Cuadernos de la Guardia Civil

Revista de Seguridad Pública

Núm. 64-2021

GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR
GUARDIA CIVIL
DIRECCIÓN GENERAL

CUADERNOS DE LA GUARDIA CIVIL

REVISTA DE SEGURIDAD PÚBLICA

3ª ÉPOCA

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: 126-15-005-2
NIPO: 126-19-068-8 (edición epub)

EDITA

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

Páginas oficiales de Cuadernos de la Guardia Civil
http://www.guardiacivil.es/es/institucional/Cuadernos_de_la_Guardia_Civil/index.html
http://cuadernosdelaguardiacivil.es/

Lista de los números en KOBLI
https://biblioteca.guardiacivil.es/cgi-bin/koha/opac-shelves.pl?op=view&shelfnumber=59

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 debe remitir su trabajo treinta días antes de la publicación de la Revista. El primer número de cada año se publica a finales del mes de marzo, el segundo a finales de junio, el tercero a finales de septiembre y el cuarto a finales de diciembre. 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:

https://biblioteca.guardiacivil.es/cgi-bin/koha/opac-shelves.pl?op=view&shelfnumber=59

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

LA AMENAZA HÍBRIDA EN LA ZONA GRIS: APROXIMACIÓN CONCEPTUAL

BALBINO ESPINEL

COMANDANTE. ESTADO MAYOR DE LA GUARDIA CIVIL

Fecha de recepción: 03/03/2021. Fecha de aceptación: 04/06/2021

RESUMEN

En el actual contexto de las sociedades líquidas descritas por Bauman, en las que los términos “amigo, enemigo, competidor y adversario” se han difuminado, la amenaza híbrida surge como una manera de erosionar los valores democráticos. Las políticas de seguridad nacional deben estar preparadas para hacer frente a esta amenaza, que se presentará a través de estrategias híbridas en el umbral del espectro del conflicto conocido como “zona gris”.

El objetivo de este artículo es contribuir al estudio de los conceptos amenaza híbrida y zona gris, cada vez más recurrentes en el ámbito actual de la seguridad nacional y las relaciones internacionales, realizando un repaso por la evolución de su significado y proponiendo un nuevo matiz con el ánimo de facilitar su comprensión.

PALABRAS CLAVE: Amenaza híbrida, zona gris, seguridad nacional, Unión Europea, OTAN.

ABSTRACT

In today’s liquid societies described by Bauman, in which terms such as “friend, enemy, competitor, and adversary” have been blurred, the hybrid threat/warfare emerges as a way to erode democratic values. National security policies must be prepared to face this threat, which will present itself through hybrid strategies in the area of the conflict spectrum known as the “grey zone”.

The main objective of this article is to contribute to the study of the concepts of hybrid threat/warfare and grey zone, increasingly recurrent in the current field of national security and international relations, reviewing the evolution of their meaning and proposing a new nuance with the aim of facilitate their understanding.

KEYWORDS: Hybrid threat, hybrid warfare, gray zone, national security, European Union, NATO.

1. INTRODUCCIÓN

En ocasiones, en el ámbito de la seguridad surgen nuevos conceptos que, pese a ser utilizados reiterativamente, no siempre están suficientemente definidos

conceptualmente. Son los conocidos como buzzwords[1], caracterizados por Haas (2017) como «*términos de moda de utilidad analítica cuestionable y recorrido habitualmente efímero*» (citado en Jordán, 2018:130).

Tanto los términos "amenaza híbrida" como "zona gris" podrían considerarse a priori dentro de esta categoría y solo el paso del tiempo determinará si realmente han llegado para quedarse. En todo caso, en el entorno de la seguridad nacional y las relaciones internacionales estos conceptos están en boga y, pese a que aún no existe una armonización de su significado —el cual parece estar en un continuo proceso de construcción—, este artículo pretende profundizar en su origen y en el contexto en los que en la actualidad se utilizan.

Según la Doctrina para el empleo de la Fuerzas Armadas (JEMAD, 2018b), la zona gris es un continuo del espectro del conflicto situado entre la guerra y la paz. Muchas de las actuaciones que se realizan en esta zona se encuentran «*al margen del principio de buena fe entre estados» (Ibíd.:párr.363), alterando* notablemente la paz, pero sin cruzar las líneas rojas que permitirían una posible respuesta armada.

Es precisamente en esta indefinición donde la "amenaza híbrida" puede desarrollarse con mayor facilidad y donde diferentes actores, tanto estatales como no estatales, desarrollan las llamadas "estrategias híbridas".

Las primeras referencias al concepto de "guerra híbrida" surgieron en 2002 en alusión a los procedimientos empleados por la insurgencia chechena contra Rusia durante la Guerra de Chechenia (1994-1996). Sin embargo, no fue hasta 2005, con la publicación del artículo "La guerra del futuro: la llegada del conflicto híbrido", del general James N. Mattis y el teniente coronel Franck G. Hoffman, «*cuando se le dotó de contenido teórico*», teniendo lugar «*su primera gran manifestación práctica*» en la guerra de 2006 entre Hezbolah e Israel (Colom, 2014:2). Posteriormente, en 2013, el general ruso Valery Gerasimov realizó unas declaraciones conocidas como «*"Doctrina Gerasimov" sobre la guerra híbrida*», que provocaron «*la incorporación automática de este concepto al debate militar*» (Pérez, 2017).

Desde entonces, "lo híbrido" ha experimentado una serie de transformaciones conceptuales. Actualmente, según Colom (2019:4-5), las distintas concepciones abarcan «*desde cualquier actividad informativa, cibernética, subversiva o cinética realizada bajo el umbral del conflicto armado*», hasta «*cualquier manifestación de guerra política que entrañe el empleo de medios diplomáticos, informativos, militares, económicos, financieros, legales o de inteligencia en tiempo de paz, crisis o guerra*».

Por su parte, la visión de la Federación de Rusia acerca de la amenaza híbrida resulta muy interesante en cuanto que, para Rusia, son la OTAN y la Unión Europea quienes usan este tipo de estrategias, considerando que es precisamente la OTAN quien utiliza lo híbrido en los antiguos países del Pacto de Varsovia con el objetivo de atraerlos hacia Occidente. Lo más peculiar de esta circunstancia es que, a pesar de las distintas concepciones que tienen Rusia y Occidente sobre este concepto, según el contralmirante finlandés Georgij Alafuzoff (2018), «*las dos partes consideran que la amenaza híbrida es la más importante de nuestros días»* (citado en Palacios, 2019).

1 Según la web del *"Cambigde Dictionary", una buzzword es* «una palabra o expresión de un tema en particular que se ha puesto de moda al usarse mucho, especialmente en la televisión y *en los periódicos». Disponible en:* https://dictionary.cambridge.org/es/diccionario/ingles/buzzword.

En cualquier caso, no se debe perder de vista que, tal y como expone Colom (2018:36), «*el pensamiento militar ruso es más sistémico, complejo, sofisticado, solvente y estable de lo que nos sugieren los grandes titulares*».

Siguiendo los postulados de Robert Johnson (2017), el conflicto híbrido «*no es un fenómeno nuevo, sino el producto de un momento particular en las relaciones internacionales*» en las que la confianza de Occidente se ha depositado en la supremacía del poder militar, y actores, quizás menos potentes militarmente, se han visto obligados a utilizar estas estrategias penetrando «*en los dominios político, diplomático, militar, social y económico*», y cuyos resultados son «*complejos y desbordantes*» (citado en Curt, 2019:174).

Por todo ello, desde sus orígenes, "lo híbrido y lo gris" se sitúan en el centro de un debate académico en el que se discute si se trata de una nueva amenaza, o bien es una nueva manera de catalogar conceptos anteriores (conflicto asimétrico, estrategias por debajo del umbral de respuesta, etc.). Aunque este artículo no pretende entrar a dirimir el fondo de esta cuestión, el autor comparte la tesis de que las amenazas híbridas «*pese a no constituir en sí mismas realidades nuevas, sí que poseen componentes novedosos asociados a las tácticas que vienen utilizándose para su despliegue»,* entre las que destaca «*el uso del ciberespacio» (Galán,* 2018:22).

