práctica totalidad de las tareas de gobierno, incluido el mantenimiento de la ley y el orden.

Como se ha dicho, surgen serias dudas de si esta asunción de funciones fue premeditada, sin embargo en lo que no existen dudas es en que las normas y directrices de la organización no estaban preparadas para tal reto, como demuestra que los primeros contingentes policiales internacionales que tuvieron que aplicar la ley en Kosovo debieron hacerlo siguiendo sus propias leyes ante la ausencia de un ordenamiento propio de aquel territorio y las reticencias de las instituciones que se iban formando apresuradamente para aplicar las leyes yugoslavas que consideraban represoras.

Esta falta de planificación supuso que los contingentes policiales debieran improvisar, sobre todo en los primeros momentos de su despliegue, y buscaran soluciones imaginativas como, por ejemplo, la incautación temporal del vehículo a los infractores de las normas de tráfico (normas de sentido común) ante la imposibilidad de imponer sanciones, por la ausencia de la legislación y la estructura administrativa necesaria para ello.

Las Naciones Unidas no promulgaron normas ni directrices para la realización de tareas policiales de carácter ejecutivo como las señaladas, seguramente porque consideraron esta función una excepción, como demuestra el hecho de que no se hayan vuelto a realizar con posterioridad.

Esta variedad de funciones y tareas desempeñadas por la policía civil de Naciones Unidas le ha permitido ampliar sus contingentes y ejercer funciones de gran importancia en las actuales misiones multidimensionales, habiéndose unido a la lista de tareas la protección de personas, material e instalaciones, tanto locales o pertenecientes a las propias NNUU.

La nueva doctrina puesta en marcha para sustentar este nuevo tipo de operaciones se basa en diversas aportaciones, como el denominado “informe Barhimi” del año 2000 o Informe del Grupo de Trabajo sobre las Operaciones de Paz de las Naciones Unidas o el concepto “integración”, introducido en la pasada década para describir la respuesta global de las NNUU a su implicación en países emergiendo de un conflicto, cuyo principal objetivo es maximizar el impacto individual y colectivo de los diversos esfuerzos de las NNUU para apoyar la consolidación de la paz.

Otros hitos importantes en la formación del sustento doctrinal de las operaciones de NNUU han sido la reestructuración, en el año 2007, del DPKO y la creación del Departamento de Apoyo de Campo (*Department of Field Support)* y la publicación al año siguiente de *Operaciones de Paz de las Naciones Unidas: Principios y Directrices*, conocida como la doctrina “piedra angular” (*capstone doctrine).*

5. UNIDADES POLICIALES REUNIDAS. CONCEPTO Y EVOLUCIÓN

Una vez que hemos concretado la normativa de las Naciones Unidas en la que se basa el actual concepto de Operación Multidimensional, que es el que se está aplicando en la actualidad, y descritas las principales funciones y tareas que desarrolla el componente policial, debemos centrarnos en describir la rama más novedosa de la

policía civil, las Unidades Formadas de Policía, que han permitido a la función policial aumentar no sólo el número de policías civiles en las operaciones, sino también que su papel abarque un amplio abanico de capacidades.

Pese a que la propia página web de Naciones Unidas, cuando presenta las actuales Unidades Formadas de Policía, sitúa como su antecedente la SPU de la UNMIK (Kosovo) puesta en marcha en 2000, su verdadero precedente sería la Unidad Especial de Policía (SPU) desplegada en Haití bajo el mandato de una misión específicamente policial, la MIPONUH, que entre sus componentes contaba con una unidad de tales características que llegó a contar con 110 componentes, procedentes de la Gendarmería Nacional de Argentina, y que se desplegó en diciembre de 1997[21].

Unas unidades similares fueron establecidas por la OTAN en Bosnia-Herzegovina, las Multinational Specialized Units. Las MSU, en cuyo nombre se evitaba la palabra "policía", estaban compuestas por personal procedente de cuerpos policiales con estatuto militar, o bien por unidades de policía militar. La primera MSU se desplegó en la SFOR de Bosnia i Herzegoviona en 1998, si bien en la posterior KFOR de la OTAN en Kosovo se desplegó otra MSU, que convivió con las SPU de NNUU[22].

La Unión Europea ha tomado el concepto de unidades reunidas de policía y ha diseñado dos tipos de unidades: las Integrated Police Units (IPU) y las Formed Police Units, (FPU). Contar con estos dos tipos de unidades confiere a las operaciones de paz de la UE una gran flexibilidad y capacidad de adaptación a la situación en el terreno.

El diseño de estas unidades responde a la doctrina establecida en el Consejo de Niza (2000), por el que se establecían dos conceptos relativos al despliegue de unidades policiales en misiones de gestión de crisis, el refuerzo y la sustitución.

El concepto de refuerzo supone el conseguir llevar a las fuerzas policiales locales hasta los estándares internacionales, mientras que el concepto de substitución se dirigía a la restauración de la seguridad pública en países fallidos, remplazando y apoyando a los servicios locales. Una característica fundamental de las misiones de sustitución es la necesidad de su rápido despliegue.

La IPU es una unidad robusta estructurada en torno a una unidad ya existente con su propia cadena de mando y puede desempeñar una variada serie de funciones policiales. La IPU puede en caso necesario actuar bajo mando militar, si bien esto depende de si lo permite la legislación del país del que depende la unidad. Se da la circunstancia de que la Constitución de un socio de gran peso dentro de la Unión, como Alemania, prohíbe que su policía actúe bajo mando militar por claras circunstancias históricas, lo que limita a sus fuerzas policiales su participación en este tipo de unidades.

La FPU es una unidad de menor entidad, pudiendo estar formada por la unión de varias unidades menores de diferente origen, sus funciones no incluyen la investigación y se dirigen hacia ocupaciones policiales regulares.

Finalmente otra característica que diferencia ambos tipos de unidades es que la IPU dispone de capacidades logísticas propias mientras que la FPU se debería apoyar en la IPU.

21 Informes del Secretario General núm. 144/98 y 150/00.
22 www.nato.int

Con la puesta en marcha de esta doctrina, la UE demuestra tener unos importantes recursos de planeamiento y una amplia capacidad de adaptación a una gran variedad de entornos y situaciones. No obstante, existe un fuerte contraste con su voluntad política, como demuestra el escaso uso que se ha hecho, hasta la fecha, de las potencialidades de la Fuerza de Gendarmería Europea (EUROGENDFOR). En este sentido, la actual misión en Republica Centroafricana que se está poniendo en marcha, y que cuenta con una IPU proporcionada por la EUROGENDFOR, supondrá un hito importante en la consolidación de una doctrina, tan largamente planificada, como es la de la Gestión de Crisis en la Unión Europea.

6. LAS MISIONES POLICIALES EN LA UNIÓN EUROPEA. UN ACTOR DE PESO EN EL PANORAMA INTERNACIONAL

La Unión Europea se encuentra en el momento actual en una encrucijada. Los cambios legislativos y estructurales iniciados con la entrada en vigor del Tratado de Lisboa, junto a las consecuencias de la actual crisis económica, han supuesto un empuje y un freno simultáneos a su consolidación como actor internacional diferente a sus propios estados miembros.

A lo anterior sumamos la actual reestructuración del equilibrio de poder internacional, con la vuelta de los Estados Unidos a la senda de la política multilateral durante la administración Obama, la cada vez mayor influencia de las nuevas potencias económicas, especialmente de China, y la vuelta de Rusia al papel de potencia hegemónica, al menos a nivel regional, como demostró la crisis de Georgia de 2008 y parece estar demostrando su actuación en la actual crisis de Ucrania.

Todos estos factores nos dejan una Unión Europea con grandes dificultades para hacerse respetar, pese a su indudable poderío económico, por las vulnerabilidades que todavía suponen la dependencia energética exterior y su incapacidad de salir definitivamente de la crisis económica de los estados que la integran, que parecen reacios a afrontar políticas comunes que puedan poner en riesgo una situación económica aún frágil.

Pese a estos problemas, la Unión Europa ha tenido un importante papel en el mantenimiento de la paz y la seguridad internacionales, como demuestra su importante implicación en este ámbito que se inició tan sólo hace 12 años.

En el año 2002 se firman los Acuerdos Berlín Plus, por los que la incipiente política de seguridad de la Unión Europea obtiene acceso a los medios y capacidades de la OTAN para realizar sus operaciones, consiguiendo en tan corto espacio de tiempo convertirse en un importante y exitoso actor en este ámbito.

Este éxito puede explicarse por dos factores principales:

En primer lugar por el peso de la propia Unión, como agrupación de algunos de los estados más ricos del globo, lo que incita a muchos gobiernos de países en crisis a solicitar la actuación de la Unión Europea como paso previo a la obtención de su acceso a algún tipo de ayudas económicas paralelas. La “Demanda de UE” no deja de crecer desde los Acuerdos de Ohrid en la Antigua República Yugoslava de Macedonia. Primero en el resto de los Balcanes, luego en África y después de forma imparable en el Cáucaso, Oriente Medio y Asia.

Como segundo factor del éxito de la Unión Europea en el ámbito de las operaciones de paz, se considera el propio diseño de las operaciones, con la combinación innovadora de instrumentos diversos de carácter civil y militar, que permiten abordar las crisis de forma global.

Esta capacidad de combinar elementos civiles y militares responde a la realidad reflejada en la Estrategia Europea de Seguridad (Objetivo II pág. 7) que afirma que ninguna de las nuevas amenazas es puramente militar, ni puede abordarse por medios exclusivamente militares.

La entrada en vigor del Tratado de Lisboa, el 1 de diciembre de 2009, encuentra una acción exterior en el campo de la paz y la seguridad internacionales ya consolidada, que había puesto en marcha 22 operaciones civiles, militares y mixtas, no obstante dicho tratado pretende reforzar la Política Exterior y de Seguridad Común (PESC) con diversas iniciativas, como la creación de un Alto Representante que preside el Consejo de Asuntos Exteriores y que es, a su vez, vicepresidente de la Comisión Europea.

A partir del Consejo de Niza (2000) se va consolidando una estructura permanente sobre política exterior y de seguridad común, el Comité Político y de Seguridad Común (COPS), compuesto por embajadores de los países miembros.

La Política Común de Seguridad y Defensa (PCSD) forma parte de la PESC y debe ofrecer a la Unión Europea una capacidad operativa basada en medios civiles y militares. La Unión podrá recurrir a dichos medios en misiones fuera de la Unión, que tengan por objetivo garantizar el mantenimiento de la paz, la prevención de conflictos y el fortalecimiento de la seguridad internacional, conforme a los principios de la Carta de las Naciones Unidas.

Estas misiones son herederas de las llamadas “Misiones Petersberg” de la Unión Europea Occidental (UEO) de 1992 y abarcarán las actuaciones conjuntas en materia de desarme, las misiones humanitarias y de rescate, las misiones de asesoramiento y asistencia en cuestiones militares, las misiones de prevención de conflictos y de mantenimiento de la paz, las misiones en las que intervengan fuerzas de combate para la gestión de crisis, incluidas las misiones de restablecimiento de la paz y las operaciones de estabilización al término de los conflictos.

La PCSD muestra una gran flexibilidad, permitiendo que las operaciones se encomienden a un grupo de países y no teniendo por qué implicarse la totalidad de los estados miembros, siendo también posible que se constituyan fuerzas multinacionales por parte los estados miembros y se pongan a disposición de la PCSD.

De estas fuerzas multinacionales existen varios ejemplos de carácter permanente, uno de ellos sería la Fuerza de Gendarmería Europea, que es un instrumento de la política común de seguridad y defensa (PCSD) de la Unión Europea y puede actuar no sólo bajo mandato de la UE, sino también de la ONU, la OTAN o la OSCE[23].

La Unión Europea afronta los aspectos civiles de la gestión de crisis utilizando un amplio abanico de capacidades en los ámbitos de la policía, la judicatura, la fiscalía, las prisiones, la administración civil, las aduanas o los derechos humanos, entre otros. Para gestionar las complejas misiones que resultan de tan diversas capacidades, la

23 Tratado Constitutivo de la Fuerza de Gendarmería Europea (2007).

Unión Europea creó en el año 2000 el Comité para los Aspectos Civiles de la Gestión de Crisis (CIVCOM), para poner en marcha los objetivos marcados en el Consejo de Feira de junio de 2000 en materia de capacidades civiles en las diferentes áreas prioritarias: la policía, el fortalecimiento del Estado de Derecho, el fortalecimiento de la administración civil y la protección civil.

Con la aprobación de la Estrategia Europea de Seguridad la Unión Europea se dota de un Plan de Acción para los aspectos civiles de la PCSD, que incorpora a las áreas prioritarias marcadas en Feira la capacidad de conducir misiones de observación, así como el apoyo genérico a las oficinas de los representantes de la UE.

Con el fin de incrementar la capacidad de respuesta rápida y mantener una capacidad de respuesta adecuada y efectiva en la gestión civil de crisis, la Unión Europea se dotó en junio de 2005 de los Equipos de Respuesta Civil (Civil Response Team), que se definen como una capacidad de reacción rápida para la gestión civil de crisis, de tamaño y composición flexibles y participación de expertos de los estados miembros y, en principio, de la Secretaría del Consejo.

En 2007 se crea la Capacidad Civil de Planeamiento y Conducción, con la misión de planear y dirigir las misiones civiles de la PCSD bajo la dirección política y estratégica del Comité Político y de Seguridad (COPS), heredando y ampliando los cometidos de la antigua Unidad de Policía.

Pese a que la información disponible en la página web de la Unión Europea tampoco es lo precisa y uniforme que sería deseable, podemos hacernos una visión de conjunto de las operaciones puestas en marcha por la Unión Europa, resultando que se han llevado a cabo un total de 31 operaciones, de las cuales 16 están aún en marcha. De ellas 11 de carácter militar, 19 de carácter civil y una mixta, en apoyo a la Misión de la Unión Africana en Darfur[24].

Las misiones de la UE presentan en general unos números inferiores a las de las Naciones Unidas siendo muy pocas las que cuentan con más de un millar de componentes, siendo su duración media de cuatro años.

En cuanto a su localización, la gran mayoría se han desarrollado en lo que se podrían considerar las zonas de influencia europeas, o sea los Balcanes, África en su totalidad, Oriente Medio y el Cáucaso, habiéndose extendido dicha influencia hacia Afganistán como resultado de la política de alianza con los Estados Unidos. Dentro de África las operaciones se concentran en el norte del continente y las regiones de El Sahel, Grandes Lagos y el Cuerno de África.

La propia denominación de las misiones nos ofrece información sobre su actividad. La primera misión recibió la denominación EUPM (European Union Police Mission), que no se ha vuelto a repetir, siendo denominadas las misiones de carácter policial como EUPOL, aunque la misión que sustituyó a la EUPOL PROXIMA, en la Antigua República Yugoslava de Macedonia, fue denominada EUPAT para que se diferenciara de la misión a la que sustituía. Otras denominaciones muy indicativas serían las EUBAM, dedicadas a la asistencia fronteriza, las EUCAP, cuya prioridad es la capacitación de las autoridades locales, las EUJUST y las EULEX, dedicadas al “imperio de la ley”, si bien la última con especial atención al sistema judicial.

24 www.eea.europa.eu

En cuanto a las misiones de carácter militar se han denominado como EUFOR, si bien las de formación han recibido la denominación de EUTM o EUSEC, esta última dedicada a la formación de personal militar, aunque está considerada como una misión de carácter civil.

7. CONCLUSIONES

Una vez realizado este repaso a las operaciones de paz, y especialmente a su componente policial, contamos con argumentos suficientes para responder a las preguntas que nos planteamos al iniciar el presente estudio.

La primera parte del estudio, dedicada al análisis de los datos numéricos de las operaciones de paz, se ha realizado conforme a los datos disponibles en la página web de las Naciones Unidas, aunque por desgracia sólo se han encontrado datos de calidad relativos a las operaciones iniciadas a partir del año 1993.

En cuanto a los mandatos y la normativa del Consejo de Seguridad, necesarios para elaborar la parte dedicada a la evolución de las operaciones, se ha podido constatar que los propios mandatos, en su redacción, demuestran una importante evolución, partiendo de mandatos cortos y genéricos a documentos mucho más largos paulatinamente y a la vez mucho más detallados. Asimismo se ha podido comprobar la importancia de los informes del secretario general para establecer las diversas funciones dentro de cada operación.

En lo que se refiere a la hipótesis inicial sobre la evolución de las operaciones de paz, se demuestra una clara evolución desde unas operaciones iniciales poco intrusivas y dedicadas a la interposición entre contendientes, en las que predomina el contingente militar hacia operaciones intervencionistas y en las que el componente civil va ganando fuerza, incluyendo el componente policial, consolidándose la figura del monitor policial, con una actuación menos pasiva, así como la implicación de la comunidad internacional en la reforma y restructuración de las instituciones policiales locales. En suma se trata de solucionar el problema que motivó el conflicto que se produce comúnmente dentro de un país y sentar las bases para la consolidación de la paz.

Llegados a este punto se desvela otra incógnita, las operaciones de paz están fuertemente influenciadas por la situación internacional imperante, como demuestra que durante la Guerra Fría hubiera un número relativamente escaso de operaciones como consecuencia de la situación de equilibrio entre los dos bloques hegemónicos y que la situación iniciada con la caída de la Unión Soviética propiciara la puesta en marcha de una gran número de nuevas operaciones con mandatos más intrusivos. Otro hecho que pone de manifiesto esta relación entre operaciones y situación internacional, se dio con las intervenciones de la Alianza Atlántica en los Balcanes, impensables con el Pacto de Varsovia activo y que fueron consecuencia de la situación hegemónica de los Estados Unidos en aquellos momentos.

La evolución del componente policial, cuestión central de este estudio, está respaldada por los datos numéricos, que indican un aumento en la importancia relativa de la policía civil sobre el resto de componentes uniformados participantes en las operaciones. En cuanto a su papel, su presencia gana importancia dentro de las operaciones, como ejemplo de ello se puede citar el caso de la ONUMOZ de Mozambique, donde su presencia

no estaba prevista en los acuerdos de paz y hubo que hacer una enmienda posterior que permitiera la participación en la operación de un fuerte contingente de policía civil, con un despliegue muy repartido en el difícil territorio mozambiqueño y con importantes funciones de monitorización y tutoría de la PRM (Policía de la República de Mozambique).

La asunción de nuevas funciones y mayores poderes por parte del componente policial en operaciones de paz tiene su culminación a finales de los años noventa, con el desempeño de funciones ejecutivas en Kosovo y Timor Oriental, donde sus miembros dejan de ser "Police Monitors" para ser "Police Officers". Además, aunque este tipo de funciones no se ha repetido, el hecho de que se hayan podido realizar, permite que la actual doctrina de actuación recoja la posibilidad de su asunción si las circunstancias lo aconsejan y que los actuales despliegues puedan ejecutar un amplio abanico de actividades, incluyendo la prestación de protección tanto al personal y material de las Naciones Unidas como a la población local, esto último normalmente en apoyo de las fuerzas policiales locales, pero dotando al componente policial internacional de capacidades que le permiten realizar funciones que van de las análogas a los Observadores Militares a las que realizan la Tropas al servicio de las Naciones Unidas.

La asunción de dichas funciones ha sido posible gracias a la creación de una nueva herramienta dentro del componente policial, las unidades reunidas de policía, que comenzaron denominándose "Special Police Units" (SPU), para llamarse actualmente "Formed Police Units" (FPU), cuya puesta en marcha ha sido uno de los principales logros de las operaciones de la presente década.

En lo que se refiere al papel de la Unión Europea en las operaciones de paz, ya desde muy temprano en el proceso de consolidación de la Unión como actor diferenciado de los estados que la componen, demostró estar capacitada para apoyar, complementar e incluso sustituir a las Naciones Unidas en su papel en defensa de la paz y la seguridad internacionales.

Este papel de la Unión Europea como potencia mundial, se fundamenta en dos características fundamentales que guardan una clara relación la una con la otra. En primer lugar su papel como motor económico y comercial, lo que va ligado a su importante actividad en la cooperación internacional al desarrollo, que refuerza su papel en la gestión de crisis.

En segundo lugar se puede hablar del factor de calidad en sus despliegues, motivado por la atención que se presta desde las instituciones europeas a este asunto, lo que le ha dotado de herramientas normativas y de doctrina muy eficaces para ello y por la preparación y profesionalidad del conjunto de sus fuerzas, tanto militares como policiales o civiles, lo que le permite hacerse cargo de situaciones de gran inestabilidad y dificultad de despliegue, incluso como paso previo a una ulterior actuación de las Naciones Unidas.

Este conjunto de cualidades de las misiones de la UE hacen que se pueda hablar del valor añadido europeo en este campo, que se basa en su elevada capacidad de planeamiento y posibilidades de ejecución en un amplio espectro de posibilidades con la conjunción de elementos diversos, lo que permite que pueda poner en marcha operaciones verdaderamente multidimensionales.

Fecha de recepción: 11/11/2014. Fecha de aceptación: 17/12/2014

ANÁLISIS COMPARATIVO DE LA ESTRATEGIA DE SEGURIDAD NACIONAL DEL AÑO 2013 CON SU PREDECESORA DE 2011

JOSÉ MIGUEL GARCÍA MALO DE MOLINA MARTÍNEZ

RESUMEN

En 2013 el Gobierno español aprobó la actual Estrategia de Seguridad Nacional, apenas dos años después de que hubiese sido aprobada en España la primera Estrategia de Seguridad. Por tal motivo, se estima interesante proceder a un análisis comparativo de ambos documentos con el objeto de poder valorar el alcance de dicha modificación, es decir, si la Estrategia de 2013 se trata únicamente de una revisión continuista de la de 2011 o si, por el contrario, se puede afirmar que los cambios operados en la segunda son tan sustanciales que obliguen a pensar que se trata realmente de una nueva estrategia.

Este análisis comparativo va a realizarse desde la perspectiva de los elementos esenciales que debe contener un documento de este tipo: Concepto de Seguridad Nacional, Intereses Nacionales, Compromisos Internacionales, Riesgos y Amenazas y Líneas Generales de Actuación.

Palabras clave: Estrategia Seguridad Nacional, comparativa, intereses nacionales, riesgos y amenazas, líneas generales de actuación.

ABSTRACT

In 2013 the Spanish government approved the current National Security Strategy, only two years after it had been approved in Spain the first Security Strategy. Therefore, it is estimated interesting to carry out a comparative analysis of both documents in order to be able to assess the scope of the amendment, that is, if the Strategy 2013 is only a continuity revision of 2011 or whether, on the other side, we can say that the changes in the second one are so substantial that oblige think that we really have a new strategy.

This comparative analysis will be performed from the perspective of the essential elements required in a document of this type: National Security Concept, National Interest, International Commitments, Risks and Threats and General Action Lines.

Keywords: National Security Strategy, comparative, national interests, risks and threats, general guidelines.

1. INTRODUCCIÓN

Durante el último cuarto del siglo pasado, coincidiendo con el final de la Guerra Fría, surgió un fenómeno nuevo conocido como *globalización* que, además de haber aportado grandes beneficios y ventajas para nuestra sociedad, ha generado sin embargo nuevos riesgos y amenazas que hasta fechas recientes no existían o no se

contemplaban como tales. Entre éstos se pueden citar el terrorismo internacional, el crimen organizado, los flujos migratorios, la seguridad energética o la económica, algunos de los cuales pueden incluso presentarse interconexionados entre ellos.

En este contexto, las formas clásicas de hacerles frente no son ya útiles, ya que el seguimiento, control o actuación contra los mismos excede, en la mayoría de los casos, no solo las capacidades o posibilidades de un departamento ministerial en concreto, sino también las tradicionales fronteras políticas y los recursos propios de los estados considerados de forma individual. De modo que, ante estas nuevas amenazas, se hace imprescindible recurrir a nuevas formas, alianzas y procedimientos.

Por tal motivo, con el objeto de hacer frente a estas amenazas de una manera más global, muchos países occidentales, entre ellos España, han decidido dotarse de una Estrategia de Seguridad Nacional (ESN). Con carácter general, este tipo de documentos deberían contemplar, al menos, los siguientes elementos:

- Cuáles son nuestros intereses nacionales, a partir de los cuales se podrán determinar los objetivos nacionales.
- Cuáles son nuestras políticas y compromisos internacionales, que van a condicionar nuestras posibles líneas de actuación, ya que se deberá evitar que se produzcan interferencias con los intereses de otros estados. En este punto, el gobierno debería definir qué posición quiere ocupar en el orden internacional, qué papel quiere jugar y al lado de quién se quiere posicionar.
- Cuáles son los riesgos y amenazas a las que nos enfrentamos, contra qué nos tenemos que prevenir o defender.
- Cuáles son nuestras limitaciones, tanto desde el punto de vista legal o jurídico, económico, social, etc.
- Y, por último, cuáles son nuestras capacidades, con qué medios, tanto militares como no militares, vamos a poder contar para desarrollar esa estrategia.

A la vista de lo anterior, la Estrategia de Seguridad Nacional podría definirse como el conjunto de líneas generales mediante las que el presidente del Gobierno determina y revela los intereses nacionales, los riesgos y amenazas que pueden vulnerar el normal funcionamiento de la Nación, y los propósitos o compromisos que ésta desea adquirir en el contexto internacional para, a partir de aquellos, definir los objetivos políticos que desea alcanzar y precisar las directrices para el establecimiento de políticas sectoriales que permitan su consecución.

En el caso español, en el año 2011, el entonces presidente de Gobierno José Luis Rodríguez Zapatero aprobó la que sería nuestra primera Estrategia de Seguridad, denominada “Estrategia Española de Seguridad: Una responsabilidad de todos”. Con este título se pretendía reflejar que se ha evolucionado a un concepto más amplio de la seguridad, en el que ésta se ve amenazada por un amplio elenco de riesgos de naturaleza muy diversa a los que resulta muy difícil enfrentarse utilizando las herramientas y procedimientos tradicionales.

Este nuevo concepto de seguridad pretende preservar intereses de muy diversa índole, para lo que es preciso no solo el empleo de herramientas estrictamente militares o policiales, sino también del concurso y participación de otros instrumentos

institucionales, como son la diplomacia, la economía, la justicia, la política exterior, etc. Es decir, en los tiempos actuales es prácticamente impensable poder hacer frente a los nuevos riesgos y amenazas desde una única perspectiva, siendo por lo tanto necesaria la respuesta global o integral de todas las herramientas puestas en poder del estado ("comprehensive approach"[1]).

La publicación en España de la primera Estrategia de Seguridad se ha llevado a cabo de una manera relativamente tardía, cuando muchos de los países de nuestro entorno ya disponían de la suya propia desde hacía tiempo[2]. A pesar de que en el año 2008, al comienzo de la X Legislatura, el presidente anunció la elaboración de dicha estrategia, no fue sin embargo hasta 2011 cuando finalmente se aprobó, en un momento en el que el gobierno se encontraba débil y se presagiaba ya un inminente cambio de partido político en el poder.

Lamentablemente, esta primera Estrategia tuvo una escasa repercusión debido a que fue modificada cuando tan solo llevaba dos años de vigencia, tiempo insuficiente como para poder poner en práctica las disposiciones en ella establecidas.

Uno de los motivos más que probable, entre otros, para que el nuevo gobierno decidiese su rápida modificación es que en la preparación y elaboración de la primera estrategia no se tuvo en cuenta al Parlamento, en especial al primer partido de la oposición, con lo que éste no se sentía identificado con ella. Y es que, a pesar de que existía la voluntad inicial, finalmente la Estrategia Española de Seguridad (EES) de 2011 no fue presentada al Parlamento.

Además, si bien es más que de agradecer el esfuerzo realizado por el gobierno de la Nación existente en ese momento para llevar a cabo la elaboración de la que sería nuestra primera Estrategia de Seguridad, se echa en falta sin embargo la participación de representantes de partidos políticos de la oposición, como sí ha sucedido para la elaboración del Libro Blanco de la Defensa y Seguridad Nacional francés[3]. Este hecho quizás contribuyó a que la anterior estrategia, o más bien sus autores, cayesen en

1 El concepto de "enfoque integral" o "comprehensive approach", considerado como una extensión del conocido UK Military Effects-Based Approach (EBA), se recogió por primera vez en la doctrina militar del Reino Unido a comienzos del año 2006. No obstante, este concepto ya comenzó a surgir a raíz de la participación del ejército británico en la crisis de los Balcanes en el año 1991, concretamente en la misión internacional de Bosnia, durante la que miembros de ese ejército observaron cómo en la resolución de un conflicto de esas características tomaban parte numerosos actores civiles y militares, así como otras organizaciones internacionales, organizaciones no gubernamentales (ONG,s) e, incluso, medios de comunicación social, y cuya participación se estimó como relevante para cubrir diversos aspectos de la gestión de crisis que no podían ser satisfechos de manera exclusiva a través de los medios militares

2 A modo de ejemplo, en los Estados Unidos desde el año 2002 ("The National Security Strategy of the United States of America"), en el Reino Unido desde 2008 ("The National Security Strategy: Security in an interdependent world"), en Holanda desde 2007 ("National Security. Strategy and Work Programme 2007-2008"), en Francia desde 2008 ("Libro Blanco de la Defensa y Seguridad Nacional") o en Australia desde 2008 ("First National Security Statement to the Australian Parliament").

3 Para su redacción se formó una comisión compuesta por un presidente y 36 miembros, entre los que se puede encontrar desde representantes de las distintas administraciones con competencias en el campo de la Seguridad y Defensa hasta expertos en asuntos culturales y sociales sin experiencia en este campo, pasando por personalidades del mundo académico. Asimismo destaca la presencia de dos diputados y dos senadores, dos pertenecientes a la mayoría parlamentaria y otros dos a la oposición, así como representantes de todos los partidos políticos.

la autocomplacencia, dedicando una gran parte de la misma a referenciar los éxitos y progresos que se habían realizado durante el período de gobierno de Rodríguez Zapatero, lo que podría haber llevado al principal partido de la oposición a hacer una lectura propagandística de la misma.

Estos desaciertos, que propiciaron la falta de consenso entre las fuerzas políticas, han intentado ser subsanados durante la elaboración de la nueva estrategia. Para ello, además de contar con las principales fuerzas políticas y con un Comité de Expertos para su elaboración, el documento fue rápidamente presentado ante la Comisión Constitucional del Congreso de los Diputados[4].

Otro de los motivos para modificar la EES, con tan poco tiempo de vigencia, fue la intención de considerar la Seguridad Marítima como una amenaza propia. Como se verá más adelante, la Seguridad Marítima no era considerada así en el primer documento, sino como uno de los ámbitos (terrestre, aéreo, marítimo...) en los que se podían desarrollar el resto de amenazas.

Consecuentemente, apenas dos años después de estar en vigor, y un año y medio después de la formación del nuevo gobierno, en el año 2013 se aprobó la nueva Estrategia de Seguridad Nacional.

2. ANÁLISIS COMPARATIVO DE AMBAS ESTRATEGIAS

La propia ESN de 2013 declara que “continúa y revisa la Estrategia de Seguridad Nacional aprobada en 2011, adaptando y actualizando su contenido a los cambios del escenario estratégico, configurando un nuevo Sistema de Seguridad Nacional e implicando a la sociedad civil en los ámbitos de interés prioritario de la Seguridad Nacional”. El hecho de que se trate de una Estrategia de carácter continuista no sorprende a nadie, ya que transcurrido tan poco tiempo entre la publicación de una y otra esa es la opción más lógica. Era de esperar que tanto nuestros intereses, riesgos y amenazas, como nuestros compromisos internacionales no hubiesen cambiado sustancialmente durante la corta vigencia de nuestra primera EES.

No obstante, pese a que la nueva Estrategia mantiene la misma línea que su predecesora en lo que respecta tanto a la estructura del documento como a los elementos más esenciales de la misma, existen sin embargo importantes variaciones que son dignas de estudiar, como es por ejemplo cuando se determina la manera en la que se pretende hacer frente a cada una de las amenazas, es decir, cuáles son los objetivos estratégicos definidos en cada uno de los ámbitos de actuación.

Comenzando con el análisis comparativo de ambos documentos, se puede afirmar que la ESN actual es considerablemente más corta que su predecesora del año 2011 (58 páginas frente a 90).

En cuanto a su estructura, además del Resumen Ejecutivo que ambas contienen, la del año 2013 tiene una Introducción del presidente del Gobierno. Por lo que respecta al cuerpo principal de las mismas, si bien ambas constan de cinco capítulos, se aprecian sin embargo algunas diferencias.

4 Con fecha 9 de julio de 2013.

Aunque el Capítulo 1 se titula de manera diferente en un documento que en otro[5], presentan ambos básicamente los mismos elementos: visión general del entorno actual de seguridad, la difusión existente hoy en día entre Seguridad Interior y Seguridad Exterior, Intereses Nacionales, etc.

El Capítulo 2 presenta el mismo título en ambos casos: "La Seguridad de España en el mundo". En él se procede a describir la dimensión global e internacional de la seguridad y a identificar los entornos estratégicos para nuestro país. En este capítulo ambas Estrategias establecen cuáles son nuestras zonas de interés estratégico, en cuyo estudio se profundizará más adelante.

El Capítulo 3 ya cambia entre ambos documentos. El de 2011 se encuentra dedicado a "Los Potenciadores del Riesgo", de los que dice que se trata de fenómenos globales que propician la propagación o transformación de las amenazas y riesgos y que incrementan nuestra vulnerabilidad. Entre éstos destaca las disfunciones de la globalización, los desequilibrios demográficos, la pobreza y desigualdad, el cambio climático, los peligros tecnológicos y las ideas radicales y no democráticas. Sin embargo, la Estrategia actual no dedica un capítulo a este aspecto, limitándose únicamente a reseñarlos al comienzo del mismo, el cual está dedicado a "Los riesgos y amenazas para la Seguridad Nacional".

A continuación, en el Capítulo 4 de la EES de 2011 se analizan las "Amenazas, Riesgos y Respuestas". Tras definir amenaza como "toda circunstancia o agente que ponga en peligro la seguridad o estabilidad de España", y como riesgo "toda contingencia o probabilidad de que una amenaza se materialice produciendo un daño", procede a enumerar las principales amenazas que pueden afectar a nuestra seguridad para, a continuación, fijar las Líneas Estratégicas.

A diferencia de la ESN actual, que dedica un capítulo a las amenazas y otro a las Líneas Estratégicas, en la de 2011 ambos aspectos se recogían en el mismo. Es decir, tras describir cada una de las amenazas, procedía a continuación a determinar los objetivos estratégicos para cada una de ellas.

Por último, en el Capítulo 5 de ambas Estrategias, aunque con distinto título[6], se establece la estructura orgánica que será responsable de la concepción, gestión y seguimiento de la Seguridad Nacional, para lo que se crea el Consejo de Seguridad Nacional.

A continuación se va a realizar un análisis comparativo más pormenorizado de cada uno de los elementos más esenciales de ambas Estrategias.

2.1. CONCEPTO DE SEGURIDAD NACIONAL

En la Estrategia Española de Seguridad del año 2011 no se establecía en ninguna parte del documento qué debía entenderse por Seguridad Nacional o por Estrategia de Seguridad. Llama sin embargo poderosamente la atención el hecho de que dicho concepto sí hubiese sido recogido en los documentos preliminares elaborados por la

5 "Una Estrategia necesaria" en la de 2011 y "Una visión integral de la Seguridad Nacional" en la de 2013.

6 "Un modelo institucional integrado" en la EES de 2011 y "Un nuevo Sistema de Seguridad Nacional" en la ESN de 2013.

Comisión responsable de su elaboración, en los que se llegó a definir de la siguiente manera[7]:

"A efecto de esta Estrategia Española, la búsqueda de la seguridad es la de una situación en la que se dan las condiciones necesarias para garantizar el normal funcionamiento del estado y su ordenamiento constitucional, los intereses de España así como el desenvolvimiento de la sociedad, los derechos fundamentales, modos de vida y prosperidad de los ciudadanos frente a las amenazas y riesgos futuros"

El documento finalmente aprobado en 2011, en lugar de aportar una definición de Seguridad Nacional, se centraba en definir cuál era el objeto de dicha Estrategia: "analizar el contexto actual de seguridad, aportar una visión prospectiva y fijar las líneas para defender los intereses de España y su contribución a un entorno nacional, europeo, regional e internacional más seguro, pacífico y justo"[8]. Asimismo, aportaba cuáles eran sus objetivos centrales: "analizar las amenazas y riesgos a nuestra seguridad, identificar líneas de respuesta y definir mecanismos de coordinación".

Por su parte, la actual ESN define 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"[9].

En este sentido, la EES de 2011 parece hallarse más alineada con las Estrategias de Seguridad anglosajonas (Estados Unidos y Reino Unido), en las que sus respectivos documentos, en lugar de aportar una definición de qué debe entenderse por Seguridad Nacional, proceden sin embargo a establecer cuál es la finalidad de la misma[10]. Por su parte, la ESN de 2013 se encuentra más próxima a la de los países de nuestro entorno (Francia, Alemania u Holanda), documentos en los que sí aparece el concepto de seguridad nacional.

2.2. LOS INTERESES NACIONALES

Como cabía esperar, los intereses vitales definidos en la Estrategia Española de Seguridad del año 2011 no diferían apenas de los que hasta entonces habían sido declarados por el nivel político[11]. En este sentido, establecía como intereses vitales los relativos a los derechos fundamentales: la vida, la libertad, la democracia, el bienestar

7 Definición que constaba en uno de los Borradores de la Estrategia Española de Seguridad.

8 "Estrategia Española de Seguridad: Una responsabilidad de todos". Presidencia de Gobierno. Pág.11.

9 "Estrategia de Seguridad Nacional: Un proyecto compartido". Presidencia de Gobierno. Págs. 7 y 8.

10 "The National Security Strategy of the United States of America (NSS)". The White House. Mayo de 2010. Introduccción y pág 1: El objetivo es perseguir una estrategia de renovación nacional y liderazgo global, una estrategia que levante los cimientos de la fuerza e influencia americana. "A Strong Britain in an Age of Uncertainty: The National Security Strategy". Cabinet Office. United Kingdom. Octubre de 2010. Pág 3: El objetivo principal es el de transformar la manera en la que se venía organizando la seguridad nacional, y así poder organizarse y protegerse frente a las amenazas que están surgiendo como consecuencia de los cambios radicales que se están experimentando en esta época de incertidumbre en la que nos encontramos.

11 Ley Orgánica 5/2005 de la Defensa Nacional. Art. 2; Directiva de Defensa Nacional 2008, pág. 6; Revisión Estratégica de la Defensa 2003, pág. 47; Libro Blanco de la Defensa, págs. 68 a 71.

y el desarrollo de los españoles, así como los relativos a los elementos constitutivos del Estado, como la soberanía, la independencia e integridad territorial, el ordenamiento constitucional y la seguridad económica[12].

Además, también establecía como intereses estratégicos aquellos que atañen a la consecución de un entorno pacífico y seguro, como la consolidación y el buen funcionamiento de la UE, la instauración de un orden internacional estable y justo, de paz, seguridad y respeto a los derechos humanos, la preservación de la libertad de intercambios y comunicaciones y unas relaciones constructivas con nuestra vecindad.

Por contra, la actual ESN no establece de manera concreta cuáles son estos intereses nacionales. En este caso, es preciso acudir a una lectura detenida del documento para poder entresacar algunos de ellos, entre los que se puede llegar a identificar la libertad, la democracia o el respeto a la dignidad del ser humano.

Esta ausencia contrasta bastante con el hecho de que, metodológicamente, los intereses nacionales son uno de los elementos esenciales que debe constar en toda Estrategia de Seguridad y es que, en este tipo de documentos, es preciso determinar qué es lo que se pretende proteger y contra qué se debe proteger. Además, en este aspecto, nuestra actual Estrategia se separa de la corriente seguida en los países de nuestro entorno, en cuyas estrategias se detalla en mayor o menor medida cuáles son estos intereses nacionales a proteger[13]. Esta ausencia, sin duda deliberada, puede obedecer a criterios de economía literaria y es que, los autores de dicho documento, en ese empeño por no reflejar en la ESN aquello que no fuera preciso para su cumplimiento, pretendieron no ser repetitivos, ya que los intereses nacionales de España habían quedado ya claramente definidos en la Directiva de Defensa Nacional 1/2012[14], que había sido aprobada por el mismo gobierno tan solo unos meses antes.

2.3. LOS COMPROMISOS INTERNACIONALES

En el apartado de las políticas y compromisos internacionales se aprecia alguna diferencia a la hora de abordar la enunciación de los principios básicos de acción que van a articular la proyección exterior del gobierno. De esta manera, la EES del año 2011 establecía como principios el enmarcar nuestra actuación dentro del marco europeo de referencia; el multilateralismo, la legitimidad y la legalidad internacional;

12 "Estrategia Española de Seguridad: Una responsabilidad de todos". Op. Cit. Pág. 8.

13 Estados Unidos: La seguridad, la prosperidad, el respeto de los valores y un orden internacional liderado por los Estados Unidos. El Reino Unido: La Seguridad, la Prosperidad y la Libertad. Francia: La defensa de la población y del territorio, garantizar su seguridad y la defensa de los valores republicanos (democracia, las libertades individuales y colectivas, el respeto de la dignidad humana, la solidaridad y la justicia). Alemania: La justicia, la libertad y democracia. La soberanía e integridad. Conflictos y crisis regionales. Los retos de la globalización. Los derechos humanos y el orden internacional. Holanda: La Seguridad Territorial, la Seguridad Económica, la Seguridad Ecológica, la Seguridad Física y la Estabilidad Social y Política.

14 "Directiva de Defensa Nacional 1/2012: Por una Defensa necesaria, por una Defensa responsable". Presidente del Gobierno. Consejo de Defensa Nacional. Julio de 2012: declara como intereses esenciales la soberanía, la integridad territorial y el ordenamiento constitucional, así como el asegurar la libertad, la vida y la prosperidad de sus ciudadanos. Asimismo, añade que los intereses de España y de los españoles se extienden más allá de nuestras fronteras, añadiendo por este motivo la consecución de un orden internacional estable, de paz, seguridad y respeto de los derechos humanos.

y la construcción de la paz. Asimismo, afirmaba que, para alcanzar un orden internacional estable, debía actuarse en los siguientes frentes: impulsar la reforma de las organizaciones internacionales; reforzar nuestra influencia en los foros e iniciativas multilaterales; y fortalecer las relaciones bilaterales.

No obstante, la ESN del año 2013, por su parte, si bien mantiene estos mismos frentes en los que afirma que es preciso articular la proyección exterior, abandona sin embargo cualquier mención a los anteriores principios básicos de actuación en el marco internacional.