El cambio del orden mundial, «*cuyos componentes sociales, políticos y económicos no han dejado de alterarse desde el fin de la Guerra Fría*» (Galán, 2018:5-6); unas relaciones internacionales en las que «*no hay aliados eternos, sino intereses permanentes*» en continuo estado de transformación (Baños, 2017); y la actual interdependencia fruto de la globalización han incentivado la amenaza híbrida.

La Unión Europea, en consonancia con la OTAN y con los propios Estados miembros, ha tomado conciencia de las graves consecuencias que estas amenazas pueden provocar en la seguridad y en los valores democráticos que sustentan el actual sistema político. En consecuencia, desde el pasado año 2016 se está desarrollando toda una legislación enfocada a contrarrestar esta amenaza. La OTAN por su parte, preocupada también por sus efectos, está trabajando en la misma dirección y trata de buscar sinergias con la Unión Europea para combatir dichas amenazas.

Más allá de los avances supranacionales, en España la amenaza híbrida no ha tenido un desarrollo normativo determinante a pesar de algunas referencias que aparecen en diferentes documentos oficiales, como en la vigente Estrategia de Seguridad Nacional (ESN17) o en la Estrategia Nacional de Ciberseguridad (Presidencia del Gobierno, 2017, 2019).

El documento estratégico publicado por el Centro Superior de Estudios de la Defensa Nacional (CESEDEN) "Entorno Operativo 2035" (CCDC, 2019:19) describe «*el futuro escenario geopolítico y de seguridad basándose en las características de los entornos VUCA*», espacios volátiles, inciertos, complejos y ambiguos (por sus siglas en inglés), en los que «*los conceptos de "zona gris" y "amenaza híbrida" acabarán imponiéndose y monopolizando el debate sobre el conflicto*» (Ibíd.:61).

El Sistema de Seguridad Nacional, establecido en la Ley 36/2015 de Seguridad Nacional, es por definición el marco estratégico existente en España para afrontar la amenaza híbrida que se desarrolla en la zona gris. En este sentido, en la próxima Estrategia de Seguridad Nacional 2021, que actualmente está en fase de desarrollo, es probable

que la amenaza híbrida adquiriera un mayor peso específico. Esto provocará que todos los actores del Sistema de Seguridad Nacional, en el que el Ministerio del Interior tiene especial importancia por su papel dentro del Consejo de Seguridad Nacional, cada vez tengan que familiarizarse más al uso de esta terminología.

Las Fuerzas y Cuerpos de Seguridad, y en concreto el Cuerpo de la Guardia Civil, que contribuye a los quince ámbitos de la seguridad nacional que se recogen en la ESN17 y que tiene una importante participación en los diferentes Comités Especializados del Sistema de Seguridad Nacional, deben seguir sensibilizándose acerca de los riesgos de la amenaza híbrida, así como estudiando la manera de contribuir con sus capacidades a su detección y, llegado el caso, a su neutralización.

2. AMENAZA HÍBRIDA

En declaraciones oficiales de la OTAN y de la Unión Europea se utiliza habitualmente el concepto «*amenaza híbrida»* como traducción del término *hybrid warfare*[1]*. La traducción literal de este término es "el modo de hacer la* guerra utilizando armas híbridas", y no "la guerra híbrida" como tal, que en inglés se traduce como *hybrid war (Jordán,* 2018a). Fruto del escaso rigor en la traducción del término inglés *warfare por guerra, en sus* orígenes la amenaza híbrida y la guerra híbrida se utilizaban como sinónimos pese a ser dos conceptos diferentes como se expone a continuación.

Por otro lado, resulta importante distinguir, desde un punto de vista conceptual, la diferencia entre "amenaza" y "riesgo". Así, una *amenaza es cualquier* circunstancia que ponga en peligro la seguridad, mientras que el *riesgo es la* probabilidad de que una determinada amenaza se materialice provocando un daño (JEMAD, 2018b:párr.009).

2.1. DEFINICIONES ACADÉMICAS Y DOCTRINALES

Según Colom (2019:14), híbrido (entiéndase "amenaza híbrida") es «*cualquier actividad de influencia, de proyección del poder, de explotación social con vectores físicos, financieros, legales, informativos o psicológicos o la combinación de actividades militares regulares e irregulares*», pudiéndose establecer una continuidad en todo el espectro del conflicto, «*desde la paz hasta la guerra abierta, con actividades de distinto perfil, huella o atribución*».

Para el Mando de Adiestramiento y Doctrina del Ejército de Tierra (MADOC) (2017:4) lo híbrido es una «*forma ambigua de confrontación, que puede combinar acciones militares convencionales y no convencionales con acciones no militares basadas en una estrategia de desestabilización del adversario mediante el uso de acciones diversas, complementarias y sin restricciones, que integran todos los instrumentos de poder disponibles*[2]».

Una de las referencias más importantes en la delimitación de este concepto se encuentra en los documentos del proyecto *Countering Hybrid Warfare* (CHW)[3], elaborados en el entorno de la iniciativa *Multinational Capability Development Campaign*

2 Instrumentos de poder diplomático, militar, económico, social y de información, conocidos por el acrónimo DMESI.

3 *Countering Hybrid Warfare,* traducido como: Contrarrestar la amenaza híbrida.

(MCDC)[4], cuyo objetivo es precisamente desarrollar un marco analítico útil para comprender el actual "concepto híbrido"[5].

Así, para Reichborn-Kjennerud y Cullen (2017), *hybrid warfare (amenaza* híbrida) se define como el uso sincronizado de múltiples instrumentos de poder ejercidos sobre diferentes vulnerabilidades a lo largo de todos los ámbitos de un Estado, para lograr efectos sinérgicos de manera no lineal[6].

Según el modelo CHW#1, la amenaza híbrida tiene tres características:

«El uso combinado de múltiples instrumentos de poder para lograr asimetría a través de un amplio rango de vulnerabilidades», «el uso de estrategias híbridas que provoquen efectos sincronizados y de diferentes intensidades», y «el énfasis en la creatividad y la ambigüedad, para lograr efectos sinérgicos (incluso en el dominio cognitivo)» (Monaghan, Cullen y Wegge, 2019:13).

2.2. ORGANIZACIONES INTERNACIONALES

Para la OTAN (2016:párr.72), la amenaza híbrida (*hybrid warfare)* consiste en «*el empleo integrado por actores estatales y no estatales, de una combinación amplia, compleja y adaptativa de medios convencionales y no convencionales, y de medidas militares, paramilitares y civiles abiertas y encubiertas, para lograr sus objetivos». El actual secretario general Stoltenberg (2015) afirmó que «lo híbrido es el lado oscuro de nuestro Enfoque Integral»* (citado en Colom, 2019:5). A pesar de no ser una definición al uso, expresa de manera gráfica que lo híbrido consiste en poner en juego, de manera coordinada, los diferentes instrumentos de poder del Estado.

Una de las primeras definiciones de amenaza híbrida —*hybrid threat*— aparece en una publicación del Parlamento Europeo, en la que se expone que «*es un fenómeno resultante de la convergencia e interconexión de diferentes elementos, que en conjunto forman una amenaza más compleja y multidimensional*» (2015:1).

Según la Comunicación conjunta sobre la lucha contra las amenazas híbridas de la Unión Europea (2016:2), estas son una «*mezcla de actividades coercitivas y subversivas, de métodos convencionales y no convencionales (es decir, diplomáticos, militares, económicos y tecnológicos), […] utilizados de forma coordinada, […] para lograr objetivos específicos, manteniéndose por debajo del umbral de una guerra declarada oficialmente*».

En una Comunicación conjunta posterior (2018:1), se matiza que las estrategias híbridas presentan «*múltiples facetas y combinan las medidas coercitivas con las subversivas, y las herramientas y las tácticas convencionales con las no convencionales (diplomáticas, militares, económicas y tecnológicas), todo con el fin de desestabilizar al adversario*». Añadiendo además que estas «*están concebidas para que resulte*

4 Iniciativa multinacional liderada por los EE.UU. para desarrollar colaborativamente conceptos y capacidades para abordar nuevos desafíos asociados a las operaciones militares combinadas.

5 Su objetivo es que sirva de guía a los legisladores y miembros de las fuerzas armadas para desarrollar posibles soluciones a esta amenaza. Hasta ahora ha habido tres Proyectos de la MCDC sobre Hybrid Warfare, durante los ciclos 2015-16 (CHW#1), 2017-18 (CHW#2) y 2019-20 (CHW#3). Este tercero se encuentra en pleno desarrollo. España, ha participado en el 2 y en el 3, coordinando el Grupo de trabajo nacional el coronel Bonifacio Gutiérrez de León (MADOC).

6 Textualmente: «*The synchronized use of multiple instruments of power tailored to specific vulnerabilities across the full spectrum of societal functions to achieve synergistic effects*» (p.8).

difícil detectarlas o atribuirles autoría, y pueden ser llevadas a cabo por actores tanto estatales como no estatales».

Por su lado, según el *Hybrid Center of Excellence (Hybrid CoE)* la amenaza híbrida posee tres características[7]: es una acción coordinada y sincronizada contra las vulnerabilidades sistémicas de los Estados e instituciones democráticas a través de una amplia gama de elementos de poder; se aprovechan de los umbrales de detección y atribución (guerra/paz, amigo/enemigo); y su objetivo es influir en la toma de decisiones a nivel local (regional), estatal o institucional, para favorecer los objetivos estratégicos del agente provocador mientras socava los del objetivo atacado.

2.3. ESTRATEGIAS HÍBRIDAS

Según el Concepto de Empleo de las Fuerzas Armadas 2017-Cambio 2 (CEFAS17c2) las estrategias híbridas, «*con mayor o menor grado de ambigüedad y visibilidad, persiguen crear un clima de desinformación y confusión*» para desestabilizar y debilitar a sus adversarios (JEMAD, 2018a), se llevan a cabo en la zona gris del espectro del conflicto, dejando por lo tanto fuera del marco de estudio todo aquello relacionado directamente con la guerra híbrida[8].

«*Cuando una amenaza se materializa, mediando voluntad, se transforma en una agresión*» (JEMAD, 2018b:párr.011). En este sentido, las estrategias híbridas son la materialización de la propia amenaza híbrida utilizada por el adversario[9], lo que significa que las acciones pueden ser realizadas por «*actores, estatales o no, con capacidades convencionales y no convencionales suficientes para llevar a cabo una estrategia híbrida que les permita alcanzar sus objetivos*» (MADOC, 2017:6).

Por las razones antes mencionadas, algunas de las definiciones que se han publicado para conceptos como “acciones híbridas” o “amenazas híbridas”, en realidad se refieren a las propias estrategias híbridas. Así, la ESN17 (2017:16) define acciones híbridas como una combinación de acciones «*que pueden incluir, junto al uso de métodos militares tradicionales, ciberataques, operaciones de manipulación de la información, o elementos de presión económica, que se han manifestado especialmente en procesos electorales*», cuyo objetivo principal es «*la desestabilización, el fomento de movimientos subversivos y la polarización de la opinión pública*», y que pueden ser «*perpetradas tanto por Estados como por actores no estatales*» (Ibíd.:32).

Esto también ocurre cuando Galán (2018:3) se refiere a las amenazas híbridas como «*acciones coordinadas y sincronizadas […] que atacan deliberadamente*

7 Ver web oficial de “*The European Centre of Excellence for Countering Hybrid Threats”*. Disponible en: https://www.hybridcoe.fi/hybrid-threats/.

8 Las estrategias híbridas, propias de la zona gris, no se desarrollan exclusivamente en ella, sino que pueden darse también dentro de un conflicto armado. En ese caso, nos encontraríamos ante una situación de guerra híbrida, que se produce según explica el Mando de Adiestramiento y Doctrina del Ejército de Tierra (2017:8) «*cuando la amenaza híbrida no consigue sus objetivos estratégicos mediante acciones en la zona gris, o cuando los efectos de estas sobrepasan el umbral de respuesta del adversario».* Entonces –continúa- «*seguirá empleando todos sus instrumentos de poder y, además, combinará un amplio uso de actividades irregulares con operaciones militares convencionales».*

9 Según la PDC-01 (JEMAD, 2018b:párr.337), se considera adversario al «*conjunto de actores de un conflicto a los que se les reconoce como potencial o abiertamente hostiles para los intereses propios o aliados y contra los cuales se puede prever el uso de la fuerza».*

vulnerabilidades sistémicas de los Estados y sus instituciones a través de una amplia gama de medios y en distintos sectores objetivo (políticos, económicos, militares, sociales, informativos, infraestructuras y legales) utilizando el ciberespacio como la herramienta más versátil y adecuada para sus propósitos».

En el estudio de la polemología[10], la definición de estrategia del general Beaufre (citado en Santamaría, 2017), «*el arte de la dialéctica de voluntades», está muy* relacionado con el concepto de estrategia híbrida, puesto que aplicaba el concepto de estrategia a la conducción de todas las herramientas que dispone el Estado en situaciones de paz o de guerra, para lograr los objetivos establecidos por el poder político.

Para Ludendorf, en su teoría de la guerra total, la victoria se debe conseguir atacando «*los puntos débiles del enemigo, bien en un solo ataque, bien en varios ataques violentos»* (Rivas, 2011:71), proponiendo para ello usar «*todos los medios disponibles, los militares, los diplomáticos, los económicos, los psicológicos, en el interior como en el exterior».*

2.4. CONCEPTO DE AMENAZA HÍBRIDA

Teniendo en cuenta que los componentes de las diferentes definiciones son, grosso modo, los mismos, la conceptualización que realiza el MCDC anteriormente expuesta (sección 2.1 de este apartado) resulta muy interesante por considerarse la más completa. Además, es importante reseñar que la amenaza híbrida, ejercida a través de las estrategias híbridas, se puede encontrar en todo el espectro del conflicto (MADOC, 2017:4).

Por lo tanto, se observa que mientras que para hacer referencia a la amenaza híbrida en el entorno de la OTAN se utiliza el término *hybrid warfare,* en el ámbito de la Unión Europea se usa la forma en plural *hybrid threats[11]. Sin embargo, en documentos oficiales* europeos, es común encontrar *hybrid threats, traducido también por amenazas híbridas,* a pesar de que la redacción más acertada en la mayoría de ocasiones debería ser "estrategias híbridas", mientras que otras veces hace referencia a las distintas acciones utilizadas para lleva a cabo dichas estrategias (la desinformación[12], los ciberataques, el terrorismo, etc.)

A pesar de que en ocasiones se usen indistintamente, se considera importante usar estos términos con el mayor rigor posible. En el ámbito de este artículo se usa el concepto amenaza híbrida para referirse a la amenaza en sí y estrategias híbridas (no

10 La polemología, según el propio profesor francés Gaston Bouthoul, que introdujo el término en 1946, es la «ciencia de la guerra en general, estudio de sus formas, de sus causas, de sus *efectos y de sus funciones, como fenómeno social» (Serrano,* 1971:147).

11 En ocasiones la OTAN también ha hecho referencia a *hybrid threats, como en el documento* que hace una década analizaba las capacidades militares de la Alianza respecto a las amenazas híbridas. Entonces, el *Bi-Strategic Commands (2010:2), las definía como aquellas que plantean los* adversarios cuando presentan la capacidad de emplear simultáneamente medios convencionales y no convencionales de forma adaptativa en la búsqueda de sus objetivos.

12 Usando una definición de la Comisión Europea [COM (2018) 236 final], la desinformación es aquella «*información verificablemente falsa o engaños a que se crea, presenta y divulga con fines lucrativos o para engañar deliberadamente a la población y que puede causar un perjuicio público. El perjuicio público comprende amenazas contra los procesos democráticos políticos y de elaboración de políticas, así como contra los bienes públicos, como la protección de la salud, el medio ambiente o la seguridad de los ciudadanos de la UE. La desinformación no incluye los errores de información, la sátira y la parodia ni las noticias y los comentarios claramente identificados como partidistas».*

amenazas híbridas), para reflejar el uso sincronizado de instrumentos de poder que forman parte de la amenaza.