Por otro lado, al establecer las zonas regionales de actuación en las que se enmarcan nuestros principales compromisos internacionales, ambas Estrategias coinciden plenamente en las mismas, si bien existe alguna pequeña matización en su enunciado. Por ejemplo, la EES del año 2011 hablaba de nuestra vecindad del Sur, mientras que la del 2013 se refiere de manera concreta al Mediterráneo. Asimismo, mientras que la de 2011 hablaba de Iberoamérica la de 2013 lo hace de América Latina.

Por lo que se refiere a las principales diferencias existentes en el contenido de los compromisos declarados en cada una de ellas, se puede afirmar que con respecto a **la Unión Europea** se mantiene exactamente la misma posición en una Estrategia que en la otra, otorgándola ambos documentos un papel decisivo como polo de estabilidad y progreso en el orden internacional y declarando, por otro lado, a la colonia británica de Gibraltar como una anomalía en la Europa actual.

Por lo que respecta al **Mediterráneo**, ambas Estrategias vinculan la seguridad de nuestro país y la del resto de Europa a la prosperidad de la ribera meridional del Mediterráneo. No obstante, en la del año 2013 se ha añadido una mención a las crisis surgidas en la otra orilla del Mediterráneo, concretamente en Libia y Siria[15].

Asimismo, ambas Estrategias declaran que **el Magreb** es también una zona prioritaria para España, si bien la de 2013, a diferencia de su predecesora, no menciona a las ciudades autónomas de Ceuta y Melilla. No obstante, debe hacerse constar que la anterior EES las nombraba únicamente para recordar su presencia en esta zona, sin llegar a realizar ninguna valoración sobre su seguridad ni sobre las posibles amenazas que pudiesen recaer sobre ellas[16].

En este mismo ámbito, al enumerar ambas Estrategias las herramientas para impulsar en esta zona la cooperación y la integración regional, la ESN del año 2013 añade la Iniciativa de Cooperación de Estambul del año 2004[17].

15 Si bien la conocida “Primavera Árabe” comenzó a finales de 2010 y se extendió rápidamente por otros países de la región, curiosamente la Estrategia del año 2011 no hace ninguna mención a dicha crisis. Como “Primavera Árabe” se conoce coloquialmente a las protestas populares que surgieron en Túnez en diciembre de 2010 y en Egipto en enero de 2011 y que consiguieron derrocar rápidamente a sus respectivos gobiernos. Este sentimiento se contagió también a primeros de ese mismo año a Libia, si bien el derrocamiento de su presidente, Muamar Gadafi, no se produjo hasta el mes de octubre tras una guerra civil. Asimismo, a comienzos de 2012, parte de la población siria se levantó contra su dirigente, Bashar al-Asad, si bien el conflicto interno se mantiene todavía abierto.

16 “Estrategia Española de Seguridad: Una responsabilidad de todos”. Op. Cit. Pág. 22.

17 Las otras herramientas a las que se refieren ambos documentos son: la Unión para el Mediterráneo (UpM), la Política de Vecindad de la Unión, la Iniciativa 5+5 y el Diálogo Mediterráneo de la OTAN, todas ellas comentadas en el Capítulo IV de este trabajo.

Para finalizar esta área regional, la del año 2013 hace una mención expresa a la cuestión del Sahara Occidental, de la que afirma su compromiso para alcanzar una solución política justa, duradera y mutuamente aceptable para las partes.

Por lo que se refiere a **América Latina**, la nueva ESN reconoce a Brasil y a Méjico como nuevos actores globales. Asimismo, destaca también la importancia de las relaciones de esta región con la zona del Pacífico, a la que define como muy relevante en el nuevo entorno estratégico, haciendo especial mención a la *"Alianza del Pacífico"*[18].

Como instrumento clave para debatir y desarrollar estas cuestiones, la EES del año 2011 hacía referencia a las Cumbres Iberoamericanas, a las que la del año 2013 ha añadido también la acción bilateral, los foros regionales y la UE.

En cuanto a **los Estados Unidos**, la anterior EES ofrecía a nuestro país para representar un papel clave en las relaciones transatlánticas, en el que su cercana posición al continente africano le confiere una posición de ventaja como mediador entre las dos orillas del Atlántico. Asimismo, en la actual ESN también ha desaparecido la mención que, en el ámbito de la Defensa, hacía la del año 2011 al Convenio de Cooperación para la Defensa entre España y Estados Unidos[19] y al Comité Bilateral de Alto Nivel Hispano-Norteamericano (CBAN)[20], instrumentos que consideraba de suma importancia para garantizar la coordinación y la cooperación bilateral en este ámbito.

Respecto a la región de **África**, ambos documentos reconocen la importancia creciente que esta zona está teniendo sobre nuestro país, como consecuencia de fenómenos tan preocupantes como la pobreza, las migraciones descontroladas o el cambio climático. Asimismo, ambas Estrategias destacan tres zonas de especial interés: el Sahel, el Cuerno de África y el Golfo de Guinea.

Por otro lado, si en la EES del año 2011 **el Sahel** se configuraba ya como un espacio clave, considerándolo como un terreno propicio para redes delictivas y grupos terroristas *yihadistas*, en la del año 2013 no cabe ya duda de la importancia de este área tras la revuelta touareg que tuvo lugar en febrero de 2012 en el norte de Malí, y que tuvo como consecuencia un golpe de Estado y, en enero del año 2013, la intervención de la comunidad internacional liderada por Francia en la llamada *"Operación Serval"*[21],

18 La Alianza del Pacífico es una iniciativa de integración regional conformada por Chile, Colombia, México y Perú, creada el 28 de abril de 2011, mediante la que se busca la integración profunda de servicios, capitales, inversiones y movimiento de personas.

19 "Convenio entre el Reino de España y los Estados Unidos de América sobre cooperación para la Defensa", de 1 de diciembre de 1988, revisado por el "Protocolo de Enmienda de 10 de abril de 2002", entrando en vigor el 12 de febrero de 2003. BOE núm. 45. 21 de febrero de 2003. La vigencia del Convenio modificado es de de ocho años a contar desde esta última fecha, es decir hasta el 12 de febrero de 2011, prorrogándose automáticamente por periodos de un año, salvo decisión expresa de una de las partes.

20 Dicho Comité se creó el 11 de enero de 2001, en Madrid, como consecuencia de la Declaración Conjunta Piqué-Albright, mediante la cual se decidió consolidar y reforzar las relaciones bilaterales y establecer un marco legal de cooperación. Se trata de un instrumento que garantiza la coordinación de esfuerzos en materia de Defensa y la representación institucional. Su presidencia la comparten el ministro de Defensa español y el secretario de Defensa de los Estados Unidos. http://www.defensa.gob.es/politica/seguridad-defensa/contexto/europea-atlantica/EEUU/

21 Operación militar llevada a cabo en el norte de Malí, desde enero de 2013, liderada por Francia y el gobierno de Malí, y que cuenta con el apoyo de varios países africanos y occidentales. Bajo el amparo de la ONU, tiene el objetivo de frenar el avance de los rebeldes islamistas que desde el año 2012 gobiernan de facto en el norte de ese país.

operación en la que participa España a través del despliegue de un Destacamento del Ejército del Aire en Dakar (Senegal), desde donde desarrolla misiones de apoyo a las fuerzas francesas que participan en la misma.

Por otro lado, ambas Estrategias reconocen el creciente peso del poder económico y político de **Asia**, haciendo una especial mención a China y a la India. Si bien la EES de 2011 destaca la importancia estratégica que en materia de seguridad tienen países como Pakistán, India o Indonesia, la de 2013 se centra más en Afganistán, Pakistán y Corea del Norte, así como en las reivindicaciones territoriales de China.

Asimismo, si el documento del año 2011 destacaba la importancia que en asuntos de lucha contra el terrorismo y de control de la inmigración tienen países como Australia y Nueva Zelanda, en el de 2013 se menciona únicamente al primero, no aludiendo en ningún momento a Nueva Zelanda.

Para finalizar este área, la EES de 2011 destacaba el importante papel estabilizador que la Asociación de Naciones del Sureste Asiático (ASEAN) puede desempeñar en esta zona[22].

Con respecto a **Rusia**, ninguna Estrategia aporta gran cosa, pudiendo resumirse que, en ambos casos, se estima que la posición estratégica de Rusia, y los fuertes lazos que tiene con los países de la región del Caúcaso y Asia Central, han llevado a considerarla como un socio europeo estratégico en una de las zonas más inestables del mundo.

Por último, en relación con **las organizaciones internacionales**, ambas Estrategias mencionan a la ONU, la OTAN, la OSCE, el G20 y al Consejo de Estabilidad Financiera. Por otro lado, la EES de 2011 dedicaba casi una página completa a la" *"Alianza de Civilizaciones"*[23][24], habiendo desaparecido toda referencia a la misma en el documento de 2013.

2.4. LOS RIESGOS Y AMENAZAS

Como ya se ha comentado anteriormente, la Estrategia Española de Seguridad del año 2011 procedía a definir amenaza como "*toda circunstancia o agente que ponga en peligro la seguridad o estabilidad de España"* y como riesgo *"toda contingencia o probabilidad de que una amenaza se materialice produciendo un daño"*[25]. Sin embargo, la del año 2013, pese a utilizar el término *"amenaza"* hasta en 70 ocasiones, y el de *"riesgo"*

22 Se trata de una organización regional de estados del sudeste asiático, creada el 8 de agosto de 1967, con el objeto de acelerar el crecimiento económico y fomentar la paz y la estabilidad regional. Hoy en día la conforman diez países: Indonesia, Malasia, Filipinas, Singapur, Tailandia, Brunei, Vietnam, Laos, Miamar y Camboya. http://www.asean.org/asean/about-asean

23 "Estrategia Española de Seguridad: Una responsabilidad de todos". Op. Cit. Pág. 26.

24 La Alianza de Civilizaciones es una iniciativa de Naciones Unidas, copatrocinada por España y Turquía, que tiene como objetivo fomentar el diálogo y la cooperación entre diferentes comunidades, culturas y civilizaciones y construir puentes que unan a los pueblos y personas más allá de sus diferencias culturales o religiosas, desarrollando una serie de acciones concretas destinadas a la prevención de los conflictos y a la construcción de la paz. El proyecto fue presentado por el entonces presidente del Gobierno, José Luis Rodríguez Zapatero, ante la Asamblea General de Naciones Unidas el 21 de septiembre de 2004. En torno a la Alianza se creó un Grupo de Amigos compuesto por 136 países y organizaciones internacionales. http://www.exteriores.gob.es/Portal/es/PoliticaExteriorCooperacion/NacionesUnidas/Paginas/AlianzaCivilizaciones.aspx

25 "Estrategia Española de Seguridad: Una responsabilidad de todos". Op. Cit. Pág. 34.

en otras 61, no llega sin embargo a definir en ningún momento qué debe entenderse por cada uno de estos conceptos. Preguntado el hecho de porqué se había abandonado en el nuevo documento la definición de ambos conceptos, la respuesta volvió a ser la de la economía literaria, ya que los autores de la nueva ESN entendían que ambos conceptos eran ya sobradamente conocidos y que no hacía falta volver a explicarlos.

Asimismo, la anterior EES establecía de manera novedosa los ámbitos en los que estos riesgos y amenazas se pueden presentar, estableciendo como tales el terrestre, aéreo, marítimo, espacial, cibernético y el de la información[26]. No obstante, la ESN de 2013 abandona la idea de concebir estos riesgos y amenazas en unos determinados ámbitos.

Por otro lado, la Estrategia de 2011 introducía, en su Capítulo 3, el concepto de potenciadores del riesgo o *"drivers"*, procediendo a su definición como *"fenómenos globales que propician la propagación o transformación de las amenazas y riesgos que afrontamos e incrementan nuestra vulnerabilidad"*[27]. Por su parte, la Estrategia actual no dedica un Capítulo a este aspecto, sino que se limita únicamente a mencionarlos.

En este sentido, ambas Estrategias coinciden básicamente en la declaración de estos potenciadores[28], si bien la del año 2013 elimina el originado por las disfunciones de la globalización que sí contemplaba su antecesora.

Por último, por lo que se refiere al establecimiento de los riesgos y amenazas que pueden afectar a nuestra seguridad, ambos documentos, como cabía esperar, no difieren mucho uno del otro. No obstante, el documento de 2013, además de contemplar todas las amenazas que se reflejaban en la Estrategia de 2011[29], añade otras dos: el espionaje, que en la Estrategia de 2011 estaba incluido dentro de las ciberamenazas, y la vulnerabilidad del espacio marítimo.

Entre las diferencias que se pueden encontrar entre una y otra Estrategia en este ámbito, se pueden citar:

Con respecto a la amenaza de los **conflictos armados**, ambas Estrategias estiman que las consecuencias de las guerras internas pueden desbordar los límites geográficos del país o territorio en el que se desarrollan y afectar a los países vecinos, originando nuevos riesgos de desestabilización en la zona. Por su parte la EES de 2011 reconoce tres posibles tipos de conflictos en los que podría verse involucrada España[30]:

- Conflictos no compartidos con nuestros aliados.
- Conflictos en un contexto multilateral que afecte a los intereses de España.
- Participación derivada de nuestros compromisos internacionales sin que afecte a los intereses de España.

26 Íbidem. Págs. 34 a 36.
27 Íbidem. Págs. 27.
28 La pobreza, la desigualdad, los extremismos ideológicos, los desequilibrios demográficos, el cambio climático y la generalización del uso nocivo de las nuevas tecnologías.
29 Los Conflictos Armados; el Terrorismo; las Ciberamenazas; el Crimen Organizado; la Inestabilidad Económica y Financiera; la Vulnerabilidad Energética; la Proliferación de Armas de Destrucción Masiva; los Flujos Migratorios Irregulares; las Emergencias y Catástrofes y, por último, la Vulnerabilidad de las infraestructuras críticas y servicios esenciales.
30 "Estrategia Española de Seguridad: Una responsabilidad de todos". Op. Cit. Pág. 37.

Por lo que se refiere a la amenaza del **terrorismo**, la ESN del año 2013 da ya por sentada la derrota de la banda terrorista ETA, de la que tan solo espera su definitiva disolución. Por tal motivo, el documento se centra más en la amenaza procedente del terrorismo internacional, del que destaca su mayor letalidad. Como posibles Potenciadores del Riesgo ambos documentos hacen mención a la proximidad al Sahel; la posible radicalización de los emigrantes, tanto de primera como de segunda generación (la EES de 2011 se centraba más en los de esta segunda generación); la reivindicación del Al-Andalus como parte del imaginario del Islam y, por último, la participación de España en misiones internacionales, en especial en la lucha contraterrorista. No obstante, la ESN actual no contempla la interconexión entre las actividades y métodos del crimen organizado y del terrorismo como uno de los potenciadores de esta amenaza.

Por último, la Estrategia de 2011 enumeraba, quizás de manera más mediática que práctica, cuáles habían sido las recientes mejoras en el ámbito de la lucha antiterrorista[31].

En relación con las **ciberamenazas**, ambos documentos consideran que la seguridad en el empleo del ciberespacio puede verse comprometida tanto por causas técnicas como por fenómenos naturales o ataques ilícitos. Como diferencias entre ambas Estrategias, citar que la de 2013 introduce una enumeración de los potenciadores del riesgo existentes en este ámbito[32]. Por su parte, como ya se ha comentado anteriormente, la de 2011 incluye en este ámbito la amenaza del espionaje, especialmente el espionaje económico.

En cuanto al **crimen organizado**, ambas Estrategias lo consideran como una de las amenazas más graves para la seguridad del estado y de sus ciudadanos, ya que constituye un poderoso factor de desestabilización de los cimientos políticos y económicos. Entre las distintas modalidades del crimen organizado, ambos documentos coinciden en señalar el tráfico de drogas, armas y seres humanos y el blanqueo de capitales como las principales amenazas. Por su parte, la Estrategia de 2011 contemplaba también el contrabando, los delitos tecnológicos y la falsificación de moneda[33], mientras que la de 2013 ha incorporado la piratería[34].

31 Principio de disponibilidad inmediata, mediante el cual se comparten los datos antiterroristas; la cláusula de solidaridad, según la cual la Unión y sus estados miembros actuarán de forma conjunta si un estado miembro es objeto de un ataque; la creación del Centro Nacional de Coordinación Antiterrorista (CNCA); la implicación del sistema judicial, para reforzar la eficacia en la acción punitiva, mediante una política penal de prevención de atentados terroristas, cooperación judicial internacional y represión de actividades de financiación del terrorismo; el Plan Operativo Antiterrorista para las FCSE, en el que se prevé la cooperación de las FAS para la protección y vigilancia de grandes infraestructuras; el incremento de los recursos humanos, materiales y técnicos; la potenciación del CNI; establecimiento de Planes Específicos para la protección NRBQ, de los transportes nacionales e internacionales, y para la eficacia en el control de las fronteras exteriores; el desarrollo de una política penitenciaria específica frente al terrorismo; y, por último, las operaciones de las FAS en Afganistán.

32 La ausencia de una legislación armonizada en la materia y el hecho de que Internet haya sido diseñado como un canal de comunicación accesible, sencillo y útil, en donde no se tuvo en cuenta la dimensión de su seguridad. Asimismo, como el bajo coste y mínimo riesgo que este tipo de actividades suponen para el atacante. “Estrategia de Seguridad Nacional: Un proyecto compartido”. Op. Cit. Pág. 27.

33 “Estrategia Española de Seguridad: Una responsabilidad de todos”. Op. Cit. Pág. 50.

34 “Estrategia de Seguridad Nacional: Un proyecto compartido”. Op. Cit. Pág. 27.

En cuanto a la amenaza derivada de **la inestabilidad económica y financiera**, la Estrategia de 2013 la define como una de las principales de hoy en día, no solo por la conflictividad política y social que en sí misma genera sino también por su capacidad de alimentar y reforzar otros riesgos existentes. Además, reconoce que este tipo de riesgos han cobrado un mayor protagonismo en los últimos años como consecuencia de la profunda crisis económica que se está sufriendo a nivel mundial.

Ambas Estrategias proceden a enumerar las principales amenazas y riesgos que pueden desestabilizar el sistema económico y financiero. Básicamente son las mismas en ambos documentos: los desequilibrios macroeconómicos o de los mercados, las actuaciones ilegales, la gran interdependencia económica existente, la volatilidad de los mercados, el desarrollo de las comunicaciones y la logística y, por último, las bruscas variaciones en el precio de los alimentos, las materias primas y la energía.

Por su parte, la Estrategia de 2011 mencionaba también las crisis financieras sistémicas, las actividades delictivas y la competencia por los recursos[35]. La del año 2013 incluye igualmente el deficiente funcionamiento de los organismos supervisores, la existencia de paraísos fiscales, la innovación tecnológica y, por último, la complejidad y competitividad de los sistemas de producción[36].

Por otro lado, ya en el ámbito de la **vulnerabilidad energética**, ambas Estrategias recogen la tradicional amenaza que supone una interrupción grave del suministro o que pueda afectar al normal funcionamiento de infraestructuras y redes de transporte, bien por desastres naturales, ataques terroristas o ciberataques. Además, la Estrategia del año 2013 menciona también el riesgo que supone la competencia por los escasos recursos energéticos ya que, además de afectar a los precios como consecuencia de la ley de la oferta y la demanda, puede acabar en un conflicto por el control de estos recursos. Asimismo, menciona también la necesidad de promover una sostenibilidad medioambiental[37].

Por lo que respecta a la amenaza que para la seguridad supone, no solo para España sino para la comunidad internacional, **la proliferación de armas de destrucción masiva**, ambas Estrategias prestan una especial importancia al riesgo que significa que grupos terroristas puedan llegar a adquirir sustancias nucleares, químicas, biológicas o materiales radiológicos.

Junto a esta tradicional amenaza, la ESN de 2013 realiza una mención concreta al caso de Irán, donde el desarrollo de su programa nuclear puede llegar a suponer una amenaza en caso de que se termine utilizando para un uso no exclusivamente civil.

Asimismo, la actual Estrategia considera como una amenaza el desarrollo de programas balísticos que permitan alcanzar una capacidad autónoma para la producción de misiles de medio y largo alcance, así como de misiles de crucero y de vehículos aéreos no tripulados[38].

Por otro lado, aunque **los flujos migratorios** son procesos que han tenido lugar en todos los momentos históricos, y en principio no tiene porqué ser en sí mismo un

35 "Estrategia Española de Seguridad: Una responsabilidad de todos". Op. Cit. Pág. 53.
36 "Estrategia de Seguridad Nacional: Un proyecto compartido". Op. Cit. Págs. 28 y 29.
37 Íbidem. Pág. 29.
38 Íbidem. Pág. 32.

problema ni representar un riesgo, las dinámicas que se han experimentado en las últimas décadas, así como su volumen, han terminado por transformar este fenómeno en un asunto con implicaciones para la política de seguridad.

En este ámbito, la ESN de 2013 establece como *"drivers"* o elementos que pueden impulsar la inmigración desde los países pobres hacia los países desarrollados: la ausencia de expectativas vitales, de seguridad personal y de derechos, derivadas de factores como la pobreza, la desigualdad, los conflictos bélicos; los riesgos medioambientales; la debilidad institucional y los regímenes autoritarios existentes en determinados países en desarrollo.

Por su parte, la Estrategia de 2011, en lugar de centrarse en los elementos que pueden potenciar este riesgo, enunciaba directamente cuáles eran para ella los riesgos y amenazas que los movimientos migratorios podrían implicar para la seguridad española[39].

Por lo que respecta al ámbito de las **emergencias y catástrofes**, ambas Estrategias coinciden en que nos enfrentamos a riesgos de origen natural (pandemias, huracanes, terremotos,…) o bien provocados por la propia acción del hombre (accidentes nucleares, incendios forestales,…). Al proceder cada uno de los documentos a enumerar los diferentes riesgos y amenazas que pueden poner en peligro en este ámbito la seguridad de las personas, ambos coinciden de manera general en señalar los incendios forestales, los seísmos, erupciones volcánicas, el uso insostenible de los recursos hídricos, la contaminación ambiental, los vertidos y emisiones industriales, tóxicos o contaminantes, la protección de los espacios naturales y forestales y de la fauna y flora terrestre, marítima y fluvial y las pandemias.

En relación con la expansión a gran escala de determinadas enfermedades, la ESN de 2013 señala alguna de reciente aparición, como el síndrome respiratorio agudo severo, o alguna que ya se creía totalmente erradicada, como la tuberculosis.

Por último, con respecto a **la protección de las infraestructuras críticas y servicios esenciales**, ambas Estrategias consideran como relevantes las infraestructuras, suministros y servicios críticos relacionados con la energía, las redes de comunicación y las finanzas, el transporte, el agua, la salud o la alimentación. Asimismo, ambos documentos establecen que este tipo de infraestructuras y servicios pueden ver alterado su normal funcionamiento a causa de fenómenos naturales, errores humanos, fallos tecnológicos o, en el peor de los casos, por atentados terroristas o *ciberataques*.

Por su parte, la EES de 2011, centrándose en el aspecto concreto de nuestro sistema de transporte, enunciaba alguna de las debilidades que lo hacen aún más vulnerable en caso de sufrir algún percance, entre las que destaca: nuestra situación

39 La conflictividad social, la cual puede ser aprovechada por grupos racistas o xenófobos. La aparición de guetos urbanos, que pueden dar lugar a espacios de marginación que fomenten la inseguridad, la violencia y el extremismo ideológico y religioso. La explotación económica de los inmigrantes por parte de organizaciones criminales. La desestabilización de ciertos sectores productivos de la economía con el consiguiente incremento de la economía sumergida. La radicalización extremista y de carácter identitario, falta de integración y el sometimiento a credos radicales e intolerantes. La presencia de personas de otros países, sobre las que no hay datos sobre su verdadera identidad ni nacionalidad. "Estrategia de Seguridad Nacional: Una responsabilidad de todos". Op. Cit. Págs. 71 y 72.

geográfica periférica, la proximidad a pasillos con intenso tráfico de petroleros (como el Cabo de Finisterre o el Estrecho de Gibraltar), la altísima cuota del transporte interior de mercancías por carretera, la insuficiente conexión del ferrocarril con los puertos y los grandes centros logísticos y las escasas interconexiones de transporte terrestre con Europa[40].

Entre las debilidades que afectan al suministro del agua en nuestro país, este mismo documento citaba la situación geográfica y su climatología, las sequías cíclicas, inundaciones y avenidas de carácter torrencial y cursos fluviales en general poco caudalosos[41].

2.5. LÍNEAS GENERALES DE ACTUACIÓN

Una vez realizada la comparativa de los diferentes riesgos y amenazas que recoge cada una de las dos Estrategias, en el presente apartado se va a llevar a cabo un análisis comparativo de las líneas estratégicas establecidas por cada uno de los documentos.

En este sentido, la primera diferencia radica en que mientras que en la EES de 2011 los riesgos y amenazas y las líneas estratégicas se recogían en el mismo capítulo, en la de 2013 cada unos de estos dos aspectos goza de un capítulo propio.

Asimismo, la metodología seguida también varía algo: mientras que en la de 2011 algunas de las líneas estratégicas no están plenamente definidas o concretizadas, la de 2013 establece en cada uno de los ámbitos, en primer lugar, el objetivo general a alcanzar para, a continuación, enumerar las líneas de acción estratégicas u objetivos particulares precisos para alcanzar aquél.

Es en este apartado, el de las líneas estratégicas, en el que se encuentran las mayores diferencias entre una y otra Estrategia, pudiendo llegar a ser totalmente distintas las establecidas en un documento o en el otro. En cada uno de los distintos ámbitos de actuación las principales diferencias son:

En el ámbito de los **conflictos armados**, la EES de 2011 abogaba por actuar en los mismos desde la triple perspectiva de la anticipación y la prevención, la gestión y resolución y la consolidación de la paz[42]. Asimismo, pretendía alcanzar un enfoque integral, en el que participasen tanto medios civiles como militares.[43] Por otro lado, establecía potenciar la anticipación y la prevención, para lo que destacaba las representaciones diplomáticas, el CNI (Centro Nacional de Inteligencia) y el CIFAS (Centro de Inteligencia de las Fuerzas Armadas). Por último, abogaba por la disuasión, como complemento de la anticipación y la prevención.

40 "Estrategia Española de Seguridad: Una responsabilidad de todos". Op. Cit. Págs. 80-81.

41 Íbidem. Pág. 81.

42 Consiste pues en actuar "antes" (para evitar que surjan los enfrentamientos), "durante" (para resolverlos) y "después" (para recuperar la normalidad y establecer las condiciones que impidan un rebrote del mismo).

43 El documento abogaba por la creación de una Unidad de Respuestas Integrada Exterior (URIE). Esta Unidad, con carácter interministerial, podría estar integrada por jueces, fiscales, guardias civiles, policías, bomberos, médicos, ingenieros,… Su contribución estaba prevista producirse en las misiones en el extranjero donde se pudiera requerir personal civil, ya fueran multinacionales o nacionales. Íbidem. Pág. 43.

Por su parte, la ESN de 2013 se centra en dotar a las Fuerzas Armadas de las capacidades militares que precisan para el cumplimiento de su misión; llevar a cabo una transformación continua de las FAS; fomentar la conciencia y cultura de defensa; y, por último, fortalecer la industria española[44].

Por lo que supone al establecimiento de las líneas estratégicas para la **lucha contra el terrorismo**, ambos documentos adoptan la respuesta que establece la Estrategia de la Unión Europea Contra el Terrorismo, la cual se basa en los cuatro pilares de prevenir, proteger, perseguir y responder[45].

En lo que respecta al caso particular de la lucha contra el terrorismo de E.T.A.[46], mientras que el documento de 2011 establecía los principios sobre los que se debía basar la lucha contra esta banda[47], la ESN de 2013 ya da por sentada la derrota de este grupo terrorista, afirmando que *"la madurez de la sociedad española, con las víctimas como referencia ética, la unidad de los partidos políticos, la actuación de las Fuerzas y Cuerpos de Seguridad del Estado y de los Servicios de Inteligencia, el trabajo de los jueces y fiscales, así como la cooperación internacional, han logrado imponerse a la amenaza de la banda terrorista. La fortaleza del Estado de Derecho, la solidez de sus instituciones y la eficacia de las acciones implementadas han derrotado a ETA…"*[48].

Por lo que respecta a la lucha contra las **ciberamenazas**, ambos documentos presentan elementos comunes al establecer las líneas estratégicas para hacer frente a esta amenaza, difiriendo una de otra en pequeñas cuestiones prácticas y de aplicación. Por ejemplo, la EES de 2011 promueve fortalecer la legislación, sin que ello suponga poner en riesgo la privacidad, mientras que la de 2013 pretende incrementar la capacidad de prevención, detección, investigación y respuesta con el apoyo de un marco jurídico operativo y eficaz.

Asimismo, ambos documentos pretenden fomentar la colaboración entre el sector público y el privado, con especial atención a la seguridad de los sistemas de información y las redes de comunicaciones que soportan las infraestructuras críticas. En este aspecto, la ESN de 2013 hace una mención especial a la mejora de la seguridad y la resiliencia de las TIC en el sector privado, para lo que cuenta utilizar las capacidades de los poderes públicos.

Si bien ambos documentos apuntaban a la necesidad de elaborar una Estrategia Nacional de Ciberseguridad, ha sido a raíz de la ESN de 2013 cuando esta previsión se ha materializado[49]. Mediante esta Estrategia de Ciberseguridad, siguiendo el conocido

44 Debe hacerse constar que, con respecto a este último punto, la EES de 2011 dedicaba un apartado completo a la industria española, en el que afirmaba que "la base industrial y tecnológica asociada a la seguridad y la defensa constituye un elemento esencial de nuestra capacidad de respuesta a las amenazas y riesgos". Ídibem. Pág. 42.

45 Comúnmente conocida como la Estrategia de las 4 P's.

46 E.T.A. (Euskadi ta Askatasuna, en castellano Patria Vasca y Libertad): organización terrorista aparecida en España en el año 1959 y que busca, mediante la consecución de actos terroristas, la independencia del País Vasco y el logro de una Patria Vasca Abertzale y Socialista. Desde su creación, dicho grupo terrorista ha matado a más de 800 personas.

47 El consenso y la firmeza política; el impulso a los servicios antiterroristas y de inteligencia; y la cooperación política, policial, judicial y de inteligencia a nivel internacional. Ídibem. Pág. 50.

48 "Estrategia de Seguridad Nacional: Un proyecto compartido". Op. Cit. Pág. 25.

49 Finalmente aprobada en la reunión del Consejo de Seguridad Nacional de 5 de diciembre de 2013.

despliegue normativo de Yarger[50], se pretende desarrollar las previsiones que la Estrategia de Seguridad Nacional ha establecido en este ámbito. Esta Estrategia, al emanar de su hermana mayor, la ESN, se encuentra plenamente alineada con la misma. Ambas mantienen una estructura similar y misma sistemática. Ambas siguen la metodología de, a partir de un objetivo general, establecer objetivos parciales de los que van a emanar acciones o medidas a adoptar. Asimismo, mediante esta nueva Estrategia, se continúa el desarrollo del Sistema de Seguridad Nacional, creando al amparo del Consejo de Seguridad Nacional un Comité Especializado de Ciberseguridad.

También ambas Estrategias propugnan mejorar la cooperación nacional e internacional, si bien la ESN de 2011 es un poco más concisa al expresar qué pretende realizar en este ámbito: impulsar la cooperación para desarrollar acuerdos de control de las *ciberarmas*; luchar contra las ciberamenazas a escala europea, ampliando y consolidando los medios ya existentes[51]; homogeneizar la legislación penal de los estados miembros de la UE[52]; y, por último, ampliar la lucha contra la delincuencia cibernética más allá de la UE.

Como otros aspectos diferenciadores en este ámbito, la EES de 2011 apuntaba igualmente la necesidad de elaborar mapas de riesgos y catálogos de expertos, recursos y buenas prácticas. Por su parte, la de 2013 destaca la necesidad de implantar una cultura de ciberseguridad sólida.

Por lo que respecta a la amenaza del **crimen organizado**, entre las líneas estratégicas que establecía la Estrategia del año 2011 figuraban algunas que ya habían sido recogidas anteriormente en la Estrategia Española contra el Crimen Organizado 2005-2010[53] y de las que, según la literalidad de la EES, se podía llegar a interpretar que

50 El planeamiento estratégico fluye en cascada desde el nivel político representado por el presidente del Gobierno, el propio Gobierno o las Cortes Generales, hasta los distintos actores ministeriales encargados del planeamiento estratégico en sus respectivos departamentos para, posteriormente, desde allí seguir fluyendo a las agencias y servicios responsables del planeamiento para su ejecución. YARGER, Harry R. "Strategic Theory for the 21st Century: The Little Book on Big Strategy". Strategic Studies Institute. United States Army War College. Monografía. Febrero de 2006. http://www.strategicstudiesinstitute.army.mil/pubs/display.cfm?PubID=641

51 En 2004 se creó la Agencia Europea de Seguridad de las Redes y de la Información (ENISA), con una doble finalidad: lograr que las redes y la información de la Unión alcancen un alto grado de seguridad y propiciar el desarrollo de una cultura de la seguridad de las redes y de la información en beneficio de toda la sociedad.

52 En aspectos tales como el acceso ilegal al conjunto o una parte de los sistemas de información, la intromisión, interrupción, obstaculización o daño sobre un sistema de información, o la intromisión ilegal en sus datos.

53 Tal como expone la propia Estrategia Española contra el Crimen Organizado 2011-2014, entre los años 2005-2010 se articuló dicha estrategia en torno a cinco grandes ejes que han sido satisfactoriamente logrados, a pesar de lo cual son recogidos nuevamente en la EES:
- Constitución del Centro de Inteligencia contra el Crimen Organizado (CICO), como órgano para la elaboración de inteligencia estratégica y de evaluación de la amenaza.
- Incremento significativo de los recursos humanos especializados de la Policía y de la Guardia Civil frente al crimen organizado.
- Creación de nuevas y especializadas unidades operativas, tanto centrales como territoriales (GRECO y ECO).
- Incremento de la cooperación y coordinación policial, aduanera y judicial, tanto en el ámbito nacional como internacional.
- Adecuación y perfeccionamiento de la legislación y los instrumentos jurídicos frente a las diferentes modalidades del crimen organizado.

"Estrategia Española contra el Crimen Organizado 2011-2014". Op. cit. Pág. 5.

ya habían sido alcanzadas durante ese período. Por tal motivo, este autor considera que dichas líneas estratégicas carecían verdaderamente de contenido por cuanto ya se habían cumplido, por lo que nuevamente se puede interpretar que este documento tenía una alta carga propagandística. Entre estas medidas se pueden destacar[54]:

- La mejora de los sistemas de información e inteligencia, para lo que se ha creado el CICO[55].
- La creación de nuevas Unidades para la investigación de las diferentes modalidades de delincuencia económica, fraude y corrupción urbanística, afirmando que con ese objetivo se ha creado la Unidad Central de Delincuencia Económica y Fiscal[56]. El documento afirma que, en el ámbito territorial, también se han creado los GRECO,s y los ECO,s[57].
- Incrementar los recursos humanos de las unidades especializadas y los medios materiales y tecnológicos.
- Potenciar la colaboración y cooperación policial, de inteligencia, aduanera y judicial, así como las vinculadas a los servicios de Inteligencia en el exterior.
- Dotar de nuevas competencias a la Fiscalía General contra la corrupción.

Este mismo documento afirma que estos avances deberían complementarse en una triple dirección:

- Mediante la potenciación de los recursos y capacidades de inteligencia del CICO. Para lo que se creará una comisión coordinadora con los servicios especializados de la Fiscalía General del Estado y de otros órganos de la Administración Pública.
- Mejorando la coordinación entre organismos nacionales e internacionales, para lo que se considera que las operaciones conjuntas en el ámbito de la Unión Europea facilitan el acceso a los datos y a la información.
- Adaptando y mejorando permanentemente los instrumentos jurídicos para poder luchar con eficacia contra todas las modalidades del crimen organizado.

54 "Estrategia Española de Seguridad: Una responsabilidad de todos". Op. Cit. Págs. 50-52.

55 C.I.C.O. (Centro de Inteligencia contra el Crimen Organizado): creado por el "Real Decreto 991/2006, de 8 de septiembre, por el que se desarrolla la estructura orgánica básica del Ministerio del Interior", es el responsable, entre otros aspectos, de elaborar la inteligencia estratégica en la lucha contra todo tipo de delincuencia organizada, así como, en su caso, establecer criterios de coordinación operativa de los servicios actuantes en los supuestos de coincidencia o concurrencia en las investigaciones.

56 La Unidad Central de Delincuencia Económica y Fiscal es una Unidad del Cuerpo Nacional de Policía creada con el objeto de realizar la investigación y persecución de las actividades delictivas en materia de delincuencia económica y fiscal. No obstante, sorprende cómo la ESN no hace mención al Departamento de investigación de delitos económicos y delincuencia internacional existente en el seno de la Unidad Central Operativa (U.C.O.) de la Guardia Civil, cuyos cometidos son los mismos que los de la Unidad del CNP.

57 Los G.R.E.C.O.'s (Grupos de Respuesta contra el Crimen Organizado) del Cuerpo Nacional de Policía son ocho y se encuentran desplegados en: Pontevedra (Galicia), Las Palmas (Canarias), Chiclana (Cádiz), Marbella (Málaga), Benidorm y Orihuela (Alicante), y Palma de Mallorca e Ibiza (Baleares). Por su parte, los E.C.O.'s (Equipos contra el Crimen Organizado) de la Guardia Civil son siete y se encuentran desplegados en Pontevedra (Galicia), Las Palmas y Tenerife (Canarias), Málaga, Alicante, Palma de Mallorca (Baleares) y Barcelona.

Por su parte, la ESN de 2013 mantiene algunas de las principales líneas estratégicas de su antecesora, como son las relativas a la potenciación y mejora de los recursos, mecanismos y procedimientos, la mejora de la coordinación y colaboración internacional y la realización de reformas legislativas.

Como puede apreciarse, la EES de 2011 contenía gran cantidad de elementos que no aportaban gran cosa a su futuro cumplimiento. Es éste uno de los ámbitos en los que más se recreaba, precisamente en los logros que se habían conseguido durante los años previos a su aprobación, conteniendo a su vez elementos que deberían contemplarse, más bien, en una Estrategia de segundo nivel que desarrollase aquella, es decir, lo que debería ser una Estrategia de Lucha contra el Crimen Organizado. Por tal motivo, en la nueva Estrategia han desaparecido todas estas referencias.

Por otro lado, como consecuencia de los numerosos casos de corrupción política existente en el momento de proceder a la elaboración y posterior aprobación de la nueva Estrategia, el documento orienta alguna de estas medidas hacia la mejora de la investigación policial en casos relacionados con el tráfico de influencias en las instituciones y hacia la corrupción en todas sus formas, así como hacia la potenciación y mejora de las investigaciones relacionadas con el blanqueo de capitales[58].

Además, la ESN de 2013 introduce como líneas estratégicas el hecho de sensibilizar y concienciar a la sociedad de que la lucha contra este fenómeno es global, por un lado, y el realizar un tratamiento integral de este problema, para lo que pretende la implicación no solo de los actores públicos, sino también de los privados y, especialmente, del mundo universitario.

Por lo que respecta al ámbito de la **seguridad económica y financiera**, en ambos documentos es patente el entorno de crisis económica en que han sido aprobados, sobre todo en el de 2013. En este sentido, ambas Estrategias hacen referencia a la necesidad de adoptar medidas que permitan desarrollar un modelo de crecimiento económico sostenible, mitigar los desequilibrios de los mercados, proceder a una supervisión de los agentes económicos y sociales, avanzar en la gobernanza económica o establecer mecanismos de supervisión y regulación.

Asimismo, ambos documentos hacen referencia al Sistema de Inteligencia Económica (SIE) como herramienta para analizar y facilitar información económica, financiera y empresarial estratégica relevante, oportuna y útil para apoyar la acción del estado y una mejor toma de decisiones. Igualmente, ambas Estrategias proponen potenciar la presencia económica internacional de España, para lo que establecen, entre otras medidas, potenciar la "marca España". Por último, ambos documentos destacan el papel del sector privado en la seguridad de las infraestructuras y los servicios financieros de los que son responsables.

Por su parte, la EES de 2011 realizaba una mención expresa a la lucha contra el blanqueo de capitales procedente del crimen organizado[59], medida que en la ESN de 2013 viene reflejada en el apartado de lucha contra el crimen organizado[60].

58 Estrategia de Seguridad Nacional: Un proyecto compartido. Op. Cit. Pág. 25. Puntos 2 y 5.
59 "Estrategia Española de Seguridad: Una responsabilidad de todos". Op. Cit. Pág. 54.
60 "Estrategia de Seguridad Nacional: Un proyecto compartido". Op. Cit. Pág. 43. Pto. 5.

Como novedad, el documento del año 2013 hace referencia a la necesidad de *"establecer un marco socio-laboral que contribuya a una gestión eficaz de las relaciones laborales, basado en el diálogo social con vistas a la adopción de medidas consensuadas que coadyuven a reducir los niveles de conflictividad y favorezcan la paz social, que facilite la estabilidad en el empleo, la creación de puestos de trabajo y la eficiencia del mercado de trabajo"*[61].

En el ámbito de **la seguridad energética**, si bien ambos documentos se centran en actuar sobre los tres mismos ámbitos: abastecimiento, suministro y consumo, sin embargo cabe destacar que la ESN de 2013 es bastante más detallada que la del año 2011.

En este sentido, en el ámbito del abastecimiento, ambos documentos abogan por la diversificación de las fuentes de energía y de abastecimiento, para lo que realizan una apuesta estratégica por las energías renovables. De igual manera ambas Estrategias apuestan por una política energética europea que potencie las interconexiones entre los estados miembros y, en especial, entre la Península Ibérica y el resto de Europa, alcanzando de esta manera un mercado europeo de electricidad y gas natural plenamente integrado. Además, la de 2013 pretende impulsar la investigación y explotación de yacimientos de hidrocarburos y diseñar planes de viabilidad para la extracción de estos recursos[62].

Es en el ámbito de la distribución donde más se centra la ESN de 2013. Ambos documentos pretenden reforzar el control de las comunicaciones, pero mientras que la de 2011 se limitaba al espacio marítimo, la de 2013 lo amplía también a las comunicaciones terrestres. Asimismo, ambas Estrategias abogan por la potenciación de las diferentes formas de almacenamiento, para lo que la de 2011 apostaba por situar las plantas de regasificación en diferentes puertos.

También ambos documentos pretenden mejorar la fiabilidad de las redes de abastecimiento, de hecho el de 2011 proponía dotarlas de sistemas redundantes e independientes de otras tecnologías y operadores, considerando clave en este ámbito el Plan de Protección de Instalaciones Críticas. Así, las dos Estrategias promueven la potenciación de la flexibilidad operativa del sistema nacional de redes de transporte de energía y la revisión de los planes de canalización y priorización de la demanda en caso de interrupción o escasez en el suministro.

Por su parte, la ESN de 2013 añade la colaboración público-privada con el objeto de garantizar el suministro en caso de que las infraestructuras críticas se vean afectadas.

Para finalizar en este ámbito, por lo que respecta al área del consumo, también ambos pretenden impulsar el ahorro y la eficiencia energética. Aunque los dos pretenden promover la liberación de los mercados, la EES de 2011 no indica cómo, mientras que la de 2013 dice que *"mediante el favorecimiento de un marco regulatorio armonizado, transparente y objetivo que incremente la seguridad jurídica y la competitividad de las empresas"*[63]. Además, la ESN de 2013 pretende también impulsar la sostenibilidad energética a través de actuaciones que contemplen los aspectos fiscales, medioambientales y el uso eficiente de los recursos disponibles.

61 Debe hacerse constar el ambiente de crispación social en el que dicho documento fue aprobado, en el que se asistía de manera casi cotidiana a demostraciones de descontento social a causa de algunas de las medidas adoptadas por el gobierno para luchar contra la crisis.

62 "Estrategia de Seguridad Nacional: Un proyecto compartido". Op. Cit. Pág. 45. Pto. 3.

63 Ibidem. Pág. 45. Pto. 11.

Continuando con los distintos ámbitos de actuación de la Estrategia de Seguridad Nacional, por lo que respecta a **la No Proliferación de Armas de Destrucción Masiva** (ADM), se puede afirmar que la EES de 2011 era bastante más vaga e imprecisa en los objetivos a alcanzar que su sucesora de 2013.

Como es lógico en una Estrategia de carácter continuista, ésta contiene muchos elementos comunes con su predecesora. Así, ambos documentos basan su estrategia en el desarrollo de un trabajo preventivo, siempre enmarcado en un multilateralismo eficaz y en la cooperación activa, especialmente en el ámbito de la ONU y de la Unión Europea. En sentido parecido, ambas Estrategias fijan su atención sobre el control de productos y tecnologías de doble uso relacionados con este tipo de armas. En este aspecto, la EES de 2011 alude de manera especial al control preciso para que el comercio de uranio con fines pacíficos no se desvíe hacia la proliferación, realizando mención expresa a sus compromisos con la Iniciativa de Seguridad contra la Proliferación (ISP)[64], la Iniciativa Global contra el Terrorismo Nuclear (IGTN)[65] y el Grupo de Suministradores Nucleares (GSN)[66].

A continuación, ambos documentos pretenden limitar la proliferación de los misiles de medio y largo alcance que permitirían el lanzamiento de este tipo de armas a gran distancia. Asimismo, ambas Estrategias declaran su intención de proseguir participando en el Programa de Defensa Antimisiles de la OTAN[67]. En este ámbito, la ESN de 2013 amplía además su intención de secundar el desarrollo de una capacidad autónoma de defensa antimisiles en el marco de la OTAN y de armonizar el principio de la disuasión mínima con los compromisos internacionales de desarme.

64 La ISP constituye un esfuerzo global para detener el tráfico ilícito de armas de destrucción masiva, sus vectores de lanzamiento y materiales relacionados, hacia y desde estados y actores no estatales, poniendo énfasis en la interceptación del tráfico ilícito como mecanismo de contraproliferación. La ISP fue lanzada en 2003. En total suman más de 90 países, entre los que se encuentra España. http://www.exteriores.gob.es/Portal/es/PoliticaExteriorCooperacion/Desarme/Documents/INSTRUMENTOS%20Y%20REG%C3%8DMENES%20PRINCIPALES.doc

65 La IGTN es una iniciativa lanzada conjuntamente por los presidentes de Estados Unidos y de la Federación Rusa en la Cumbre del G-8 que tuvo lugar en San Petersburgo, en julio de 2006. La iniciativa tiene el objetivo de desarrollar la cooperación de un número creciente de estados – actualmente 85 – que, en el marco de la lucha contra el terrorismo, adopten también medidas para prevenir atentados con materiales nucleares o radiactivos, tomando como referencia las recomendaciones del OIEA. Desde 2010 España ejerce la función de coordinador técnico de la Iniciativa desde el llamado Implementation Assessment Group. http://www.exteriores.gob.es/Portal/es/PoliticaExteriorCooperacion/Desarme/Documents/INSTRUMENTOS%20Y%20REG%C3%8DMENES%20PRINCIPALES.doc

66 El GSN es un grupo de países suministradores nucleares que tiene como objetivo contribuir a la no proliferación de las armas nucleares, mediante la aplicación de dos conjuntos de Directrices a la exportación de productos nucleares y de productos relacionados, sin por ello impedir el comercio y la cooperación internacional en el ámbito nuclear. http://www.exteriores.gob.es/Portal/es/PoliticaExteriorCooperacion/Desarme/Documents/INSTRUMENTOS%20Y%20REG%C3%8DMENES%20PRINCIPALES.doc

67 El trabajo de la OTAN sobre el Programa de Defensa Antimisiles se inició en la década de los 1990, en respuesta a la proliferación de armas de destrucción en masa y sus sistemas vectores, incluidos los misiles. El enfoque inicial se centró en la protección de tropas de la OTAN desplegadas (Theatre Missile Defence), pero el trabajo se amplió en 2002 para incluir consideraciones sobre la protección de los centros de población y territorio (Territorio Missile Defence). En la Cumbre de la OTAN del año 2010 en Lisboa, se decidió desarrollar una capacidad de defensa contra misiles balísticos (BMD) para continuar con la defensa colectiva. http://www.nato.int/cps/en/natolive/topics_49635.htm

Por su parte, como elementos diferenciadores entre ambas Estrategias, se puede afirmar que la de 2011 manifiesta de manera más precisa su compromiso en el logro de alcanzar un mundo sin armas nucleares. Para ello enumera algunos de los instrumentos en los que participa España, como el Tratado de No Proliferación (TPN) de 1987, anteriormente mencionado, o el Tratado de Prohibición Completa de Ensayos Nucleares (TPCEN)[68], así como las iniciativas que pretende apoyar, como la eliminación de la producción de material fisible para armamento o la constitución de Zonas Libres de Armas Nucleares; además define cuál es la política de España en esta materia, como es la renuncia al arma nuclear, la prohibición de su paso por el territorio nacional y la lucha contra la proliferación y en pos del desarme nuclear mundial[69].

Por su parte, la Estrategia del año 2013 introduce aspectos como el desarrollo y actualización de los Planes Nacionales de prevención de la proliferación y mitigación de riesgos en los ámbitos nuclear, químico y biológico, destacando la puesta en marcha de un Plan Nacional de Biocustodia[70]. Asimismo, plasma por escrito por primera vez su voluntad de combatir las transferencias intangibles de conocimiento, tecnología, bienes y equipos y de luchar contra la financiación ilegal en este ámbito.

Asimismo, este documento realiza una mención expresa a la posibilidad del acceso por parte de grupos terroristas y otros agentes no estatales a los materiales y fuentes radioactivas, así como la realización de atentados terroristas con este tipo de materiales, nucleares o de ambos tipos. Para ello pretende adoptar medidas preventivas de vigilancia en relación con el uso de la red.

Continuando con el desarrollo y comparación de las diferentes líneas estratégicas, en el ámbito de la **lucha contra la inmigración irregular** ambas Estrategias son muy parecidas, recogiendo prácticamente los mismos objetivos estratégicos: la ordenación eficaz de los flujos migratorios, que responda a nuestras necesidades demográficas y laborales y a nuestra capacidad de acogida; el control y vigilancia eficaz de los accesos a las fronteras exteriores españolas[71]; la cooperación con los países de origen y tránsito migratorio; la defensa de la legalidad y preservación de la seguridad ciudadana, para facilitar la lucha contra el crimen organizado, las redes de inmigración irregular y de tráfico de seres humanos; la lucha contra la discriminación y garantía

68 El TPCEN prohíbe las explosiones nucleares en todo el mundo, en todas partes: en la superficie de la Tierra, en la atmósfera, bajo el agua y bajo tierra. El Tratado fue negociado en Ginebra entre 1994 y 1996. 183 países han firmado el Tratado, de los cuales 159 lo han ratificado. http://www.ctbto.org/

69 "Estrategia Española de Seguridad: Una responsabilidad de todos". Op. Cit. Pág. 62.

70 Esta biocustodia afecta, por un lado, a los agentes biológicos, para lo que sería preciso implantar estándares de calidad por medio de acreditaciones, auditorias o el establecimiento de licencias individuales y corporativas. Asimismo, afectaría también a todo el personal que desarrolle sus actividades en el ámbito biológico. Por último, sería necesario realizar un inventario de instalaciones donde se manejen o puedan manejarse agentes biológicos, sea cual sea su nivel de bioseguridad. Ministerio de Defensa. Instituto Español de Estudios Estratégicos. "Proliferación de ADM y de Tecnología avanzada". Cuadernos de Estrategia. Nº 53. Septiembre de 2011.

71 En este punto, la ESN de 2013 hace mención al Sistema Integrado de Gestión de las Fronteras Exteriores de la UE. El objetivo es el de instaurar mecanismos comunes de control para incrementar la seguridad de las fronteras exteriores, como ha sido la creación, en 2004, de la Agencia Europea para la gestión de la cooperación operativa en las fronteras exteriores de los estados miembros de la Unión Europea (FRONTEX), la realización de patrullas conjuntas o la creación de equipos de intervención rápida en las fronteras.

del principio de igualdad[72], con atención especial a los colectivos más vulnerables, y la promoción de la integración social.

Como elementos diferenciadores entre lo establecido en una y otra Estrategia, únicamente señalar que en la del año 2011 se hacía alusión a promover los objetivos asumidos por la *Alianza de Civilizaciones* y a favorecer el diálogo con las confesiones religiosas de las poblaciones inmigrantes[73], y en la de 2013 a estrechar la colaboración entre las Administraciones Públicas y, en su caso, con las ONG y el sector privado[74].

Continuando con la definición de las líneas estratégicas para luchar contra la amenaza procedente del **espionaje,** como ya se ha comentado anteriormente, en la EES de 2011 no constaba como una amenaza autónoma, sino que se recogía incluida dentro de las ciberamenazas, en las que, a pesar de dedicarle un apartado en exclusiva, centra sus líneas de actuación únicamente en potenciar las capacidades de inteligencia y contrainteligencia del estado, tanto a nivel tecnológico como humano.

Por su parte, la Estrategia del año 2013, además de contemplar también la potenciación de estas capacidades, amplía sus líneas de actuación a elaborar una normativa que regule la protección de la información clasificada, a sensibilizar al personal que maneja información clasificada y a la protección y sensibilización de los ciudadanos españoles que desarrollan sus actividades fuera del territorio nacional y que, por tanto, pueden ser más vulnerables a las acciones hostiles de otros estados, grupos o individuos.

Por lo que respecta a las líneas de acción que la Estrategia de Seguridad Nacional fija en **la protección ante emergencias y catástrofes**, como cabía esperarse, ambos documentos contienen elementos comunes, si bien se puede afirmar que la ESN de 2013 es algo más completa en este aspecto que su predecesora.

En este sentido, ambos documentos hacen referencia a la necesidad de reconfigurar el Sistema Nacional de Gestión de Situaciones de Crisis, debiendo alcanzarse un enfoque integrador y potenciador de las actuaciones entre la Administración General del Estado, las Comunidades Autónomas y las Administraciones Locales y a la necesidad de establecer un nuevo marco jurídico de la protección civil en el que predomine la prevención y la coordinación interadministrativa[75].

Asimismo, ambos promueven una mayor cooperación europea e internacional, así como la promoción entre los ciudadanos de una cultura de prevención. Con respecto a este último aspecto, la ESN de 2013 añade la promoción en centros escolares de programas de educación para la prevención.

72 En este aspecto, la EES de 2011 hacía mención a continuar el Plan Estratégico de Ciudadanía e Integración 2007-2010. Este Plan estaba orientado a potenciar la cohesión social a través de políticas basadas en la igualdad de oportunidades, en la igualdad de derechos y deberes, en el desarrollo de un sentimiento de pertenencia de la población inmigrada a la sociedad española y en el respeto a la diversidad. Aprobado en reunión del Consejo de Ministros el día 16 de febrero de 2007. Ministerio de Trabajo y Asuntos Sociales. http://extranjeros.empleo.gob.es/es/Integracion-Retorno/Plan_estrategico/pdf/PECIDEF180407.pdf

73 "Estrategia Española de Seguridad: Una responsabilidad de todos". Op. Cit. Pág. 73.

74 "Estrategia de Seguridad Nacional: Un proyecto compartido". Op. Cit. Pág. 47. Pto. 5.

75 La actual Ley de Protección Civil data del año 1985. Jefatura del Estado. "Ley 2/1985, de 21 de enero, sobre Protección Civil". Boletín Oficial del Estado, núm. 22. 25 de enero de 1985.

Como elementos diferenciadores, la EES de 2011 apoyaba el fomento de la participación ciudadana y el establecimiento de programas de colaboración entre la Administración General del Estado y las Comunidades Autónomas para la elaboración de una cartografía de riesgos.

Por su parte, la del año 2013 añade aspectos tales como el establecimiento de protocolos de actuación coordinada, la constitución de una red de alerta nacional de riesgos naturales y la creación de un sistema inteligente de planificación en red que permita identificar, evaluar, prevenir y mitigar los distintos riesgos. Además del mantenimiento de directorios de recursos para una gestión eficiente de la respuesta asistencial en situación de emergencias y catástrofes.

Continuando con las distintas líneas de acción recogidas en la Estrategia de Seguridad Nacional del año 2013, por lo que respecta a **la seguridad marítima**, si bien la EES de 2011 no la recoge propiamente como amenaza, sí la cita sin embargo como uno de los ámbitos en los que se pueden manifestar riesgos y amenazas que pueden afectar de manera transversal a una serie de infraestructuras, servicios y suministros críticos.

En este ámbito, el documento de 2011 propugna la vigilancia y la seguridad marítima mediante la integración eficiente de los medios civiles y militares, así como el impulso de las iniciativas internacionales tendentes a garantizar unas vías de comunicación seguras para el suministro de recursos básicos y a mejorar la gobernanza de los espacios marítimos[76].

Por su parte, el documento de 2013 establece como objetivos estratégicos la necesidad de adoptar un enfoque integral y de potenciar la actuación coordinada y cooperativa; la necesidad de integrar las capacidades de prevención y respuesta; el fomento de la cooperación internacional, en especial en el ámbito de los acuerdos bilaterales internacionales; y, por último, la colaboración con el sector privado[77].

Por lo que respecta a la **protección de las infraestructuras críticas**, las líneas estratégicas de la EES de 2011 se centraban en la protección de las infraestructuras críticas, así como en el refuerzo de la resistencia y capacidad de recuperación de las mismas (resiliencia) y en la necesidad de llevar a cabo un esfuerzo conjunto de las Administraciones Públicas y de las empresas.

La ESN de 2013, además de recoger las anteriores líneas estratégicas, las completa y amplía en los siguientes aspectos: en lo que respecta a la cooperación público-privada, establece la creación de un sistema que haga posible la cooperación mutua y el intercambio de información de interés para todas las partes. Pretende establecer un sistema de planificación que permita identificar, evaluar, prevenir y mitigar los riesgos. También procura catalogar las infraestructuras de manera priorizada para permitir una racionalización en la asignación de recursos.

En el ámbito de la resiliencia, el documento propugna la existencia de sistemas redundantes o aislados y la adecuada dotación de elementos de reposición. Para la promoción de la cooperación internacional, propone impulsar el cumplimiento

76 "Estrategia Española de Seguridad: Una responsabilidad de todos". Op. Cit. Pág. 35.

77 El 5 de diciembre de 2013, el Consejo de Seguridad Nacional aprobó la Estrategia de Seguridad Marítima.

del Programa Europeo de Protección de Infraestructuras Críticas (EPCIP)[78] y de la Directiva Europea 2008/114/CE del Consejo[79].

3. SISTEMA DE SEGURIDAD NACIONAL

En ambos documentos se establece un Sistema de Seguridad Nacional mediante el que se pretende garantizar el funcionamiento óptimo, integrado y flexible de todos los recursos disponibles a tal fin. Ambos Sistemas presentan elementos comunes, ya que en los dos se prevé la constitución de un Consejo de Seguridad, si bien en la EES de 2011 se llama Consejo Español de Seguridad y en la de 2013 Consejo de Seguridad Nacional. Este órgano, dependiente de la Presidencia de Gobierno, está presidido por el presidente del Gobierno o, en su caso, por S.M. el Rey. Además de la vicepresidenta, lo componen también los ministros de Asuntos Exteriores y de Cooperación, de Defensa, de Hacienda y Administraciones Públicas, del Interior, de Fomento, de Industria, Energía y Turismo y de Economía y Competitividad, el director del Gabinete de la Presidencia del Gobierno, el secretario de Estado de Asuntos Exteriores, el jefe de Estado Mayor de la Defensa, el secretario de Estado de Seguridad y el secretario de Estado-director del Centro Nacional de Inteligencia.

Como complemento a este Consejo de Seguridad, ambos documentos prevén también la constitución de órganos de segundo nivel, con la misión de apoyarlo. En la EES de 2011 su designación era la de Comisiones Interministeriales y en la de 2013 de Comités Especializados.

Sin embargo, la principal diferencia entre un documento y otro no se encuentra en la forma de organizar sobre el papel este sistema de Seguridad Nacional, sino en cómo se han materializado las previsiones contenidas en ambas Estrategias. En este sentido, cabe reconocer la voluntad demostrada a raíz de la ESN de 2013 para que ésta no se convirtiese en papel mojado. Para ello, nada más presentarse la nueva Estrategia, se aprobó el Real Decreto 385/2013, mediante el que se crea el Consejo de Seguridad Nacional como Comisión Delegada del Gobierno para la Seguridad Nacional y mediante el que se aprueba su composición y funciones[80]. Tras su reunión constitutiva del pasado 11 de julio de 2013, las reuniones de dicho Consejo se vienen celebrando con una periodicidad bimensual.

Además, prosiguiendo en la conformación de este Sistema de Seguridad Nacional

78 Comisión de las Comunidades Europeas. “Comunicación de la Comisión sobre un Programa Europeo para la Protección de Infraestructuras Críticas. COM (2006) 786 final”. Bruselas, 12 de diciembre de 2006. El objetivo de este Programa es el de mejorar la protección de las infraestructuras críticas de la UE, para lo que estima preciso la creación de un marco de la UE relativo a su protección. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:EN:PDF

79 Consejo de la Unión Europea. “Directiva 2008/114/CE del Consejo, de 8 de diciembre de 2008, sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección”. Diario Oficial de la Unión Europea. L 345/75. 23 de diciembre de 2008. Esta Directiva, además de establecer un procedimiento de identificación y designación de infraestructuras críticas europeas, establece también un planteamiento común para evaluar dichas infraestructuras, con el fin de mejorar y, así, proteger las necesidades de la población. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32008L0114:ES:NOT

80 Consejo de Ministros. “Real Decreto 385/2013, de 31 de mayo, de modificación del Real Decreto 1886/2011, de 30 de diciembre, por el que se establecen las Comisiones Delegadas del Gobierno”. BOE núm. 131, de 1 de junio de 2013.

previsto en la Estrategia, se han constituido los Comités Especializados de Ciberseguridad y el de Seguridad Marítima.

En definitiva, no solo se ha creado el instrumento jurídico que permite el desarrollo de la ESN, y evitar así que ésta se convierta en papel mojado, sino que se están adoptando todas las medidas para que la Estrategia de Seguridad Nacional tenga realmente un carácter global e integral e inspire así los planeamientos estratégicos de los niveles inferiores, alcanzando de esta manera la sinergia precisa para poder cumplir los objetivos establecidos.

4. CONCLUSIONES

La publicación en España de nuestra Estrategia de Seguridad lo ha sido de una manera tardía con respecto a la de los países de nuestro entorno. Este primer documento, además de no contar con el consenso de las principales fuerzas políticas, recogía en su cuerpo numerosos elementos que no aportaban gran cosa al cumplimiento de la Estrategia y que, por el contrario, podían llegar a ser interpretados en clave propagandística como logros del gobierno durante la IX Legislatura y gran parte de la X, lo que, obviamente, no debía ser del agrado de la oposición.

Consecuentemente, con tan solo dos años de vigencia, el nuevo gobierno del Partido Popular decidió la modificación de la EES. En esta ocasión, con el objetivo de evitar los anteriores desaciertos, en el proceso de elaboración del nuevo documento se buscó el consenso, para lo que se contó con un Comité de Expertos de alto nivel y; además, con el mismo objetivo, el documento fue rápidamente presentado ante el Parlamento.

Otro de los motivos para modificar la EES fue la intención de considerar la Seguridad Marítima como una amenaza propia, ya que hasta ese momento no era considerada como tal, sino más bien como uno de los ámbitos (terrestre, aéreo, marítimo,...) en los que se podían desarrollar el resto de amenazas.

Por su parte, la ESN actual es considerablemente más corta que la de 2011. Esta diferencia de tamaño obedece, principalmente, a que el nuevo documento se ha desembarazado de todos aquellos elementos que no aportaban gran cosa al cumplimiento de la Estrategia. Asimismo, se aprecia claramente que la elaboración de la Estrategia de 2013 se ha llevado a cabo en un contexto de fuerte crisis económica, lo que ha llevado, además de considerar la crisis financiera y económica como uno de los mayores retos para la Seguridad Nacional, a establecer como uno de los principios informadores de la misma la eficiencia y la sostenibilidad en el uso de los recursos, principio que debe toda actuación en cualquiera de los ámbitos de actuación.

En cuanto a su estructura, constan ligeras variaciones: en la de 2013 existe un capítulo para las amenazas y otro para las líneas estratégicas, mientras que en la de 2011 ambos aspectos se recogían en el mismo. Por su parte, la del año 2011 dedicaba un capítulo entero a los Potenciadores del Riesgo, mientras que la actual se limita a reseñarlos al comienzo del capítulo dedicado a los riesgos y amenazas.

Del análisis comparativo de sus elementos esenciales se pueden extraer las siguientes conclusiones:

- Por lo que respecta al concepto de Seguridad Nacional, a pesar de que en los

borradores preliminares de la del año 2011 se recogía inicialmente, sin embargo dicho concepto no fue finalmente contemplado en su versión final. No así en la del año 2013, que aporta una definición clara y concisa de qué debe entenderse por Seguridad Nacional. No obstante, realizando una interpretación finalista de la misma, la EES de 2011 define cuáles son sus objetivos principales.

- En cuanto a los intereses nacionales, los definidos en la Estrategia Española de Seguridad del año 2011 no diferían enormemente de los que hasta ese momento habían sido establecidos por el nivel político. Por su parte, la actual ESN no establece de manera concreta cuáles son estos intereses nacionales. En este caso, es preciso acudir a una lectura detenida del documento para poder entresacar algunos de ellos, entre los que se puede llegar a identificar la libertad, la democracia o el respeto a la dignidad del ser humano.

  En este aspecto, nuestra actual Estrategia se separa de la corriente seguida en los países de nuestro entorno, en cuyas Estrategias se detallan en mayor o menor medida cuáles son sus intereses nacionales a proteger. Es curiosa esta ausencia porque la declaración de estos intereses es un elemento esencial en cualquier Estrategia de Seguridad, ya que, metodológicamente, es preciso determinar qué es lo que pretende proteger. Se estima que esta ausencia quizás se deba a que estos intereses habían sido ya previamente declarados en la Directiva de Defensa Nacional 1/2012, aprobada por el mismo gobierno tan solo unos meses antes.

- En el apartado de las políticas y compromisos internacionales, el documento de 2013 recoge los mismos frentes que el de 2011 en los que es preciso articular la proyección exterior española. Sin embargo, la ESN de 2013 no establece cuáles son nuestros principios en acción exterior, lo que sí realizaba la de 2011.

  Al definir las zonas regionales de actuación, ambas Estrategias coinciden plenamente en las mismas, si bien existen algunas matizaciones. Por lo que respecta a la política a desarrollar con respecto a Europa, se aprecia una línea continuista entre una Estrategia y la otra, y es que en este ámbito no queda realmente mucho margen de actuación para un gobierno o para otro.

  Por el contrario, sí se aprecia la evolución de los recientes conflictos en nuestra vecindad del sur, como así lo atestigua la mención que la ESN de 2013 realiza a las crisis surgidas en la otra orilla del Mediterráneo, concretamente en Libia y Siria. De esta manera, lo que a finales del año 2010 comenzó siendo lo que se conocería como *"Primavera Árabe"*, que gozaba de la simpatía y apoyo de los países occidentales por entender que se trataba de un proceso de democratización de algunos de los países de la ribera sur del mediterráneo, acabó sin embargo en problemas de estabilidad regional y de conflictos enquistados.

  Asimismo, si en la EES del año 2011 el Sahel se configuraba ya como un espacio clave, en la del año 2013 no cabe ya duda de la importancia de este área tras la revuelta touareg que tuvo lugar en febrero de 2012 en el norte de Malí y que ha llevado a España a participar en la Operación "SERVAL", en apoyo de las fuerzas francesas que operan en el norte del país.

- Por lo que respecta a los riesgos y amenazas, la ESN de 2013, pese a utilizar en

numerosas ocasiones ambos términos, no los define, cosa que sí realizaba su predecesora. Esta ausencia obedece nuevamente a criterios de economía literaria. Por otro lado, la ESN de 2013 abandona la idea de concebir estos riesgos y amenazas en unos ámbitos concretos.

El documento de 2013, además de contemplar todas las amenazas que se reflejaban en la Estrategia de 2011, añade otras dos: el espionaje, que en la Estrategia de 2011 estaba incluida dentro de las ciberamenazas, y la vulnerabilidad del espacio marítimo.

Con respecto a la amenaza concreta del terrorismo, el nuevo documento da ya por sentada la derrota de la banda terrorista ETA, de la que tan solo espera su disolución definitiva.

Por otro lado, condicionada por el contexto económico y por los numerosos escándalos de corrupción registrados, la ESN de 2013 ha incluido como amenaza a la seguridad económica y financiera el deficiente funcionamiento de los organismos supervisores y la existencia de paraísos fiscales.

- En lo que concierne a las diferentes líneas estratégicas o de actuación, mientras que en la de 2011 algunas de éstas no están plenamente definidas, la de 2013 establece en cada uno de los ámbitos el objetivo general a alcanzar para, a continuación, enumerar las líneas de acción estratégicas u objetivos particulares precisos para alcanzarlo. Como aspectos más significativos en algunos de estos ámbitos, se pueden destacar:

  1. En el ámbito de la lucha contra el terrorismo, se le da continuidad a la anterior Estrategia de Lucha contra el Terrorismo, basada en los principios de la Prevención, la Protección, la Preparación de la respuesta y la Persecución.

  2. En el ámbito de la ciberseguridad, respondiendo al despliegue normativo necesario para desarrollar las previsiones contenidas en este ámbito en la ESN, se ha aprobado la primera Estrategia de Ciberseguridad Nacional. Esta Estrategia, al emanar de la ESN, se encuentra plenamente alineada con ella, con la que mantiene una estructura y metodología similar. Asimismo, mediante esta Estrategia se continúa el desarrollo del Sistema de Seguridad Nacional, para lo que se ha creado un Comité Especializado de Ciberseguridad, dependiente del Consejo de Seguridad Nacional.

  3. En el ámbito del crimen organizado, la actual Estrategia se ha desembarazado de todos aquellos elementos que no contribuían directamente a su futuro cumplimiento y que se limitaban a ensalzar los logros que se habían alcanzado durante los años previos a su publicación. Asimismo, también ha eliminado algunos elementos cuya inclusión corresponde más bien a una estrategia de segundo nivel que, en este ámbito, desarrolle la ESN.

  4. Asimismo, como consecuencia de los numerosos casos de corrupción política, la ESN orienta alguna de estas medidas hacia la mejora de la investigación policial en casos relacionados con el tráfico de influencias en las instituciones y hacia la corrupción en todas sus formas, así como hacia la potenciación y mejora de las investigaciones relacionadas con el blanqueo de capitales.

5. En el ámbito de la seguridad económica y financiera, aportación novedosa como consecuencia del ambiente de crispación social en el que dicho documento fue elaborado, pues se asistía de manera casi cotidiana a demostraciones de descontento social que podían llegar a generar auténticos problemas para la seguridad pública, la Estrategia se ha propuesto establecer un marco socio-laboral que coadyuve a reducir los niveles de conflictividad y que favorezca la paz social, facilite la estabilidad en el empleo, la creación de puestos de trabajo y la eficiencia del mercado de trabajo.

6. Por lo que se refiere a la amenaza procedente del espionaje, en la ESN de 2013 este aspecto ha sido desarrollado de manera totalmente autónoma, constituyendo por sí sola una amenaza sujeta a regulación, y en la que, además de reforzar las capacidades de inteligencia, presta una especial importancia a la protección de la información.

7. Por último, en el ámbito de la seguridad marítima, de manera similar a como ha sucedido en el ámbito de las ciberamenazas, se ha aprobado la primera Estrategia de Seguridad Marítima Nacional. Igualmente presenta una estructura y metodología similar a la ESN y ha servido, a su vez, para crear Comité Especializado de Seguridad Marítima, también dependiente del Consejo de Seguridad Nacional.

Por otro lado, la nueva ESN de 2013 ha configurado un Sistema de Seguridad Nacional que pretende funcionar como tal y no quedar como un mero elemento decorativo, como así lo manifiesta las periódicas reuniones del Consejo de Seguridad Nacional, la creación de los Comités Especializados de Ciberseguridad y de Seguridad Marítima o la elaboración del primer Informe Anual de Seguridad Nacional sobre el grado de desarrollo y cumplimiento de la ESN[81]. En esta línea, se están adoptando todas las medidas para que la Estrategia de Seguridad Nacional tenga realmente un carácter global e integral e inspire así los planeamientos estratégicos de los niveles inferiores, alcanzando de esta manera la sinergia precisa para poder cumplir los objetivos establecidos en la misma.

En definitiva, como conclusión final de todo lo anteriormente expuesto, se puede destacar que la ESN actual puede ser considerada una revisión de su predecesora del año 2011, destacando su carácter continuista. No obstante, el hecho de que fuese modificada cuando tan solo llevaba dos años de vigencia, puede responder a las siguientes causas:

- En primer lugar, proceder a una actualización del entorno de seguridad y de los riesgos y amenazas. Es cierto que en tan solo dos años el entorno de seguridad no puede haber sufrido grandes cambios; no obstante, sí era voluntad del nuevo gobierno que el espionaje y la seguridad marítima figurasen como amenazas autónomas, máxime cuando en el nuevo documento, al desechar la inclusión de los ámbitos en los que se pueden presentar los distintos riesgos y amenazas, desaparecía entonces cualquier mención al ámbito marítimo y la cuestión de seguridad en el mismo.

81 Aprobado por el Consejo de Seguridad Nacional en su reunión del pasado mes de abril y que sería presentado ante la Comisión Constitucional del Congreso con fecha 15 de julio de 2014.

- Búsqueda de consenso en la nueva Estrategia. En la elaboración del nuevo documento se pretendía buscar el consenso del arco parlamentario, al menos de las principales fuerzas políticas, para lo que fueron tenidas en cuenta en el proceso de elaboración y el documento fue rápidamente presentado ante la Comisión Constitucional del Congreso de los Diputados.
- Simplificación y reducción de la nueva Estrategia. La primera EES era excesivamente larga. Contaba con numerosos elementos que no aportaban gran cosa para su cumplimiento, además de poder ser considerados en clave propagandística del anterior gobierno, ya que en algunas ocasiones se limitaban a referenciar lo que se había logrado durante el gobierno de Rodríguez Zapatero. Además, la primera Estrategia carecía de una metodología y sistemática propia, habiendo sido introducida en la de 2013 mediante la definición, para cada uno de los ámbitos, de un objetivo general a alcanzar y de los objetivos singulares que van a coadyuvar al cumplimiento del mismo.

	ESPAÑA	EUROPA	ESTADOS UNIDOS	REINO UNIDO	FRANCIA	ALEMANIA	HOLANDA
DOCUMENTO	Estrategia de Seguridad Nacional: Un proyecto compartido	Estrategia Europea de Seguridad: Una Europa segura en un mundo mejor	The National Security Strategy of the United States of America	A Strong Britain in an Age of Uncertainty: The National Security Strategy	Libro Blanco de la Defensa y Seguridad Nacional	White Paper 2006 on German Security Policy and the Future of the Bundeswehr	National Security. Strategy and Work Programme 2007-2008
AÑO	2013	2003	2010	2010	2008	2006	2007
CONCEPTO/ OBJETIVO	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	Documento que define los retos mundiales y las principales amenazas contra la seguridad de la Unión y clarifica los objetivos estratégicos de la UE para hacer frente a las mismas	Perseguir una estrategia de renovación nacional y liderazgo global, una estrategia que levante los cimientos de la fuerza e influencia americana	Transformar la manera en la que se venía organizando la seguridad nacional, y así poder organizarse y protegerse frente a las amenazas que están surgiendo como consecuencia de los cambios radicales que se están experimentando en esta época de incertidumbre en la que nos encontramos	Respuesta al conjunto de los riesgos y amenazas que pueden vulnerar la vida de la nación	Instrumento para tomar medidas preventivas y reducir al mínimo los riesgos de seguridad, y garantizar una intervención eficaz en el caso de producirse	La defensa y protección de los intereses vitales del Estado y de la sociedad ante situaciones de gran envergadura social
INTERESES NACIONALES	La libertad, la democracia o el respeto a la dignidad del ser humano	----	La seguridad, la prosperidad, el respeto de los valores y un orden internacional liderado por los Estados Unidos	La Seguridad, la Prosperidad y la Libertad	La defensa de la población y del territorio, garantizar su seguridad y la defensa de los valores republicanos (democracia, las libertades individuales y colectivas, el respeto de la dignidad humana, la solidaridad y la justicia)	La justicia, la libertad y democracia. La soberanía e integridad. Conflictos y crisis regionales. Los retos de la globalización. Los derechos humanos y el orden internacional	La Seguridad Territorial, la Seguridad Económica, la Seguridad Ecológica, la Seguridad Física y la Estabilidad Social y Política

	ESPAÑA	EUROPA	ESTADOS UNIDOS	REINO UNIDO	FRANCIA	ALEMANIA	HOLANDA
COMPROMISOS INTERNACIONALES	La Unión Europea. El Mediterráneo. América Latina. Los Estados Unidos y las nuevas relaciones transatlánticas. África, en la que establece tres zonas vitales: Cuerno de África, el Sahel y el Golfo de Guinea.. Asia. Rusia. La ONU, la OTAN y otros foros multinacionales.	Naciones Unidas. Instituciones financieras internacionales. La OTAN. La relación transatlántica. Rusia. Japón, China, Canadá y la India.	Fortalecer la OTAN, las Naciones Unidas, el Banco Mundial o el Fondo Monetario Internacional. Europa: Balcanes, Cáucaso y Chipre. Turquía. Asia: Japón, Corea del Sur, Australia, Filipinas y Tailandia. América del Norte: Canadá y Méjico. Oriente Medio: Irak, Israel e Irán.	Estados Unidos, la Unión Europea, la OTAN y las Naciones Unidas Afganistán, Pakistán, Somalia, Yemen e Irán. Las economías emergentes de Asia (entre las que destaca a China y la India), América Latina y del Golfo. G20	El eje que se extiende desde el Océano Atlántico hasta el Océano Índico, pasando por el Mar Mediterráneo y el Golfo Pérsico. África del Oeste y las Antillas. La Unión Europea La OTAN	La OTAN. La Unión Europea. La OSCE. Las Naciones Unidas.	La Unión Europea. Las Naciones Unidas. La OTAN. La OSCE.

	ESPAÑA	EUROPA	ESTADOS UNIDOS	REINO UNIDO	FRANCIA	ALEMANIA	HOLANDA
RIESGOS Y AMENAZAS	Los Conflictos Armados. El Terrorismo. Las Ciberamenazas El Crimen Organizado La Inestabilidad Económica y Financiera. La Vulnerabilidad Energética. La Proliferación de Armas de Destrucción Masiva. Los Flujos Migratorios Irregulares El Espionaje. Las Emergencias y Catástrofes, La Vulnerabilidad del Espacio Marítimo. La Vulnerabilidad de las infraestructuras críticas y servicios esenciales.	El Terrorismo. La proliferación de armas de destrucción masiva. Los conflictos regionales. El debilitamiento de los Estados. La delincuencia organizada.	Las armas de destrucción masiva. El espacio y el ciberespacio. La dependencia de combustibles fósiles. El cambio climático. Las pandemias. Los Estados fallidos. La criminalidad organizada. La economía global.	**Primer grupo (alta probabilidad, alto impacto):** El terrorismo internacional. Ataques NRBQ. Terrorismo en Irlanda del Norte. Ataque cibernético. Grandes catástrofes o riesgos naturales. Conflictos militares internacionales. **Segundo grupo (alto impacto, baja probabilidad):** Un ataque contra el Reino Unido o sus territorios. Inestabilidad, insurgencia o guerras civiles en el extranjero. Crimen organizado. La interrupción de la comunicación de satélites. **Tercer grupo (bajo impacto, baja probabilidad):** Ataque militar sin empleo de armas NRBQ. Terrorismo, crimen organizado, inmigración ilegal o el contrabando. La interrupción del suministro de gas o petróleo. Una fuga radiactiva. Un ataque convencional de un Estado contra otro perteneciente a la OTAN o a la Unión Europea. Un ataque contra territorios de ultramar. La interrupción de suministros de recursos básicos.	El terrorismo La amenaza de misiles. Los grandes ataques contra los sistemas de información. El espionaje y las estrategias de influencia. Los grandes tráficos criminales. Los nuevos riesgos naturales y sanitarios. Los riesgos tecnológicos crecientes. La exposición de los ciudadanos en el extranjero.	La Globalización. El terrorismo. La proliferación de armas de destrucción masiva y el rearme. Los conflictos regionales. El comercio ilegal de armas. Las rutas de transporte y los recursos. La Seguridad energética. La inmigración. Las epidemias y pandemias.	Brechas en la paz y seguridad internacional. Países débiles o corruptos. Riesgos químicos, biológicos, radiológicos o nucleares. Terrorismo. Ataques terroristas, extremismo. Crimen organizado internacional. Tráfico de drogas, conexiones entre el mundo legal y el mundo criminal. Vulnerabilidad social. Tensiones raciales, pérdida de sentido de ciudadanía. Seguridad digital. Seguridad económica. Escasez de materias primas o de energía. Cambio climático y desastres naturales. Inundaciones, temperaturas extremas, plagas... Enfermedades infecciosas. Pandemias, virus

	ESPAÑA	EUROPA	ESTADOS UNIDOS	REINO UNIDO	FRANCIA	ALEMANIA	HOLANDA
LÍNEAS ESTRATEGICAS	Defensa nacional. Lucha contra el terrorismo. Ciberseguridad. Lucha contra el Crimen Organizado. Seguridad económica y financiera. Seguridad energética. No Proliferación de Armas de Destrucción Masiva. Ordenación de flujos migratorios. Contrainteligencia. Protección ante Emergencias y Catástrofes. Seguridad Marítima. Protección de las Infraestructuras Críticas.	Compromiso preventivo. Políticas más activas. Fomento de la capacidad de los ejércitos, de movilización de los medios civiles y de los recursos diplomáticos. Mejor coherencia. Agrupar instrumentos y medios de las políticas europeas. Trabajar con sus socios.	**Seguridad:** Seguridad y Resiliencia. Interrumpir, desmantelar y derrotar a Al Qaeda. Armas nucleares y biológicas. Paz y seguridad en Oriente Medio. Capacidad de los socios fuertes y capaces. Asegurar el Ciberespacio. **Prosperidad:** Educación y capital humano. Ciencia, Tecnología e Innovación. Crecimiento equilibrado y sostenible. Desarrollo Sostenible. Gastar sabiamente. **Valores:** Ejemplo. Democracia y derechos humanos en el extranjero. Dignidad. **Orden internacional:** Alianzas. Cooperación con otros centros de influencia. Instituciones y mecanismos de cooperación. Cooperación amplia.	Identificar y monitorizar riesgos y oportunidades. Abordar la raíz de las causas de inestabilidad. Influencia para explotar las oportunidades y gestionar los riesgos. Respetar las leyes domésticas y reforzar las normas internacionales. Proteger al Reino Unido. Controlar las amenazas físicas y electrónicas. Ayudar a resolver los conflictos y contribuir a la estabilidad. Proporcionar resiliencia. Alianzas y partenariados para lograr respuestas más fuertes.	El conocimiento y la anticipación para poder preparar y orientar los medios de defensa y de Seguridad Nacional. La prevención para impedir o limitar la amenaza de guerra. La disuasión para que ningún Estado crea que puede socavar los intereses vitales de la nación sin exponerse a un riesgo. La protección, para garantizar la seguridad de los ciudadanos, de la sociedad y de la vida económica. La intervención para dar a la Seguridad Nacional la profundidad, adaptabilidad y movilidad necesaria	Prevenir los conflictos internacionales y la gestión de crisis, incluida la lucha contra el terrorismo internacional. Apoyar a los aliados. Protejer Alemania y su población. Rescate y evacuación. Colaboración y cooperación. Asistencia subsidiaria.	----

	ESTRATEGIA ESPAÑOLA DE SEGURIDAD AÑO 2013	ESTRATEGIA ESPAÑOLA DE SEGURIDAD AÑO 2011
DOCUMENTO	Estrategia de Seguridad Nacional: Un proyecto compartido	Estrategia Española de Seguridad: Una responsabilidad de todos
AÑO	2013	2011
Nº PÁGINAS	58	90
ESTRUCTURA	Introducción del Presidente de Gobierno. Resumen Ejecutivo. Capítulo 1: Una visión integral de la Seguridad Nacional. Capítulo 2: La seguridad de España en el mundo. Capítulo 3: Los riesgos y amenazas para la Seguridad Nacional. Capítulo 4: Líneas de acción estratégicas. Capítulo 5: Un nuevo Sistema de Seguridad Nacional.	Resumen Ejecutivo. Capítulo 1: Una Estrategia necesaria. Capítulo 2: La seguridad de España en el mundo. Capítulo 3: Potenciadores del Riesgo. Capítulo 4: Amenazas, Riesgos y Respuestas. Capítulo 5: Un modelo institucional integrado.
CONCEPTO/ OBJETIVO	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	La Estrategia analiza el contexto actual de seguridad, aporta una visión prospectiva y fija las líneas para defender los intereses de España y su contribución a un entorno nacional, europeo, regional e internacional más seguro, pacífico y justo. Sus objetivos son analizar las amenazas y riesgos a nuestra seguridad, identificar líneas de respuesta y definir mecanismos de coordinación.
INTERESES NACIONALES	Si bien no se definen de manera específica, se pueden llegar a identificar la libertad, la democracia o el respeto a la dignidad del ser humano.	**Intereses vitales**, los relativos a los derechos fundamentales: la vida, la libertad, la democracia, el bienestar y el desarrollo de los españoles, así como los relativos a los elementos constitutivos del Estado, como la soberanía, la independencia e integridad territorial, el ordenamiento constitucional y la seguridad económica. **Intereses estratégicos**, aquellos que atañen a la consecución de un entorno pacífico y seguro, como la consolidación y el buen funcionamiento de la UE, la instauración de un orden internacional estable y justo, de paz, seguridad y respeto a los derechos humanos, la preservación de la libertad de intercambios y comunicaciones, y unas relaciones constructivas con nuestra vecindad.