3. ZONA GRIS

La zona gris es otro ejemplo de *buzzword que apenas tiene diez años de* antigüedad. A pesar de que aún no se ha alcanzado un consenso conceptual, se han utilizado diferentes definiciones, cuyo estudio comparado permite encontrar las principales características de este concepto que, haciendo referencia a Clausewitz, está muy relacionado con la incertidumbre y la confusión que produce la "niebla de la guerra".

Los conflictos aparecen cuando varios Estados o actores no estatales tratan de alcanzar objetivos incompatibles entre sí. Aunque generalmente se trata de resolver los conflictos acudiendo a la diplomacia o a las organizaciones internacionales, la realidad es que no siempre se tiene éxito, existiendo continuamente un gran número de conflictos de muy diversa intensidad.

3.1. DEFINICIONES ACADÉMICAS

Según Baqués (2017), el conflicto en la zona gris es una «*competición estratégica entre dos o más Estados […] discurre por debajo del umbral de violencia política del conflicto armado menor*» (citado en Jordán, 2018a:131). Para Jordán (2018a: 133), «*es un espacio intermedio en el espectro de conflicto político que separa la competición acorde con las pautas convencionales de hacer política, del enfrentamiento armado directo y continuado*» cuyas principales características (Ibíd.:131-133) son: «*ambigüedad: ni relaciones pacíficas ni conflicto armado*», «*estrategias multidimensionales*», «*intereses sustanciales en juego*» y «*gradualismo*».

Por consiguiente, la primera deducción es que la zona gris es una parte del espectro del conflicto diferenciada por un extremo del conflicto armado —de la guerra— y por otro de la paz, entendida esta como la forma de hacer política situada dentro de parámetros mayoritariamente aceptados, conocidos como *politics as usual,* o principio de buena fe, la *bona fide (Jordán,* 2018b).

Una característica propia de esta zona gris es el uso mayoritario de herramientas de poder multidisciplinares: políticos, económicos, sociales, de información y diplomáticos, quedando relegados los instrumentos militares a la mínima expresión. El uso de la fuerza militar en la zona del espectro del conflicto es simbólico, al no estar en el umbral del conflicto armado se limita principalmente a la coerción.

El conflicto en la zona gris, el entorno por excelencia para poner en juego la amenaza híbrida, es de largo recorrido y con las acciones que se desarrollan en él se pretende lograr objetivos de manera paulatina, a través de una serie de acciones interconectadas. Según Mazarr (2015) y Echevarría (2016), consiste en intentar «*evitar respuestas contundentes al tiempo que va modificando la situación estratégica por suma de efectos» (citado* en Jordán, 2018:133). Los objetivos que se pretenden lograr al adentrarse en ella deben superar los grandes perjuicios que supone abandonar las normas diplomáticas convencionales en una paz, que «*no es sinónimo de armonía»* (Jordán, 2020).

Por todo ello, conceptualmente la zona gris se sitúa en el espacio ubicado entre la guerra híbrida y la paz en su estricto sentido teórico, que incluye la buena fe en la relación entre Estados. En puridad, la zona gris está dentro de la paz, si bien se trata de una paz intencionadamente forzada por alguno de los actores, hasta convertirla en el *modus operandi adecuado para alcanzar objetivos similares a* los de una guerra. Pero todo ello sin llegar a cruzar la línea roja que la definiría como tal de acuerdo con el derecho internacional e, idealmente, sin soliviantar el *statu quo entre los* diferentes actores.

Por el contrario, la guerra híbrida es, como su propio nombre indica, una manera de hacer la guerra. Así, cuando se hace relación a la guerra híbrida es importante conceptualizar este término en la zona del espectro conocido como conflicto armado, entrando en juego en consecuencia las leyes y usos de la guerra.

Jurídicamente (RAE/CGPJ, 2020) se define conflicto armado como la «*lucha entre partes contendientes con utilización de las armas, persistencia y manifiesta voluntad hostil*». Una herramienta que puede ayudar a clasificar el nivel de un conflicto es la definición de conflicto armado utilizado por el "*Uppsala Conflict Data Program*" (*UCDP*)[13], según el cual «*tiene que existir uso de fuerza armada entre al menos dos partes, y tiene que producirse más de veinticinco muertes relacionadas con el conflicto a lo largo de un año*» (Högbladh, 2019:28).

3.2. PUBLICACIONES OFICIALES

La primera vez que se utilizó el concepto de "conflicto en la zona gris" fue en la *Quadrennial Defense Review* estadounidense (2010) y su significado aludía «*al espectro del conflicto político que separa la paz (blanco) de la guerra (negro)*» (citado en Jordán, 2018:130).

Según la Publicación Doctrinal Conjunta PDC-01 (A) (JEMAD, 2018b:párr.358), «*el espectro de los conflictos [sic] relaciona el grado de violencia del entorno con el tipo de capacidades y actividades que la fuerza emplea en las operaciones*». Además, tal y como se señala en la Introducción, según la doctrina conjunta (Ibíd.:párr.362), «*el espectro de los conflictos [sic] se extiende desde las actuaciones en tiempo de paz, hasta el combate generalizado de alta intensidad, pasando por una zona gris de transición», situada «por debajo del umbral del conflicto armado»* (MADOC, 2017:4).

Según la doctrina militar estadounidense, en lugar de un mundo en paz o en guerra, el *competition continuum describe un mundo de competencia duradera* conducida a través de una mezcla de cooperación, de competencia por debajo del umbral del conflicto armado y de los propios conflictos armados (US JCS, 2019).

En el ámbito de la Unión Europea se utiliza el término "conflicto híbrido" como sinónimo de "conflicto en la zona gris". Así, el Servicio de Estudios del Parlamento Europeo distingue entre "conflicto híbrido" y "guerra híbrida"[14], aduciendo que son dos

13 El UCDP distingue entre conflicto armado estatal y conflicto armado no estatal, siendo la diferencia el requisito de que, en el primero de ellos, una de las partes tiene que ser un gobierno estatal.

14 Para el Parlamento Europeo, la GH es una «*situación en la que un país recurre al uso abierto de la fuerza (armada) contra otro país o contra un actor no estatal, además de usar otros medios (por ejemplo, económicos, políticos o diplomáticos)*» (European Parliament, 2015).

categorías mediante las cuales un Estado utiliza tácticas híbridas para lograr sus fines estratégicos. Para el Parlamento Europeo, el conflicto híbrido es una «*situación en la cual las partes se abstienen del uso abierto de la fuerza (armada) y actúan combinando la intimidación militar (sin llegar a un ataque convencional) y a la explotación de vulnerabilidades económicas, políticas, tecnológicas y diplomáticas*» (European Parliament, 2015; Galán, 2018:4).

3.3. IMPLICACIONES LEGALES DE LA ZONA GRIS

Identificar la naturaleza de la guerra es un desafío básico que se ha vuelto muy complicado en la actualidad, dado que las declaraciones de guerra se han convertido en cosas del pasado y el estado de guerra ha perdido gran parte de su estatus legal formal (Craig, 2012).

Hoy en día, la frontera entre la guerra y la paz se ha difuminado provocando que la mayor parte de los conflictos se sitúen en la zona gris. Según la PD1-001 del Ejército de Tierra (2011:2-1) el conflicto surge «*cuando dos o más colectividades o Estados persiguen objetivos incompatibles, que se excluyen mutuamente*».

Las implicaciones legales de la zona gris son muy beneficiosas para aquellos adversarios que pretendan lograr objetivos estratégicos sin recurrir al conflicto armado. Al no estar dentro del ámbito del conflicto armado, sus acciones no están sujetas a las normas del derecho de la guerra dado que, «*solo cuando existe un conflicto armado declarado y no encubierto […], se activa la aplicación del Derecho Internacional Humanitario*»[15] (Galán, 2018:4).