	ESTRATEGIA ESPAÑOLA DE SEGURIDAD AÑO 2013	ESTRATEGIA ESPAÑOLA DE SEGURIDAD AÑO 2011
COMPROMISOS INTERNACIONALES	La Unión Europea. El Mediterráneo. América Latina. Estados Unidos y las nuevas relaciones transatlánticas. África, en la que establece tres zonas vitales: Cuerno de África, el Sahel y el Golfo de Guinea.. Asia. Rusia. La ONU, la OTAN y otros foros multinacionales.	La Unión Europea. Estados Unidos y las nuevas relaciones transatlánticas. Rusia. Iberoamérica. Nuestra vecindad del Sur: el Mediterráneo y el Magreb. África, en la que establece tres zonas vitales: Cuerno de África, el Sahel y el Golfo de Guinea. Asia. La ONU, la OTAN y otros foros multilaterales.
RIESGOS Y AMENAZAS	Los Conflictos Armados. El Terrorismo. Las Ciberamenazas El Crimen Organizado La Inestabilidad Económica y Financiera. La Vulnerabilidad Energética. La Proliferación de Armas de Destrucción Masiva. Los Flujos Migratorios Irregulares El Espionaje. Las Emergencias y Catástrofes, La Vulnerabilidad del Espacio Marítimo. La Vulnerabilidad de las infraestructuras críticas y servicios esenciales.	Los Conflictos Armados. El Terrorismo. El Crimen Organizado La Inseguridad Económica y Financiera. La Vulnerabilidad Energética. La Proliferación de Armas de Destrucción Masiva. Las Ciberamenazas (espionaje). Los Flujos Migratorios no controlados. Las Emergencias y Catástrofes, Infraestructuras, suministros y servicios críticos.

LÍNEAS ESTRATÉGICAS	RECOGIDAS EN AMBAS ESTRATEGIAS	SÓLO EN LA ESTRATEGIA DEL AÑO 2013	SÓLO EN LA ESTRATEGIA DEL AÑO 2011
CONFLICTOS/ DEFENSA NACIONAL		Capacidades militares. Seguridad colectiva. Acción exterior del Estado y posición internacional. Transformación continua de las FAS. Eficiencia. Compartir capacidades con nuestros aliados. Conciencia y cultura de defensa, en especial la juventud. Industria española de Defensa. Vínculos entre Industria, Universidad y Defensa.	Triple perspectiva: Anticipación y prevención; gestión y resolución; consolidación de la paz después del conflicto. Enfoque integral, en el que participen tanto medios civiles como militares (Unidad de Respuestas Integrada Exterior). Potenciar la anticipación y la prevención (representaciones diplomáticas, CNI y CIFAS). La disuasión, como complemento de la anticipación y la prevención.
LUCHA CONTRA EL TERRORISMO	**Prevención:** Evitar la captación de nuevos terroristas. Política internacional concertada y coordinada. **Protección**: **Persecución**: Capacidades de investigación e inteligencia. **Preparación de la respuesta**: resiliencia. Recuperación de los sectores de actividad esenciales.	**Prevención**: Internet. **Protección:** Disminuir vulnerabilidades. Mejora capacidades nacionales en España, extranjero y en el espacio virtual. **Persecución**: Impedir su planificación, financiación y acceso a los materiales. **Preparación de la respuesta**: Sinergia y coordinación. Atención a las víctimas.	**Anticiparse**: cooperación con los de la Unión y otros países aliados. **Prevenir**. Involucrando a toda la población. Apoyar a los elementos moderados del Islam. **Proteger**: **Responder**: que se dispongan los recursos necesarios - operativos y jurídicos- y que estén preparados.
CIBERSEGURIDAD	Colaboración entre el sector público y el privado. Infraestructuras críticas. Cooperación nacional e internacional	Capacidad de prevención, detección, investigación y respuesta (Marco jurídico operativo y eficaz). Seguridad de sistemas y redes comunes. Esquema Nacional de Seguridad. Infraestructuras críticas. Seguridad y resiliencia de TIC's en sector privado. Seguridad TIC en sector industrial. Promoción profesionales en ciberseguridad. Plan de I+D+i para la industria. Cultura de ciberseguridad. Ciudadanos, profesionales y empresas.	Fortalecer la legislación, sin que ello suponga poner en riesgo la privacidad. Cooperación internacional: acuerdos de control de las ciberarmas; luchar a escala europea; homogeneizar la legislación penal en la UE ; y, por último, lucha cibernética más allá de la UE. Mapas de riesgos y catálogos de expertos, recursos y buenas prácticas. Elaboración Estrategia Española de Ciberseguridad.
LUCHA CONTRA EL CRIMEN ORGANIZADO	Potenciación y mejora de los recursos, mecanismos y procedimientos. Colaboración con órganos judiciales y Fiscalía. Mejora de la coordinación y colaboración internacional. Realización de reformas legislativas	Sensibilización y concienciación. Armonizar las legislaciones con otros países. Mejora de la investigación en el tráfico de influencias y la corrupción. Blanqueo de capitales. Tratamiento integral. Implicación de actores públicos y privados, y mundo universitario.	Mejora de sistemas de información e inteligencia: CICO. Creación de nuevas Unidades: GRECO,s y los ECO,s . Colaboración y cooperación policial, de inteligencia, aduanera y judicial, así como servicios de Inteligencia en el exterior. Nuevas competencias para la Fiscalía General contra la corrupción. Potenciación recursos y capacidades del CICO. Creación de Comisión coordinadora de la Fiscalía General de Estado. Operaciones conjuntas en el ámbito de la Unión Europea..

LÍNEAS ESTRATEGICAS	RECOGIDAS EN AMBAS ESTRATEGIAS	SÓLO EN LA ESTRATEGIA DEL AÑO 2013	SÓLO EN LA ESTRATEGIA DEL AÑO 2011
SEGURIDAD ECONÓMICA Y FINANCIERA	Promover desarrollo económico sostenible. Mitigar los desequilibrios de los mercados. Supervisar los agentes económicos y sociales. Cohesión social. Marco socio-laboral. Gobernanza económica y financiera de la UE. Promover una economía internacional abierta Establecer mecanismos de supervisión y regulación. Establecer un Sistema de Inteligencia Económica (SIE). Potenciar la presencia económica internacional de España. Marca España.	Consensos internacionales. Seguridad jurídica de empresas españolas en el exterior. Instrumentos comunes y políticas coordinadas. Paraísos fiscales. Desarrollo de la seguridad económica. Cooperación público-privada para seguridad de infraestructuras y servicios financieros.	Lucha contra el blanqueo de capitales procedente del crimen organizado. Gestión adecuada de servicios e infraestructuras críticas por parte de inversores extranjeros. Garantizar la capacidad de los servicios críticos económicos y financieros Amenazas: complejidad técnica, catástrofes naturales y actividades delictivas.
SEGURIDAD ENERGÉTICA	**En el abastecimiento**: Ampliación fuentes de energía. Energías renovables. **En la distribución**: Política energética europea que potencie las interconexiones entre los Estados miembros y, en especial, entre la Península Ibérica y el resto de Europa, alcanzando de esta manera un mercado europeo de electricidad y gas natural plenamente integrado. **En el consumo**: Ahorro energético y eficacia energética.	**En el abastecimiento**: Mix energético. Fuentes energéticas autóctonas. Política común europea. Interconexiones. Mercado europeo de electricidad y gas natural. Conectividad. Gestión de las reservas petrolíferas. Investigación y explotación de yacimientos de hidrocarburos. **En la distribución**: Flexibilidad de redes de transporte. Planes de canalización y priorización de la demanda. Control de las comunicaciones. Potenciación almacenamiento. Mejora fiabilidad de las redes de abastecimiento. Colaboración público-privada. **En el consumo**: Sostenibilidad energética. Marco regulatorio armonizado, transparente y objetivo.	**En el abastecimiento**: Potenciar diferentes formas de almacenamiento de energía, aumentando la capacidad instalada de bombeo hidráulico y de almacenamiento de gas Desarrollo de infraestructuras. Permite garantizar la seguridad del abastecimiento. **En la distribución**: Liberalización de los mercados. Reforzar el control del espacio marítimo con estos fines. Garantizar las instalaciones críticas. Plan de Protección de Instalaciones Críticas. **En el consumo**: Fomento del transporte público. Incremento de la cuota del ferrocarril en el transporte de mercancías.
NO PROLIFERACIÓN DE ARMAS DE DESTRUCCIÓN MASIVA	Evitar que terroristas puedan llegar a adquirir sustancias nucleares, químicas, biológicas o materiales radiológicos. Multilateralismo eficaz y cooperación activa. Cooperación con UE y OTAN. Tratados e instrumentos internacionales. Participación en el Programa de Defensa Antimisiles de la OTAN. Control exportaciones y tráfico productos doble uso (uranio). Limitación de la proliferación de los misiles de medio y largo alcance	Vigilancia de la red. Planes nacionales de prevención. Plan nacional de biocustodia. Combatir las transferencias de conocimiento, tecnología, bienes y equipos. Financiación ilegal. Cooperación regional. Capacidades de prevención de atentados.	Estrategia Europea contra la proliferación de armas de destrucción masiva. Aspiración a un mundo sin armas nucleares.

LÍNEAS ESTRATÉGICAS	RECOGIDAS EN AMBAS ESTRATEGIAS	SÓLO EN LA ESTRATEGIA DEL AÑO 2013	SÓLO EN LA ESTRATEGIA DEL AÑO 2011
ORDENACIÓN FLUJOS MIGRATORIOS	Ordenación eficaz de los flujos migratorios. Control y vigilancia eficaz fronteras exteriores. Cooperación con los países de origen y tránsito Legalidad y seguridad ciudadana. Lucha contra la discriminación. Igualdad. Atención especial a los colectivos más vulnerables. Promoción de la integración social.	Colaboración entre Administraciones Públicas y con ONG,s y sector privado.	Alianza de Civilizaciones. Favorecer el diálogo con las confesiones religiosas de las poblaciones inmigrantes.
CONTRAINTELIGENCIA	Potenciar las capacidades de inteligencia.	Normativa protección información clasificada. Sensibilización personal que maneja información clasificada. Protección y sensibilización de los españoles en el extranjero. Cooperación internacional.	
EMERGENCIAS Y CATÁSTROFES	Reconfigurar el Sistema Nacional de Gestión de Situaciones de Crisis. Enfoque integrador entre Administraciones. Marco jurídico ante emergencias y catástrofes. Énfasis en la prevención. Coordinación interadministrativa. Cooperación europea e internacional. Cultura de prevención.	Marco de referencia para coordinación de esfuerzos, priorización y optimización de recursos. Red de alerta nacional de riesgos. Detección temprana. Creación de un sistema inteligente de planificación en red. Directorios de recursos para una gestión eficiente de la respuesta. Resiliencia. Programas de educación en centros escolares. Planes de preparación y respuesta ante pandemias. Protocolos de situaciones de crisis alimentarias.	Fomento de la participación ciudadana. Programas de colaboración entre la Administración General del Estado y las Comunidades Autónomas para la elaboración de una cartografía de riesgos
SEGURIDAD MARÍTIMA	Optimización y uso eficaz de los recursos. Búsqueda de sinergias. Integración de medios civiles y militares. Cooperación internacional.	Enfoque integral. Actuación coordinada y cooperativa. Integración de las capacidades de prevención y respuesta. Acuerdos bilaterales internacionales. Colaboración con el sector privado.	Vigilancia y seguridad marítima. Impulso de iniciativas internacionales tendentes a garantizar unas vías de comunicación seguras para el suministro de recursos básicos y a mejorar la gobernanza de los espacios marítimos

LÍNEAS ESTRATÉGICAS	RECOGIDAS EN AMBAS ESTRATEGIAS	SÓLO EN LA ESTRATEGIA DEL AÑO 2013	SÓLO EN LA ESTRATEGIA DEL AÑO 2011
PROTECCIÓN INFRAESTRUCTURAS CRÍTICAS	Responsabilidad compartida y cooperación público-privada. Protección de las infraestructuras críticas. Plan Nacional de Protección de Infraestructuras Críticas. Refuerzo de la resistencia y capacidad de recuperación (resiliencia),	Planificación escalonada a partir de un enfoque integral multiriesgo y homogeneizador. Equilibrio y eficiencia. Concentrar los esfuerzos sobre las áreas más vitales. Sistemas redundantes o aislados. Coordinación entre la gestión de riesgos y la gestión de crisis. Cooperación internacional. Programa Europeo de Protección de Infraestructuras Críticas y Directiva Europea 2008/114/CE. Canales internacionales de información, alerta temprana y respuesta.	

BIBLIOGRAFÍA

Cabinet Office. (2008). The National Security Strategy: Security in an interdependent world. United Kingdom.

Cabinet Office y National security and intelligence. (2010). A Strong Britain in an Age of Uncertainty: The National Security Strategy. United Kingdom.

Comisión de la Unión Europea. (2006). Comunicación de la Comisión sobre un Programa Europeo para la Protección de Infraestructuras Críticas. COM(2006), 786 final. Bélgica.

Consejo de la Unión Europea. (2008). Directiva 2008/114/CE del Consejo, de 8 de diciembre de 2008, sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección. Diario Oficial de la Unión Europea, L 345/75. Bélgica.

Federal Ministry of Defence. (2006). White Paper 2006 on German Security Policy and the Future of the Bundeswehr. Germany.

Ley 2/1985, de 21 de enero, sobre Protección Civil. Boletín Oficial del Estado, 25 de enero de 1985, num. 22, pp. 2092-2095. España.

Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas. Boletín Oficial del Estado, 29 de abril de 2011, núm. 102, pp. 43370-43379. España.

Ley Orgánica 5/2005, de 17 de noviembre, de la Defensa Nacional. Boletín Oficial del Estado, 18 de noviembre de 2005, num. 276, pp. 37717-37723. España.

Ministerio de Defensa. (2011). Proliferación de ADM y de Tecnología avanzada. Instituto Español de Estudios Estratégicos, Cuaderno de Estrategia Nº 153. España.

Ministerio de Defensa. (2000). Libro Blanco de la Defensa. Secretaría General Técnica, Centro de Publicaciones. España.

Ministerio de Defensa. (2003). Revisión Estratégica de la Defensa. Secretaría General de Política de Defensa, Centro de Publicaciones. España.

Ministerio del Interior. (2011). Estrategia Española contra el Crimen Organizado 2011-2014. España.

Ministerio de Trabajo y Asuntos Sociales. (2007). Plan Estratégico de Ciudadanía e Integración 2007-2010. España.

Ministry of Defence. (2006). The Comprehensive Approach. Joint Discussion Note 04/05. Joint Doctrine and Concepts. United Kingdom.

Ministry of the Interior and Kingdom Relations. (2007). Strategy and Work Programme 2007-2008. The Netherlands.

Presidencia del Gobierno de España. (2011). Estrategia Española de Seguridad: Una responsabilidad de todos. España.

Presidencia del Gobierno de España. (2012). Directiva de Defensa Nacional 1/2012:

Por una Defensa necesaria, por una Defensa responsable. Madrid.

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

Presidente de la República Francesa. (2008). Libro Blanco de la Defensa y Seguridad Nacional. Francia.

Prime Minister of Australia. (2008). First National Security Statement to the Australian Parliament. Australia.

Protocolo de enmienda del Convenio de Cooperación para la defensa entre el Reino de España y los Estados Unidos de América, de 1 de diciembre de 1988. Boletín Oficial del Estado, 21 de febrero de 2003, núm. 45, pp. 7215-7227. España.

Real Decreto 385/2013, de 31 de mayo, de modificación del Real Decreto 1886/2011, de 30 de diciembre, por el que se establecen las Comisiones Delegadas del Gobierno. Boletín Oficial del Estado, 1 de junio de 2013, num. 131, pp. 41487-41490. España.

Real Decreto 1181/2008, de 11 de julio, por el que se modifica y desarrolla la estructura orgánica básica del Ministerio del Interior (Art. 2). Boletín Oficial del Estado, 16 de julio de 2008, núm. 171, pp. 31041-31054. España.

The White House. (2002). The National Security Strategy of the United States of America. United States of America.

The White House. (2010). The National Security Strategy of the United States of America. United States of America.

Yarger, H. R. (2006). Strategic Theory for the 21st Century: The Little Book on Big Strategy. Strategic Studies Institute of the US Army War College. United States of America.

Fecha de recepción: 25/11/2014. Fecha de aceptación: 17/12/2014

LAS PRIMERAS APORTACIONES DE LA GUARDIA CIVIL A LA ACCIÓN EXTERIOR DEL ESTADO

JOSÉ FÉLIX GONZÁLEZ ROMÁN

RESUMEN

La década de los noventa constituyó para la Guardia Civil el inicio de una serie de actividades en el extranjero que hicieron emerger su valor como parte de la acción exterior del Estado: las misiones dedicadas a la formación de cuerpos policiales en distintas repúblicas de Hispanoamérica y África, las de observación del cumplimiento de acuerdos de paz en países en conflicto, la actuación como policía ejecutiva en diferentes países en los momentos iniciales del posconflicto, así como su participación en las operaciones militares encaminadas a preservar la paz en diferentes escenarios -especialmente en los Balcanes- hicieron revalorizar a nuestro Cuerpo como garante y modelo de la seguridad pública.

A la vista de los hechos expuestos anteriormente, cabría la posibilidad de caer en el error si se pensara que estas acciones son nuevas para la Guardia Civil. Nada más apartado de la realidad. Las siguientes páginas pretenden ilustrar o refrescar la memoria del lector, para dejar constancia de que esta institución, desde los primeros tiempos de sus actividades, fue empleada como pieza de importancia en la potenciación del prestigio internacional de España. La Guardia Civil, por tanto, como en la actualidad, también ha servido como parte de la acción exterior del Estado.

El artículo acomete el tema de la actuación exterior de la Guardia Civil en tres modalidades diferentes: la llevada a cabo como consecuencia del despliegue en provincias españolas de Ultramar, colonias y zonas de interés, la realizada con el fin de crear cuerpos homólogos en distintos países de América y, finalmente, la ejecutada en el desarrollo de una campaña militar en el exterior.

Como podrá leerse en el cuerpo del artículo, la Guardia Civil ha servicio como modelo de organización y de servicio en la creación de nuevos cuerpos de seguridad en otras naciones. Tanto en la América hispana como en África, los guardias civiles contribuyeron a crear las estructuras de seguridad que permitieron a no pocos países gozar de unas fuerzas destinadas a proteger las vidas y propiedades de sus ciudadanos.

Por último, se destaca la labor que la Guardia Civil ha desempeñado en el desarrollo de las campañas militares llevadas a cabo por nuestro Ejército y Marina, desde sus iniciales cometidos como policía militar hasta su reconocimiento como fuerza combatiente.

Palabras clave: acción exterior, asistencias técnicas, modelo profesional, policía militar, fuerza combatiente.

ABSTRACT

For the Civil Guard, the 90’s represented the beginning of a series of activities abroad which boosted its value as an important actor of the State’s international action:

police formation missions throughout Latin American and African republics, observance of the compliance of peacekeeping agreements in conflict countries, its role as the executive police body in post-conflict states as well as its participation in military operations towards peacekeeping in different scenarios –specially in the Balkans- increased the value of our Body as the guarantor and model of public security.

As a consequence of the exposed facts, it would not be hard to be mistaken about these actions as something new for the Civil Guard. This is not true at all. This article tries to illustrate or refresh the lector's memory in order to confirm that this institution, from the beginning of its activities, has been used as a very important strengthener of Spain's international prestige. Therefore, the Civil Guard, like nowadays, has also served as a part of the State's international action.

This article explains the Civil Guard's international action from three approaches: action as a consequence of the deployment of Spanish overseas provinces, colonies and interesting areas, action in order to create equivalent bodies in American countries and, lastly, action towards an international military campaign.

As may be read in this article, the Civil Guard has served as an organizational and service model in the creation of new security bodies in other nations. Both in Latin America and Africa, civil guards have created security structures that permitted several countries to have forces destined to protect lives and properties from the citizens.

Finally, it is important to underline the Civil Guard's work in relation to the development of military campaigns carried out by our Armed Forces and Navy, from its creation as a military police to its recognition as a fighting force.

Key words: international action, technical assistance, professional model, military police, fighting force.

1. INTRODUCCIÓN

Que la aparición de la Guardia Civil supuso para la sociedad española del siglo XIX una excelente mejora cuantitativa y cualitativa en la seguridad de sus personas y propiedades es un hecho incontestable, que fue reconocido por todos los actores políticos de la época, autoridades nacionales y locales y por la propia sociedad en general.

El acierto de los sucesivos gobiernos de la corona permitió la configuración de una fuerza moderna, con una acendrada vocación de servicio al pueblo y a la nación. Si González Bravo fue capaz de diseñar una seguridad pública moderna, por primera vez -y bajo el concepto de la separación de poderes- dependiente del Ministerio de la Gobernación[1], Narváez modificó los elementos de la misma[2] que podían hacer tropezar el nuevo proyecto en las mismas piedras en las que se precipitó el último intento del antiguo régimen de organizar la seguridad pública: el servicio político de la institución.

1 Mediante la promulgación del Decreto de 26 de enero de 1844 por el que se organizaba la seguridad pública en España.

2 Al modificar el decreto de 28 de marzo de 1844 con el de 13 de mayo del mismo año, variando las dependencias de la Guardia Civil y anulando, entre otras cuestiones, la facultad de los entonces denominados jefes políticos en el nombramiento de determinados mandos del Cuerpo (sargentos y cabos).

En muy pocos años la Guardia Civil pasó de ser un experimento que no pocos veían con recelo a una institución con la que todas las administraciones y autoridades deseaban contar: de sobra es conocida la prueba de fuego que tuvo que superar al caer el gobierno de Narváez, pues sólo la encendida defensa que su segundo inspector general (el general Infante) llevó a cabo en el Congreso, junto a la protesta generalizada de los alcaldes de España, evitó que se dispusiera su desaparición.

La buena fama que adquirió la Guardia Civil hizo que este organismo se constituyera rápidamente como referente para muchas otras naciones, lo que, unido a la demanda que de la misma hacían las autoridades nacionales, provocó la expansión de sus servicios hacia territorios y cometidos que excedían de los que inicialmente le fueron encomendados.

Cuando observamos la intervención internacional de los años 90 del siglo pasado en los Balcanes o en distintos territorios del continente americano, podemos caer en el error de pensar que ese es el inicio de la actuación de la Guardia Civil fuera de nuestras fronteras. Nada más apartado de la realidad. Incluso podríamos pensar que la actuación del Cuerpo con los distintos contingentes militares es fruto de una reciente decisión. Las siguientes líneas pretenden, mediante la recopilación de lo ya escrito en distintas publicaciones históricas sobre la Guardia Civil, refrescar la memoria del lector, para dejar constancia de que esta institución, desde los primeros tiempos de sus actividades, fue empleada como pieza de importancia en la potenciación del prestigio internacional de España. La Guardia Civil, por tanto, como en la actualidad, también ha servido como parte de la acción exterior del Estado.

No es pretensión del autor -ni lo hace- aportar novedad alguna en la historiografía del Cuerpo, dado que su objeto es presentar de una forma global la actuación institucional en estos escenarios, exponiendo a grandes rasgos sus principales hitos, con la idea de que puedan proporcionar una perspectiva integral para aquellos que, de aquí en adelante, aborden estudios concretos relacionados con el mismo tema.

2. LA ACTUACIÓN EXTERIOR DE LA GUARDIA CIVIL

Como había quedado establecido en el artículo 2 del Decreto de creación de la Guardia Civil[3], esta institución fue creada para “proveer al buen orden, a la seguridad pública y a la protección de las personas y propiedades, fuera y dentro de las poblaciones”. Era, por tanto, una fuerza de seguridad integral en competencias y demarcación territorial.

Sin embargo, este carácter integral del Cuerpo tenía dos límites bien definidos: no se contemplaba ni una actuación de sus componentes fuera de las fronteras nacionales, ni la realizada en el marco de una campaña militar, puesto que para su servicio estaba “bajo la dependencia del Ministerio de la Gobernación de la Península”[4].

3 Denominaremos así al decreto de 28 de marzo de 1844, para distinguirle del de fecha 13 de mayo, al que llamaremos decreto de fundación, dado que los primeros guardias civiles se establecieron e iniciaron sus servicios con arreglo a lo dispuesto en el segundo decreto, que introdujo importantes modificaciones con respecto al anterior.

4 Artículo 1º del decreto de 28 de marzo.

En las próximas líneas, al hablar de la actuación exterior de la Guardia Civil[5] expondremos tres modalidades diferentes:

- La llevada a cabo como consecuencia del despliegue en provincias españolas de Ultramar, colonias y zonas de interés (Cuba, Puerto Rico, Santo Domingo, Filipinas, Guinea Ecuatorial, territorios del norte de África).
- La realizada con el fin de crear cuerpos homólogos en distintos países de América.
- La ejecutada en el desarrollo de una campaña militar en el exterior.

3. EL DESPLIEGUE DE LA GUARDIA CIVIL EN EL NORTE DE ÁFRICA Y ULTRAMAR

3.1. PROTECTORADO DE MARRUECOS

Tras la campaña de Melilla de 1893, las fuerzas de la Guardia Civil que acompañaron al Ejército de operaciones volvieron a la península, si bien se dispuso que una sección quedase desplegada en la ciudad, para realizar su servicio peculiar en la misma con carácter permanente. En 1896, se aprobó la orden por la que esta sección quedaba administrativamente afecta a la comandancia de Málaga.

De manera similar, en 1898 se creó una sección en Ceuta, afecta a la comandancia de Cádiz. A partir de esta fecha, las fuerzas del Cuerpo que formaron parte del Protectorado de Marruecos se extrajeron de las Secciones de Ceuta y Melilla, cuyos efectivos fueron aumentando con arreglo a las necesidades que aparecían en cada momento.

La reanudación de las campañas militares desde 1909 supuso un aumento considerable de la Guardia Civil que culminó con la creación, en 1926, del tercio de Marruecos, numerado como 28º. Esta Unidad sufrió diversas transformaciones, como la de 1932 que lo denominó “Tercio Móvil” que, con entidad de compañía, tenía ubicada su Plana Mayor en Jerez de la Frontera y estaba compuesto por cinco líneas: Ceuta, Tetuán, Larache, Melilla y Villa Sanjurjo.

El tercio se transformó en comandancia exenta de Marruecos en 1934[6], para prestar sus servicios en Ceuta, Melilla y territorio de Ifni. Ya en plena guerra civil, en 1937, se redujeron sus efectivos a la mitad, quedando establecidas únicamente cuatro compañías, con sede en Ceuta, Melilla, Tetuán y Sidi-Ifni.

Tras su cambio de denominación en 1941 por la de “Comandancia exenta 200 de la Guardia Civil” y con compañías en Ceuta y Melilla, en 1947 se reorganizó como tercio exento, con dos comandancias (Tetuán y Melilla) y cabecera en Ceuta, permaneciendo así hasta 1956 cuando, tras la transferencia de poderes a las autoridades marroquíes, se inició el repliegue de la Guardia Civil a las ciudades españolas, finalizándose en 1960 cuando las fuerzas de seguridad marroquíes completaron su despliegue en el antiguo protectorado.

5 Nos referimos con el término “exterior” a los territorios ubicados fuera de la península ibérica y archipiélagos balear y canario, fueran o no parte del territorio nacional en el momento histórico considerado.

6 Mediante Decreto de la Presidencia del Consejo de Ministros de 21 de noviembre, y confirmada por Ley de 31 de mayo de 1935.

3.2. GUINEA ECUATORIAL

El 27 de septiembre de 1900, se reconoció la soberanía de España sobre Guinea Ecuatorial y las islas de Fernando Poo, Annobon, Corisco y las Elobey. Para su gobierno, se decretó en 1904 la constitución de la entidad denominada "Territorios Españoles del Golfo de Guinea"[7], que contaba con cuatro distritos: Fernando Poo, Bata, Elobey y Annobón.

Se ordenó a la Guardia Civil que se hiciese cargo del Cuerpo de Policía y Orden Público para la colonia. Para ello, se organizó la Guardia Colonial, bajo la premisa de que todos los cuadros de mando -cabos incluidos- serían españoles.

El reglamento de la Guardia Colonial era copia del de la Guardia Civil. Se articuló en cuatro compañías (establecidas en Santa Isabel, Bata, Mikomesén y Elobey), líneas y puestos.

En 1911 hubo de llevar a cabo una expedición de castigo contra insurgentes armados que, alentados por instigadores de Nigeria, ocuparon diversos poblados. Allí el Cuerpo recibió su bautismo de fuego en esas tierras. En 1913, debido a estos hechos, le fue concedido el derecho al uso de bandera de combate.

El 2 de julio de 1946 se confirió un nuevo Reglamento al Cuerpo, que pasó a depender de la Presidencia del Gobierno. Se le cambió su denominación por la de "Guardia Territorial", siendo su inspector el gobernador general de los territorios y su jefe operativo un jefe del Ejército.

En cuanto a la orgánica del nuevo Cuerpo, se aumentaron a cinco las compañías[8], organización que permaneció invariable hasta que, en 1959, se organizó una nueva compañía móvil, con la misión de vigilar la frontera con Gabón y Camerún, intentando evitar el contagio independentista. La organización de esta nueva compañía se le encomendó a la Guardia Civil, y se instaló en Bata. En 1961 se organizó otra compañía de iguales características, con la misión de velar por el mantenimiento del orden público, que estableció su sede en Santa Isabel.

Por Decreto de 28 de septiembre de 1968, se creó el "Mando de las Fuerzas Armadas en la Guinea Ecuatorial", que estaba constituido por las fuerzas aéreas destacadas, las de la Armada y las dos compañías de la Guardia Civil (que constituían el contingente del Ejército de Tierra). No obstante, el mando global de las Fuerzas Armadas estaba ostentado por un coronel del Ejército de Tierra. La Guardia Territorial, ya desprovista de las dos compañías de la Guardia Civil, continuaría dependiendo del comisario general.

Como dato anecdótico cabe recordar que las últimas tropas españolas en abandonar Guinea[9] fueron precisamente las compañías móviles de Santa Isabel y Bata.

3.3. CUBA

Siendo capitán general de Cuba el conde de Alcoy, y ante la situación de inseguridad que vivía la isla, remitió en 1849 un informe a la Península solicitando la creación en

7 Real Decreto de 11 de julio de 1904.
8 Con cabecera en Santa Isabel, Bata, Ebebiyin, Evinayong y Mikomeseng.
9 Abril de 1969.

la isla de un cuerpo similar al de la Guardia Civil, al trascender los buenos resultados que estaban dando sus servicios.

Sería su sucesor, el capitán general De la Concha quien, en 1851, materializaría la presencia efectiva de Guardia Civil mediante la organización -en una decisión personal- de un "Tercio en comisión" en la isla. Esta Unidad, concebida con una composición inicial de tres compañías de Infantería y tres de Caballería[10], se constituyó finalmente con una única compañía mixta de Infantería/Caballería. De la Concha remitió un proyecto de creación de la Guardia Civil en Cuba al Gobierno peninsular, que fue archivado[11]. Es de destacar que el propio De la Concha propuso inmediatamente la "amalgama" de la Guardia Civil de Cuba con la peninsular[12].

Tras el cese de De la Concha se aprobó oficialmente la organización de la Guardia Civil de Cuba[13]. El tercio estaba compuesto por seis oficiales de Caballería y 118 hombres de tropa de Infantería, recomendándose la organización de una sección de Caballería.

En octubre de 1854 De la Concha volvió a ser nombrado capitán general de la isla. Dado que consideró insuficiente el número de guardias civiles en Cuba, reorganizó el tercio a final del mismo 1854, que pasó a tener la composición de un batallón de 600 hombres, a similitud de los del Ejército, y limitó la demarcación territorial de sus servicios a la capital.

El 1 de marzo de 1857 se le aumentaron los efectivos al añadírsele dos Escuadrones de Caballería, procedentes de los regimientos del Ejército en la isla.

En 1869, debido al inicio de la "Guerra Grande", se aumentó la Guardia Civil en otro tercio, con 1.000 hombres. A final de ese año, la Guardia Civil tenía una fuerza de dos tercios, compuestos cada uno por un batallón de seis compañías de Infantería y dos escuadrones de Caballería.

En 1870 se aumentaron dos compañías a cada uno de los tercios.

Debido a que el problema del bandolerismo en las islas de Cuba y Puerto Rico aumentaba cada vez más, interpretándolo como consecuencia de la inferior calidad de los servicios prestados por los tercios de Ultramar, en 1871 el Gobierno de Madrid decidió homogeneizar los tercios del Cuerpo de la Península y las Antillas, mediante la decisión de la amalgama[14] de la Guardia Civil de Cuba y Puerto Rico con la peninsular.

El personal de los tercios de las Antillas ingresó en el Cuerpo general, si bien se les permitió –en caso de no querer cambiar de Cuerpo- continuar en la Guardia Civil como agregados, hasta causar baja por ascenso u otros motivos.

El resultado de la reorganización derivada de la amalgama fue que la Guardia Civil quedó establecida en Cuba (1872) por una Subinspección -al mando de un brigadier- y tres tercios.

10 La extracción del personal y material era de los Regimientos del Ejército de Cuba, siendo independiente de la Inspección General de la Guardia Civil.
11 Compuesto por las ya mencionadas seis compañías.
12 LUENGO MUÑOZ, Manuel: La Guardia Civil en las islas de Cuba y Puerto Rico. Revista de Estudios Históricos de la Guardia Civil (número 5) pág. 112.
13 Mediante Decreto de 20 de junio de 1854.
14 Real Orden de 10 de julio.

En diciembre de 1876 el capitán general Martínez Campos logró la aprobación de creación de dos nuevas comandancias en Colón y Sagua y, posteriormente, otra en Holguín[15].

Tras la Guerra Chiquita (1880) se decretó un aumento de 1.000 efectivos más en los tercios de Cuba, consistente en cuatro compañías de Infantería y cinco escuadrones de Caballería[16].

Pero la modificación más importante sufrida en la orgánica de la Guardia Civil insular fue la establecida por la Real Orden de 7 de enero de 1885, que dispuso la desaparición de la Subdirección del Cuerpo y la supresión de los tercios, quedando toda la Guardia Civil de Cuba -ya con 10 comandancias- bajo el mando de un coronel subinspector, quien dependía directamente del capitán general.

Como consecuencia del descenso de fuerza del Cuerpo en la isla aumentaron los problemas de bandolerismo y el capitán general solicitó un aumento de efectivos, que se autorizó en la Real Orden de 22 de noviembre de 1886, por la que se restablecieron las 12 comandancias del Cuerpo.

En estos años cabe reseñar la actividad llevada a cabo por la sección topográfica de la Guardia Civil, organizada por el teniente de la comandancia de Vuelta Abajo Luis Romero Aguirre, que confeccionó los planos de las demarcaciones de la comandancia del Cuerpo y, posteriormente, de la isla, mejorando el empleado hasta el momento por el Estado Mayor[17].

Por Real Orden de 23 de julio de 1888 se agrupó la fuerza del Cuerpo en dos tercios -la unidad tradicional de mando del Instituto- y se mantuvo el coronel subinspector, distribución que sólo estuvo unos meses, ya que por RO de 16 de febrero de 1889 se distribuyó la fuerza en tres tercios.

En esta época -con el general Salamanca como capitán general- se realizaron dos reformas de capital importancia: se dotó de enlace telefónico a todos los puestos del Cuerpo -en la Península todavía no era posible- y se cambió el armamento.

En 1892 se redujeron los efectivos del Cuerpo, agrupándolos en dos tercios.

En 1893, y debido al clima de pre-insurrección general en la isla, se publicó el Decreto de 8 de agosto, por el que volvió a reorganizar la Guardia Civil de Cuba: se nombró un general de brigada subinspector del Cuerpo y se articuló el Cuerpo en tres tercios y 12 comandancias, con un total de casi 4.700 hombres.

Es de destacar que en todo momento la Guardia Civil continuó desempeñando sus servicios con total normalidad, siendo reconocido su trabajo por las autoridades insulares quienes, en 1894, inauguraron un Centro de Instrucción para los guardias civiles en Marianao.

3.4. PUERTO RICO

El primer impulsor del nacimiento de la Guardia Civil en Puerto Rico fue su capitán general, José Lémery, quien en 1857 solicitó la creación de un tercio “en comisión”

15 Mediante Reales Órdenes de 8 y 20 de diciembre de1876, respectivamente.
16 Real Orden de 27 de agosto de 1881.
17 Confeccionado por Esteban Pichardo y Tapia en 1874.

-a imagen de lo establecido en Cuba- compuesto por dos comandancias y unos 400 hombres.

No fue hasta 1868, sin embargo, cuando se decidió la organización del Cuerpo, debido a la sublevación independentista de Manuel Rojas en Lares.

En octubre de 1869 se organizó un tercio de la Guardia Civil, compuesto por individuos elegidos de los batallones de Infantería de la propia isla. Estaba compuesto por dos compañías mixtas de Infantería y Caballería.

El Decreto de Amalgama de 1871 se materializó en Puerto Rico el 30 de septiembre de 1872, cuando el teniente coronel Castrillón, de la Guardia Civil peninsular, se hizo cargo del tercio como coronel subinspector de la Guardia Civil de la isla, suprimiendo las dos compañías mixtas y formando una comandancia con dos compañías de Infantería y un escuadrón, que fueron dos en 1875.

En 1887 la fuerza del Cuerpo aumentó hasta un total de 454 hombres, organizados en una comandancia -el tercio se había suprimido en 1886- compuesta por tres compañías de Infantería y dos escuadrones de Caballería.

Por Real Orden de 8 de marzo de 1889 se restableció el tercio y se formaron dos comandancias: en San Juan de Puerto Rico (con un escuadrón y dos compañías) y en Ponce (con un escuadrón y una compañía). Un total de 737 hombres.

El 20 de octubre de 1898 abandonaron la isla las fuerzas de la comandancia de Ponce, últimas de la Guardia Civil, observando desde el barco la ceremonia de arriado de la bandera nacional, al dejar de pertenecer Puerto Rico a España.

3.5. SANTO DOMINGO

Una vez consiguió su independencia de España en 1821, la República Dominicana fue invadida por su vecina Haití. En 1844 el general Santana solicitó la anexión a España, que fue rechazada. En 1855 España concedió a Santo Domingo la posibilidad de nacionalizarse españoles a quienes desearan. Ante el peligro de una nueva invasión haitiana, en 1860 Santana volvió a solicitar la anexión a España, siéndole nuevamente rechazada, pero permitiendo el establecimiento de un protectorado.

Se izó la bandera española, Santana fue nombrado capitán general y se enviaron tropas a la isla.

En 1863 se produjo una insurrección liderada por dos generales y se envió una compañía de la Guardia Civil de Cuba, que se distinguió en los distintos combates que allí se libraron. En 1865, acordado el abandono pacífico de la isla de las tropas españolas tras la renuncia a la soberanía, se embarcaron de regreso a Cuba.

3.6. FILIPINAS

Al igual que el resto de la guarnición militar, la Guardia Civil en Filipinas era mayoritariamente indígena. El 24 de marzo de 1868 se creó un tercio de comisión en Luzón, que constituyó el inicio de las fuerzas de seguridad en el archipiélago.

Aun cuando esta Guardia Civil no sufrió el proceso de "amalgama" con la de la península, debe precisarse que en todo momento la Guardia Civil del archipiélago se sometió al mismo reglamento que su hermana mayor.

Los sucesos de Cavite de 1872 -sublevación de un sargento indígena con 200 paisanos, que fueron finalmente reducidos por la Guardia Civil de Manila- pusieron de manifiesto la necesidad de atender adecuadamente los requerimientos de la seguridad ciudadana. Así, el 1 de mayo de 1872 se aprobó la creación de otro tercio como el que existía en comisión y un tercio de Guardia Civil Veterana para Manila[18].

En 1874 fue designado como capitán general de Filipinas el contralmirante Malcampo y Monje, quien llevó a cabo distintas expediciones de castigo contra los insurgentes de Joló. En la primera de ellas (febrero de 1875), formaron parte dos compañías del Cuerpo[19], embarcadas respectivamente en los vapores "Emuy" y "Ormoc", constituyendo el núcleo principal de la tropa de desembarco y formando parte de la media Brigada de vanguardia, en la que se destacó por las repetidas cargas a la bayoneta que tuvo que realizar contra los joloanos en la jornada del día 26[20].

En 1885 tres guardias civiles del primer tercio defendieron el poblado de Panguil de una partida de medio centenar de nativos que lo habían asaltado. Ayudados por algunos paisanos, los guardias lograron hacerlos huir, causándoles varias bajas mortales y recuperando parte del botín robado, por lo que fueron condecorados con cruces de la Real y Militar Orden de San Fernando, dos de ellas de primera clase y una de segunda, siendo ésta la primera concesión de una cruz laureada a un guardia civil[21] de que se tiene conocimiento hasta la fecha.

En enero de 1887 tropas del primer tercio y de la Veterana se embarcaron en la expedición que se organizó hacia Mindanao, donde tomaron parte en una operación anfibia con una compañía de Infantería de Marina en Lintucán.

En septiembre de 1887 se enviaron fuerzas del primer tercio a la expedición a la isla de la Pata[22].

En 1890 fuerzas del Cuerpo realizan una expedición para ocupar el monte Isarog (en el archipiélago de Las Carolinas), mandadas por el comandante de la Guardia Civil Hernán Alvarado Aguado.

En 1893 se inicia una nueva reorganización de la administración de Filipinas, impulsando la creación de un nuevo tercio del Cuerpo, que finalizó en 1895, con lo que la fuerza de la Guardia Civil era de 3.685 hombres, divididos en tres tercios, el tercio de Guardia Civil Veterana y la fuerza de Caballería.

En 1895 se llevaron a cabo operaciones militares para la ocupación de Puntar y Kabasaran, donde hubo que concentrar más de 2.000 hombres, bajo el mando del jefe

18 A semejanza de la Guardia Civil Veterana que se organizó en Madrid.
19 MONTERO VIDAL, José: Historia de la piratería malayo-mahometana en Mindanao, Joló y Borneo. Pág. 523.
20 MONTERO VIDAL, José: Op. Cit. Pág. 532.
21 El guardia laureado es Domingo Pablo Sebastián, de origen filipino, al igual que sus dos compañeros (Cándido Sánchez Alana y Germán Galafón Domingo), recompensados con la cruz sencilla de primera clase.
22 Una de las islas del archipiélago de Joló.

del 20º tercio del Cuerpo, coronel Victoriano Olaría Tombo.

Fue destacada la desarticulación por la Guardia Civil veterana el 19 de agosto de 1896 del "Kapitunan democrático", organización independentista filipina que iba a dar el paso definitivo a la revolución.

3.7. TERRITORIO DE IFNI

Tras la victoria española en la denominada "Guerra de África" de 1859-60 se reconoció nuevamente nuestra soberanía en el territorio de Ifni. En el Tratado de Paz y Amistad de Tetuán, suscrito el 20 de abril de 1860 por el sultán de Marruecos, se concedió a perpetuidad dicha zona.

Sin embargo no fue hasta la 2ª República en que se volvió a proceder a su ocupación. El 11 de junio de 1934, Ricardo Samper Ibáñez, presidente del Gobierno de la Segunda República disponía, como elemento indispensable para el mantenimiento del orden y seguridad del Territorio español de Ifni, la creación del Cuerpo armado "Guardia Civil de Ifni", dependiente de la Oficina de Asuntos Indígenas. Esta presencia duró hasta 1969, cuando la presencia española finalizó en ese territorio.

En su composición mezcló tanto fuerzas de origen europeo -procedentes de la Guardia Civil española- como de procedencia autóctona, en su mayor parte de las Fuerzas de Regulares Indígenas y de las Mehal-Las Jalifianas desplegadas en el Protectorado español de Marruecos.

El nuevo Cuerpo, al mando de un capitán de la Guardia Civil, estaba organizado en tres líneas y compuesto por fuerzas de infantería y caballería.

Al crearse la comandancia de Marruecos, la Guardia Civil de Ifni quedó como una de las tres compañías de la misma[23].

Este territorio recibió un ataque el 23 de noviembre de 1957 por las bandas armadas del denominado "Ejército de Liberación marroquí", que afectó a numerosos puestos españoles y que daría lugar al inicio de la llamada Guerra de Ifni.

Como consecuencia de ello, la Guardia Civil de Ifni volvería a escribir una larga y desconocida página en la historia de aquel territorio que se cerraría el 6 de mayo de 1959, cuando el cabo 1º Juan Rubio Martos, comandante del puesto fronterizo de Tabelcut, fue liberado junto a su esposa e hijos, tras sufrir año y medio de cautiverio como prisioneros de guerra.

En 1969 el territorio de Ifni fue entregado a Marruecos, que había alcanzado su independencia de España y Francia en 1956.

4. LAS MISIONES DE OBSERVACIÓN EN EUROPA. LAS ASISTENCIAS TÉCNICAS DE LA GUARDIA CIVIL EN AMÉRICA.

El bien ganado prestigio de la Guardia Civil en España pronto franqueó las fronteras, tanto de Europa como atlánticas. Si en el viejo continente fue designada para

23 Las otras estaban en Ceuta y Melilla.

monitorizar el plebiscito del Sarre[24] en 1934, desde distintos países hispanoamericanos se requirió la presencia del Cuerpo para la constitución de instituciones similares en aquellas tierras.

4.1. GUATEMALA

En 1894 el propio Gobierno de Guatemala solicitó, con el fin de instaurar un Cuerpo similar a la Benemérita, que durante dos años "como modelos vivos se les facilitasen, a ser posible, dos sargentos o cabos, y caso contrario, dos guardias, uno de Caballería y otro de Infantería, que tengan de 25 a 35 años de edad, y voluntariamente deseen pasar a aquella República".

Tras la correspondiente selección realizada durante junio de 1894, los comisionados marcharon a Guatemala en 1895 regresando dos años después.

4.2. EL SALVADOR

El 3 de febrero de 1912, el presidente Araujo creaba en El Salvador el Cuerpo de la Guardia Nacional. Al objeto de que fuera lo más parecido posible a la Guardia Civil española, se solicitó de la península el envío de una misión del Cuerpo por un período de dos años. El capitán don Alfonso Martín Garrido fue designado como jefe de misión, siendo a su llegada a El Salvador asimilado a coronel y nombrado director general de la Guardia Nacional.

Se creó un centro de instrucción y se redactaron los reglamentos del nuevo Cuerpo, exactos a los de la Guardia Civil. Se organizó el despliegue con un tercio y cinco comandancias, con un total de sesenta y cinco puestos.

El contingente español permaneció hasta 1919, pero en 1922 se envió -a instancia de las autoridades de El Salvador- una nueva misión, compuesta por un comandante -José Tomás Romeu- y dos capitanes. Se reorganizó el Cuerpo estableciendo una Dirección General y un despliegue territorial de dos tercios, cuatro comandancias y ocho compañías.

4.3. COLOMBIA

El Ministerio de Estado de Colombia cursó en 1916 una solicitud de misión para la creación de un Cuerpo de Orden Público. Para tal objeto fueron designados el comandante José Osuna Pineda, dos oficiales y dos sargentos.

Al estar el Estado configurado en Departamentos, como estados federados, era imposible crear un Cuerpo centralizado. Se optó por crear tantos cuerpos como Departamentos existían (15), si bien únicamente se constituyeron los Cuerpos denominados Guardia Civil en Tolima, Cundinamarca y Antioquía.

24 Región alemana que, tras la Primera Guerra Mundial, fue administrada por la Sociedad de Naciones y explotada económicamente por Francia. En 1934 se llevó a cabo un plebiscito que culminó con la vuelta de la región a Alemania. Lamentablemente, y debido al inicio de los sucesos revolucionarios de Asturias, la misión no pudo llevarse a cabo.

Dichos Cuerpos tenían la misma reglamentación que la Guardia Civil española, si bien la de Tolima presentaba unas características más civiles que militares, con organización mixta (personal uniformado y de paisano) y bajo el mando directo del gobernador del Departamento, quien era su jefe máximo.

4.4. COSTA RICA

Con la intención de crear el Cuerpo de Guardia Rural, el Gobierno costarricense solicitó el 18 de octubre de 1920 el envío de un oficial de la Guardia Civil. Fue designado el capitán Lisardo Doval Bravo, quien permaneció en dicha república por tres años.

Se creó un Cuerpo gemelo de la Guardia Civil, dependiente del Departamento de la Guerra.

4.5. HONDURAS

Poco tiempo después de la misión en Costa Rica se realizó otra en Honduras, creando un Cuerpo similar a la Guardia Civil[25].

4.6. PERÚ

En similitud a lo sucedido en los países anteriormente citados, el presidente de la República -Leguía- solicitó, el 16 de agosto de 1921, una misión de la Guardia Civil para establecer en esa república un sistema de seguridad pública que resultaba una copia exacta del existente en España en aquellas fechas. Así, la actividad de los componentes del Cuerpo se centró en:

- Organizar un Cuerpo de Guardia Civil, similar a la española.
- Organizar otro Cuerpo de Seguridad, con el esquema de la Guardia Civil.
- Crear un Cuerpo de Investigación y Vigilancia.

La misión fue iniciada el 22 de noviembre de 1921 por el teniente coronel Pedro Pueyo España, auxiliado por un capitán, un teniente y un sargento, y fue continuada por otras en 1923, 1928 y 1931.

4.7. VENEZUELA

En 1936 se solicitó el asesoramiento de la Guardia Civil para crear el Cuerpo de la Guardia Nacional.

En el propio mes de octubre de 1936 llegó la comisión, mandada por el capitán Cecilio Marrero Suárez, que elaboró la cartilla del Guardia Nacional que vino a ser el catecismo profesional de los futuros miembros de la Institución.

A día de hoy, la Guardia Nacional Bolivariana mantiene como lema “el honor es su divisa”.

25 AGUADO SÁNCHEZ, Francisco: Historia de la Guardia Civil. Tomo 4. Pág. 180.

5. LA INTERVENCIÓN DE LA GUARDIA CIVIL EN LAS CAMPAÑAS MILITARES.

Para conocer la participación de las fuerzas del Cuerpo en las campañas militares es suficiente con enumerar las realizadas por el Ejército español desde la creación de la Guardia Civil. Salvo excepciones concretas y lógicamente justificadas[26], la presencia de la Guardia Civil se hizo precisa para garantizar el orden y seguridad de militares y civiles que seguían a las columnas, así como a los vecinos de las poblaciones por las que aquellas pasaban.

Por propia iniciativa del duque de Ahumada, y con motivo de la inminente partida del ejército expedicionario a Portugal, se aprobó la R. O. de 7 de junio de 1847, por la que se aprobaban los cometidos de la Guardia Civil en su servicio de campaña. Su contenido fue el siguiente:

- "La sección de la Guardia Civil en un Ejército de operaciones depende directamente del jefe del Estado Mayor General.
- Se le considerará siempre de servicio y todos los militares, de cualquier graduación, deben acatar las indicaciones que le hagan referentes a su instituto;
- Debe vigilar sobre la perpetración de delitos comunes, arrestar a los culpables y mantener el orden.
- Una de sus principales obligaciones es proteger a los habitantes del país ocupado.
- Igualmente debe comprobar las autorizaciones de cuantos paisanos sigan a las tropas, arrestando a los que no estén provistas de ellas.
- En las marchas la Guardia Civil detendrá a cuantos se separen del grueso por la vanguardia o flancos e incorporará a los rezagados.
- Se encargará del "cumplimiento de las órdenes del jefe de Estado Mayor con respecto a la marcha de equipajes, brigaderos y vivanderos".
- En los pueblos por donde pasen las tropas cuidará del orden en los puestos donde se venden los artículos de primera necesidad, vigilando que no haya alteración ni fraude en las pesas y medidas;
- Por otra parte, el comandante de la Guardia Civil elegirá de acuerdo con el gobernador general del cuartel el local destinado a prisión.
- En los cuarteles generales [el Cuerpo] cuidará de la ejecución de las leyes del Reino, bandos, órdenes generales del Estado, o de las del jefe de Estado Mayor general y gobernador general del Cuartel, y para cuidar su puntual observancia, mantendrá patrullas de parejas que celan su cumplimiento.
- La fuerza de la Guardia Civil se alojará en las proximidades del jefe del Estado

26 La Guardia Civil no participó ni en la Expedición a Italia (1849-1850) ni en la de la Conchinchina (1857-1862).

En cuanto a la primera de ellas, en 1849, Narváez organizó la expedición a Gaeta para establecer a Pío IX en Roma tras la proclamación de la República de Roma. En ella, la Guardia Civil no fue requerida para acompañar a las fuerzas regulares del Ejército.

La expedición a la Conchinchina, se compuso de fuerzas del ejército de Filipinas, por lo que careció de la presencia de la Guardia Civil, ya que ésta no estaba establecida en el archipiélago.

Mayor General o del gobernador general del Cuartel".

Esta redacción fue incluida en el Reglamento Militar del Cuerpo de 1852.

En cuanto a las vicisitudes acaecidas a la Guardia Civil en el desempeño de su servicio en campaña, se considera más adecuado realizar el estudio de manera cronológica, repasando las distintas campañas llevadas a cabo por el Ejército español desde 1844, fecha de fundación de la Guardia Civil, hasta la guerra civil de 1936-39[27].

5.1. EXPEDICIÓN A PORTUGAL (1847)

Como se dijo anteriormente, la determinación de los cometidos de la Guardia Civil en campaña fueron consecuencia de la expedición española a Portugal, llevada a cabo con ocasión de las diversas insurrecciones de los septembristas en Portugal, que culminaron en los comienzos de 1847 al extenderse la revuelta por Oporto, Braga y casi toda la provincia de Miño. Los carlistas portugueses pidieron ayuda a Inglaterra y España se ofreció, en cumplimiento de los compromisos adquiridos en el tratado de la Cuádruple Alianza, a aportar un Cuerpo de Ejército (12.000 hombres).

La aportación de la Guardia Civil constaba de 41 hombres de Caballería, al mando de un capitán (Francisco Aguirre).

Tras ocupar las tropas españolas Braganza y Alcañices, César de Vasconcellos –jefe de los rebeldes lusos- indicó que la capitulación de Oporto sólo sería tratada con el jefe de la fuerza española, general de la Concha, ignorando a los propios portugueses.

Caída Oporto el 30 de junio, la Guardia Civil estableció un servicio de patrullas para garantizar la seguridad de la ciudad. En julio se retiraron las tropas y la Guardia Civil participó del reconocimiento internacional por la actuación en la campaña.

5.2. GUERRA DE ÁFRICA (1859-1860)

El 25 de julio de 1859, mientras se estaba firmando el convenio de Tetuán[28], algunos componentes de la cábila de Anyera intentaron atacar la plaza de Ceuta, derribando unas construcciones militares.

Al ejército de operaciones, que se constituyó inicialmente, se le asignaron un total de 62 hombres en una compañía mixta del Cuerpo.

Al aumentar las fuerzas del Ejército (unos 40.000 hombres), se hizo lo propio con las del Cuerpo, que formaron una compañía de Infantería y un escuadrón de Caballería que se distribuyeron por secciones en los diferentes cuarteles generales (tres Cuerpos de Ejército, una División de reserva y otra de Caballería). El núcleo principal permaneció en el de O'Donnell, jefe del Ejército español.

27 Mención especial merecería también la participación de unos 300 guardias civiles como "Gendarmería de Campaña" en la División Española de Voluntarios durante la 2ª Guerra Mundial en el Frente Ruso. NÚÑEZ, Jesús. La Guardia Civil en la División Española de Voluntarios. En Aportes nº 61, 2006. Págs. 86-118

28 Cesión de territorios exteriores a Ceuta a España (el llamado Campo Exterior) por el rey de Marruecos.

Gistau[29] relata de esta manera la actuación de la Guardia Civil en esta campaña:

"Aunque no destinada a batirse en primera línea, a causa de la especialidad de su servicio, la Guardia Civil del Ejército de África, y particularmente la de Caballería que formaba el núcleo de las escoltas del General en Jefe y Comandantes Generales de cuerpo de ejército, tomó parte en casi todos los combates..., pero donde se distinguió de modo extraordinario, llamando la atención del General en Jefe, fue en la célebre carga del 23 de enero contra el grueso de las fuerzas enemigas.

Era en los llanos de Tetuán, y el General O'Donnell, tanteando las posiciones del adversario, preparaba su famosa batalla del 4 de febrero siguiente. Un batallón del Regimiento de Cantabria, acosado por fuerzas extraordinariamente superiores y en situación muy comprometida, tuvo que formar el cuadro, y entonces el bravo Brigadier Romero Palomeque, con la Guardia Civil del Cuartel General, dos escuadrones de lanceros de Farnesio y una sección de AIbuera, se lanzó a la carga, arrollando y destruyendo cuanto encontró a su paso…"

En los combates anteriores la fuerza del Cuerpo también había participado, logrando sus componentes condecoraciones y sufriendo bajas ante el fuego enemigo, sin faltar lances apurados que se resuelven favorablemente por la intervención de los guardias, como el 9 de diciembre de 1859 muy cerca del Cuartel General de O'Donnell y en la batalla de Wad-Ras, donde Teodoro Camino cargó contra los africanos 12 veces consecutivas, al mismo tiempo que lo hacía también con sus hombres el alférez Vicente Herrero. La Guardia Civil dejó constancia de su existencia tanto en combate como en cumplimiento de su misión específica en los ejércitos de operaciones. Finalizada la guerra, las tropas españolas iniciaron el regreso, entrando en Madrid en un desfile encabezado por una sección del Cuerpo.

5.3. EXPEDICIÓN A MÉJICO (1861-1862)

La Guardia Civil envió una fuerza que estuvo compuesta por 35 individuos constituyendo una sección de Infantería procedente del tercio en comisión de Cuba, concretamente de La Habana.

En esta campaña cumplieron las misiones encomendadas por Orden de 1847, en especial las referentes a la protección de los campamentos.

5.4. GUERRA DE SANTO DOMINGO (1863-1865)

La compañía enviada desde Cuba, bajo el mando del capitán Felipe Plaza, tomó parte en todas las acciones junto a las tropas expedicionarias, distinguiéndose en las de San Lorenzo de Guayabín, Sierra del Cibao, Santiago de los Caballeros, Mote Cristo, Puerto Plata y otras.

5.5. GUERRA GRANDE DE CUBA (1868-1878)

Tras la acción de Céspedes en Yara, se inició la "guerra larga" o "guerra grande". El Gobierno contaba con una fuerza de entre 6.000 y 7.000 hombres, de los cuales casi 1.000 eran guardias civiles.

29 GISTAU FERRANDO, Miguel: La Guardia Civil. Historia de esta Institución y de todos los cuerpos armados que en España estuvieron destinados a la persecución de malhechores desde la reconquista a nuestros días. Págs 474-475.

Hasta que se produjo el aumento de efectivos del Ejército en 1869 (40.000 hombres), las fuerzas del Cuerpo tuvieron que luchar como cualquier otra fuerza militar, sin dejar de atender su servicio peculiar.

Desde mediados de 1870, las actividades de los separatistas disminuyeron, transformándose más bien en actividades propias de los bandoleros e incendiarios.

Cuando en 1874 se recrudeció la guerra, la Guardia Civil fue empleada masivamente de nuevo como tropa combatiente. Las fuerzas del Cuerpo del Departamento Occidental fueron destinadas a cubrir la Trocha[30], custodiar los penados y proteger sus trabajos.

En 1875 se asignaron los Escuadrones de Caballería del Cuerpo a las distintas columnas regulares, librando numerosos combates.

El aumento de tropa del Ejército regular en 15.000 hombres a la llegada de Martínez Campos -1876- parecía liberar al Cuerpo del servicio distinto al suyo propio. Sin embargo, en 1877 el propio general Martínez Campos ordenó la afección de las comandancias del Cuerpo a los Cuarteles Generales de las Comandancias Generales. Las fuerzas del Cuerpo fueron distribuidas entre las Grandes Unidades regulares. De esta forma, en 1878 el Cuerpo finalizó su actuación en la guerra.

5.6. GUERRA CHIQUITA DE CUBA (1879-1880)

La intervención del Cuerpo en esta guerra, iniciada el 28 de agosto de 1879, tuvo como hechos principales los siguientes:

- Apresamiento de los principales revolucionarios en las inmediaciones de la hacienda de Guanayara, en los primeros días de septiembre.
- Solución de la insurrección general de Remedios, por el comandante Críspulo Antolín.
- Sitio del puesto de Corralito (comandancia de Holguín) el 7 de octubre de 1879. Un sargento y siete guardias fueron atacados por una partida guerrillera y presentando una tenaz resistencia les hicieron retirarse sin lograr sus objetivos (armamento y munición).

Como consecuencia destacada de las actuaciones de la Guardia Civil en las distintas campañas, se hizo preciso determinar perfectamente sus cometidos y modificar algunos de ellos dado que, a pesar de combatir en numerosas ocasiones, dicha misión no se encontraba entre las asignadas a los individuos del Cuerpo. Así, el Reglamento para el servicio de Campaña, aprobado por Ley de 5 de enero de 1882, determinaba las competencias de policía de la Guardia Civil (art. 119) y se reconocía la posibilidad de emplear las fuerzas del Cuerpo como combatientes (art. 129).

5.7. CAMPAÑA DE MELILLA (1893-1894)

Los reiterados ataques por parte de los cabileños a las fuerzas de Ingenieros que construían las defensas en los alrededores de Melilla ocasionaron muchas bajas entre

30 Camino militar fortificado establecido entre el Júcaro y Morón que, cruzando la isla por su parte más estrecha, estaba destinada a reducir la movilidad de las partidas enemigas, dejándolas aisladas a cada lado de dicho camino.

las tropas españolas. La ofensiva cabileña culminó con la muerte del general Margallo.

Para contrarrestar la ofensiva, se organizó un ejército de operaciones, asignándole el mando de sus 20.000 hombres al general Martínez Campos.

La Guardia Civil reforzó la fuerza en Melilla con una sección, que realizó los servicios propios del Cuerpo en Campaña, dedicándose principalmente a la persecución del contrabando de armas con destino a los cabileños.

5.8. GUERRA DE CUBA (1895-1898)

Al lanzarse el grito de "Baire" contaba la guarnición de Cuba con 14.000 hombres. Además, también estaban desplegados 5.500 guardias civiles.

Las fuerzas del Cuerpo combatieron en unión con las del Ejército regular, integradas en columnas heterogéneas, organizando cada comandancia un batallón.

La escasa caballería española era principalmente la de la Guardia Civil, centralizada por el coronel Guillermo Tort y Gil, jefe del 17º tercio. Actuó agrupada en diez escuadrones, coordinados por Tort y excepcionalmente asignadas por secciones a las columnas.

Martínez Campos concentró los puestos del Cuerpo en tres compañías de policía militar y organizó seis columnas mixtas, de las que dos fueron mandadas por dos guardias civiles: el coronel Tort y Gil y el teniente coronel Paglieri, jefe de la comandancia de la Habana.

Weyler reorganizó las fuerzas, dándolas un carácter homogéneo. La Guardia Civil quedó en la misma columna, mandada por el coronel Tort y con la misión de asegurar el campo de La Habana. Estos guardias civiles tomaron parte en numerosos hechos de armas.

Fueron muy frecuentes los ataques a los puestos del Cuerpo. Destacaron entre ellos los siguientes:

- Puesto de Provincial, mandado por el cabo Lucas. Fueron atacados el 14 de julio de 1895 por más de 200 mambises. Tras más de 20 horas de lucha se retiraron hasta encontrarse con tropas españolas. El cabo Lucas recibió la Cruz de San Fernando.
- Fuerte Taguasco, defendido por un teniente y 20 guardias durante seis días. Agotadas las municiones se les autorizó a rendir la posición. El jefe insurrecto se negó a recibir la espada del oficial, por su valor y decisión. Tras una comida en común fueron puestos en libertad.
- Puesto de Guayos, 25 de octubre de 1895. el cabo Rojo Franco, comandante del puesto, ordenó la defensa hasta sus últimas consecuencias. Tras atacar el puesto en diez ocasiones e incendiar el pueblo, los insurrectos se retiraron.
- Puesto de Dolores, mandado por un guardia 2º, sitiado por el cabecilla Moreno Rojas quien, tras un intercambio de misivas, reconoció el valor del guardia y se retiró.

- Puesto de Dolores, defendido en esta ocasión -enero de 1897- por el guardia Bernardo Badal Suay. Resistió el ataque de 500 enemigos con artillería hasta que pudo replegarse al ingenio de Dolores, distante dos kilómetros. Al guardia Badal le fue concedida por esta acción la Cruz de San Fernando.

5.9. GUERRA DE FILIPINAS (1896-1898)

Siendo capitán general Ramón Blanco, se inició una serie de levantamientos contra el poder español, en la que los tagalos invadieron (30 de agosto de 1896) los arrabales de Sampaloc, donde fueron batidos por una columna de 70 guardias civiles.

Era muy habitual que los españoles buscaran refugio en los cuarteles de la Benemérita, donde se les acogía y protegía de las acciones insurgentes.

Para garantizar la seguridad periférica de Manila se organizó una columna de guardias civiles y cazadores, al mando del coronel Pintos, jefe del 21º tercio.

Como en el resto del Ejército, la Guardia Civil sufrió un 40% de deserciones por pasarse sus efectivos al enemigo con armas y municiones, al tratarse de tropas indígenas. Únicamente la Artillería -compuesta por europeos en su totalidad- y el tercio de Guardia Civil Veterana fueron leales en su conjunto, siendo el tercio del Cuerpo el único que no experimentó ni una sola deserción, a pesar de estar integrado por nativos.

Como en Cuba, fueron muy frecuentes los ataques a los puestos del Cuerpo, con el fin de apoderarse del armamento. Sufrieron en numerosas ocasiones acciones que los mantuvieron en permanente peligro.

En diciembre de 1896, Blanco fue relevado por Polavieja[31]. Contaba con 24.000 soldados y 4.000 guardias civiles, de los que asignó 800 guardias civiles a las cuatro brigadas de la 1ª División, con misiones de exploración y protección de los cuarteles generales.

En abril de 1897 el capitán general Primo de Rivera intentó una mezcla de procedencias entre europeos y nativos en las Unidades, comenzando su “experimento” en el tercio de la Guardia Civil Veterana.

Debido a la ejemplar conducta de la Guardia Civil Veterana, el 20 de octubre de 1897 se crea, para la tropa indígena del tercio, un distintivo denominado “Escudo de Lealtad”. El 24 de octubre, festividad de San Rafael -patrón de la Guardia Civil Veterana- y en acto público, en el marco de una parada militar, se procedió a imponer los distintivos -adquiridos por suscripción popular-, coincidiendo con la adopción por esas tropas de nuevos uniformes.

El 20 de noviembre de 1897 se firmó el pacto de Biac-Na-Bató, por el que el insurrecto Emilio Aguinaldo se comprometió a retirarse y no volver a tomar las armas contra España a cambio de una cantidad de dinero.

Tras la derrota naval de Cavite ante la escuadra norteamericana del Pacífico -1 de

31 Tras la misiva del arzobispo de Manila -fray Nozaleda- que le acusaba de indecisión cuando no de implicación directa en actividades de desprestigio de la administración de las islas por las órdenes religiosas. ANDRÉS GALLEGO, José: La política religiosa en España 1889-1913. Págs. 93-94.

mayo de 1898- el nuevo capitán general, Augusti decretó la movilización general. En el sitio de Manila, la Guardia Civil Veterana volvió a demostrar su lealtad combatiendo hasta el momento de la capitulación, el 13 de junio.

Entre junio y noviembre, los tercios de la Guardia Civil fueron disueltos, integrándose sus componentes europeos en los batallones de cazadores de Visayas y Mindanao, a la espera de ser repatriados.

5.10. GUERRA DE PUERTO RICO (1898)

Las fuerzas del Cuerpo participaron en esta campaña y sufrieron el bombardeo naval de San Juan de Puerto Rico el 11 de mayo de 1898.

5.11. CAMPAÑA DEL RIF (1909)

Tras la muerte de varios obreros españoles que trabajaban en la compañía de Minas del Rif, se envió una División a Melilla.

Inicialmente no se trasladaron refuerzos de la Guardia Civil al estallar la Semana Trágica en Barcelona y tener que atender prioritariamente el Cuerpo al restablecimiento del orden público en la península.

Una vez finalizado este suceso se enviaron fuerzas del Cuerpo, por lo que el ejército constituido (40.000 hombres), a las órdenes del general Marina, contó con una fuerza de la Guardia Civil compuesta por 153 hombres.

La Guardia Civil se empleó en la consolidación de posiciones tomadas por las fuerzas del Ejército, así como en la ocupación completa del Gurugú.

5.12. CAMPAÑA DEL KERT (1911-1912)

Debido a las agresiones a obreros topográficos, que levantaban mapas de la zona del río Kert -cercano a Melilla- se inició una nueva campaña, con el fin de ensanchar las posiciones españolas en un frente de 60 Km.

La Guardia Civil envió como apoyo al Ejército –bajo el mando del general García Aldave- una sección para realizar su servicio de campaña, no pudiendo aumentar su entidad al tener que atender el orden público en el territorio peninsular, lo que demandaba la mayor cantidad de efectivos posible.

5.13. GUERRA DE ÁFRICA (1913-1917)

En 1913 se estableció la organización del Protectorado español en Marruecos. Desacuerdos por el nombramiento del Jalifa Muley el Mehdi hicieron que el Muley Ahmed el Raisuni se pusiera al frente de una rebelión, que duró hasta 1917, tras reducir la cabila de Anyera.

La Guardia Civil prestó su servicio de campaña con el personal de las propias Unidades territoriales.

5.14. CAMPAÑA DE MARRUECOS (1918-1927)

Un destacamento de la comandancia exenta de Marruecos -un teniente, dos cabos y diez guardias de Infantería y Caballería- constituyó la escolta permanente del comandante general, protegiéndolo en las operaciones de guerra y tomando parte activa en diversas acciones.

En las operaciones para la toma de Xauén (1920) las columnas del Ejército fueron apoyadas por una compañía mixta de la Guardia Civil -50 hombres de Infantería y 20 de Caballería-. El Alto Comisionado entraría en la ciudad escoltado por fuerzas de la Guardia Civil.

Hasta 1921 la Guardia Civil continuó prestando su servicio específico y el de campaña en campamentos, fuertes y destacamentos del Ejército, todo ello desde la propia comandancia de Marruecos.

En 1921 se adscribió una sección mixta del Cuerpo al cuartel general del comandante general de Larache, acompañándole en diversas operaciones y tomando parte en varias acciones.

Al iniciarse las acciones que culminarían con el tristemente famoso “desastre de Annual”, los puestos de la Guardia Civil quedaron aislados y sin comunicación, actuando cada uno según la iniciativa de sus respectivos mandos. Unos se replegaron con sus familias sobre Melilla; otros lo hicieron sobre fuertes militares; a otros no les quedó más remedio que prepararse para la defensa del propio cuartel.

La defensa más famosa fue la de Nador, atacada el 24 de julio de 1921. Sería un asedio en toda regla, especialmente para los defensores que se parapetaron en la fábrica de harinas.

Tras la reconquista de los territorios perdidos, el Cuerpo siguió prestando su servicio peculiar, tanto en el frente como en retaguardia. Igualmente se realizaba el servicio de campaña. Fue muy importante la lucha contra el bandolerismo, dirigido contra personas y viviendas de europeos y rifeños que no se habían sumado a la rebelión.

En las instrucciones preparatorias del desembarco de Alhucemas, se preveía el envío de pequeñas patrullas del Cuerpo para ejercer de policía militar con cada columna, permitiéndose llegar a ellas al personal civil necesario (proveedores, cantineros, etc.).

Tras el desembarco -en el que participaron más de 20 guardias civiles- el número de guardias en servicio de campaña se incrementó según las tropas iban avanzando. Mientras unos iban organizando nuevos puestos, el resto se incorporó a las unidades de primera línea, donde tomaron parte activa en las diferentes operaciones militares.

6. OTRAS CONSIDERACIONES

En cumplimiento de sus obligaciones como militares, ya sea en su servicio peculiar o como consecuencia de una campaña militar, las cifras de las recompensas de la Real y Militar Orden de San Fernando -destinada a premiar el valor militar en grado “heroico” o “muy distinguido” y, por tanto, la más prestigiosa de la milicia española-

concedidas al personal de la Guardia Civil[32] son las siguientes:

833 componentes del Cuerpo fueron recompensados con condecoraciones de la Orden.

Se concedieron un total de 1.041 cruces, de las cuales 40 fueron laureadas (las que premian el valor en grado “heroico”).

Cuatro Unidades de la Guardia Civil recibieron la Cruz Laureada con carácter colectivo.

Este reconocimiento por parte de las más altas autoridades militares pone de manifiesto el enorme prestigio que, en el cumplimiento del deber, supieron labrarse los componentes del Cuerpo -y el Cuerpo mismo- a lo largo de la ya dilatada historia de esta institución.

Al terminar la lectura de estas páginas el lector habrá podido advertir la presencia de la Guardia Civil en cuantas empresas han acometido los distintos Gobiernos de nuestra nación.

En todos los territorios gobernados por España, la Guardia Civil ha desempeñado un papel principal en el mantenimiento de la seguridad pública, especialmente en aquellos escenarios donde la estabilidad política y social ha estado más amenazada.

El modelo de organización y de servicio del Cuerpo ha servido de inspiración para la creación de nuevos Cuerpos de seguridad en otras naciones. Tanto en la América hispana como en África, los guardias civiles han contribuido a crear las estructuras de seguridad que han permitido a no pocos países gozar de unas fuerzas destinadas a proteger las vidas y propiedades de sus ciudadanos.

Por último, es de destacar la importante labor que las fuerzas de la Guardia Civil han desempeñado en el desarrollo de las campañas militares llevadas a cabo por nuestro Ejército y Marina. Desde la concepción inicial de su servicio como policía militar interna de los ejércitos de operaciones, en pocos años se consideró su valor para formar parte de la fuerza combatiente -siempre en caso excepcional- al quedar recogida esta posibilidad en el Reglamento para el Servicio de campaña de 1882[33], posibilidad que, a día de hoy, permanece activa en las disposiciones que regulan estas actividades[34].

BIBLIOGRAFÍA

Aguado, F. (1984). Historia de la Guardia Civil. 7 tomos. Madrid: CUPSA y Planeta.

Andrés-Gallego, J. (1975). La política religiosa en España 1889-1913. Madrid: Editora Nacional.

32 Aquí se incluyen también las concedidas al personal del Cuerpo de Carabineros, ya que la Guardia Civil es heredera del historial de este instituto, toda vez que el mismo se integró en la Benemérita como consecuencia de la promulgación de la Ley de 15 de marzo de 1940, que suprimió la Inspección General de Carabineros -pasando sus cometidos y funciones a la Dirección General de la Guardia Civil- y dispuso que su personal se integrara en la Guardia Civil.

33 Ley de 5 de enero.

34 Reglamento para el servicio de la Guardia Civil de 1943 (servicio en campaña, no derogado) y Real Decreto 1438/2010, sobre misiones de carácter militar que pueden encomendarse a la Guardia Civil.

Dirección General de la Guardia Civil. Estado Mayor. (1970). Guardia Civil Española. Madrid: Imprenta-Escuela de Huérfanos de la Guardia Civil.

Geijo, J. G. (1914). La Guinea Española y la Guardia Colonial. Gijón: Imprenta La Fe.

Gistau, M. Revista Técnica de la Guardia Civil. Creada en 1910. Declarada de utilidad por Real Orden del Ministerio de la Guerra de 18 de mayo de 1916. Desaparecida en 1936. Madrid.

Gistau, M. (1907). La Guardia Civil. Historia de esta Institución y de todos los cuerpos armados que en España estuvieron destinados a la persecución de malhechores desde la reconquista a nuestros días. Valdemoro, Madrid: Imprenta de la Guardia Civil.

González, J. F., y Pérez, G. (2013). Caballeros de la Real y Militar Orden de San Fernando (Guardia Civil y Carabineros). Madrid: Ministerio de Defensa, Subdirección General de Publicaciones y Patrimonio.

Inspección General del Arma. (1846). Cartilla del Guardia Civil. Madrid: Imprenta de D. Victoriano Hernando.

López, M. (2005). Guardia Civil en la Restauración (1875-1905): militarismo contra subversión y terrorismo anarquista. Madrid: Actas.

López, D. (2004). La Guardia Civil y los orígenes del Estado centralista. Madrid: Alianza.

Luengo, M. (1969-1971). La Guardia Civil en las islas de Cuba y Puerto Rico. Revista de Estudios Históricos de la Guardia Civil, num. 4-7. Madrid: Imprenta-Escuela de Huérfanos de la Guardia Civil.

Martínez, E. (1976). Creación de la Guardia Civil. Madrid: Editora Nacional.

Montero, J. (1888). Historia de la piratería malayo-mahometana en Mindanao, Joló y Borneo. 2 volúmenes. Madrid: Imprenta y Fundición de Manuel Tello.

Morales, A. (1980). Las Fuerzas de Orden Público. Madrid: San Martín.

Núñez, J. (2000). La Guardia Territorial de la Guinea Española. SERGA, Revista de Historia Militar del Siglo XX, 3. Madrid: Almena.

Núñez, J. (2001). La Guardia Civil en las Campañas de Marruecos (1909-1927). En VV.AA., Las Campañas de Marruecos (1909-1927) (pp. 256-301). Madrid: Almena.

Núñez, J. (2000). Los orígenes de la Guardia Civil de Ifni. Revista Guardia Civil, 674, 76-80. Madrid.

Opisso, A. (1906). La Guardia Civil y su tiempo: Episodios de la historia contemporánea de España. 2 volúmenes. Barcelona: Molinar y Maza.

Osuna, J. (1915). Hechos gloriosos de la Guardia Civil. Madrid: Establecimiento tipográfico.

Puig, J. J. (1984). Historia de la Guardia Civil. Barcelona: Mitre.

Sidro y Surga, J., y De Quevedo y Donis, A. (1858). La Guardia Civil: historia de esta institución y de todas las que se han conocido en España con destino a la persecución

de malhechores, desde los tiempos más remotos hasta nuestros días.... Madrid: A. Pérez Dubrull.

Ximénez, C. (1858). Las Instituciones de Seguridad Pública en España y sus dominios de Ultramar. Madrid: Imprenta y Estereotipia de M. Rivadeneyra.

(1908). Reglamento de la Guardia Colonial de los Territorios Españoles del Golfo de Guinea. Madrid: Imprenta de Vicente Rico.

Fecha de recepción: 18/11/2014. Fecha de aceptación: 17/12/2014

LA PROBLEMÁTICA DE LAS AMENAZAS EN TEXTOS ESCRITOS REALIZADAS POR AUTOR DESCONOCIDO

ANA ISABEL ÁLVAREZ APARICIO

RESUMEN

Las amenazas son una realidad creciente en un mundo cada vez más globalizado, donde las nuevas tecnologías facilitan, cada vez en mayor grado, el anonimato del autor. El presente trabajo tiene por objeto dotar al lector de una visión global sobre el estado actual de la evaluación de amenazas, entendiendo estas como un peligro potencial creciente, que debe analizarse, valorarse y, en su caso, atajarse. A tal fin, y en base a las aportaciones de diversos autores y a la escasez de estudios al respecto, trataremos de realizar una primera aproximación a su estudio, así como a lo que entendemos deben ser unos parámetros objetivos a tener en cuenta, para la valoración de credibilidad de amenazas en textos escritos, especialmente de carácter anónimo.

Palabras clave: amenaza, texto escrito, anónimos, credibilidad, evaluación, valoración y marcador lingüístico.

ABSTRACT

Threats are a growing reality in an increasingly globalized world, where new technologies make increasingly greater extent, the anonymity of the author. The present study aims to provide the reader an overview of the current state of threat assessment, understanding these as a growing potential to be analyzed, evaluated and, where appropriate, tackled danger. To this end, and based on the contributions of various authors and the scarcity of studies on the subject, try to make a first approach to study and to understand what must be objective parameters to consider for the assessment of credibility of threats in written texts, especially anonymously.

Keywords: threat, written text, anonymous, credibility, evaluation, assessment and linguistic marker.

1. INTRODUCCIÓN

Lejos de lo que pueda pensarse, la realización de amenazas, sean estas escritas, orales o gestuales, a través del teléfono, el ordenador o el correo postal, es una realidad creciente en un mundo globalizado, donde la proliferación de las nuevas tecnologías facilitan, cada vez en mayor grado, el anonimato del autor de las mismas.

Si entendemos por amenaza “el hecho de intimidar a alguien con el anuncio de la provocación de un mal grave para él o su familia” (RAE, 2001), tipificado en el Capítulo II del Título VI del Libro II del Código Penal de 1995 (artículos 169 a 171) orientado a proteger la libertad de los individuos; vemos cómo son dos, básicamente, los bienes jurídicos tutelados que se quebrantan: el sentimiento de tranquilidad, que afecta a todos los supuestos, y el ataque a la libertad en la formación de la voluntad (es decir,

la libertad de decisión del sujeto libre de injerencias externas que influyan sobre su voluntad, como es el derecho de poder pensar y decidir qué es lo que quiere hacer en cada momento), que se ve afectada, fundamentalmente, en los supuestos de amenazas condicionales.

Así, para la jurisprudencia del Tribunal Supremo, "el delito de amenazas, de mera actividad[1], constituye una infracción contra la paz individual y contra la libertad, pues, mediante aquellas, se impone al sujeto pasivo realizar un acto o cumplir con una condición en contra de su voluntad. Descansa, fundamentalmente, en la conminación del mal, en un amedrentamiento a través o por medio de actos o conducta determinada, en adecuada relación de causa a efecto" (Sentencia de la Sala Segunda, de 12 de abril de 1991).

El mal, además, con que se amenaza, de acuerdo a la Sentencia del Tribunal Supremo de 5 de junio de 2003, ha de ser "serio, real, perseverante y generador de una repulsa social indudable, futuro, injusto, determinado y posible, dependiente exclusivamente de la voluntad del sujeto activo"; siendo la diferencia entre un mal constitutivo de delito y otro no constitutivo, la tipificación o no como delito de dicho mal.

Por otro lado, la gravedad del mal y su adecuación para intimidar tiene que relacionarse con la persona del amenazado y con las circunstancias que lo rodean, pero no es preciso que la amenaza llegue a intimidar necesariamente al receptor de la misma, sino que basta con que objetivamente sea adecuada para ello. Así, como señala Stamatoulous (2014), este delito es eminentemente circunstancial, debiendo valorarse la ocasión en que se profiere, las personas intervinientes, actos anteriores, simultáneos y, sobre todo, posteriores al hecho material de la amenaza.

En base a la legislación española vigente, podríamos hablar de amenazas graves (constitutivas o no de delito, chantaje o "sui géneris" o con finalidad terrorista) y de amenazas menos graves, recogidas estas últimas en el artículo 171 del Código Penal; siendo la pena variable según se exija cantidad o se impongan condiciones al amenazado y según el autor hubiere o no conseguido su propósito.

Así mismo, dentro de las amenazas calificadas como graves, podríamos distinguir entre:

- Aquellas de tipo básico, condicionales[2], cuando se exige una cantidad o se impone cualquier otra condición (posible, al menos potencialmente), aunque no sea ilícita, y no condicionales[3]. En ambos casos el delito de amenazas se consuma cuando el propósito del agente de causar un mal llega a conocimiento del ofendido.

1 El delito de amenazas es un delito de simple actividad, de expresión o de peligro, y no de verdadera lesión, de tal suerte que si esta se produce, actuará como complemento del tipo.

2 Recogidas en el artículo 169.1 del Código Penal. Lo constitutivo de delito es el mal con que se amenaza, y no la condición que se impone, que puede ser perfectamente lícita (a excepción del chantaje, recogido en el artículo 171.2 del Código Penal). En dicho artículo se contempla además un subtipo agravado, debido a la mayor capacidad para quebrar la libertad de obrar del sujeto pasivo, para todos los casos de amenaza condicional de un mal delictivo, se obtenga o no la condición impuesta, cuando la amenaza se hiciera por escrito, por teléfono o por cualquier medio de comunicación o de reproducción, o en nombre de entidades o grupos reales o supuestos.