Actualmente, tanto la ONU como la OTAN y la Unión Europea trabajan en la mejora de la gobernanza de los espacios comunes globales para tratar de definir en qué ocasiones sería posible apelar a la defensa colectiva y las cláusulas de seguridad ante estrategias llevadas a cabo en la zona gris.

Además, otras organizaciones como la Organización para la Cooperación y el Desarrollo Económicos (OCDE) y la Organización para la Seguridad y la Cooperación en Europa (OSCE), constituyen también foros que fomentan las medidas de confianza, promoviendo comportamientos responsables entre los Estados.

3.4. CONCEPTO DE ZONA GRIS

La zona gris es, por lo tanto, el espacio del espectro del conflicto donde lo híbrido y el mantenimiento de los niveles de confrontación atentan contra los marcos de convivencia establecidos, pero sin llegar a la agresión (DSN, 2018).

15 El derecho internacional humanitario (DIH), se denomina también “derecho de la guerra” o “derecho de los conflictos armados”, y «*rige las relaciones entre los Estados, las organizaciones internacionales y otros sujetos del derecho internacional en tiempo de conflictos armados. Es una rama del derecho internacional público que consiste en un conjunto de normas cuya finalidad es proteger a las personas que no participan, o han dejado de participar, en las hostilidades y limitar los medios y los métodos de hacer la guerra»* (Jabre, Babic y Bouvier, 2018:8)

Figura nº 1. Espectro del conflicto. (Elaboración propia).

Pese a que no existe una definición consensuada tal y como se ha comprobado en los párrafos anteriores, las principales características de la zona gris son recurrentes en todas las conceptualizaciones de esta nueva realidad (figura 1).

- Es un continuo a lo largo del espectro del conflicto entre la confrontación —el conflicto armado[16], generalmente híbrido— y la paz. A pesar de la ambigüedad que suele rodear a las zonas grises, hay que tener en cuenta que, en puridad, estas se ubican dentro de la paz, siendo precisamente una de sus características el que no se lleguen a sobrepasar las líneas rojas que convertirían dichas realidades en conflictos armados.
- Busca objetivos estratégicos —generalmente a largo plazo—, cuyos beneficios esperados contrarrestan el problema que supone actuar al margen del principio de *bona fide.* Ejemplos de dichos objetivos podrían ser: la independencia de una parte de su territorio; la anexión, total o parcial de un territorio ajeno; forzar cambios de régimen, o incluso de gobierno, cuando ello implica cambios geopolíticos de relevancia —v. gr.—, entrar o salir de una organización internacional (Baqués, 2020).
- Es habitual un empleo gradual y coordinado de estrategias híbridas, realizando acciones sostenidas en el tiempo para tratar de alcanzar los mencionados objetivos. El instrumento de poder militar, en caso de utilizarse, está limitado a realizar acciones coercitivas.

Por todo ello, la zona gris es diferente al conflicto armado híbrido o guerra híbrida[17], no pudiendo clasificarse un conflicto en ambas categorías.

4. LA AMENAZA HÍBRIDA EN LA ZONA GRIS

La mayoría de autores asumen que uno de los atributos de la zona gris es el uso de estrategias híbridas, dando lugar a que al establecer las características de la zona gris (un tipo de conflicto), estas converjan con las de la amenaza híbrida (un tipo de amenaza). Sin embargo, hay que distinguir ambos términos por ser conceptualmente distintos.

16 Según la PDC-01 (A) (JEMAD, 2018b:párr.013), «*el conflicto armado se caracteriza por la confrontación entre colectividades organizadas, no necesariamente reconocidas a la luz del derecho internacional, y en donde se utilizan medios de combate con la finalidad de imponer una voluntad sobre la otra».*

17 La guerra híbrida es un conflicto armado en el que coexisten estrategias militares convencionales e híbridas, pero predominan estas últimas.

«En la zona gris, la amenaza híbrida identificará las "líneas rojas" que podrían provocar la respuesta armada del adversario y actuará dentro de esos límites, en los que sus oponentes no pueden responder de igual modo debido a la ambigüedad o a las restricciones legales o éticas. Para ello empleará, de forma coordinada y sincronizada, todos sus instrumentos de poder, combinando todo tipo de actividades coercitivas, subversivas, etc., y con la ambigüedad como elemento esencial para dificultar la respuesta del contrario. Centrará sus objetivos en la sociedad civil y en el deterioro de su modo de vida, cohesión y economía.

Estas acciones, de naturaleza político-estratégica, con baja visibilidad y huella reducida, se caracterizan por su agresividad en los fines, la inseguridad jurídica de la población civil, y la desinformación dirigida hacia terceros actores (comunidad internacional) para inducir percepciones erróneas en todos los niveles» (MADOC, 2017:7).

Conviene resaltar que, entre los objetivos últimos de este tipo de conflictos, subyace el deseo de deteriorar la confianza de los ciudadanos en las instituciones, tanto globales como nacionales, además de ganar poder relativo con relación al sujeto sobre que el que desarrollan estas estrategias, debilitando su capacidad de decisión y reduciendo su libertad estratégica.

Centrarse en la zona gris implica poner el foco en el umbral del espectro del conflicto conocido como tal, y cuyas características se han visto en el apartado anterior, distinguiéndolo del umbral de la guerra híbrida, zona diferente del espectro del conflicto, incluida en el conflicto armado, y donde también se utilizan estrategias híbridas.

Una dificultad detectada, al estudiar conceptualmente estos términos, es que ciertos autores se limitan a contemplar la posibilidad de que esta amenaza esté protagonizada por actores estatales. La mayoría, sin embargo, son menos exclusivos, admitiendo que «*las amenazas híbridas pueden partir tanto de Estados como de agentes no estatales*» (Galán, 2018:4).

5. CONCLUSIONES

Aunque las estrategias híbridas se han utilizado históricamente en los conflictos para desestabilizar al enemigo, lo que marca la diferencia actualmente es la velocidad e intensidad en los cambios, y la disrupción tecnológica fruto de la digitalización y la interconectividad global. En este contexto surgen los *buzzwords "híbrido",* "zona gris" y otros tantos conceptos relacionados (amenaza híbrida, guerra híbrida, conflicto híbrido). Como se ha expuesto a lo largo del artículo, a pesar de que no existe una definición consensuada, la amenaza híbrida y la zona gris son conceptos semánticos diferentes, por lo que no es conveniente que se usen de forma aleatoria.

Como se ha expuesto, las estrategias híbridas se emplean en la mayor parte del espectro del conflicto, si bien son más habituales en la zona gris (o conflicto híbrido) y en los conflictos armados híbridos (o guerra híbrida). La diferencia entre ambas es que la zona gris está situada conceptualmente en la paz. Por este motivo, en las estrategias híbridas las acciones militares se limitan de manera que no se escalen hasta generar un conflicto armado.

Un problema fundamental radica en la categorización de la zona gris. Pese a que entre sus características figura el uso habitual de estrategias híbridas, no parece que estas sean necesarias para poder definir un conflicto como tal. La contextualización de las relaciones internacionales implica que ciertas situaciones complejas puedan ser consideradas como híbridas, pero la tendencia en algunos medios de comunicación a

caracterizar casi cualquier comportamiento "extraño" como guerra híbrida, abusando del término, supone generar un alarmismo innecesario. De hecho, que la paz no sea sinónimo de armonía no significa que los Estados estén permanentemente siendo objeto de estrategias híbridas.

Así, para que una acción (un ciberataque dirigido contra una infraestructura crítica, por ejemplo) esté contemplada dentro de una estrategia híbrida, el adversario debe utilizar otros vectores de manera sinérgica, como una campaña de desinformación o medidas de presión económica, y además todos ellos deberían tener un objetivo dirigido a socavar los intereses más profundos de un Estado.

Por consiguiente, muchos ciberataques e incluso campañas de desinformación tienen otros objetivos y no forman parte de campañas híbridas, pudiendo llegar en algunas ocasiones a constituir meros delitos más o menos graves.