3 Se regulan en el artículo 169.2. del Código Penal El comportamiento típico únicamente afectará al sentimiento de tranquilidad del sujeto, sin que necesariamente haya de suponer interferencia alguna en su proceso motivacional.

- Aquellas de tipo agravado, recogidas en el artículo 170 del Código Penal, y que aglutinarían aquellas amenazas dirigidas a atemorizar a los habitantes de una población, grupo étnico, cultural o religioso, o colectivo social o profesional, o a cualquier otro grupo de personas, y que tuvieran la gravedad necesaria para conseguirlo; así como aquellas en que se reclame públicamente la comisión de acciones violentas por parte de bandas armadas, organizaciones o grupos terroristas, independientemente de que la acción se dirija contra un individuo o contra una colectividad.

Igualmente se considera un subtipo agravado, la amenaza del mal que sea cometida por escrito, por teléfono o por cualquier medio de comunicación o reproducción, o en nombre de grupos o entidades reales o supuestos (artículo 169.1 del Código Penal), al entenderse que esto supone un mayor impacto sobre la libertad del receptor, al estar ante medios calificados por la jurisprudencia como serios y persistentes, y por tanto, con una mayor capacidad para incidir negativamente en la libertad de obrar del sujeto amenazado, consistente esta en la libertad que toda persona tiene para realizar sus propias acciones y llevarlas adelante sin que estas se vean obstaculizadas. Es precisamente en estos casos, donde el presente artículo pretende incidir.

Como podemos ver, e independientemente del tipo de amenaza proferida, cualquiera puede ser sujeto activo de estas comunicaciones, basta con exteriorizar su propósito de un modo que haga creer al sujeto pasivo que este es real, serio y persistente (aún cuando su verdadera intención no sea llevar a la práctica la amenaza). En la misma línea, cualquiera, exceptuando los casos de amenazas leves de los artículos 171.4 y 171.5 (en los que la víctima debe ser la esposa, pareja con la que conviva o persona vulnerable), podría ser sujeto pasivo de este tipo de delito. Tipo que quedaría consumado en el momento mismo en que la amenaza fuese recibida por el ofendido y que contemplaría también la figura de la tentativa. Así, hablaríamos de “tentativa acabada” cuando el sujeto activo realiza todas las conductas necesarias pero el fin no llega a materializarse por causas ajenas a su voluntad, como puede ser el caso de una misiva amenazante que no llega a su destinatario porque el cartero se equivoca de domicilio, o un correo electrónico que es identificado por el ordenador como “no deseado” y eliminado automáticamente. Hablamos de “tentativa inacabada’’ cuando quien emite la amenaza no consigue el resultado típico ya que se interrumpe la realización de los actos ejecutivos correspondientes para conseguir el efecto esperado, como ocurriría en el caso de que se produjera la detención del sujeto activo por las FF.CC.SS.EE.

Muchas son las vías o canales a través de los cuales una amenaza puede ser emitida. Ya sea de forma verbal o escrita, a través de un ordenador, un teléfono o una simple hoja de papel. Las amenazas constituyen, por norma general, un verdadero desasosiego para el receptor de las mismas, que en muchos casos desconoce quién es el autor material y si su intención es realmente llevar a término la advertencia proferida.

Pero esta preocupación se hace extensiva también a los propios investigadores policiales, que se ven en la obligación de dar respuesta no solo a una identificación positiva del autor de la amenaza cuando esta se realiza de forma anónima, para así determinar las responsabilidades penales derivadas del hecho, sino a si de la amenaza proferida puede seguirse una conducta que ponga en peligro la integridad física y mental de la víctima, sus allegados o sus bienes.

Sintomatología de carácter ansioso, depresivo, dificultades para iniciar o mantener el sueño, pesadillas, niveles anormalmente elevados de activación o *arousal* que pueden conducir a una hipersensibilidad y reactividad a estímulos externos ambiguos percibidos como amenazantes, así como dificultades para concentrarse o el consumo de sustancias, son solo algunas de las problemáticas asociadas a la recepción de amenazas. Aspectos todos ellos que pueden verse potenciados, dando lugar a verdaderas patologías, cuando las misivas se repiten en el tiempo, son de carácter anónimo y se producen de forma aleatoria y variable.

Desarrollar instrumentos efectivos y eficaces, que permitan a los profesionales valorar de forma rigurosa la credibilidad de una amenaza y, por tanto, la posibilidad de llevarse a la práctica, se convierte, por tanto, en una necesidad imperiosa, en un mundo cada vez más globalizado, donde la proliferación de amenazas a través de medios que facilitan el anonimato cada vez es mayor. Es precisamente en este punto, donde se inscribe el presente artículo. Y, más específicamente, en las amenazas escritas realizadas por autor desconocido.

2. ESTADO ACTUAL

Pocos son los estudios existentes hasta el momento sobre amenazas y lo que estas comportan a todos los niveles. Y, menos aún, aquellos centrados en la evaluación y valoración de las amenazas en textos escritos. Así, la mayor parte de las investigaciones sobre esta materia se han centrado principalmente en víctimas de alto riesgo como celebridades y figuras públicas, políticos o jueces y en aspectos como las características del autor de la amenaza (edad, nivel socio-cultural, rasgos de personalidad, salud mental, historial de violencia y comportamiento criminal, historia de abuso de sustancias, etc).

En las investigaciones sobre las comunicaciones amenazantes, se ha prestado especial atención a las características físicas del documento, como el modo de comunicación (cartas, correos electrónicos, llamadas telefónicas, etc.), el método a través del cual se crea la comunicación (ordenador, máquina de escribir, escritura a mano, recortes de revistas, etc.), el contenido o tema sobre el que versa la misma y las características gramaticales y léxicas del lenguaje amenazador. Estos aspectos han sido investigados con el propósito de determinar el grado de intención del autor de la amenaza de acercarse y/o hacer daño al destinatario, principalmente. No obstante, los resultados obtenidos en este aspecto han sido contradictorios, ya que no se ha podido establecer ninguna categoría que mida con exactitud el grado de peligro de las comunicaciones amenazantes (Álvarez, Gil y Mena, 2014).

Así, a día de hoy, los intentos realizados por diferentes autores de crear una base teórica metodológicamente sólida, que permita una evaluación y valoración de las amenazas emitidas de forma válida y fiable, han resultado infructuosos.

A la falta de estudios, ya señalada, se le une la ausencia de un cuerpo escritural extenso, que permita la sistematización de los resultados obtenidos. Solo países como Estados Unidos, a través de la Oficina Federal de Investigación (Federal Bureau of Investigation, FBI), principal rama de investigación del Departamento de Justicia, constituyen una excepción a este factor. A tal fin, el FBI ha diseñado la Base de Datos de Evaluación de Comunicaciones Amenazantes (Communicated Threat Assessment

Database, CTAD), una base de datos lingüística informatizada, diseñada para ser el depósito principal de todas las amenazas comunicadas y otras comunicaciones con orientación delictiva, con una gran capacidad de búsqueda que permite categorizar detalladamente lo expresado en las amenazas en veinticuatro categorías y está orientada a evaluar la posibilidad de que la acción amenazada se lleve a cabo y, si es posible, determinar su autoría (Fitzgerald, 2007).

3. LAS AMENAZAS EN TEXTOS ESCRITOS REALIZADAS POR AUTOR DESCONOCIDO

Esta modalidad de amenaza, por su complejidad e implicaciones, merece especial atención.

Como ya hemos indicado, el propio Código Penal español considera la comunicación de una amenaza a través de medios escritos un subtipo agravado de responsabilidad criminal, al igual que hacerlo en nombre de grupos o entidades reales o supuestos, algo relativamente frecuente en amenazas anónimas.

Pero esta modalidad de comunicación amenazante, no solo conlleva especiales implicaciones legales, sino también policiales y psicológicas.

Así, el desconocimiento del autor de la amenaza, unido a una forma de transmisión del comunicado que favorece el anonimato, no solo conlleva unas dificultades añadidas para los investigadores, que no pueden realizar un perfil del emisor que facilite una evaluación y posterior valoración de la credibilidad del mensaje y riesgo potencial de realizarse, sino unas consecuencias psicológicas para el receptor del mismo.

No todas las personas reaccionan igual ante una situación percibida como amenazante o peligrosa, ni todas las personas son igual de vulnerables a sufrir algún tipo de alteración psicológica como consecuencia de ello. Como señalan Robles y Medina (2002), tres serían las variables que intercorrelacionarían, determinando la respuesta del afectado: a) el estresor (la situación de amenaza con sus componentes objetivos, tales como tipo de amenaza, duración, intensidad; y subjetivos, como la percepción e interpretación del suceso por la persona), b) el organismo sometido a la amenaza (historia personal del sujeto, variables tipo estado como antecedentes psiquiátricos previos, variables tipo rasgo, o mecanismos de defensa) y c) las variables ambientales (ej. apoyos sociales y familiares).

Factores como la novedad de la situación (las personas habitualmente no reciben amenazas), la falta de predictibilidad (considerada como el grado en que puede predecirse lo que va a ocurrir), la incertidumbre sobre lo que puede pasar, la ambigüedad que se produce cuando la información sobre la situación (duración, frecuencia, autoría…) no es clara o suficiente, el hecho de que la situación sobrepase los recursos del individuo o que no sepa qué hacer son considerados los principales elementos (estresores) que pueden provocar que la persona perciba la situación como estresante, viéndose negativamente afectada por ella. Estresores, todos ellos, presentes en los comunicados de amenazas, máxime cuando son realizadas por un autor desconocido.

Por tanto, que la persona desconozca quién es el autor de la misiva, qué intenciones tiene, y si estas amenazas realmente van a llevarse a la práctica constituye una importante fuente de distrés[4].

En los casos de amenazas escritas, el anonimato del autor se facilita en gran medida.

Las amenazas pueden ser de muchos tipos. En el caso de las amenazas escritas pueden ser manuscritas, realizadas con composición de recortes, diseñadas ex profeso, mecanografiadas o dactilografiadas. En estos últimos casos además, sobre todo cuando son realizadas mediante máquina de escribir u ordenador, la identificación se dificulta enormemente, ya que, aunque en el caso de las máquinas de escribir es más factible cotejar el documento dubitado con los indubitados de varios sospechosos, respecto a los ordenadores, salvo que la amenaza se haya impreso y pueda apreciarse la micrografía identificativa de la impresora, es harto complejo obtener resultados determinantes para la investigación. En estos casos el estudio lingüístico del mensaje resulta fundamental (Viñals y Puente, 2009).

La lingüística forense, rama de la lingüística aplicada, que se encarga de estudiar los diversos puntos de encuentro entre el lenguaje y la ley y de aportar evidencias lingüísticas en los procesos judiciales; resulta de suma importancia a la hora de analizar las amenazas, particularmente las realizadas de forma escrita.

Así, a través de la sociolingüística, la pragmalingüística, la retórica, el análisis del discurso, la lingüística textual o la computerizada; podríamos obtener un perfil, más o menos completo del autor de la comunicación, una correcta “descodificación” del mensaje emitido, acorde al contexto, así como la identificación de la intencionalidad del sujeto activo, la detección de las estrategias lingüísticas empleadas para la obtención del fin planeado o el grado de influencia o manipulación pretendida y obtenida (Viñals y Puente, 2003).

En el caso de los comunicados amenazantes escritos, se da además otro componente que aparece con menor frecuencia en los comunicados orales o de otro tipo: un nivel más elevado de planificación, preparación y por tanto premeditación, junto a niveles menores de impulsividad, lo que suele generar mayor temor en el receptor de la amenaza, así como, de ser creíble, mayor riesgo de llevarse a la práctica.

4. ANÁLISIS, EVALUACIÓN Y VALORACIÓN DE LAS AMENAZAS

Toda amenaza implica una intencionalidad por parte del sujeto activo de la misma. Así, las amenazas representan un tipo doloso[5], consistente, según se recoge en la Sentencia del Tribunal Supremo de 5 de junio de 2003, en “ejercer presión sobre la víctima, atemorizándola y privándola de su tranquilidad y sosiego, máxime al encerrar un plan premeditado de actuar”.

Las amenazas, bien sean verbales o escritas, pueden perseguir diferentes propósitos:

4 La respuesta de estrés es una reacción inmediata e intensa, que implica la movilización general de los recursos del organismo, para hacer frente a una situación que se percibe como una pérdida, una amenaza, o un reto. Esta respuesta no es nociva (eutrés), salvo que se produzca de forma frecuente, intensa o duradera (distrés).

5 En derecho, se entiende por dolo la voluntad deliberada de cometer un delito a sabiendas de su ilicitud (RAE, 2001).

infundir temor, ya sea por el mero hecho de intimidar a la víctima o para conseguir una acción por su parte que beneficie al amenazador (material o simbólicamente), dar rienda suelta a la ira o la frustración, llamar la atención, demostrar la firmeza de sus intenciones, etc. En cualquier caso, la persona que profiere la amenaza pretende obtener poder sobre el destinatario de esta, que queda bajo su control (Álvarez, et al., 2014).

Pero para que una amenaza sea interpretada y definida como tal, no basta con la intención de su autor. Como señala Storey (1995) las amenazas son intrínsecamente bidireccionales por naturaleza. Es decir, para que una amenaza tenga sentido, para que una amenaza sea considerada una amenaza, debe ser aceptada, o al menos reconocida, por la persona que está siendo amenazada. En otras palabras, el efecto perlocucionario, que es el efecto que el enunciado produce en quien lo recibe, debe ser aceptado o reconocido por el receptor de esa amenaza. Esto, naturalmente, implica que tanto emisor como receptor compartan un contexto (individual y social), que permita una interpretación unívoca de la comunicación como amenazante.

Determinar, por parte de los profesionales, si la comunicación emitida en primer término puede considerarse una amenaza, qué grado de peligrosidad tiene, de serlo, y si es factible y probable que se lleve a la práctica, se convierte en una cuestión harto compleja de resolver, al carecer de protocolos genéricos de evaluación, valoración y, de ser necesario, intervención.

En este sentido, autores como Napier y Mardigian (2003) o Álvarez et al. (2014), coinciden en las líneas a seguir para la creación de un protocolo sólido de análisis y evaluación de los comunicados amenazantes.

Según los citados autores, una vez se concluye que una comunicación plantea realmente una amenaza, se debe identificar de qué tipo es (directa, condicional o indirecta), ya que cada categoría implica diferentes niveles de peligro potencial.

De forma análoga a la clasificación realizada en el Código Penal español, Fitzgerald (2007) emplea una tipología basada en tres tipos de amenazas: directas, condicionales y veladas o indirectas.

Las amenazas directas no están sujetas a condiciones y en su formulación se utiliza un lenguaje explícito, que no da lugar a equívocos, considerándose grave cuando se identifica claramente el tipo de acción amenazada (por ejemplo asesinato, envenenamiento, lesiones) , el método con el que se llevará a cabo la amenaza (por ejemplo efectuar disparos con un arma, envío de sustancias químicas tóxicas o la colocación de una bomba), el objetivo al que va dirigido (una persona o conjunto de personas o una propiedad) y el momento y lugar concretos en que se producirá el incidente.

Por su parte, las amenazas condicionales están relacionadas directa o indirectamente con una demanda y suelen ser formuladas como una proposición sujeta a que la víctima realice la petición solicitada. Este tipo de amenazas son evaluadas como más o menos graves dependiendo de la verosimilitud, el grado de planificación y la cantidad de detalles manifestados sobre la acción amenazada.

Por último, las amenazas veladas, que son las más difíciles de evaluar, suelen tener un tono de advertencia o reproche, utilizándose habitualmente un lenguaje vago e impreciso, con frases simbólicas y, en ocasiones, sin sentido, que dificultan su

identificación y la estimación de su peligro potencial (Álvarez et al., 2014).

Una vez precisado el tipo de amenaza ante la que nos encontramos, es necesario determinar qué probabilidad existe de que el autor ejecute la acción amenazada. Para realizar esta evaluación, la mayor parte de los autores (Rugala y Fitzgerald, 2003; Álvarez et al., 2014) coinciden en utilizar tres designaciones generales del nivel de amenaza: bajo, moderado y alto, en función de la probabilidad estimada de que la amenaza se lleve a término. En este sentido, el FBI, y más concretamente la Unidad de Análisis del Comportamiento[6] (Behavioral Analysis Units, BAU), dispone de un sistema de evaluación del nivel de peligrosidad de una amenaza, consistente en un examen detallado de los elementos fundamentales que la conforman, para valorar su credibilidad y plausibilidad, así como el grado de intención del autor de provocar daño. La estimación de estos aspectos se basa en el estudio exhaustivo de una serie de categorías como el grado de rabia o de frustración expresado en la comunicación amenazante, revelado a través de descripciones gráficas de actos violentos, insultos u obscenidades; la evidencia de personalización o conocimientos específicos sobre la víctima, a través del empleo de nombres propios, direcciones de domicilios o descripción de rutinas, que indican un seguimiento por parte del autor; el grado de detalle de la acción prevista o concreción de la amenaza, mediante detalles específicos sobre la forma en que se producirá el daño, el método que se usará y en qué momento y lugar exactos tendrá lugar el hecho amenazado; el nivel estimado de conocimientos técnicos, sobre armas, sustancias tóxicas o maneras de burlar las medidas de seguridad que posee el autor para llevar a cabo su propósito; el nivel de compromiso potencial del autor, evidenciado por la cantidad de tiempo, esfuerzo y dinero invertido en la amenaza; la ocurrencia de eventos complementarios a las comunicaciones amenazantes, como puede ser el envío de paquetes con contenidos extraños, incidentes de vandalismo o llamadas telefónicas; y la escalada de la intensidad de la amenaza mediante el empleo de un lenguaje amenazante cada vez más duro y explícito o el aumento en la frecuencia de los comunicados.

Como recogen Álvarez et al. (2014), atendiendo al riesgo que un comunicado amenazante puede tener, en el caso de Amenazas de nivel bajo la probabilidad de ejecución estimada es del 25% o menor, por lo tanto, se considera que existe poco riesgo para el destinatario o para terceros. Las amenazas con baja probabilidad de llevarse a cabo suelen estar formuladas utilizando un lenguaje desorganizado, sin sentido o divagante, con frases condicionales, un léxico que suaviza la dureza de la acción amenazada y/o la descripción de acciones inverosímiles o poco razonables. En estos casos no se proporcionan detalles en cuanto al momento o lugar donde ocurrirá la acción, ni se muestra un conocimiento preciso sobre la víctima con detalles que hagan suponer que el autor de la amenaza ha realizado un seguimiento minucioso de la misma.

En cuanto a las *Amenazas de nivel medio*, cuentan con una probabilidad estimada de ejecución en torno al 50%. Una amenaza de nivel medio o moderado es una amenaza que, en general, es más realista y creíble que la de nivel bajo, pero muestra ciertos aspectos que hacen dudar de su veracidad. Se categoriza una amenaza en este

6 La misión de la BAU es proporcionar información sobre el comportamiento del individuo basado en investigación y/o apoyo operacional, mediante la aplicación de la experiencia, la investigación y la formación.

nivel cuando existe concreción sobre la forma en que la víctima va a sufrir la acción amenazada. Las declaraciones de este tipo muestran cierto nivel de planificación de cómo se llevará a cabo la amenaza y el lenguaje empleado es más concreto y descriptivo. La acción relatada es verosímil, evidenciando un plan de ataque viable y conocimientos por parte del autor sobre cómo ejecutarlo. Es común en estas amenazas la utilización de expresiones que tratan de reforzar la seriedad de las intenciones (ej. "va en serio", "no es ninguna broma").

En el caso de las *Amenazas de nivel alto*, la probabilidad de que las amenazas categorizadas en este nivel se lleven a término es igual o mayor a 75%. Las declaraciones amenazantes de nivel alto son muy verosímiles, ya que incluyen una descripción detallada de cómo se ejecutará la amenaza, que demuestra un gran nivel de planificación y preparación logística, un alto grado de familiaridad con el objetivo y su estilo de vida. Es habitual que se incluya el marco de tiempo en el que la acción amenazada va a ocurrir, se establezcan "fechas límite", así como que se preseleccione un lugar de entrega (en el caso de amenazas condicionales) y se constituyen futuros medios de comunicación. Además, la forma de entrega de la amenaza es próxima a la víctima (por ejemplo, el autor deja la carta en el buzón de su casa). En este tipo de amenazas, el alto compromiso manifestado por el autor con su causa se evidencia en la cantidad de tiempo, esfuerzo y dinero invertido en la amenaza (Napier y Mardigian, 2003).

Por lo que al lenguaje empleado en las amenazas se refiere, podemos señalar que otro elemento fundamental en su análisis y valoración son los comportamientos que están estrechamente relacionados con las personas que las realizan, que se manifiestan en sus elecciones léxico-gramaticales a lo largo de sus declaraciones, ya sean verbales o escritas. El comportamiento amenazante se ve reflejado, por tanto, en determinadas categorías gramaticales e indicadores verbales.

El lenguaje varía en función de los condicionamientos verbales de quien lo utiliza y, como ya hemos señalado, disciplinas como la sociolingüística, la pragmalingüística, la retórica, el análisis del discurso, la lingüística textual o la computerizada, pueden resultar de gran ayuda en el análisis, evaluación y valoración de las amenazas. Así, aunque el tema excede la extensión del presente artículo, resulta imprescindible detenerse en la sociolingüística, rama de la lingüística que estudia el uso del lenguaje en el contexto socio-cultural donde se produce.

Como señalan Viñals y Puente (2009), reconocer las marcas lingüísticas, es decir, variedades lingüísticas de una misma lengua relacionadas con factores extralingüísticos como el sexo, la edad, la extracción social, la etnia o el origen geográfico, presentes en todos los niveles del lenguaje (fonológico, morfosintáctico y léxico semántico), permiten elaborar un perfil de personalidad aproximado del autor de la amenaza, que puede ser esencial en la determinación de la autoría de un escrito, su credibilidad y su potencial peligrosidad.

Así, y como marcas lingüísticas más destacadas, nos encontramos con el sexolecto (registro lingüístico determinado por la pertenencia a un determinado género), dialecto generacional (registro por segmentos de edad), dialecto social (macro y micro social), tecnolecto (relacionado con actividades profesionales), dialecto geográfico (variaciones lingüísticas vinculadas a una zona geográfica específica), transferencias o fenómenos lingüísticos producto del contacto entre lenguas (ya sean estos interferencias

o préstamos), etnolecto (registro propio de una etnia), idiolecto (variables lingüísticas personales e identificativas, como los errores, muletillas o las faltas ortográficas) o el dialecto histórico, propio de un determinado periodo.

Varios son los estudios realizados sobre el empleo de cierto lenguaje en los comunicados amenazantes. Ya las primeras investigaciones realizadas por Kent (1967), sobre este aspecto, trataron de determinar el efecto que el lenguaje empleado en las amenazas podía tener sobre el receptor de las mismas, concluyendo que la condicionalidad, ya fuere implícita o explícita, es una característica definitoria de las amenazas. Así, lo explícito de las cláusulas condicionales, a diferencia de lo implícito, reduce al mínimo la posibilidad de malos entendidos entre los sujetos activo y pasivo y por lo tanto aumenta la fuerza de la amenaza. De este modo, cuanto más lingüísticamente completa sea una amenaza condicional (por ejemplo, si no haces X, entonces voy a hacer Y), más creíble será para el destinatario y será más probable que el destinatario acepte la condición.

Milburn y Watman (1981), por su parte, realizaron uno de los primeros exámenes de las amenazas y sus efectos sobre el comportamiento social y verbal. Su trabajo hace hincapié principalmente en los factores extralingüísticos, como el tono de voz y el contexto que lo rodea. Así, si el tono denota enfado o si la amenaza se produce en un contexto de conflicto entre las partes, hay mayor probabilidad de que esta se tome en serio. Del mismo modo, un lenguaje insultante o despectivo, se espera que aumente la intensidad de la sensación de amenaza.

En suma, aun cuando no se ha verificado empíricamente qué papel juegan, se ha planteado que las características gramaticales y léxicas y las funciones generalmente inherentes al lenguaje amenazante incluyen: cláusulas condicionales; marcadores adverbiales o nominales de tiempo; una descripción de la acción amenazada; obscenidades, insultos o lenguaje despectivo; un comportamiento específico de la víctima que merece ser castigado, centrándose en la víctima como se demuestra a través del uso de los pronombres en segunda persona; direcciones o referencias directas y nombres propios; un enfoque en sí mismo como víctima, como se evidencia a través del uso de los pronombres en primera persona; un compromiso con la acción que se pretende realizar, a través de modales de obligación en comparación con el uso del lenguaje de mitigación; marcadores negativos; conjunciones que retractan o mitigan las declaraciones anteriores, en lugar de aquellos que las conjugan; órdenes, preguntas retóricas y términos léxicos que se refieren a la desesperanza, las armas, el suicidio y la fantasía (Gales, 2010).

5. CONCLUSIONES

Quizá, junto a la vida, la libertad sea uno de los bienes más preciados con los que contamos.

Como ya hemos visto, en el caso de las amenazas, esta libertad, bien jurídico del que solo puede disponer su titular, se ve seriamente afectada. Así, a todos se nos presupone una libertad de querer, que permitiría a una persona decidir sobre sus acciones, presentes o futuras sin que su voluntad esté determinada por el querer de otros sujetos o fuerzas ajenas a su voluntad; y una libertad de obrar, que permite a una persona realizar sus propias acciones y llevarlas adelante sin que estas se vean

obstaculizadas. Libertades recogidas en el Título VI del Código Penal, que regula los delitos contra la libertad de las personas, entre los que se encuentran las amenazas. Tema que precisamente nos ocupa en este artículo.

Hoy por hoy, las amenazas son una realidad presente y, lo que es más importante, creciente; en particular aquellas realizadas de forma enmascarada o anónima o en nombre de grupos o colectivos reales o supuestos, legales o ilegales, disimulando la autoría particular de los individuos, y vienen favorecidas por el anonimato que facilita un mundo cada vez más globalizado.

Las amenazas, sean estas realizadas de manera oral, escrita, gestual o mediante cualquier otro tipo de signos o conductas y transmitidas a través de cualquier soporte, canal o medio, suponen graves consecuencias para el receptor de las mismas, que ve quebrado su derecho al sosiego y la tranquilidad personal, al sentimiento de seguridad y a la libertad en la toma de decisiones, sin agentes externos que las limiten o determinen.

Especial gravedad presentan aquellas amenazas realizadas de manera escrita, telefónica o por cualquier medio de comunicación o de reproducción (o en nombre de entidades o grupos), como así queda recogido en el artículo 169.1 del Código Penal español, por entenderse un mayor impacto sobre la libertad del amenazado al tratarse de medios calificados por la jurisprudencia como serios y persistentes. Es en este punto donde el presente trabajo ha tratado de hacer hincapié por su relevancia y, más en concreto, en las amenazas realizadas de forma escrita por autor desconocido.

A la intencionalidad presente en toda amenaza se le une una más que probable preparación, haciendo para el receptor más creíble su contenido y más posible su puesta en práctica. Esto, indudablemente, supone un reto para los investigadores, que desconocen la autoría de la comunicación y, por ende, la personalidad del emisor, que podría aportar una valiosa información de cara a valorar credibilidad y riesgo potencial.

La preocupación que el sujeto pasivo desarrolla se hace extensiva a los investigadores, que deben ser capaces de dar la respuesta rápida que se les demanda, de cara a evitar un daño potencial en la víctima, físico, por supuesto, pero también psicológico.

De esta forma, las implicaciones que las amenazas suponen a todos los niveles hacen necesario el desarrollo de instrumentos efectivos y eficaces, que permitan analizar y determinar su credibilidad, en un primer momento, y valorar el riesgo de que se hagan realidad en uno posterior.

Pocos son los estudios al respecto, mucho menos en lengua española (variable fundamental, como hemos visto) y menos aún los protocolos desarrollados (cabe destacar en este punto el propuesto por Álvarez et al. en 2014, sobre la base de textos en lengua castellana).

La escasez de estudios que permitan la elaboración de protocolos de actuación eficaces, junto con el pobre cuerpo escritural existente actualmente, y su falta de sistematización, son algunos de los problemas que hacen de la valoración y evaluación de las amenazas un objetivo harto complejo. Complejidad a la que habría que añadir las dificultades a la hora de extrapolar las conclusiones obtenidas en otros países con diferente lengua y cultura a la nuestra.

No obstante, el campo sobre evaluación de amenazas es relativamente reciente y las posibilidades para continuar avanzando en esta materia son muchas y muy variadas. Este trabajo ha pretendido precisamente eso. De un lado dar una visión general sobre la problemática de las amenazas en textos escritos realizadas por autor desconocido, de otro servir de acicate para posteriores estudios e investigaciones que completen y enriquezcan los ya existentes, dando así respuesta a las demandas tanto del receptor de las mismas como de los investigadores que las analizan.

REFERENCIAS BIBLIOGRÁFICAS

Álvarez, A. I., Gil, L., y Mena, J. (2014). Valoración de las Amenazas en Textos Escritos. Createspace.

España. (2014). Código penal y legislación complementaria. 40ª Edición. Madrid: Civitas.

Fitzgerald, J. (2007). The FBI‘s Communicated Threat Assessment Database: History, design, and implementation. FBI Law Enforcement Bulletin, 76(2), 1-21.

Gales, T. A. (2010). Ideologies of Violence: A Corpus and Discourse Analytic Approach to Stance in Threatening Communications. California: University Of California.

Kent, G. (1967). The effects of threats. Columbus, Ohio, United States: Ohio State University.

Milburn, T. W., y Watman, K. H. (1981). On the nature of threat: A psychological analysis. New York, United States: Praeger Publishers.

Napier, M., y Mardigian, S. (2003). Threatening messages: The essence of analyzing communicated threats. Public Venue Security, September/October, 16-19.

Real Academia Española. (2001). Diccionario de la lengua española. 22a Edición. Disponible en: http://www.rae.es/rae.html

Robles, J. I., y Medina, J. L. (2002). Intervención Psicológica en las catástrofes. Madrid: Síntesis.

Rugala, E., y Fitzgerald, J. (2003). Workplace violence: From threat to intervention. Clinics in Occupational and Environmental Medicine, 3, 775-789.

Stamatoulous, C. (2014). Enciclopedia Jurídica. Recuperada el 2 de agosto de 2014. Disponible en: www.enciclopedia-juridica.biz14.com.

Storey, K. (1995). The language of threats. Forensic Linguistics, 2(1), 74-80.

Viñals, F. y Puente, M. (2003). Análisis de escritos y documentos en los servicios secretos. Barcelona: Herder.

Viñals, F. y Puente, M. (2009). Grafología Criminal. Barcelona: Herder.

Fecha de recepción: 17/11/2014. Fecha de aceptación: 17/12/2014

PROPAGANDA Y DESINFORMACIÓN EN LAS REDES SOCIALES

EVA MOYA LOSADA

RESUMEN

Esta reflexión pretende sentar unas bases para realizar un análisis previo que ayude a valorar si las campañas de propaganda y desinformación en las redes sociales pueden convertirse en una posible amenaza real a los intereses de nuestro país, no solo desde el punto de vista de un enfoque de seguridad, sino también desde la perspectiva de la Inteligencia Económica. Veremos cómo los últimos acontecimientos nos demuestran que las consecuencias del impacto de estas campañas sobre la sociedad cada vez son más peligrosas. Cabe pensar que la tendencia va en aumento y por lo tanto convendría que estuviera presente en nuestros planes contra posibles amenazas a nuestro país en el futuro.

Palabras clave: Propaganda, decepción, redes sociales, amenazas, Twitter, Facebook, inteligencia económica, seguridad y defensa.

ABSTRACT

These considerations aim to set up a basis for a preliminary analysis as a help for assessing whether the propaganda and disinformation campaigns in social networks can become a possible real threat to the interests of our country, not only from security approach, but also from the perspective of Economic Intelligence. We will be able to identify how recent events show that the consequences of these campaigns impact on society are turning out more threatening. The trend is increasing, therefore it would be wise that these scenarios are considered in our plans against possible threats to our country in the future.

Key words: Propaganda, deception, social network, threat, Twitter, Facebook, economic intelligence, security and defence.

1. INTRODUCCIÓN

Se ha pretendido abordar el tema de la propaganda y decepción en redes sociales a raíz del incremento de la presencia gubernamental internacional directa o indirecta en la Red, entre otros, debido al aumento de los ciberataques y el ciberespionaje con origen en EEUU y China. Actualmente, nos enfrentamos a una Red cada vez más regulada, donde la convivencia entre las diferentes culturas, filosofías y leyes se ha vuelto muy compleja.

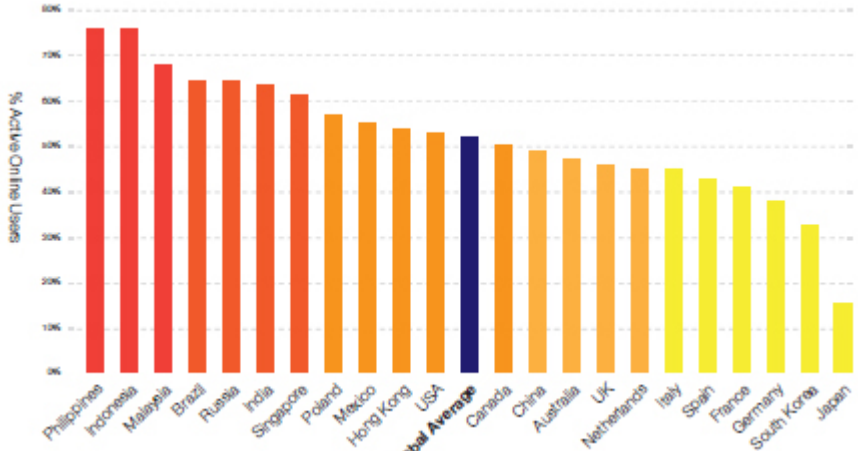
En este sentido, el término “propaganda” en este artículo se refiere a aquellas campañas de comunicación dirigidas a impactar sobre distintos públicos objetivos con la intención de sensibilizarles, hacerles partícipes e incitarles a la acción sobre alguna causa. Estas campañas se particularizan especialmente por un lenguaje emocional que sólo muestra a los públicos objetivos el lado interesado de quienes realizan la

campaña. Por tanto, no se busca informar. En cuanto al concepto “decepción”, lo consideraré como aquellas actuaciones en las redes sociales que buscan engañar, tanto con los mensajes como a través de las cuentas de usuario que lo transmiten.

Si bien es cierto, que para iniciar este camino reflexivo se hace necesario un resumen del estado de la situación actual, en relación al alcance y expansión de las redes sociales, no quiero profundizar demasiado al respecto, pues abundan los informes estadísticos que demuestran que son un fenómeno todavía en expansión y sobre todo en reformulación. Si vemos algunas de las últimas cifras entenderemos que todavía queda mucho camino por recorrer y que, lejos de desaparecer, están evolucionando hacia una nueva etapa, donde la comunicación se convierte ya en un bien innegociable para cualquier ciudadano.

Según el último informe de la Fundación Telefónica sobre la Sociedad de la Información en España, durante el año 2012 se observa que la penetración de las redes sociales crece en 6,5 puntos porcentuales hasta alcanzar el 63,7% de los internautas[1]. Comparando estas cifras con años anteriores, comprobamos que la curva de ascenso en su penetración es cada vez más suave y por tanto podemos llegar a la conclusión que, en España, han dejado tiempo atrás la fase de “tecnología emergente”. Ya no es una manifestación emergente o novedosa, sino que es un fenómeno que se está acercando a ser considerado de “masas”, especialmente si hablamos de los países occidentales y si fijamos nuestra atención en las jóvenes generaciones. En nuestro país no hay adolescente que no tenga una cuenta en Facebook, Tuenti o Twitter. Cabe recordar que los jóvenes de hoy serán los adultos que tomen las decisiones de mañana. Por eso es vital entender cómo se relacionan con este medio.

Por otro lado, si observamos el resto de los países del mundo, podemos comprobar que se enfrentan a una situación bastante similar a la española. Aunque de 2011, y seguramente con porcentajes aproximativos, el informe sobre penetración de las redes sociales[2] de la consultora Global Web Index muestra cómo los usuarios conectados en todo el mundo a las distintas plataformas sociales superan ya el 50% de su población.



Fuente: Global Web Index. **Global Social Network Penetration**

1 FUNDACIÓN TELEFÓNICA. La Sociedad de la Información en España en 2012, Madrid: Editorial Ariel, 2013, p. 12.

2 GLOBAL WEB INDEX. Global Map of Social Networking. 2011. http://globalwebindex.net/wp-content/uploads/downloads/2011/06/Global-Map-of-Social-Networking-GlobalWebIndex-June-20112.pdf.

Los usos siguen siendo diversos. Pero, en términos generales, podemos señalar dos que destacan muy por encima de los demás cuando se les pregunta directamente a los usuarios[3]: Facebook se utiliza básicamente para estar en contacto con los amigos y conocidos, mientras que Twitter tiene una finalidad meramente informativa, como si de un periódico o pase de teletipos se tratase.

Si hemos hecho este pequeño resumen de la situación actual es porque conocer en profundidad los canales y su público objetivo nos permitirá determinar las amenazas reales que pueden venir a través de ellos.

Así pues, en este sentido, podemos comenzar a extraer algunas pequeñas conclusiones iniciales, como por ejemplo que Facebook es la red social favorita para establecer relaciones y que, por lo tanto, puede ser el canal ideal a través del cual grupos terroristas y activistas peligrosos se acerquen directamente al usuario para dar a conocer sus ideologías e incluso organizar y coordinar sus futuras actuaciones. Además, Facebook puede ser una magnífica herramienta para formar a futuros miembros de estos grupos y realizar acciones de captación.

Mientras, por otro lado, aprovechando que Twitter es la red social informativa por excelencia, puede ser utilizada para poderosas campañas de desinformación, manipulando a la opinión pública de las redes con todo tipo de contenidos, y de ruido buscando incluso distraerla en un momento dado de cuestiones más importantes o sensibles. A este respecto los hashtag (palabras clave entorno a las cuales se organizan los contenidos de Twitter y que van señaladas con el símbolo “#”) podrán ser utilizados como semillas para realizar campañas de propaganda de cualquier tipo e incitados correctamente a la viralización pueden convertirse en Trending Topic (TT) en menos de 24 horas, para obtener un mayor alcance a muy bajo coste. A día de hoy quienes más han sufrido este tipo de ataques han sido grandes compañías como, por ejemplo, Nestlé en la crisis del aceite de palma. Fue cuando Greenpeace detectó que uno de sus proveedores participaba en la deforestación de los bosques de Indonesia, afectando a la supervivencia de los orangutanes que vivían en ellos, y consideró oportuno lanzar una fuerte campaña de propaganda en las redes sociales para incitar a los consumidores a dejar de consumir Kit Kat[4] y forzar un cambio en la política medioambiental de la compañía.

Si bien las grandes noticias vinculadas a las crisis en redes sociales han dado lugar a expresiones del tipo “las redes sociales cargan tintas contra...”, “crisis en las redes sociales...”, etc. Es fundamental comprender que son meras plataformas o herramientas de comunicación y que, cuando se utilizan este tipo de expresiones, se hace referencia al contenido que hay en ellas.

Quiero profundizar a continuación sobre esta idea, pues nos obliga a entender mejor cómo funcionan y por dónde pueden venir las vulnerabilidades asociadas a ellas.

3 THE COCKTAIL ANALYSIS. 5ª oleada del Observatorio de Redes Sociales, 16 de abril de 2013, p12. http://es.slideshare.net/TCAnalysis/5-oleada-observatorio-redes-sociales

4 GREENPEACE. Nestlé and palm oil, 17 de marzo de 2010. http://www.greenpeace.org.uk/nestle-palm-oil

2. LAS REDES SOCIALES SON HERRAMIENTAS, NO CONTENIDOS

El lenguaje es uno de los grandes avances del ser humano. Gracias a él podemos comunicarnos y, a veces, hasta entendernos. El lenguaje es algo vivo que nos acompaña a lo largo de toda nuestra vida, desde que balbuceamos nuestras primeras palabras. Es, pues, un compañero que nos apoya en nuestras relaciones personales y profesionales.

En un contexto tan cambiante como el actual, y ante la celeridad en la aparición de nuevas tecnologías, el lenguaje se adapta en la formulación de conceptos para describir nuevos contextos y nuevas herramientas.

Si queremos profundizar en el estudio de la comunicación online es imprescindible conocer varios aspectos propios de la naturaleza de Internet. Saber, por ejemplo, cómo funcionan aquellas aplicaciones a través de las cuales puede realizarse una campaña de propaganda o de decepción nos permite prever cómo pueden ser originadas, sus puntos fuertes y sus puntos débiles para ser contenidas, etc. Pero, eso sí, no debemos confundir la herramienta que nos ofrece múltiples opciones creativas, con el contenido que se transmite a través de ellas.

2.1. EL ENTORNO “WEB 2.0”

La web 2.0 es un concepto nacido de una tormenta de ideas en el FOO Camp de 2004. Surge de la mano de Tim O´Reilly, ferviente impulsor del software libre y código abierto, para definir la nueva generación de software que aparecía en Internet en aquellos años. Por aquel entonces se percibía que algo había cambiado en la gran Red y se analizaban nuevos modelos de negocio que estaban apareciendo con bastante éxito y que nada tenían que ver con la etapa anterior, uno de ellos por ejemplo es la conocida tienda online Amazon.

“Tú controlas tu propios datos” [5] es la clave del meme que resume la tormenta de ideas de O´Reilly Media y que nos interesa especialmente para este artículo. Porque en la nueva Internet nosotros decidimos qué datos publicamos o qué información compartimos, aunque la mayoría de las veces subamos a las redes sociales de forma espontánea cualquiera de nuestros comentarios derivados de nuestro estado emocional del momento. A este respecto, hoy día hay abierto un debate muy importante sobre la privacidad de los individuos en estas plataformas. Debate en el que no vamos a entrar a reflexionar en este documento, porque su extensión bien daría lugar a un monográfico.

A medida que se avanzaba en las reflexiones sobre la evolución del mundo de Internet, el propio O´Reilly desveló en ocho claves las bases que definirían los modelos de negocio web 2.0 de hoy en día (2006: O´Reilly). De estas ocho claves he querido resaltar aquellas que afectarán directamente al comportamiento del usuario, que es quien en la mayoría de los casos genera el contenido, a través de sus consultas o compartiendo cualquier tipo de información.

Veamos tres de las ocho claves que he decidido vincular a tres elementos fundamentales que facilitan el éxito de las redes sociales como herramientas de

5 O´REILLY, Tim. Design Patterns and Business Models for the Next Generation of Software, 2005. http://oreilly.com/pub/a/web2/archive/what-is-web-20.html?page=1#mememap

comunicación y que, por tanto, convienen a nuestro objeto de reflexión:

1. Aprovechamiento de la Inteligencia Colectiva – Participación. Los desarrollos tecnológicos en Internet en los últimos años contemplan estructuras que facilitan la interpretación de los datos y metadatos generados por los usuarios. Es por ello que este tipo de software fomenta la participación y la interacción, volviendo la Red más democrática y social. Son los propios usuarios los que comparten, intercambian, debaten, etc. Cuanta más información, más interesante se volverá la herramienta. Un ejemplo claro es la Wikipedia.

2. Enriquecimiento de las experiencias de usuario – Facilidad en la comunicación. Los usuarios se están adaptando rápidamente a las nuevas posibilidades de las aplicaciones en Internet, evolucionando con ella y demandando constantemente mejoras y nuevas opciones, a cada cual más creativa. El caso de Pinterest es otro ejemplo claro de cómo un cambio en la distribución de contenidos publicados en una red social puede agilizar y enriquecer la comunicación. Desde su aparición son ya varias redes sociales las que están copiando su estructura. Importante es también hablar de los nuevos formatos en los que se "encapsula la información". La posibilidad de compartir vídeos en Youtube ha demostrado cómo los formatos multimedia vuelven mucho más atractivo cualquier contenido llegando a generar más de varios billones de vídeos visitados al día en todo el mundo.

3. Software por encima del nivel de un dispositivo único – O Internet ubicua[6]. Sin límites temporales ni espaciales. Los avances en las telecomunicaciones y los dispositivos móviles han favorecido el salto de Internet más allá de las fronteras marcadas por el ordenador de mesa. Los usuarios pueden acceder a una misma aplicación desde cualquier tipo de dispositivo en cualquier momento y lugar. Por ejemplo, podemos consultar nuestro email desde cualquier dispositivo que tengamos a nuestro alcance.

2.2. LA TECNOLOGÍA DE LAS REDES SOCIALES COMO PUERTA DE ENTRADA A LA PROPAGANDA Y LA DESINFORMACIÓN

La primera red social virtual surgió en 1997 bajo el nombre de SixDegrees aludiendo al relato "Chains" de Frigyes Karinthy para sugerir una aplicación práctica derivada del concepto desarrollado años después por el sociólogo Duncan Watts sobre la posibilidad de estar conectados con cualquier persona del planeta en seis "saltos relacionales". Por aquel entonces, la primera red social, aunque limitada, ya contemplaba la creación de perfiles personales que se podían conectar entre sí.

Aunque SixDegrees se mantuvo abierta sólo unos años, le siguieron otras como MySpace u Orkut, que demostraron que este tipo de plataformas tecnológicas podían llegar a conectar a millones de usuarios en todo el mundo sin demasiados problemas ni limitaciones.

Finalmente, y más de nuestros tiempos, podemos disfrutar de herramientas como Facebook, Twitter, Youtube, Instangram o FourSquare.

6 BIRKENBIHL, Klaus; QUESADA, Encarna y PRIESCA BALBÍN, Pablo. Presente y futuro de la world wide web, Madrid: Novática, Revista de la Asociación de Técnicos de Informática, 2009, nº197, p.5.

Estas nuevas redes sociales son plataformas donde cualquier individuo, desde cualquier parte del mundo y de forma anónima, puede inyectar en la Red global cualquier contenido en forma de textos, imágenes, fotografías, animaciones, vídeos, urls, geoposicionamientos, códigos QR, videojuegos, etc.

Pero estas herramientas tienen dos debilidades, entre otras, que pueden motivar y facilitar especialmente actuaciones propagandísticas o de desinformación.

La primera de ellas, que trataremos brevemente, es la posibilidad de vivir en el anonimato. Contrariamente a lo que sucede con un email, las IP de los perfiles creados en redes sociales no se pueden rastrear directamente hasta el usuario (salvo aquellas en las que el propio usuario ha decidido "geolocalizarse"), sino que el resultado nos llevará a Silicon Valley o a cualquier otro lugar relacionado con las IP propias de las plataformas que estamos intentando rastrear. Es por ello que muchos perfiles mal intencionados utilizan sus cuentas de usuario anónimas para realizar amenazas, generar bulos o incluso funcionan como malware. Por tanto, lanzar una campaña de propaganda y/o desinformación a través de estas plataformas puede tener cierta cobertura de anonimato si se desea, al menos en sus comienzos.

Por otro lado, este anonimato puede ser más o menos mantenido y organizado mientras las conversaciones entre los coordinadores de la campaña sean privadas. Por tanto es un medio mucho más seguro que la comunicación vía email. Por ello, el gobierno americano lleva tiempo solicitando a estas grandes compañías informaciones propias de usuario que pueda ayudarles a obtener más información como parte de una estrategia global de ciberespionaje ordenada por el presidente Barack Obama[7], en la que no quieren que se les escape nada.

La segunda de las vulnerabilidades vamos a abordarla con más profundidad por las consecuencias que puede generar.

Los ciberataques a las cuentas de usuario como vía para las campañas de propaganda y decepción.

Una de las vulnerabilidades tecnológicas principales de estas herramientas y que se está utilizando a día de hoy, especialmente para campañas de desinformación, es el pirateo de cuentas de usuario.

Llevamos unos años ya conociendo, a través de los medios de comunicación, cómo piratas informáticos se introducen en cuentas de Facebook o Twitter para falsear los mensajes de sus usuarios. Las víctimas favoritas: artistas y personajes relevantes como futbolistas, del mundo de la farándula, etc. Pero en los últimos tiempos también los políticos, como le ha pasado al presidente Maduro en Venezuela[8], al que Anonymous ha metido en varios apuros.

Cuando nos enteramos que la cuenta de Twitter de un actor o cantante famoso ha sido vulnerada puede incluso hacernos gracia o despertar cierta simpatía. El impacto,

7 Obama tells intelligence chiefs to draw up cyber target list – full document text, The Guardian, 7 de junio de 2013. http://www.guardian.co.uk/world/interactive/2013/jun/07/obama-cyber-directive-full-text

8 Piratean de nuevo la cuenta de Nicolás Maduro en Twitter, CNN España, 12 de mayo de 2013. http://cnnespanol.cnn.com/2013/05/12/piratean-de-nuevo-la-cuenta-de-nicolas-maduro-en-twitter/

dependiendo del mensaje, no va más allá de una sorpresa, enfado y unas disculpas del propietario real cuando es consciente de que le han robado su identidad.

En este sentido, uno de los últimos ejemplos que puede parecer trivial, porque muestra el poder de este tipo de actividades, fue otro de los llevados a cabo por Anonymous. Aprovechando la rivalidad, conocida a nivel mundial, entre los dos gigantes de comida rápida McDonalds y Burger King reventó la cuenta de Burger King y la personalizó como si fuera de McDonalds.

Así quedó Burger King después de que Anonymous entrara en ella. "*Burger King ha sido vendida a Mc Donalds porque la whopper es un fracaso*".

Fuente: BurgerKing Twitter

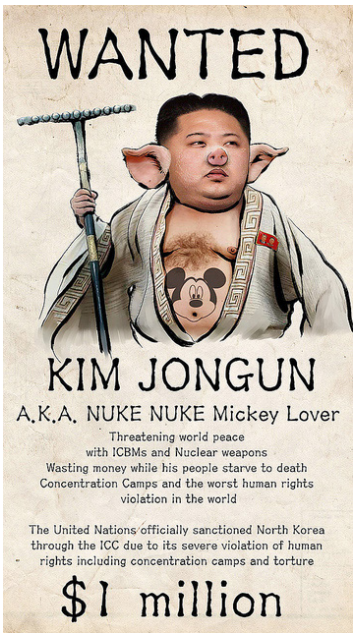
Por suerte, no tardaron demasiado tiempo en darse cuenta y retomar el control de la situación. Y para evitar tensiones derivadas de un choque entre rivales, la propia McDonalds se solidarizó con Burger King contestando con un mensaje neutral en tono de humor. Finalmente todo acabó como una pequeña broma sin consecuencias demasiado graves.

Pero, ¿qué ocurre cuando las cuentas pirateadas son de perfiles tan relevantes como políticos, organizaciones o agencias de comunicación? ¿Cuáles pueden ser los riesgos y/o amenazas?

Quizá el lector pueda pensar que las consecuencias tampoco serían demasiado graves. Ciertamente hay casos dirigidos simplemente a dañar la reputación como le sucedió a Kim Jong en abril de 2013. Como consecuencia del aumento de la tensión entre Corea del Norte y la comunidad internacional, la cuenta en Twitter @uriminzok utilizada por el gobierno Coreano para realizar sus propias campañas de propaganda[9] fue pirateada[10] con mensajes e imágenes como la siguiente.

9 North Korea using Twitter for propaganda, The Sidney Morning Herald, 15 de agosto de 2010. http://www.smh.com.au/technology/technology-news/north-korea-using-twitter-for-propaganda-20100815-1250u.html

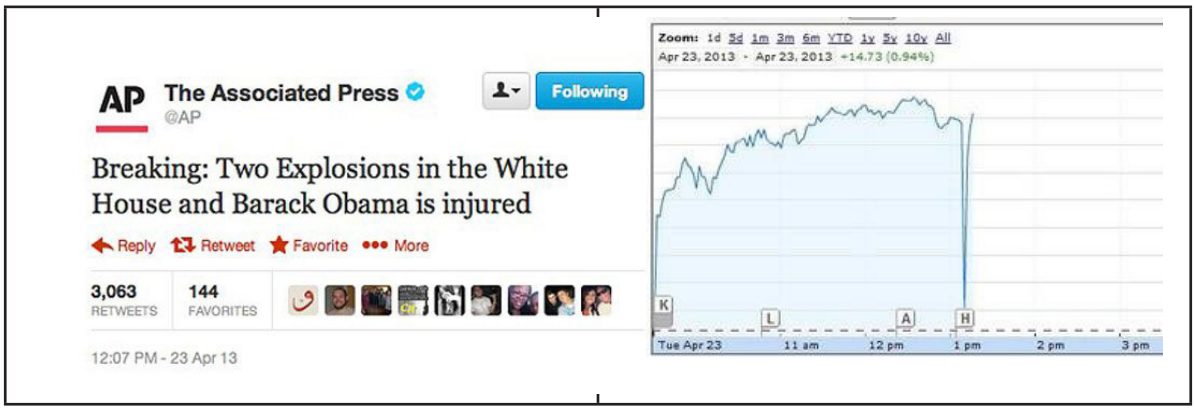
10 LEE, Youkyung. NKorea's Twitter account hacked amid tension, The Associated Press, 4 de abril de 2013. http://bigstory.ap.org/article/nkoreas-twitter-account-hacked-amid-tension



Fuente: Twitchy.com[11]

Evidentemente, este ciberataque no va más allá de una mofa internacional que puede haber herido más o menos el orgullo de los norcoreanos.

Sin embargo, ya tenemos un primer caso más serio. Sucedió después de que el perfil en Twitter de la agencia de noticias AP fuera pirateado por los autoproclamados Syrian Electronic Army (SEA). El siguiente mensaje "*Dos explosiones en la Casa Blanca. Obama está herido*" generó el pánico en Wall Street durante unos pocos segundos, hasta que se confirmó la falsedad de la noticia. Inmediatamente después se recuperó la normalidad. Sin embargo, el gráfico de la caída del Dow Jones cuando saltó la noticia falsa refleja muy bien los efectos que este tipo de ciberataques pueden provocar en la sociedad. ¿Somos conscientes que por un segundo se perdieron 145 puntos en el índice bursátil más referenciado del mundo?



Fuente: La Vanguardia[12]

11 Hacking of North Korea's Twitter and Flickr accounts includes pic of Kim Jong Un with a snout, Twitchy, 4 de abril de 2013. http://twitchy.com/2013/04/04/hacking-of-north-koreas-twitter-and-flickr-accounts-includes-pic-of-kim-jong-un-with-a-snout/

12 FORT, Màrius. 'Minicrash' en Wall Street por un falso tuit sobre un atentado contra Obama, La Vanguardia, 24 de abril de 2013. http://www.lavanguardia.com/economia/20130423/54372747540/minicrash-wall-street-hackeada-cuenta-twitter-associated-press.html.

Como hemos comentado anteriormente Twitter se ha convertido en los últimos años en una fuente de información relevante gracias a su flexibilidad, frescura e inmediatez. Prueba de ello es que, un año más, el uso de esta red social por parte de periodistas ha aumentado. Según el 6º Informe de la consultora Oriella, en 2012 el número de periodistas que usaban Twitter era del 47%, mientras que en 2013 ya es un 59%[13]. Es evidente que situaciones vividas como las revoluciones del mundo árabe o la catástrofe del terremoto de Chile han empujado al sector de la información a adaptarse a este nuevo medio.

Así pues, miles de profesionales viven pendientes de lo que se comenta y se anuncia en esta red social. Incluso los analistas de inteligencia estamos aprendiendo a utilizar este nuevo recurso como fuente de información para nuestros informes basados en OSINT (Open Source Intelligence).

Si bien es cierto que actualmente Twitter trabaja en un sistema de doble contraseña para reforzar la seguridad de sus cuentas de usuario, no debemos dejar todo el peso de la seguridad sobre la plataforma tecnológica.

Cabe preguntarse si desde la comunicación corporativa, tanto pública como privada, en nuestro país se contemplan estas situaciones como amenazas potenciales que podrían darse en un momento dado. ¿Qué ocurriría si la cuenta en Twitter de la Policía Nacional (@policía) pudiera ser pirateada y emitiera un mensaje que incitara al pánico? Actualmente es una cuenta que siguen más de 400.000 seguidores. ¿Imaginamos el impacto y la velocidad de viralización que tendría en toda la Red? Evidentemente hay cuentas más o menos fáciles de piratear en función de lo cuidadosos que sean sus gestores. Pero considero que es algo que debemos contemplar y profesionalizar en nuestros planes de crisis de comunicación y/o reputación, especialmente en relación a cuentas sensibles de nuestro país en las redes sociales.

3. NUEVOS ACTORES, NUEVAS ESTRATEGIAS

El éxito demostrado en el aumento de la visibilidad derivada de una buena presencia en las redes sociales ha generado una aparición de nuevos actores que no se había visto hasta hace muy poco tiempo. Seducidos ante la posibilidad de llegar a más gente con unos costes relativamente bajos han decidido apostar por dedicar tiempo y recursos a estas plataformas.

Un interesante ejemplo del uso de Twitter como canal de comunicación gubernamental fue protagonizado por el gobierno egipcio, de los Hermanos Musulmanes, cuando utilizaron una de sus cuentas de Twitter para darle un tirón de orejas público al Departamento de Estado de los EEUU por lo que ellos consideraban una falta de respeto a la religión musulmana, a raíz de unos comentarios satíricos realizados por la portavoz Victoria Nuland contra Bassem Youssef y las religiones. La peculiaridad no es sólo el contenido del mensaje, sino el hecho de ver cómo Los Hermanos Musulmanes de Egipto utilizan los códigos de Twitter para dirigirse al gobierno americano, llegando a mencionarle directamente a través de la "@" e incluyendo un hashtag bastante popular como es el #FJP (Freedom and Justice

13 ORIELLA PR NETWORK. Global Digital Journalism Study 2013. http://www.oriellaprnetwork.com/research

Party) para hacer todo el ruido posible con la esperanza de convertirlo en un tweet viral.

Fuente: Ikhwanweb Twitter

Cabe preguntarse qué pasaría si un gobierno cualquiera decidiera emitir a través del social media cualquier mensaje mencionando a nuestro país. ¿Tenemos los protocolos y recursos para responder? Quizá a día de hoy nos parezca que esto nos queda lejos. Pero la evolución de la tendencia es evidente: muchos gobiernos del mundo, no sólo presidentes o corte política, ya tienen su propia voz en Twitter para hablar cara a cara con los ciudadanos, sin intermediarios de ningún medio de comunicación que reinterprete sus palabras. ¿Cómo respondería la cuenta de uno de nuestros ejércitos si recibiera una crítica a través de las redes sociales acusándole de bombardear a civiles despiadadamente? Podría ser perfectamente parte de una campaña contra la presencia de la OTAN surgida en cualquiera de los países en los que estamos presentes. Por tanto ni siquiera España tendría que ser el objetivo final de la campaña. Evidentemente nos pondría en un aprieto si los medios de comunicación lo convirtieran en noticia hasta que se demostrara la falsedad.

Ahora bien, en este tipo de medios, la premura es vital. ¿Estamos preparados como país para escuchar lo que se dice de nosotros en las redes sociales? Y recordemos que no estar en las redes con cuentas de usuario gubernamentales ya no es una defensa, incluso puede considerarse un posible riesgo, puesto que el ataque viene por este canal y habrá que saber canalizarlo a través de él.

Sin duda, uno de los países que hoy por hoy utiliza la estrategia más agresiva en la gran Red, y que es un ejemplo claro de propaganda, es la que lleva ya tiempo realizando el estado de Israel. Además de haberse tomado muy en serio la formación de una unidad de ciberguerreros[14], ha optado por utilizar varias de sus cuentas de Twitter como canales de propaganda, cubriendo las 24 horas del día Twitter con mensajes de todo tipo y en todos los idiomas, con la intención de llegar a cualquier rincón del mundo virtual. Como podemos ver en estos dos ejemplos de tweets sus campañas son realmente muy directas.

14 GREENWOOD, Phoebe. Israel invests millions in drive for elite 'cyber warriors', Telegraph, 1 de noviembre de 2013. http://www.telegraph.co.uk/news/worldnews/middleeast/israel/9648820/Israel-invests-millions-in-drive-for-elite-cyber-warriors.html

Fuente: FDIonline y IDFSpokesperson Twitter

Hasta ahora hemos hablado de gobiernos como nuevos actores. Pero también podemos hablar de políticos o presidentes. En este sentido otro gran personaje con presencia relevante en las redes sociales, especialmente en Facebook, es la actual presidenta de Argentina Cristina Fernández Krichner, una gran fan del social media, de hecho su influencia en Klout pasa de los 80 puntos[15], un valor de influencia en los medios sociales muy elevado. Conocedora de este tipo de medios, mantiene sus cuentas de Twitter[16] y Facebook[17] muy activas y las utiliza para dar su punto de vista sobre todo lo que sucede en Argentina. Puede que desde España nos resulte extraña la hiperactividad que demuestra en la Red, sin embargo no podemos negar que le da muy buenos resultados. Hace poco tuvo que asumir varias críticas por su gestión en las recientes inundaciones. Aprovechando que una de ellas le había llegado a través de su cuenta en Facebook, decidió contestar públicamente sabiendo que tendría un impacto sobre su reputación mucho más elevado que haciendo un simple comunicado gubernamental. Frases del tipo "Quiero contarte que llegamos a las familias del Arroyo Maldonado gracias a tu mensaje del sábado", "El responsable del grupo es Horacito [...], hijo de detenidos desaparecidos. Nunca conoció ni conocerá a sus padres" demuestran que la señora Krichner es una gran conocedora de la comunicación en este tipo de plataformas. Además, aprovechó para utilizar fotografías que demostraban cómo había respondido inmediatamente con hechos, no sólo palabras. En definitiva, convirtió una situación que podía haber dañado su reputación en otra de la que salió todavía más reforzada.

15 http://klout.com/#/CFKArgentina
16 @CFKArgentina
17 https://www.facebook.com/CFKArgentina

Fuente: Captura del Facebook de Cristina Fernández Kirchner

El propio Barack Obama nos ha sorprendido hace meses utilizando en varias ocasiones el Hangout de Google para charlar directamente con los ciudadanos[18]. Y no es el único que usa las redes sociales para hablar a los ciudadanos. Mohamed Mursi ha utilizado varias veces el Facebook oficial para dar su opinión y defender su posición ante los ciudadanos y gobiernos extranjeros[19].

¿Y qué podemos decir de las organizaciones Internacionales? Ellas tampoco quieren desperdiciar la oportunidad de llegar a los ciudadanos directamente, sin intermediarios.

Uno de los mejores ejemplos de que las cosas están cambiando es que, hace muy poco, la propia OTAN ha decidido dar el salto a la Red creando su propio punto de encuentro en las redes sociales, como por ejemplo a través de la creación de un canal propio en Youtube, donde muestran ejemplos de sus campañas y su labor "más social".

Aunque evidentemente exponerse a luz pública a través de las redes sociales significa un riesgo igual para todos. Las grandes organizaciones internacionales son igual de vulnerables. Por ejemplo, la ONU, que lleva tiempo familiarizándose con estas plataformas, ha tenido que lidiar recientemente con una pequeña situación embarazosa que sufrió a través de su cuenta de Twitter, una cuenta que utiliza para informar al mundo de sus actividades. Los investigadores, decididos a analizar a quién consideran perfiles de influencia, es decir, de referencia, descubrieron que junto a personajes relevantes de

18 Watch: President Obama Answers Your Questions in a Google+ Hangout, The White House, 14 de febrero de 2013. http://www.whitehouse.gov/blog/2013/02/14/watch-president-obama-answers-your-questions-google-hangout

19 El presidente de Egipto anuncia en Facebook que "no aceptará renunciar de forma humillante", La información, 3 de julio de 2013. http://noticias.lainformacion.com/mundo/el-presidente-de-egipto-anuncia-en-facebook-que-no-aceptara-renunciar-de-forma-humillante_blz5yKmELt9Tj5aiVclFj6/

la política Internacional había una actriz porno llamada Penelope Black Diamond[20]. Por lo visto el community manager (cm) se había equivocado pensando que estaba usando su cuenta personal. Posiblemente al utilizar algún gestor de cuentas como HootSuite. El incidente finalizó eliminando de la lista a la actriz y despidiendo al cm.

Como estamos viendo, poco a poco políticos, gobiernos y organizaciones internacionales van haciéndose un hueco con la intención de acercarse a los ciudadanos y abrir un canal donde poder hablar con su propia voz.

Así pues, en este sentido observamos por tanto una tendencia bastante interesante que he preferido resumir en el cuadro que he elaborado y que muestro a continuación. Como decía, gracias al éxito en la visibilidad de las redes sociales han ido apareciendo nuevos actores con mayor relevancia mundial, dispuestos a establecer sus propias estrategias para utilizar estas plataformas para sus propios intereses y considero que en nuestro país se debería hacer una profunda reflexión al respecto. Además, como hemos visto, algunos de ellos están totalmente dispuestos a utilizar estas plataformas como canales de propaganda y desinformación. En los inicios de la web 2.0 sólo los individuos eran capaces de aprovechar todo lo que podían ofrecer estas herramientas, sin embargo desde 2009 aproximadamente organizaciones muy diversas utilizan este nuevo medio de comunicación en sus relaciones públicas.

Fuente: Elaboración propia[21]

4. EL LADO OSCURO EN LAS REDES SOCIALES

Ahora que conocemos un poco mejor el contexto en el que conviven los usuarios que participan de las redes sociales, y cómo estas herramientas pueden ser utilizadas

20 ORTIZ, Alex. La ONU sigue a una actriz porno en su cuenta oficial de Twitter, ABC, 7 de mayo de 2013. http://www.abc.es/tecnologia/redes/20130507/abci-pornstar-twitter-201305071614.html

21 Para fechar los comienzos de la web 2.0 se ha utilizado el bautismo del concepto por parte de O´Really. Para fechar la entrada en las RR.SS de las empresas se ha usado el momento de creación de los perfiles en Twitter de las grandes compañías The Coca-Cola Company y Disney y la cuenta de The White House. Por último, se ha utilizado la cuenta en Twitter de Obama como principal representante político con presencia en RR.SS.

para la propaganda, es el momento de abordar el lado más oscuro, falto de ética o incluso peligroso en un momento dado para un estado y sus ciudadanos. Comenzaré por cómo se traspasa la línea ética en las redes sociales desde el mundo de la empresa para derribar a la competencia. Algo que bien podría sucederle a cualquiera de las empresas españolas en un momento dado.

4.1. La desinformación en el mundo de la empresa.

Como venimos comentando desde el principio del artículo, el Social Media se caracteriza por ser una plataforma virtual donde todo el mundo puede hablar de lo que le apetezca.

En este sentido, uno de los grandes avances ha sido la posibilidad de opinar sobre un determinado producto o servicio, con la intención de crear un halo de confianza y transparencia sobre él. La Red se ha plagado de barras de estrellas a través de las cuales puntuar, por ejemplo, ese libro que hemos leído, ese hotel que hemos visitado, ese producto que hemos probado, etc. Y en algunas ocasiones, además de las barras de estrellas, tenemos la opción, incluso, de comentar directamente lo que nos ha parecido. Llegados a este punto me gustaría lanzar una pregunta, ¿cuántos de nosotros miramos los comentarios sobre un hotel cuando estamos buscando en Internet dónde alojarnos en nuestras vacaciones?.

Las empresas lo saben. Saben que el nuevo consumidor (prosumer) ya no se fía de la información que da la compañía y toma la decisión de compra guiado por las opiniones de otras personas, incluso aunque no las conozca.

Si bien desde el ámbito empresarial se habla con frecuencia de buenas prácticas en las redes sociales, no conviene hacer oídos sordos a la realidad. Una realidad que demuestra que en numerosas ocasiones, y puesto que borrar un comentario genera más problemas que mantenerlo, se siembran cientos de comentarios falsos por toda la Red. Con dos intenciones:

- Reforzar la visibilidad de un producto o servicio con comentarios positivos.
- Destruir la reputación de la competencia con comentarios negativos.

Un ejemplo de la segunda intención, relativamente reciente, es el caso de Samsung, que deseoso de empujar las ventas de su gama de los Galaxy, contrató a varios estudiantes universitarios para que hablaran mal y en falso sobre los productos de su competencia directa HTC en las redes sociales. Samsung fue descubierto y tuvo que verse ante la vergüenza de tener que pedir disculpas públicamente[22].

Lamentablemente este no es el único caso. Debido al peso reciente que tienen las redes sociales sobre las ventas o sobre el valor reputacional de una compañía, hay quien recurre a este tipo de prácticas sin demasiadas reflexiones. Y las empresas españolas pueden verse afectadas en un momento dado por un ataque de estas características.

4.2. Las Redes Sociales para las organizaciones vinculadas a defensa y seguridad.

22 Samsung probed in Taiwan over ‘fake web reviews’, BBC News, 16 de abril de 2013. http://www.bbc.co.uk/news/technology-22166606

Aunque en este artículo se aborda sólo el enfoque de las redes sociales desde el punto de vista de la difusión, considero de interés mencionar, por lo menos, que como herramientas de comunicación puede servir a los analistas de inteligencia y a las organizaciones vinculadas a defensa y seguridad desde muchos puntos de vista. Para demostrarlo, conjuntamente con J. M. Blanco Navarro (Guardia Civil), elaboramos un cuadro basado en un análisis SWOT. Nuestra intención: mostrar a simple vista cómo las oportunidades son mucho mayores que las amenazas y que, por tanto, pueden ser tenidas en cuenta como herramientas muy interesantes y económicas para alcanzar distintos objetivos dentro del ámbito de la seguridad y la defensa.

	INTERNO	**EXTERNO**
POSITIVO	***FORTALEZAS***	***OPORTUNIDADES***
	- Coste - Inmediatez - Sencillez - Interactividad - Ubicuidad - Velocidad - Transparencia - Comunicación y diálogo - Diversidad - Movilidad - Difusión - Sin limitación horaria - Fácil de compartir con el equipo	*Estratégicas:* - Información - Comunicación - Participación - Cultura de seguridad - Gestión del conocimiento - Inteligencia colectiva - Gestión de marca/reputación - Formación - Compromiso con los ciudadanos - Open Government - Transparencia - Comunicación interna - Influencia - Vía de cambio y valor *Operativas:* - Gestión de crisis y emergencias - Inteligencia e inteligencia colectiva. - Monitorización de información - Investigación policial. Perfiles. - Predicción
NEGATIVO	***DEBILIDADES***	***AMENAZAS***
	Relativas a características de social media: - Barreras de entrada - Adaptación al medio y miedo al descontrol de las oportunidades - Cambio veloz - Descentralización - Volumen - Ruido - En algunos casos falta de madurez *Relativa a su gestión:* - Falta de formación - Infravaloración - Falta de tiempo - Falta de personal y recursos - Gestión del error - Incapacidad para la gestión e integración de todo el conocimiento *Relativa a clásicos debates:* - Debate público-privado - Debate libertad-seguridad - Debate transparencia-secreto	*Relativas a la información:* - Infoxicación - Manipulación - Credibilidad y fiabilidad - Bots - Múltiples capas y puntos de vista *Relativa a características de social media:* - La parte negativa de las fortalezas - Imposibilidad de control - Sobrevaloración - División digital de los ciudadanos - Limitaciones de la comunicación *Relativas a seguridad:* - Viejos y nuevos delitos - Ingeniería social - Intimidad - Seguridad informática - Seguridad física - Uso terrorista y extremismo - Procesos maliciosos de influencia

Fuente: Modelo Moya-Blanco sobre la utilidad de las redes sociales desde el punto de la seguridad y la defensa.

Hablemos, por tanto, ahora desde un punto de vista más centrado en los posibles riesgos a la seguridad y la defensa. Para hacerlo propongo varios ejemplos de casos reales que pueden resultar muy reveladores y llevarnos hacia una profunda reflexión sobre las consecuencias de la propaganda en las redes sociales.

Propaganda de extrema derecha

La extrema derecha ha querido aprovechar desde el principio esta plataforma virtual de reciente creación para realizar sus propias campañas de propaganda. Siguiendo las palabras del profesor José San Martín, experto en la materia: "a diferencia de otras minorías ideológicas, la extrema derecha no se considera así, y busca todos los resquicios, prospecta todas las fisuras, para avanzar posiciones, desde soportes distintos, incluso contradictorios en las formas, pero coherentes en la apostasía al democratismo occidental"[23]. Por otro lado, el experto en fascismo Joan Antón Mellón nos recuerda que la esencia del fascismo se encuentra en la convicción de que la civilización avanza cuando existe un orden político "natural" por el cual los no selectos están al servicio (incluso esclavizados) de los selectos[24].

A pesar de sus intentos, no les está resultando fácil ser uno más en las redes sociales, pues es la propia comunidad de Internet la que en muchos casos se moviliza para expulsarles del medio social. Este es el caso, por ejemplo, de un grupo de extrema derecha neonazi creado en Perú, al que Facebook bloqueó su cuenta. El grupo fue abierto por dos jóvenes neonazis conocidos por hacer disparos al aire libre en una plaza peruana en 2009. Fueron denunciados por una gran cantidad de usuarios de FB a raíz de la publicación de unas fotos donde se les veía saludando a un retrato de Adolf Hitler[25].

Caso más sensible ha sido el bloqueo de la cuenta en Twitter de Besseres Hannover, grupo declarado neo-nazi y disuelto por la policía alemana debido a su vinculación al crimen organizado. Alemania solicitó que se diera de baja la cuenta, que hacía apología del nazismo. Twitter aceptó tras comprobar la peligrosidad de sus miembros[26].

A pesar de todo, siguen existiendo grupos que utilizan libremente las redes para realizar sus propias campañas de propaganda, como por ejemplo la cuenta @NSRevolution_ en Twitter que a día de hoy sigue sembrando la Red con mensajes como este: "Golden Dawn: No dejéis a los banqueros judíos asesinaros, matad a los banqueros judíos!":

23 SAN MARTÍN, José. La coartada intelectual de la extrema derecha europea, Claves de Rezón Práctica, Madrid: Promotora General de Revistas, 2012, Volumen 223, p.13.

24 ANTÓN-MELLÓN, Joan. El Eterno Retorno. ¿Son fascistas las ideas-fuerza de la Nueva Derecha Europea (ND)?, Revista Foro Interno, Madrid: Universidad Complutense, 2011, p. 90. http://revistas.ucm.es/index.php/FOIN/article/view/37009/35818

25 Facebook bloquea a neonazis peruanos, Publimetro, 11 de agosto de 2011. http://publimetro.pe/actualidad/147/noticia-no-esta-prohibido-nazismo

26 Twitter blocks neo-Nazi account to users in Germany, BBC News,18 de octubre de 2012. http://www.bbc.co.uk/news/technology-19988662

Fuente: @NSRevolution_ Twitter

Extrema izquierda

Las reflexiones realizadas sobre extrema derecha serían también extrapolables a movimientos de extrema izquierda, que manejan con elevado grado de conocimiento las redes sociales. En ocasiones, las redes han sido el campo de batalla virtual para ataques "verbales" entre grupos, que en algunas ocasiones se trasladan posteriormente al mundo físico, como los casos de Alpedrete en noviembre de 2014 o de Tetuán unas semanas antes. Datos oficiales de la policía y del Centro de Estudios e Iniciativas sobre Discriminación y Violencia muestran un repunte de actividad, tanto en actividades ligadas al fútbol, como fuera de él. Destacan en esos informes la edad, cada vez más temprana, de los arrestados. La edad es un factor fundamental para la actividad intensa en la red. Proliferan cuentas en redes, blogs, foros. La red se convierte en un medio fundamental para la información, la comunicación y la preparación de acciones.

Ciberactivismo y Ciberhacktivismo

Especialmente interesante en los últimos años es el avance del ciberactivismo en Internet. Puesto que las redes sociales facilitan la difusión de cualquier opinión o deseo, se han convertido en unas plataformas magníficas para la crítica social o para incitar a cualquier tipo de ciberactivismo o ciberhackeo de cuentas o páginas en Internet objetivo. La propia ONG Amnistía Internacional tiene una guía fácil para las personas que quieran convertirse en ciberactivistas[27].

Sin duda, el grupo más activo de ciberactivismo, basado en ciberhacking, es Anonymous, quien en numerosas ocasiones parece traspasar la línea del cibercrimen.

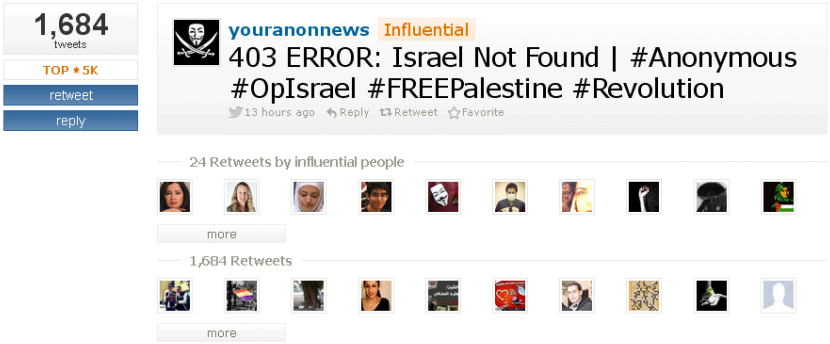
En abril de 2013, el grupo de hackers Anonymous decidió lanzar una campaña muy agresiva contra el estado de Israel con la intención de bloquear y eliminar la presencia de Israel en Internet. La campaña perseguía solidarizarse con la causa Palestina y buscar el apoyo de otros grupos de hackers activistas en el mundo para conseguir su objetivo. Para explicar los motivos concretos que les han llevado a crear esta operación deciden dar un comunicado de prensa a través de un vídeo subido a Youtube dirigido al estado de Israel [28].

27 AMNISTÍA INTERNACIONAL. Herramientas y sugerencias para un ciberactivismo eficaz. http://www.amnesty.org/es/stay-informed/publications/books/herramientas-ciberactivismo-eficaz

28 ANONYMOUS. #OPIsrael (V. 2.0). http://anonnews.org/press/item/2238/

Comenzaron con la difusión de la campaña y los hackeos de páginas en Internet el 5 de abril y finalizaron el 7, con la intención de hacerlo coincidir con el día de la Memoria del Holocausto.

Durante los tres días se pudieron ver mensajes como este, en el que se bromeaba con la desaparición de Israel del ciberespacio. Mensajes que se convirtieron en altamente virales y dieron la vuelta al mundo.



Ahora podemos preguntarnos, ¿qué pasaría si España se convirtiera en un objetivo de este tipo de campañas en las redes sociales?

La desinformación en catástrofes naturales

Desde un punto de vista empírico, y a raíz de uno de los terremotos más virulentos de Chile (27/02/2010), el centro de recursos de Yahoo! decidió investigar en profundidad el comportamiento de la difusión de los mensajes informativos suministrados por los propios usuarios de la red social que disponían de información de primera mano sobre el terremoto. En su estudio dedicaron una parte especial a la difusión de falsos rumores que contaminaban la realidad de lo que estaba sucediendo. Tras su análisis, descubrieron algunas cuestiones muy interesantes. Veamos la tabla.

Table 4: Classification results for cases studied of *confirmed truths* and *false rumors*.

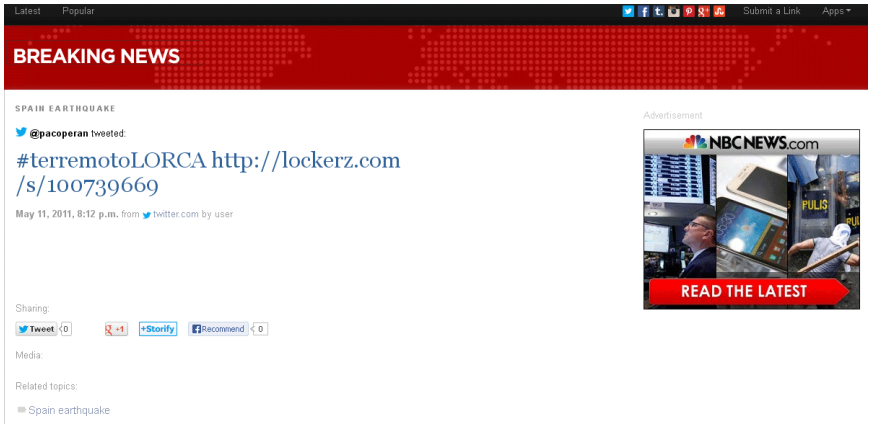
Case	# of unique tweets	% of re-tweets	# of unique "affirms"	# of unique "denies"	# of unique "questions"
Confirmed truths					
The international airport of Santiago is closed	301	81	291	0	7
The *Viña del Mar International Song Festival* is canceled	261	57	256	0	3
Fire in the Chemistry Faculty at the University of Concepción	42	49	38	0	4
Navy acknowledges mistake informing about tsunami warning	135	30	124	4	6
Small aircraft with six people crashes near Concepción	129	82	125	0	4
Looting of supermarket in Concepción	160	44	149	0	2
Tsunami in Iloca and Duao towns	153	32	140	0	4
TOTAL	1181		1123	4	30
AVERAGE	168,71		160,43	0,57	4,29
False rumors					
Death of artist Ricardo Arjona	50	37	24	12	8
Tsunami warning in Valparaiso	700	4	45	605	27
Large water tower broken in Rancagua	126	43	62	38	20
Cousin of football player Gary Medel is a victim	94	4	44	34	2
Looting in some districts in Santiago	250	37	218	2	20
"Huascar" vessel missing in Talcahuano	234	36	54	66	63
Villarrica volcano has become active	228	21	55	79	76
TOTAL	1682		502	836	216
AVERAGE	240,29		71,71	119,43	30,86

Fuente: Twitter Under Crisis: Can we trust what we RT?[29]

29 MENDOZA, Marcelo; POBLETE, Bárbara y CASTILLO Carlos. Twitter Under Crisis: Can we trust what we RT?, 1st Workshop on Social Media Analytics, Washington: Yahoo! Research, 2010, p. 7. http://research.yahoo.com/files/mendoza_poblete_castillo_2010_twitter_terremoto.pdf

Si observamos con detenimiento comprobaremos que el número de mensajes falsos en general es bastante más elevado que el número de mensajes confirmados. Las causas pueden ser múltiples, pero probablemente una de las razones sea porque son mensajes más sorprendentes y emotivos, por tanto más susceptibles de ser compartidos. Sin embargo, cuando analizamos el número de mensajes que afirmaban el contenido, vemos que es mucho mayor el relacionado con aquellos que aseveraban que el mensaje era cierto (1.123), frente a los que atestiguaban que los rumores falsos eran correctos (502). Por último, además, resultó que había más mensajes que negaban la veracidad de una noticia falsa (836) frente aquellos que desmentían una noticia verdadera (4). Por tanto, una vez más, el medio social demuestra lo que es. Cualquiera puede decir cualquier cosa, sin embargo, un buen análisis de redes sociales demuestra que son los propios usuarios quienes también actúan como periodistas validando o desmintiendo la noticia.

¿Cómo pueden aprovechar nuestros cuerpos y fuerzas de seguridad del estado la información vertida en Twitter de primera mano, muy útil en distintas situaciones, sin contaminarse con falsos rumores? Por ejemplo, en casos de emergencia como el sucedido en el terremoto de Lorca, donde el hashtag #terremotoLORCA se convirtió en un repositorio con todo tipo de información[30] útil sobre números de teléfono de ayuda, fotografías de cómo estaba la situación, etc. Entre esos mensajes también pudimos descubrir otros falsos como éste, que cuando pulsabas en la dirección web te redirigía a un portal comercial que aprovechaba la popularidad del hashtag para vender sus productos. Como gancho hacía pensar que incluía contenido importante, especialmente tras aparecer en un conocido portal de noticias en Internet llamado Breaking News, dentro de la categoría “Spain Earthquake”.



Fuente: Captura de Breaking News[31]

Un caso significativo, y lamentable, fue la utilización del caso de ébola en España para difundir falsos rumores sobre la existencia de más casos en diferentes hospitales de la geografía nacional. Muchos de estos rumores iban acompañados por falsificaciones de portadas de medios de prensa. La cuenta en twitter de Guardia Civil estuvo horas desmintiendo esas situaciones.

30 GONZALO, Paula. #TerremotoLorca despierta la solidaridad en Twitter, Periodismo Ciudadano, 13 de mayo de 2013. http://www.periodismociudadano.com/2011/05/13/terremotolorca-despierta-la-solidaridad-en-twitter/

31 @pacoperan. #terremotoLORCA, Breaking News, 11 de mayo de 2013. http://www.breakingnews.com/item/ahZzfmJyZWFraW5nbmV3cy13d3ctaHJkcg0LEgRTZWVkGMX9qwMM/2011/05/11/terremotolorca-httplockerzcoms100739669

Fuente: Cuenta en twitter de Guardia Civil @guardiacivil[32]

5. ¿CONTROLAR LO INCONTROLABLE?

Evidentemente todos los estados del mundo se plantean algún tipo de control sobre las redes sociales con la intención de vigilar que éstas no se conviertan en un problema de seguridad nacional, especialmente después del efecto amplificador que tuvo en el llamado "despertar árabe".