En aras a una mejor definición del problema, y asumiendo que una sola acción no puede catalogarse como una estrategia híbrida, se propone dividir conceptualmente la zona gris en dos partes (figura 2).

Figura nº 2. Propuesta de división del espectro del conflicto. (Elaboración propia).

Por un lado, una "Zona Gris Claro" o "*Soft Grey Zone" caracterizada por los* componentes esenciales de la zona gris pero sin que se produzcan estrategias híbridas. En esta zona del espectro, los diferentes actores emplean acciones de múltiples ámbitos, en ocasiones aprovechándose unas de las vulnerabilidades que creadas por otras[18], pero no sincronizadas entre sí. De esta manera, la *Soft Grey Zone podría ayudar* a entender de una manera más sencilla la situación actual de las relaciones entre diferentes Estados, considerando que la paz absoluta sería un ideal difícil de alcanzar, al constituir la anormalidad de la zona gris una situación cuasi permanente.

Y por otro lado la propia zona gris, entendida como aquella en la que los actores hostiles, estatales o no, sí ejercen estrategias híbridas, coordinando sus acciones con la finalidad de alcanzar unos objetivos estratégicos definidos Distinguir una zona de las otras no será sin duda un trabajo sencillo para los analistas, debido a la ambigüedad y a los efectos no lineales que rodean todo este tipo de estrategias.

18 Durante la crisis de la COVID-19, diferentes lobbies, movimientos secesionistas e incluso Estados tratan de generar desinformación para desacreditar o debilitar a las Instituciones, criticando su gestión. Este tipo de acciones no deben confundirse con la simple crítica ligada al derecho de expresión, sino que buscan una finalidad estratégica (De Pedro, 2020).

Debido a las propias vulnerabilidades que presenta nuestra sociedad en la actualidad, las operaciones de desinformación y las ciberamenazas constituyen habitualmente la punta de lanza de la amenaza híbrida. Aunque ambas constituyen dos vectores muy utilizados en las estrategias híbridas, no son ni necesarios ni suficientes para que una estrategia se pueda catalogar como tal.

La manipulación de la realidad y la mentira han sido parte de dichas relaciones de poder entre Estados, mucho antes de que Kapuściński (n.d.) descubriese que la verdad dejaba de ser importante cuando era parte de un negocio (citado en Hofer, 2018:33). El conocido como poder relacional, la posibilidad de modificar opiniones, emociones, actitudes o predisposiciones de otras personas es, probablemente hoy, el más importante de los poderes. Su ámbito de actuación principal es el ciberespacio, en el que se difuminan las fronteras, y permite que tanto actores estatales como no estatales con menos capacidades económicas estén en disposición de poner en juego su alta capacidad de influencia.

La desinformación, que tradicionalmente se ha utilizado en los conflictos, en nuestros días se ha convertido en un riesgo para la democracia. Con el desarrollo de internet y las redes sociales, urge concienciar a la población de la gravedad que esta amenaza puede producir en muchos ámbitos de sus vidas, provocando un complejo e incierto escenario en el que, a través de los medios de comunicación social, se puede llegar a manipular a la sociedad, modificando de manera subversiva los estados de opinión.

El ciberespacio es un elemento dinamizador de las estrategias híbridas. Su importancia no dejará de aumentar, lo que forzará a establecer nuevas normas legales que permitan alcanzar niveles de seguridad aceptables en el ámbito lógico. Probablemente, de lo rápida y efectiva que sea la adaptación de la sociedad a la nueva situación, dependerá el futuro de nuestro modelo de vida.

Aunque en el ámbito de las Fuerzas Armadas el concepto amenaza híbrida en la zona gris ha sido ampliamente estudiado en los últimos años, el hecho de que, en las estrategias híbridas, el componente militar sea solo una parte de los instrumentos que pueden utilizarse en las mismas (políticos, económicos, sociales, de información y diplomáticos) provoca que dicha terminología esté calando en el resto de actores de la sociedad, generando a su vez que la población sea cada vez más consciente de esta amenaza y de su necesaria participación para contribuir a la seguridad colectiva.

La sensibilización acerca de los riesgos de la amenaza híbrida y el aumento de la cultura de seguridad nacional se tornan, por consiguiente, aspectos prioritarios. Los Estados se basan en que la sociedad acepte y coopere de forma voluntaria con las estructuras de poder establecidas, y que son en sí mismas objetivos potenciales de las propias estrategias híbridas.

Por lo tanto, hay que tener en cuenta que en las actuales sociedades líquidas descritas por Bauman, en las que los términos “amigo, enemigo, competidor y adversario” se han difuminado, la amenaza híbrida surge como una manera de erosionar los valores democráticos de Occidente. Por ello, las políticas de seguridad nacional deben estar preparadas para hacer frente a esta amenaza, que se presentará como se ha expuesto a través de estrategias híbridas en la zona del espectro del conflicto conocida como “zona gris”.

Como la finalidad última de las estrategias híbridas es la propia sociedad y sus valores, y dado que el centro de gravedad de la misma son los ciudadanos y su cohesión social, estos deben tomar conciencia de la necesidad de convertirse en actores activos de la seguridad, puesto que el Estado no podrá proporcionársela sin su propia contribución. El hecho de que la amenaza híbrida no esté suficientemente definida complica la sensibilización acerca de sus verdaderos riesgos. Las instituciones tienen que ganarse la confianza de los ciudadanos generando credibilidad, para convencerles no solo de los peligros que las estrategias híbridas conllevan, sino de que estas ya podrían estar actuando.

De hecho, aunque la responsabilidad principal de la detección y la reacción recae en los diferentes Estados, la sociedad al completo debería involucrarse cada vez más en la prevención. Haciendo un paralelismo con las palabras pronunciadas por el JEMAD el mes de marzo de 2020, durante las ruedas de prensa acerca de la pandemia provocada por la COVID-19[19], la amenaza híbrida provocará "situaciones irregulares y raras que afectarán a toda la sociedad, y en las que todos los ciudadanos deberán comportarse como soldados". Por ello, resulta necesario potenciar la cultura de Seguridad Nacional conforme a las premisas de un Estado de derecho.

De todo lo anterior se deduce que para luchar contra la amenaza híbrida en la zona gris se requieren estrategias en esencias transversales, diseñadas desde puntos de vista multidisciplinares y en las que se implique no solo a las instituciones y organismos públicos, sino a la empresa privada y a los propios ciudadanos.

En este sentido, los diferentes Departamentos ministeriales, y en especial el Departamento de Seguridad Nacional dependiente de la Presidencia del Gobierno, deben ser cada vez más conscientes de su importante papel frente a la amenaza hibrida bajo la premisa de que ninguna institución u organismo en sí mismo será capaz de detectarla por sí solo, y que incluso se tornará fundamental en muchas ocasiones la cooperación internacional con nuestros socios y aliados para poder hacerle frente.

En el ámbito del Ministerio del Interior, es importante que se continúe estudiando y analizando de qué manera las Fuerzas y Cuerpos de Seguridad del Estado pueden contribuir con sus capacidades a la lucha contra la misma. Hay que tener en cuenta que, en ocasiones, detrás de acciones de índole terrorista, de acciones vinculadas al crimen organizado o incluso relacionadas con otros ámbitos de la seguridad como el entorno ciber, la protección de las infraestructuras críticas, la ordenación del flujos migratorios e incluso la preservación del medio ambiente, pueden esconderse otros intereses estratégicos superiores que supongan una verdadera amenaza híbrida en la zona gris.

Parafraseando al general MacArthur[20], quizás hoy no sea demasiado tarde, pero puede que mañana sí, para alinear todas nuestras fuerzas contra la amenaza híbrida.