Para ello cada cual está desarrollando su propia estrategia de seguridad. A continuación me gustaría mencionar algunas de ellas por lo dispares que son, buscando abrir un espacio a la reflexión y el debate de qué fórmula sería la más adecuada para España.

- *Táctica del bloqueo*. Aniversario de Tiananmen, China. Los censores toman la decisión de bloquear el acceso a medios sociales como Twitter o Flickr para evitar posibles altercados por la celebración del 20 aniversario de lo sucedido en 1989. Además, se prepara un bloqueo especial también para los medios extranjeros de manera que si se detecta que están hablando del aniversario se corte automáticamente la noticia[33].

32 Más información: http://www.clasesdeperiodismo.com/2014/10/14/guardia-civil-de-espana-alerta-de-falsas-portadas-sobre-ebola/

33 REYNOLDS, Paul. Censura en el aniversario de Tiananmen, BBC Mundo, 2 de junio de 2013. http://www.bbc.co.uk/mundo/internacional/2009/06/090602_1552_tiananmen_internet_jg.shtml

- *Táctica del "Miedo"*. Turquía sigue reflexionando a día de hoy qué hacer con las redes sociales. Si bien ha decidido que no las prohibirá, sí las vigila muy de cerca para conocer en profundidad todo lo que dicen sus conciudadanos con la intención de procesarles o multarles en función de lo que expresen[34]. Para tenerlos más controlados, además, ha decidido que prohibirá la apertura de cuentas falsas o enmascaradas por motivos de seguridad. Por tanto, todos los ciudadanos turcos que quieran usar las redes sociales deberán identificarse[35].

- *Táctica de "El Gran Hermano"*. Posiblemente la táctica más utilizada en los países occidentales y democráticos. Sin duda, uno de los casos estrella es el sucedido con el programa PRISM planteado por la NSA de EE.UU. Este programa diseña una estrategia de escuchas generalizadas en toda Internet e incluye peticiones específicas del gobierno americano a las grandes compañías de Internet, como Facebook y Google, para que les permitan acceder a contenido privado de usuarios que consideran "de riesgo"[36]. Sin embargo, como era de esperar, no sólo EE.UU. utiliza este tipo de vigilancia digital. Según Le Monde Francia también tiene un programa de estas características[37].

- *Táctica de "La siembra"*. Ésta es más bien una táctica dirigida a modificar la percepción y reputación de un país en Internet y con ello obtener todos los beneficios que una buena reputación ofrece a quien la tiene: mejora en el turismo, aumento en la compra de sus productos y servicios, mejora en las condiciones financieras internacionales, etc. Para ello, EE.UU. ha destinado $630,000 en Internet para comprar "fans"[38].

6. CONCLUSIÓN

Las redes sociales virtuales cada vez están más presentes en nuestras vidas. Más allá de los usuarios individuales que han sido quienes las han convertido en un éxito de la comunicación online, se vienen creando desde hace años perfiles que representan a distintas organizaciones internacionales públicas y privadas. Una buena gestión de estos perfiles y de la comunicación, que se realiza a través de ellos, evita la exposición a ciertos riesgos y amenazas de nueva creación, que están apareciendo conforme las redes sociales evolucionan con los nuevos actores y los nuevos intereses.

34 EFE. Un pianista turco condenado a 10 meses de cárcel por criticar el islam en Twitter, El País Internacional, 15 de abril de 2013. http://internacional.elpais.com/internacional/2013/04/15/actualidad/1366037587_412492.html

35 Fake social media accounts to be prevented: Turkish deputy PM, Turkish weekly, 21 de junio de 2013. http://www.turkishweekly.net/news/152201/fake-social-media-accounts-to-be-prevented-turkish-deputy-pm.html

36 GREENWALD, Glenn y MACASKILL, Ewen. NSA Prism program taps in to user data of Apple, Google and others, The Guardian, 7 de junio de 2013. http://www.guardian.co.uk/world/2013/jun/06/us-tech-giants-nsa-data

37 FOLLOROU, Jaques y JOHANNÈS, Frank. Révélations sur le Big Brother français, Le Mond, 4 de julio de 2013. http://www.lemonde.fr/societe/article/2013/07/04/revelations-sur-le-big-brother-francais_3441973_3224.html

38 US State Departament Facebook 'Likes': DOS Spent $630,000 On Buying Fans, International Business Times, 4 de Julio de 2013. http://www.ibtimes.com/us-state-department-facebook-likes-dos-spent-630000-buying-fans-1334457#

BIBLIOGRAFÍA

Amnistía Internacional. (2009). Herramientas y sugerencias para un ciberactivismo eficaz. Disponible en: http://www.amnesty.org/es/stay-informed/publications/books/herramientas-ciberactivismo-eficaz

Anonymous. (V. 2.0).

Antón-Mellón, J. (2011). El Eterno Retorno. ¿Son fascistas las ideas-fuerza de la Nueva Derecha Europea (ND)?. Revista Foro Interno, 11, 69-92. Madrid: Universidad Complutense. Disponible en: http://revistas.ucm.es/index.php/FOIN/article/view/37009/35818

Birkenbihl, K., Quesada, E., y Priesca, P. (2009). Presente y futuro de la world wide web. Novática: Revista de la Asociación de Técnicos de Informática, 197, 5-7. Madrid. Disponible en: http://www.ati.es/novatica/2009/197/Nv197-Presentacion.pdf

Calderón, V. La propaganda militar en 140 caracteres. El País. 20/11/2012. Disponible en: http://internacional.elpais.com/internacional/2012/11/20/actualidad/1353433014_417902.html

Calderón, V. Propaganda a golpe de Tuit. El País. 03/02/2013. Disponible en: http://sociedad.elpais.com/sociedad/2013/02/03/vidayartes/1359919995_815589.html

Castillo, M. Facebook bloquea a neonazis peruanos. Publimetro. 11/08/2011. Disponible en: http://publimetro.pe/actualidad/147/noticia-no-esta-prohibido-nazismo

Chozick, A., y Perlroth, N. Twitter Speaks, Markets Listen and Fears Rise. The New York Times. 28/04/2013. Disponible en: www.nytimes.com/2013/04/29/business/media/social-medias-effects-on-markets-concern-regulators.html

EFE. Un pianista turco condenado a 10 meses de cárcel por criticar el islam en Twitter. El País. 15/04/2013. Disponible en: http://internacional.elpais.com/internacional/2013/04/15/actualidad/1366037587_412492.html

El presidente de Egipto anuncia en Facebook que “no aceptará renunciar de forma humillante”, La Información. 03/07/2013. Disponible en: http://noticias.lainformacion.com/mundo/el-presidente-de-egipto-anuncia-en-facebook-que-no-aceptara-renunciar-de-forma-humillante_blz5yKmELt9Tj5aiVclFj6/

Fake social media accounts to be prevented: Turkish deputy PM. Journal of Turkish Weekly. 21/06/2013. Disponible en: http://www.turkishweekly.net/news/152201/fake-social-media-accounts-to-be-prevented-turkish-deputy-pm.html

Follorou, J., y Johannès, F. Révélations sur le Big Brother français, Le Monde, 04/07/2013. Disponible en: http://www.lemonde.fr/societe/article/2013/07/04/revelations-sur-le-big-brother-francais_3441973_3224.html

Fontana, J. (2013). El futuro es un país extraño. Una reflexión sobre la crisis social de comienzos del siglo XXI. Barcelona: Pasado y Presente.

Fort, M. ‘Minicrash’ en Wall Street por un falso tuit sobre un atentado contra Obama. La Vanguardia. 23/04/2013. Disponible en: http://www.lavanguardia.com/economia/20130423/54372747540/minicrash-wall-street-hackeada-cuenta-twitter-associated-press.html

Fundación Telefónica. (2013). La sociedad de la Información en España 2012. Madrid: Ariel. Disponible en: http://www.fundaciontelefonica.com/arte_cultura/sociedad-de-la-informacion/informe-sociedad-de-la-informacion-en-espana-2012/

Global Web Index. Global Map of Social Networking 2011. Disponible en: https://globalwebindex.net/wp-content/uploads/down

loads/2011/06/Global-Map-of-Social-Networking-GlobalWebIndex-June-20112.pdf

Gonzalo, P. #TerremotoLorca despierta la solidaridad en Twitter. Periodismo Ciudadano. 13/05/2011. Disponible en: http://www.periodismociudadano.com/2011/05/13/terremotolorca-despierta-la-solidaridad-en-twitter/

Greenwald, G., y MacAskill, E. NSA Prism program taps in to user data of Apple, Google and others. The Guardian. 07/06/2013. Disponible en: http://www.guardian.co.uk/world/2013/jun/06/us-tech-giants-nsa-data

Greenwood, P. Israel invests millions in drive for elite 'cyber warriors'. The Telegraph. 01/11/2012. Disponible en: http://www.telegraph.co.uk/news/worldnews/middleeast/israel/9648820/Israel-invests-millions-in-drive-for-elite-cyber-warriors.html

Lee, Y. NKorea's Twitter account hacked amid tension. Associated Press. 04/04/2013. Disponible en: http://bigstory.ap.org/article/nkoreas-twitter-account-hacked-amid-tension

Lumezanu, C., Feamster, N., y Klein, H. (2012). #bias: Measuring the Tweeting Behavior of Propagandists. Sixth International AAAI Conference on Weblogs and Social Media. Disponible en: http://www.aaai.org/ocs/index.php/ICWSM/ICWSM12/paper/view/4588/4985

Mendoza, M., Poblete, B., y Castillo, C. (2010). Twitter Under Crisis: Can we trust what we RT?. 1st Workshop on Social Media Analytics (SOMA '10). Washington, DC, USA. Disponible en: http://research.yahoo.com/files/mendoza_poblete_castillo_2010_twitter_terremoto.pdf

Moya, E., y Blanco, J. M. (2015). "Redes sociales y seguridad ciudadana". En I. Criado y F. Rojas (Eds.), Casos de éxito en redes sociales digitales de las administraciones públicas. Escola d´Administració Pública de Catalunya.

Musser, J., y O'Really, T. (2007). Web 2.0 Principles and Best Practices. O´Reilly Radar. Disponible en: http://repo.mynooblife.org/.priv8/Ebook/Web%202.0%20Principles%20and%20Best%20Practices.pdf

North Korea using Twitter for propaganda. The Sidney Morning Herald. 15/08/2010. Disponible en: http://www.smh.com.au/technology/technology-news/north-korea-using-twitter-for-propaganda-20100815-1250u.html

Obama tells intelligence chiefs to draw up cyber target list – full document text. The Guardian. 07/06/2013. Disponible en: http://www.guardian.co.uk/world/interactive/2013/jun/07/obama-cyber-directive-full-text

O' Really, T. What Is Web 2.0: Design Patterns and Business Models for the Next Generation of Software. O' Really. 30/09/2005. Disponible en: http://oreilly.com/pub/a/web2/archive/what-is-web-20.html?page=1#mememap

Oriella PR Network. Global Digital Journalism Study 2013. Disponible en: http://www.oriellaprnetwork.com/research

Ortíz, A. La ONU sigue a una actriz porno en su cuenta oficial de Twitter. ABC. 07/05/2013. Disponible en: http://www.abc.es/tecnologia/redes/20130507/abci-pornstar-twitter-201305071614.html

Piratean de nuevo la cuenta de Nicolás Maduro en Twitter. CNN. 12/05/2013. Disponible en: http://cnnespanol.cnn.com/2013/05/12/piratean-de-nuevo-la-cuenta-de-nicolas-maduro-en-twitter/

Reynolds, P. Censura en el aniversario de Tiananmen. BBC. 02/06/2013. Disponible en: http://www.bbc.co.uk/mundo/internacional/2009/06/090602_1552_tiananmen_internet_jg.shtml

Samsung probed in Taiwan over 'fake web reviews'. BBC. 16/04/2013. Disponible en: http://www.bbc.co.uk/news/technology-22166606

Sanmartín, J. J. (2012). La coartada intelectual de la extrema derecha europea. Claves de Razón Práctica, 223. Madrid.

Schulman, K. Watch: President Obama Answers Your Questions in a Google+ Hangout. The White House. 14/02/2013. Disponible en: http://www.whitehouse.gov/blog/2013/02/14/watch-president-obama-answers-your-questions-google-hangout

Spain Earthquake. Breaking News. 11/05/2011. Disponible en: http://www.breakingnews.com/item/ahZzfmJyZWFraW5nbmV3cy13d3ctaHJkcg0LEgRTZWVkGMX-9qwMM/2011/05/11/terremotolorca-httplockerzcoms100739669

The Cocktail Analysis. (2013). 5º Oleada Observatorio Redes Sociales. Disponible en: http://es.slideshare.net/TCAnalysis/5-oleada-observatorio-redes-sociales

Twitter blocks neo-Nazi account to users in Germany. BBC. 18/10/2012. Disponible en: http://www.bbc.co.uk/news/technology-19988662

United States Department of State and the Broadcasting Board of Governors. (2013). Inspection of the Bureau of International Information Programs. Office of Inspector General. Disponible en: http://oig.state.gov/system/files/211193.pdf

Waltz, E. (1998). Information Warfare: Principles and Operations. Artech House.

Weimann, G. (2006). Terror on the Internet: The New Arena, the New Challenges. Washington, DC: United States Institute of Peace Press.

Fecha de recepción: 14/11/2014. Fecha de aceptación: 17/12/2014

SEGURIDAD NACIONAL, AMENAZAS Y RESPUESTAS

LUIS DE LA CORTE IBÁÑEZ
JOSÉ MARÍA BLANCO NAVARRO

Biblioteca ICFS. 345 páginas.

Colección Acción Empresarial de LID Editorial Empresarial S.L.

ISBN13: 978-84-8356-920-7

Tal y como avanzan al principio de este libro, que muy bien pudiera ser un manual de seguridad nacional -el primero de esta naturaleza-, y parafraseando a Maquiavelo, sus autores pretenden escribir algo útil para quien lo lea, buscando la verdadera realidad de las cosas, junto a un nutrido grupo de expertos y profesionales, tanto del ámbito de la seguridad como del académico, que han conformado una simbiosis perfecta para los fines que buscaban.

Así, Luis de la Corte Ibáñez, profesor titular del Departamento de Psicología Social y Metodología de la Universidad Autónoma, y José María Blanco Navarro, director del Centro de Análisis y Prospectiva de la Guardia Civil, ambos colegas en la dirección del Área de Estudios Estratégicos e Inteligencia del Instituto de Ciencias Forenses y de la Seguridad, de la Universidad Autónoma de Madrid, han sabido coordinar una obra colectiva que, siguiendo la estructura de la propia Estrategia de Seguridad Nacional aprobada en 2013 (ESN-2013), aporta nuevos conceptos y reflexiones, profundiza en el análisis e introduce debates sobre el futuro de la materia.

La obra es pionera en aportar una definición de Seguridad Nacional novedosa, sin duda, con una nueva visión de este concepto, distinta de la de la ESN-2013. De esta forma contemplan la seguridad nacional como un estado ideal, además de los componentes clásicamente señalados (como una acción de gobierno, un sistema, un conjunto de valores o principios, o una cultura). De hecho, el primer capítulo, de los 16 de que consta, se “aproxima” a la seguridad nacional presentando múltiples conceptos de seguridad, antes de entrar de lleno en las estrategias de seguridad, su proceso de elaboración, sus contenidos y la ESN-2013, que analizan, sin olvidar la anterior, la Estrategia Española de Seguridad de 2011.

A un análisis del mundo actual, del entorno, le sigue el capítulo tres, otro de los que podemos considerar más destacables, pues habla de los facilitadores y potenciadores del riesgo, ofreciendo una visión ampliada y argumentada, sobre la existente en la ESN-2013, del contexto sobre el que podrían emerger las amenazas a la seguridad, no sólo en nuestro país sino en el mundo entero.

Los capítulos cuatro al 15 tratan sobre las amenazas señaladas en la estrategia oficial: los conflictos armados, el terrorismo, las ciberamenazas, el crimen organizado, la inestabilidad económica y financiera o la vulnerabilidad energética, así como la proliferación de armas de destrucción masiva, los flujos migratorios irregulares y el espionaje. En todos ellos, de una manera estructurada y cohesionada entre los capítulos, se ofrece una visión de la situación actual, tratando de evaluar la amenaza en cuestión y señalando cuales deben ser las acciones de respuesta.

También se comentan las emergencias y catástrofes, en el 13, la vulnerabilidad del espacio marítimo, en el 14, o de las infraestructuras críticas y los servicios esenciales, en el 15.

El capítulo 16 va más allá, al presentar una cuestión tan trascendental como es la toma de decisiones y la visión de futuro para la seguridad nacional. De hecho nos encontramos que este punto nos señala la necesidad de adoptar y desarrollar nuevas teorías de toma de decisiones y políticas públicas en seguridad, en entornos complejos y de alta incertidumbre. En esta misma línea se manifiesta que la visión de futuro, en materia de seguridad, es una necesidad y una oportunidad que no debemos dejar pasar. La detección de nuevos riesgos y amenazas y su evaluación son condiciones clave para una adecuada toma de decisiones, que precisa el mejor conocimiento y la mejor inteligencia. Recientemente se ha presentado en el Consejo de Ministros el anteproyecto de Ley Orgánica de Seguridad Nacional, que incide en estos aspectos, tratando de que la visión de una seguridad integral cuente con mecanismos ágiles para la toma de decisiones.

Tanto en la obra citada, como en la estrategia y en el anteproyecto legislativo la necesidad de desarrollar una cultura de seguridad nacional se muestra como una imperiosa necesidad. No es posible generar un compromiso que vincule a poderes públicos, sector privado, comunidades y ciudadanos, sin un previo proceso de información, de comunicación bidireccional, basado en principios de transparencia.

En definitiva, nos encontramos ante un ensayo colectivo, académico y profesional, que aborda los problemas de la seguridad nacional interpretados desde la posición y los intereses de España, teniendo presente cuando éstos conectan con los de Europa, los de Occidente y los de la comunidad internacional. Por eso nos ofrece una visión completa, profunda y a la altura de los tiempos sobre cada temática relacionada con la seguridad nacional, que además aprovecha no sólo las aportaciones institucionales, sino también los criterios y experiencia de cada uno de sus autores, así como cualquier conocimiento académico pertinente, equilibrando las visiones procedentes del mundo del conocimiento y de la práctica en el ámbito español.

El sistema de seguridad nacional español, como señalan los autores, es un proceso recientemente iniciado. Por tanto, se trata de un proceso en desarrollo que necesitará tiempo y recursos. El conocimiento sobre su importancia es un primer paso fundamental. La seguridad nacional es un elemento de cohesión social, que afecta a cualquier ciudadano, independientemente de su edad, sexo, profesión o ideología. Afecta a colectivos, a organizaciones y a empresas. Y afecta como sociedad y como nación. Como señala la Estrategia Nacional, se trata de un proyecto compartido.

Ana María Ruano
Periodista del Centro de Análisis y Prospectiva

CRIMINALIDAD ORGANIZADA
ASPECTOS JURÍDICOS Y CRIMINOLÓGICOS

JULIÁN LÓPEZ-MUÑOZ

Editorial Dykinson, Colección Estudios de Criminología

ISBN: 978-84-9085-238-5

Criminalidad Organizada está escrito por el doctor don Julián López Muñoz, comandante de la Guardia Civil, que ha recibido recientemente una calificación de Sobresaliente "Cum Laude" por la UNED, en la investigación que ha llevado a cabo en su tesis sobre la mafia rusa. El autor, como muestra en la obra, dispone de una sólida formación jurídica y criminológica, con una larga trayectoria en la investigación y lucha contra la criminalidad organizada. Toda una larga vida en el ámbito de la inteligencia y la policía judicial y, por tanto, en la acción operativa diaria, que no ha sido impedimento para desarrollar una rica actividad docente y editorial, a través de libros y colaboraciones.

La presente obra muestra algunos de los puntos clave para entender el fenómeno del crimen organizado. La criminalidad organizada transnacional surge tras el fenómeno de la globalización y la integración de mercados, flujos y libre circulación. Se trata de una de las amenazas destacadas en prácticamente la totalidad de estrategias de seguridad nacional, como la aprobada en España en 2013.

Uno de los mayores riesgos del crimen organizado deriva de su opacidad y acción silenciosa, socavando las estructuras de los sistemas políticos y económicos de los estados, y llegando a conformar, en las ocasiones más extremas, verdaderos estados paralelos. Un fenómeno en el que, además, causas y efectos se retroalimentan, incidiendo en la fragilidad de los estados, la permanencia de conflictos, la erosión de la economía y los negocios legales, el incremento de los tráficos ilícitos (drogas, armas, seres humanos) e incluso afectando al medioambiente, a través de la explotación ilegal de fauna y flora. Una actividad criminal que es potenciada por el desarrollo de las tecnologías y una alta ingeniería financiera que trata de ocultar los ingresos ilegales y "blanquearlos" para su introducción en el sistema.

Para hacer frente a esta amenaza es necesaria la utilización de instrumentos jurídicos supranacionales y acuerdos intergubernamentales, además de la adopción de un mismo concepto jurídico sobre el crimen organizado por parte de todos los países que están en la Organización de Naciones Unidas (ONU), con la finalidad de poder detectar mejor el crimen organizado diferenciándolo de otras conductas criminales. Detección y anticipación son claves de la acción, imponiéndose la necesidad de implantar sistemas de alerta temprana. Pero para ello es preciso, previamente, conocer el fenómeno, su conceptualización y los instrumentos jurídicos existentes.

Uno de los grandes problemas del crimen organizado reside en el concepto, ya que hay múltiples de ellos. Ahora bien, con este libro podremos acercarnos a este fenómeno que tanto llama la atención y del que poco sabemos, porque hace hincapié en la diferenciación de conceptos como delincuencia organizada y crimen organizado,

entre organización criminal y grupo criminal. La Convención de Palermo, en diciembre de 2000, definió el crimen organizado a través de unos parámetros clasificadores. También nos muestra los distintos tipos de jerarquización que hay, es decir, las diferentes estructuras criminales que pueden adoptar los grupos del crimen organizado.

Especial relevancia adquiere la visión que el autor nos proporciona sobre las técnicas de investigación, jurídicas y policiales, que se utilizan para luchar contra el crimen organizado. Estas técnicas son: el "agente encubierto", que es un instrumento procesal y por ende está regulado, el "agente provocador", que es una técnica policial que carece de regulación y, por último, llevar a cabo entregas vigiladas por parte de los agentes policiales.

Además, se realiza un análisis de las legislaciones de Naciones Unidas, de la Unión Europea, el Código Penal y jurisprudencia española porque afectan directamente a nuestro sistema democrático, ya que el crimen organizado perpetra delitos contra el orden público.

Este libro, en definitiva, nos sirve para conocer mejor el crimen organizado, una de las amenazas para la seguridad nacional más difíciles de percibir y evaluar, entender cómo funcionan los grupos criminales a través de su sistema de jerarquización, saber que tipos de delitos cometen y así poder adoptar las reformas normativas precisas, eliminando aquellas que no sirven, porque no son eficaces, y adoptando aquellas que permitan luchar contra el fenómeno con anticipación y con todas las garantías en los derechos y libertades de los ciudadanos, en la privacidad de sus datos, pudiendo de esta manera prevenir tanto el asentamiento como la actividad de grupos del crimen organizado en nuestro territorio.

Una obra rigurosa, necesaria y que se convierte en manual de consulta para profesionales de la seguridad, para alumnos de derecho o de criminología y para toda aquella persona que quiera profundizar en el fenómeno del crimen organizado.

Ana Quintana Martín
Alumna en prácticas en el Centro de Análisis y Prospectiva

EL FUTURO DIGITAL

ERIC SCHMIDT Y JARED COHEN

Anaya Multimedia, 352 páginas.

ISBN10: 8441535841

Eric Schmidt es presidente ejecutivo de Google, mientras que Jared Cohen es el director de Google Ideas. Schmidt forma parte del Consejo de Asesores en Ciencia y Tecnología del presidente Obama, asesora al primer ministro del Reino Unido, preside la directiva de la *New America Foundation*, forma parte de la directiva de *The Economist* y es miembro del prestigioso *Council of Foreign Relations* (CFR). Jared Cohen también está vinculado al CFR, ha formado parte del equipo de planificación del Departamento de Estado, y asesorado a Condolezza Rice y Hillary Clinton.

Julian Assange, fundador de Wikileaks, ha titulado su último libro *"Cuando Google encontró a Wikileaks"*. Señala Assange que Google actúa como una extensión del gobierno norteamericano y que cuando Schmidt y Cohen le visitaron no lo hacía la empresa, sino el Departamento de Estado. Algo que resulta obvio observando el currículum, público, de ambos directivos de Google.

En esta obra abordan cómo será nuestro futuro, centrándose en diferentes temas. Plantean un futuro en el que personas virtuales serán tan valiosas que se podrán comprar sus cuentas en mercados negros. También anticipan que un mundo vigilado en el que espiar a los ciudadanos llegará a ser legal, mientras que se disparará el sector dedicado a la protección de datos personales y las tecnologías para mantener a salvo la privacidad.

Schmidt y Cohen dedican un capítulo completo a la privacidad, al futuro de los estados, a las revoluciones, al terrorismo, la diplomacia o a las futuras guerras y conflictos. Se puede afirmar que se trata de un libro especializado sobre seguridad, en el que únicamente cambia el marco temporal, a medio y largo plazo, pero basado en tendencias ya claramente mostradas.

La obra es tremendamente amena, evita tecnicismos, por tanto es fácilmente comprensible, y alerta sobre los riesgos tecnológicos del futuro. Riesgos que, por cierto, en algunos casos están relacionados con las propias actividades que Google desarrolla. Multitud de ideas, predicciones bien argumentadas y anécdotas ilustran el futuro de nuestras sociedades. No es un libro sobre tecnología, es un libro sobre personas y sociedades en un entorno tecnológico.

¿Qué es lo que hace que este libro sea de interés, incluso necesario, para el profesional de la seguridad? Varias son las razones:

1. Google es una marca asociada a la innovación y la creatividad. El cargo de Cohen en Google Ideas y su colaboración como asesor de Seguridad Nacional muestran claramente la vinculación y la necesidad de la imaginación y la creatividad en cuestiones de seguridad. Una circunstancia manifestada en todo un capítulo del informe de la Comisión de Investigación de los atentados del 11S, pero en la que se ha avanzado muy poco.

Escasos son los trabajos reseñables sobre futuro en cuanto al análisis de riesgos y amenazas, o sobre el diseño de políticas de seguridad con dicha visión temporal. Particularmente, en España, supone una desventaja frente a las apuestas decididas de países avanzados en la necesidad de desarrollar los estudios de futuro, no únicamente en cuestiones de seguridad, sino en todos los ámbitos. Francia, Reino Unido, Estados Unidos o Colombia son sólo algunos de los ejemplos de estados en los que la prospectiva es una cuestión de estado. En España, la cultura de visión de futuro es inexistente y son pocas las organizaciones que apuestan por ella. La Guardia Civil sí lo hizo, en 1998.

2. Ahondando en el anterior punto, hay que destacar la especialidad de Cohen en temas de terrorismo. De nuevo permite vincular una materia concreta de seguridad, uno de los mayores riesgos de nuestra sociedad, destacado en todas las estrategias de seguridad nacional, y posiblemente uno de los que genera más impacto mediático y social, con la imaginación y la creatividad. Richard Clark, asesor de los presidentes Clinton y Bush en temas de seguridad, advertía, en la propia investigación de los atentados del 11S, cómo su preocupación por la seguridad aérea se debía más a la lectura de las novelas de Tom Clancy que a los informes que pasaban por su despacho.

3. Los contenidos están referidos, casi en su totalidad, a aspectos del futuro directamente relacionados con riesgos y amenazas para la seguridad: insurgencias, nuevas guerras, ataques a la privacidad, terrorismo. El vertiginoso cambio social y tecnológico al que asistimos va a afectar a todos los ámbitos de nuestra vida. Existe una creciente brecha entre el avance tecnológico y el análisis de los efectos que las mismas generan en temas de seguridad. Gran parte de los desarrollos actuales, como los drones, las impresoras 3D, la nanotecnología, precisarán tanto compromisos éticos, como regulación normativa.

4. Como apuntan los autores, la privacidad será una materia de estudio, incluso en los colegios. Nosotros nos atrevemos a añadir que la evaluación de la información, especialmente en cuanto a su naturaleza digital, se irá constituyendo en una especialidad. Es la información, y la desinformación, uno de los retos básicos del futuro: su acceso, su utilización, su tratamiento. La “Inteligencia” y la “Contrainteligencia” deberán ser aplicadas en todas las actividades y sectores.

5. De particular interés resulta el modelo que plantean sobre el éxito o fracaso de las revoluciones. Los últimos años han sido intensos en revueltas y protestas sociales, y la tendencia es que esta situación vaya a más en el futuro. Una de las claves será cómo poner en relación el ciberactivismo en redes con el activismo en calles.

El libro es de obligada lectura para analistas de seguridad, futuristas y toda aquella persona que considere que el futuro se construye a cada segundo y que, simplemente con pensar y reflexionar sobre él, somos capaces de introducir factores causales en su posible devenir, en principio hacia los futuros más deseados. Un pensamiento futuro al que debe seguir la acción estratégica presente. El futuro se crea pensando, pero sobre todo actuando, con inteligencia.

José María Blanco Navarro
Director del Centro de Análisis y Prospectiva

DATOS SOBRE LOS AUTORES DE ESTE VOLUMEN POR ORDEN ALFABÉTICO

Ana Isabel Álvarez Aparicio, licenciada en Psicología en la Especialidad de Clínica por la Universidad Complutense de Madrid. Master en Psicología Clínica y de la Salud. Máster Oficial en Psicología de la Salud. Máster en Ciencias Forenses en Psicología Forense y Penitenciaria. Máster en Análisis e Investigación Criminal. Postgrado en Psicología de Crisis, Urgencias, Emergencias y Catástrofes. Máster en Grafología Forense. Máster en Pericia Caligráfica y Documentoscopia. alvcnps@hotmail.com

Félix Brezo Fernández, doctor en Ingeniería Informática y Telecomunicación ingeniero técnico en Informática de Gestión, ingeniero en Informática e ingeniero en Organización Industrial, además de master en Seguridad de la Información y master en Análisis de Inteligencia. Hasta junio de 2013, investigador en seguridad informática en el S3Lab de la Universidad de Deusto y, a partir de entonces, analista de inteligencia de Airon Group para Telefónica Digital. También es docente de cursos a nivel universitario sobre análisis de inteligencia y seguridad informática y divulgador de contenidos científico-técnicos. felixbrezo@gmail.com

Conchita Cornejo García, administradora Civil del Estado, por oposición, licenciada en Derecho por ICADE y es Subdirectora General Adjunta de Recursos Económicos, en el Ministerio de Justicia. Ha participado en la elaboración de normativa reguladora en materia de prevención del blanqueo de capitales e instruido y tramitado expedientes sancionadores en este sentido. No solo asiste a eventos internacionales en materia de prevención del blanqueo de capitales y bloqueo de la financiación del terrorismo, sino que imparte seminarios sobre estas cuestiones en diversos países de Sudamérica y Centroamérica, así como en otros foros celebrados en España. concepcion.cornejo@mjusticia.es

Luis de la Corte Ibáñez, doctor en Psicología de la UAM y experto en Terrorismo y Crimen Organizado. Director del Área de Estudios Estratégicos e Inteligencia del Instituto de Ciencias Forenses y de la Seguridad (ICFS), de la Universidad Autónoma de Madrid. Director del título de Experto en Análisis de Inteligencia (ICFS-UAM). Profesor en títulos de posgrado relacionados con la inteligencia y la seguridad, en el Centro Superior de Estudios de la Defensa Nacional (CESEDEN), y otros organismos. Autor de libros como “La lógica del terrorismo”, “Crimen.org” o “Seguridad nacional, amenazas y respuestas”. luis.cortes@uam.es

José Miguel García Malo de Molina, teniente coronel de la Guardia Civil, actualmente destinado como agregado de Interior en la Embajada de España en Dakar (Senegal). Es doctorando en Ciencias Políticas y de la Administración, licenciado en Derecho y posee un Máster en Alta Dirección Pública, además de numerosos cursos en el ámbito de la planificación estratégica. En cuanto a cursos policiales tiene el diploma de Policía Judicial, de Información, el de profesor de tiro, el de piloto de helicópteros y el de Estado Mayor. garciamalo@gmail.com

José Félix González Román, teniente coronel de la Guardia Civil de Estado Mayor, posee una extensa formación en Policía Judicial, en Desactivación de Explosivos, Escuela donde ha pasado una gran parte de su trayectoria profesional, y en Pro-

tección de la Naturaleza, entre otras especialidades, además de estar diplomado en investigación criminal, en derecho de la guerra y derecho internacional humanitario. También ha cursado estudios avanzados por un doctorado en Derecho. jfgroman@guardiacivil.es

Eva Moya Losada, analista de Inteligencia especializada en redes sociales para la seguridad y la defensa. Actualmente trabaja como manager de la Unidad de Análisis de Inteligencia de S21sec. Anteriormente lo hizo en la Universitat Pompeu Fabra - UPF, The Coca-Cola Company, en el Instituto de Ciencias Forenses (UAM) y en Educación Madrid School of Marketing. Es máster of Branding and Corporate Reputation, Marketing/Marketing Management, General y también como analista de Inteligencia por la Universidad Rey Juan Carlos. moya.eva@gmail.com

José Alberto Ramírez Vázquez, capitán de la Guardia Civil, con destino en la Secretaría de Estado de Seguridad, en concreto en el Área de Formación y Cooperación del Gabinete de Coordinación y Estudios, de la que es jefe del servicio. Su experiencia profesional incluye la jefatura de la unidad de seguridad de la delegación de España en la Organización del Tratado del Atlántico Norte en Bruselas, la participación en la misión de las Naciones Unidas en Kosovo (UNMIK) o en la operación de Mozanbique (ONUMOZ), también de Naciones Unidas. Está graduado en Ciencia Política y de la Administración por la Universidad Nacional de Educación a Distancia. jarv@interior.es

Yaiza Rubio Viñuela, licenciada en Ciencias de la Información, en la especialidad Periodismo, además de máster en Logística, Transporte y Distribución, por la UNED, e Interuniversitario en Analista de Inteligencia, por la Universidad Carlos III/Rey Juan Carlos; además en la actualidad cursa el máster en Logística y Dirección Económica de la Defensa, de la Universidad Complutense de Madrid. Su tesina versa sobre “La sobreexposición en la red de información geográfica acerca de instalaciones de interés para la Defensa” y trabaja como analista de Inteligencia en S21SEC. yaiza_rv@hotmail.com

NORMAS PARA LOS AUTORES

Los trabajos que se remitan para su publicación en la Revista "Cuadernos de la Guardia Civil" deberán ser inéditos y no estar pendientes de publicación en otra revista. No obstante, previa solicitud al Centro de Análisis y Prospectiva, podrán ser publicados en otro medio, una vez otorgada autorización escrita en tal sentido por el Director de la revista.

Los criterios para la presentación de textos son los siguientes:

EXTENSIÓN. Un mínimo de 6.000 palabras y un máximo de 9.000 a espacio y medio, en DIN A-4.

TÍTULO Y AUTORÍA. En la primera página constará el título, en mayúsculas y negrita, y, debajo, el nombre del autor (en mayúsculas), indicando puesto de trabajo o profesión.

Se adjuntará adicionalmente breve CV del autor.

RESUMEN Y PALABRAS CLAVE. Precedido de la palabra "Resumen" se incluirá a continuación un extracto en castellano de unas 10-15 líneas. A continuación, en otro párrafo, un "Abstract", traducción al inglés del resumen anterior. En el párrafo siguiente se incluirán las palabras clave, en un máximo de cinco, precedidas por la expresión "Palabras clave". A continuación, en párrafo nuevo, esas palabras clave en inglés precedidas de la expresión "Key words".

ESTRUCTURA. Los trabajos se dividirán en apartados y secciones (2 niveles), con su propio título, numerados. Se titularán en mayúscula negrita en el primer nivel de jerarquía y con mayúscula redondo en el segundo (sin negrita). Si fuera necesario un tercer nivel se escribiría en minúscula y negrita, y el cuarto en minúscula y cursiva.

TIPO DE LETRA. Times New Roman de tamaño 12 puntos. Las notas y fuentes bibliográficas serán de la misma letra, tamaño 10 puntos.

CUADROS Y FIGURAS. Serán numerados e incluirán una breve titulación.

PÁRRAFOS. Sangrado de 5 espacios. Espacio interlineal 1,5.

Se evitará la utilización de negrita y palabras subrayadas en el cuerpo del texto. Se utilizará letra cursiva para los títulos de libros y otras fuentes o para la inclusión dentro del texto de palabras o expresiones en otro idioma diferente al del artículo.

NOTAS. Serán las imprescindibles y se situarán al final del artículo de forma numerada.

REFERENCIAS Y CITA BIBLIOGRÁFICA. Se utilizará el sistema APA (http://www.apastyle.org/ http://normasapa.com/)

- En el texto

Se utilizará el sistema APA, en el texto del artículo, para citar autoría y fecha, evitando en todo caso el uso de notas a pie de página. Ejemplo: (García, 2014) o "según García (2014) las condiciones…."

- Bibliografía

Se limitará a las fuentes bibliográficas utilizadas y referenciadas en el texto. Sigue orden alfabético de apellido de autores.

Ejemplos:

1. Libro:

Mansky, C. (2013). Public Policy in an Uncertain World. London: Harvard University Press.

2. Artículo o capítulo de libro:

Antaki, C. (1988). Explanations, communication and social cognition. En C. Antaki (Ed.), Analysing

everyday explanation. A casebook of methods (pp. 1-14). London: Sage.

3. Artículo:

Moskalenko, S.; McCauley, C. (2010). Measuring Political Mobilisation: The Distinction Between Activism and Radicalisation. Terrorism and Political Violence, vol. 21, p. 240.

4. Artículo de revista on-line:

Blanco, J. M.; Cohen, J. (2014).The future of counter-terrorism in Europe. The need to be lost in the correct direction. European Journal of Future Research, vol. 2 (nº 1). Springer. Extraído el 1 de enero de 2015 de: http://link.springer.com/article/10.1007%2Fs40309-014-0050-9

5. Contenidos on-line:

Weathon, K. (2011). Let's Kill the Intelligence Cycle. Sources and Methods. Extraído el 1 de enero de 2015 de: http://sourcesandmethods.blogspot.com/2011/05/lets-killintelligence-cycle-original.html

6. Artículos o noticias de periódico:

Schwartz, J. (10 de septiembre de 1993). Obesity affects economic, social status. The Washington Post, pp. B1, B3, B5-B7

ORGANISMOS Y SIGLAS. Siempre que sea posible se utilizarán las siglas en castellano (OTAN, y no NATO; ONU y no UNO). La primera vez que se utilice una sigla en un texto se escribirá primero la traducción o equivalencia, si fuera posible, y a continuación, entre paréntesis, el nombre en el idioma original, y la sigla, separados por una coma, pudiendo posteriormente utilizar únicamente la sigla:

Ejemplo: Agencia Central de Inteligencia (Central Inteligencia Agency, CIA).

Se acompañará en soporte informático, preferentemente Microsoft Word. Las fotografías y ficheros se remitirán también en ficheros independientes. Se podrá remitir por correo electrónico a esta dirección: CAP-cuadernos@guardiacivil.org

Los trabajos se presentarán, precedidos por una ficha de colaboración en la que se hagan constar: título del trabajo, nombre del autor (o autores), dirección, NIF, número de teléfono y de fax, situación laboral y nombre de la institución o empresa a la que pertenece. Igualmente se presentará una ficha de cesión de derechos de autor, que se facilitará oportunamente.

Los artículos serán evaluados por el Consejo de Redacción. Se enviarán a los autores las orientaciones de corrección que se estimen pertinentes, salvo aquellas de carácter menor, que no afecten al contenido y que puedan ser realizadas por el equipo de redacción (correcciones de tipo ortográfico, de puntuación, formato, etc.).

Los autores de los trabajos publicados en la Revista serán remunerados en la cuantía que establezca el Consejo de Redacción, salvo aquellos casos en que se trate de colaboraciones desinteresadas que realicen los autores.

A todos los autores que envíen originales a la Revista "Cuadernos de la Guardia Civil" se les remitirá acuse de recibo. El Consejo de Redacción decidirá, en un plazo no superior a los seis meses, la aceptación o no de los trabajos recibidos. Esta decisión se comunicará al autor y, en caso afirmativo, se indicará el número de la Revista en el que se incluirá, así como fecha aproximada de publicación.

Los artículos que no se atengan a estas normas serán devueltos a sus autores, quienes podrán reenviarlos de nuevo, una vez hechas las oportunas modificaciones.

Los trabajos que se presenten deberán respetar de forma rigurosa los plazos que se indiquen como fecha máxima de entrega de los mismos.

Ni la Dirección General de la Guardia Civil ni "Cuadernos de la Guardia Civil" asume las opiniones manifestadas por los autores.

El **Instituto Universitario de Investigación sobre Seguridad Interior** se creó mediante la firma de un convenio de colaboración suscrito entre el Ministerio del Interior, la Dirección General de la Guardia Civil y la Universidad Nacional de Educación a Distancia, el 17 de octubre de 2002, pues la Guardia Civil y la UNED llevaban vinculadas por distintos acuerdos de colaboración desde 1988 y precisaban de un centro especializado en la investigación, enseñanza y asesoramiento en materias relacionadas con la seguridad.

IUISI pretende desarrollar y promover la investigación científica de alta calidad en materias de seguridad que sean de interés para instituciones públicas y privadas, impulsar y promover la difusión de obras científicas, y crear un marco de reflexión y diálogo.

Entre sus actividades, en el plan para 2015, se incluye:

- La investigación. Ayudas/becas para la realización de trabajos según la convocatoria anual.
- La realización de seminarios y jornadas:
    - XXVI Duque de Ahumada
    - V Seminario Internacional / I Seminario en misiones internacionales
    - IV Inteligencia y Seguridad
    - III Taller Prospectiva
    - II Taller Operaciones Conjuntas
    - I Taller Fronteras
    - I Seminario Terrorismo
    - Custodia de puertos y aeropuertos
    - El ciclo político de la Unión Europea como estrategia de lucha contra el crimen organizado
    - Jornadas sobre cultura de seguridad en las Universidades
    - III Jornadas de igualdad: Los planes de igualdad y su consecución a la equidad
    - Retos, tendencias y Oportunidades de las TIC
    - Fundamentos de la contratación en el sector público
- Otras acciones que se irán anunciando en su página web: www.iuisi.es