19 Citas textuales del general del aire Miguel Ángel Villarroya Vilalta pronunciadas en marzo de 2020: «*Esto es una guerra de todos los españoles. Todos estamos involucrados en esta pelea contra el virus», «En esta guerra irregular y rara que nos ha tocado vivir o luchar, todos somos soldados» (Travieso, 2020).*

20 Cita del general MacArthur, pronunciada el 16 de septiembre de 1940 (Imparato, 2000:122): «*The history of the failure of war can almost be summed up in two words: too late. Too late in comprehending the deadly purposes of a potential enemy. Too late in realizing the mortal danger. Too late in preparedness. Too late in uniting all possible forces for resistance. Too late in standing with one's friends. […] Not too late, not tomorrow, but today*».

Lograr este reto dependerá tanto de la sociedad como de sus dirigentes y estará vinculado a la concienciación, a la cohesión y a la visión de futuro.

BIBLIOGRAFÍA

Ley 36/2015, de 28 de septiembre, de Seguridad Nacional (BOE núm. 233, de 29 de septiembre de 2015): Disponible en: https://www.boe.es/boe/dias/2015/09/29/pdfs/BOE-A-2015-10389.pdf.

Baños, P. (2017): Así se domina el mundo. Desvelando las claves del poder mundial. 1a edición. Barcelona: Ariel.

Bi-Strategic Commands (SACEUR/ SACT) (2010): Military Contribution to Countering Hibrid Threats. Belgium/ Norfolk (Virginia). Extraído el 12 de septiembre de 2020 de: https://www.act.nato.int/images/stories/events/2010/20100826_bi-sc_cht.pdf .

Centro Conjunto de Desarrollo de Conceptos (CCDC) (2019): Entorno Operativo 2035, Ministerio de Defensa.Extraído el 25 de noviembre de 2020 de: http://www.ieee.es/Galerias/fichero/O trasPublicaciones/Nacional/2019/entorno_ operativo_2035.pdf.

Colom, G. (2019): "La amenaza híbrida: mitos, leyendas y realidades", Instituto Español de Estudios Estratégicos (IEEE), (Documento de Opinión IEEE 24/2019). Extraído el 18 de noviembre de 2020 de: http://www.ieee.es/Galerias/fichero/docs_opinion/2019/DIEEEO24_2019GUICO L-hibrida.pdf.

Colom Piella, G. (2014): "¿El Auge de los Conflictos Híbridos?", Instituto Español de Estudios Estratégicos (IEEE), (Documento de Opinión 120/2014), pp. 1-13. Extraído el 13 de septiembre de 2020 de: http://www.ieee.es/Galerias/fichero/docs_opinion/2014/DIEEEO120-2014_GuerrasHibridas_Guillem_Colom.pdf.

Colom Piella, G. (2018): "La doctrina Gerasimov y el pensamiento estratégico ruso contemporáneo", Revista Ejército no 933, diciembre. Extraído el 20 de diciembre de 2020: http://www.ejercito.mde.es/Galerias/Descarga_pdf/EjercitoTierra/revista_ejercito/primer_premio_2019.pdf.

Comisión Europea (2018): Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. La lucha contra la desinformación en línea: un enfoque europeo; 26/04/2018; COM(2018) 236 final. Bruselas. Extraído el 13 de julio de 2020 de: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52018DC0236&from=PL.

Comisión Europea/Alta Representante de la Unión para Asuntos Exteriores y Política de Seguridad (2016): Comunicación conjunta sobre la lucha contra las amenazas híbridas. Una respuesta de la Unión Europea. Comunicación conjunta al Parlamento Europeo y al Consejo; 06/04/2016; JOIN (2016) 18 final. Bruselas. Extraído el 13 de agosto de 2020 de: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52018DC0236&from=PL.

Comisión Europea/Alta Representante de la Unión para Asuntos Exteriores y Política de Seguridad (2018): Aumentar la resiliencia y desarrollar las capacidades para hacer frente a las amenazas híbridas. Comunicación Conjunta al Parlamento Europeo, al Consejo Europeo y al Consejo; 13/06/2018; JOIN (2018) 16 final. Bruselas. Extraído

el 19 de diciembre de 2020 de: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52018JC0016&from=ES.

Craig, R. (2012): "Thucydides and contemporary strategy", en U.S. Army War College Guide to National Security Issues: Theory of war and strategy. 5th Ed. J. Boone Bartholomees, Jr.

Curt García, L. (2019): "La manifestación de la guerra híbrida en el ámbito marítimo: algunas claves para la seguridad nacional.", en Tirant Lo Blanch (ed.) Estrategia de seguridad marítima de España. Una agenda de actualización. Valencia.

Departamento de Seguridad Nacional (2018): "Informe Anual de Seguridad Nacional 2018". Extraído el 12 de abril de 2020 de: https://www.dsn.gob.es/es/documento/informe-anual-seguridad-nacional-2018.

European Parliament (2015): "Understanding Hybrid threats", At a glance, (June). Extraído el 21 de diciembre de 2020 de: http://www.europarl.europa.eu/RegData/etudes/ATAG/2015/564355/EPRS_ATA(2015)564355_EN.pdf.

Galán, C. (2018): "Amenazas híbridas: nuevas herramientas para viejas aspiraciones", Real Instituto Elcano, (Documento de trabajo 20/2018). Extraído el 18 de agosto de 2019 d e: http://www.realinstitutoelcano.org/wps/wcm/connect/b388b039-4814-4012-acbf-1761dc50ab04/DT20-2018-Galan-Amenazas-hibridas-nuevas-herramientas-para-viejas-aspiraciones.pdf?MOD=AJPERES&CACHEID=b388b039-4814-4012-acbf-1761dc50ab04.

Hofer, P. A. (2018): Factores de atribución por daños al honor, a la intimidad y a la propia imagen derivados de los medios masivos de comunicación. Salamanca. Extraído el 20 de mayo de 2020 de: https://gredos.usal.es/bitstream/handle/10366/139594/DDP_HoferPA_Dañosalhonor.pdf?sequence=1&isAllowed=y.

Högbladh, S. (2019): "UCDP GED Codebook version 19.1", (19.1), pp. 1-34. Extraído el 16 de octubre de 2020 de: https://ucdp.uu.se/downloads/ged/ged191.pdf.

Imparato, E. T. (2000): General MacArthur. Speeches and reports 1908-1964. Turner Publishing Company. Extraído el 3 de mayo de 2020 de: https://books.google.es/books?id=F-ILUHbWtncC&printsec=frontcover&hl=es&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=true.

Jabre, K., Babic, N. y Bouvier, A. (2018): Derecho internacional humanitario. Unión Interparlamentaria (UIP) y Comité Internacional de la Cruz Roja (CICR). Extraído el 22 de julio de 2020 de: https://www.refworld.org.es/pdfid/5b7201ad4.pdf.

JEMAD (2018a): Concepto de Empleo de las Fuerzas Armadas 2017 (Cambio 2). Madrid. Extraído el 18 de agosto de 2019 de: http://www.emad.mde.es/Galerias/home/files/170306- cefas-DEFINITIVO.pdf.

JEMAD (2018b): PDC-01(A) Doctrina para el empleo de las FAS. Madrid. Extraído el 10 de agosto de 2019 de: https://publicaciones.defensa.gob.es/pdc-01-a-doctrina-para-el- empleo-de-las-fas-libros-papel.html.

Jordán, J. (2018a): "El conflicto internacional en la «Zona Gris»: una propuesta teórica desde la perspectiva del realismo ofensivo", Revista Española de Ciencia Política, pp.

129-151. Extraído el 7 de octubre de 2020 de: https://www.ugr.es/~jjordan/Conflicto-zona-gris.pdf.

Jordán, J. (2018b): "No es una nueva Guerra Fría: son conflictos en la 'zona gris'", Agenda Global (El País). Extraído el 20 de julio de 2020 de: http://agendapublica.elpais.com/no-es-una-nueva-guerra-fria-son-conflictos-en- la-zona-gris/.

Jordán, J. (2020): "Ceuta y Melilla: ¿emplea Marruecos estrategias híbridas contra España?", Global Strategy. Universidad de Granada. Extraído el 17 de julio de 2020 de: https://global-strategy.org/ceuta-y-melilla-emplea-marruecos-estrategias- hibridas-contra-espana/.

MADOC (2011): PD1-001 Empleo de las fuerzas terrestres. Fecha entrada en vigor: 14/12/2011.

MADOC (Dirección de Investigación Doctrina Orgánica y Materiales) (2017): Concepto derivado 02/17: Lo híbrido. Granada.

Monaghan, S., Cullen, D. P. J. y Wegge, N. (2019): Countering Hybrid Warfare, MCDC Countering Hybrid Warfare Project. Extraído el 22 de septiembre de 2020 de: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/att achment_data/file/784299/concepts_mcdc_countering_hybrid_warfare.pdf.

OTAN (2016): Warsaw Summit Communiqué. 09/07/2016; Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016. Disponible en: http://www.nato.int/cps/en/natohq/official_texts_133169.htm.

Palacios, J. M. (2019): El contralmirante Alafuzoff y la guerra híbrida, Grupo de Estudios en Seguridad Internacional (GESI). Universidad de Granada. Extraído el 14 de noviembre de 2019 de: https://global-strategy.org/el-contralmirante-alafuzoff-y-la-guerra- hibrida/.

de Pedro, N. (2020): "Crisis del coronavirus: la desinformación del separatismo catalán como desafío estratégico para España", Instituto de Seguridad y Cultura. Extraído el 12 de junio de 2020 de: https://seguridadycultura.org/wp-content/uploads/2020/04/ISC_Desinfo-CAT_AFF.pdf.

Pérez Mozas, C. (2017): La desinformación como táctica de injerencia política: Rusia en el «procés» catalán. Trabajo Final de Máster. Centro Universitario de la Guardia Civil.

Presidencia del Gobierno (2017): Estrategia de Seguridad Nacional 2017. Madrid. Extraído el 22 de septiembre de 2020 de: https://www.dsn.gob.es/es/estrategias-publicaciones/estrategias/estrategia-seguridad-nacional-2017.

Presidencia del Gobierno (2019): Estrategia Nacional de Ciberseguridad. Extraído el 20 de julio de 2020 de: https://www.dsn.gob.es/es/documento/estrategia-nacional-ciberseguridad-2019.

Real Academia Española y Consejo General del Poder Judicial (2020): Diccionario del español jurídico. Madrid. Extraído el 22 de abril de 2020 de: https://dpej.rae.es/.

Reichborn-Kjennerud, E. y Cullen, P. (2017): Understanding Hybrid Warfare, MCDC Countering Hybrid Warfare Project. Extraído el 12 de noviembre de 2020 de: https://

assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/647776/dar_mcdc_hybrid_warfare.pdf.

Rivas Nieto, P. (2011): "Apuntes sobre la idea de guerra generalizada en América Latina", Analecta Política, 1(1), pp. 63-79. Extraído el 22 de julio de 2020 de: http://dialnet.unirioja.es/descarga/articulo/5206352.pdf.

Santamaría, C. (2017): "De la guerra convencional a las estrategias que definen la «guerra híbrida»", Asociación de Corresponsales de Prensa Extranjera (ACPE), 23 marzo. Extraído el 12 de julio de 2020 de: http://corresponsales.org/blog/de-la-guerra-convencional-a-la-guerra-hibrida/.

Serrano Villafañe, E. (1971): "Polemología o guerra", Revista de estudios políticos, (176), pp. 147-162. Extraído el 12 de julio de 2020 de: https://dialnet.unirioja.es/descarga/articulo/1957182.pdf.

Travieso, J. (2020): "Las frases de Miguel Villarroya, el JEMAD que considera "soldados" a los españoles", La Información, 23 julio. Extraído el 23 de marzo de 2020 de: https://www.lainformacion.com/asuntos-sociales/coronavirus-frases-miguel-villarroya-ejercito-jemad-soldados-espanoles-moncloa/6553414/.

US Joint Chiefs of Staff (2019): JDN 1-19 Competition Continuum. Extraído el 12 de enero de 2021 de: https://www.jcs.mil/Portals/36/Documents/Doctrine/jdn_jg/jdn1_19.pdf.

EL AGROTERRORISMO EN LA LUCHA CONTRA AMENAZAS BIOLÓGICAS TRANSFRONTERIZAS ESCENARIOS DE COOPERACIÓN ESPAÑA-MAGREB

LAURA MÉNDEZ GARCÍA

ANALISTA DE INTELIGENCIA Y CONTRAINTELIGENCIA

Fecha de recepción: 14/03/2021. Fecha de aceptación: 04/06/2021

RESUMEN

Los procesos de globalización han posibilitado múltiples progresos pero también han derivado en nuevos riesgos y amenazas, tales como la propagación natural de agentes biológicos patógenos. En este contexto, existiría el riesgo de que algunas organizaciones yihadistas tratasen de interferir en sectores económicos estratégicos como la agricultura, ganadería e industria de la alimentación en España, por lo que sería conveniente revalorizar el estudio del agroterrorismo en el marco de la lucha contra las amenazas biológicas transfronterizas. En este sentido, la amenaza del bioterrorismo, -expresada desde el agroterrorismo y el bioterrorismo alimentario-, precisaría de un verdadero enfoque estratégico y un desarrollo normativo e institucional más amplio. La identificación adecuada de brechas relacionadas con el bioterrorismo en España requeriría además considerar la proximidad al Magreb, especialmente la cooperación antiterrorista y los vínculos económicos y comerciales con Marruecos.

Palabras clave: Bioterrorismo, agroterrorismo, yihadismo, globalización, España, Magreb, Marruecos.

ABSTRACT

Globalization processes have resulted in multiple progress but they have also led to new risks and threats, like naturally ocurring disease outbreaks. In this context, there is a risk that some jihadist organizations could deliberately try to disrupt strategic sectors for Spain such as agriculture, livestook and industry, so it would be convenient to revalue the study of agroterrorism in the fight against transboundary biological threats. In this sense, the threat of bioterrorism, -from agroterrorism to bioterrorism associated to the food supply-, requires a true strategic approach and a broader normative and institutional development. Proper identification of bioterrorism-related gaps in Spain also requires considering proximity to the Maghreb, especially counter-terrorism cooperation and economic and commercial relations with Morocco.

Keywords: Bioterrorism, agroterrorism, yihadism, globalization, Spain, Magreb, Morocco.

1. INTRODUCCIÓN

La comunidad científica ha alertado en numerosas ocasiones del elevado riesgo de diseminación natural de agentes biológicos, una problemática agudizada por los procesos de globalización, el aumento de la movilidad internacionalización y los intercambios económicos y comerciales, así como por la inmediatez del transporte de mercancías y personas y la degradación medioambiental. Estos factores estarían complicando esfuerzos nacionales e internacionales en torno a la no propagación de agentes infecciosos, manifestándose así la necesidad de educar a la población en riesgos biológicos y reforzar la cooperación. Este avance sería igualmente aplicable en el supuesto de que un agente zoonótico[1] (un microorganismo[2] cuyo reservorio es uno o varios animales) o cualquier otro que contaminase cultivos y cosechas, fuese empleado de forma intencionada.

Pero si bien epidemias y pandemias fueron catalogadas por primera vez como desafíos en la última *Estrategia de Seguridad Nacional* (ESN-2017)[3][4], esta ofrecería una visión genérica del fenómeno del terrorismo yihadista, una problemática prioritaria para España que por el momento no contempla la variable biológica entre sus tendencias. Sin embargo, la ESN-2017 señala precisamente "su rápida mutabilidad y capacidad de adaptación a los cambios y estrategias seguidos contra ellos" (p.58) llevándonos a revaluar nuestras capacidades defensivas y la baja percepción del riesgo asociado a ataques biológicos. De hecho, estos eventos pese a su baja probabilidad, generarían consecuencias especialmente graves en términos de seguridad y salud pública[5].

Así mismo, esta desconexión habitual entre terrorismo y amenaza biológica -que tiende a privilegiar enfoques reactivos frente a medidas anticipatorias- contrastaría con el llamamiento del *Departamento de Seguridad Nacional* (DSN) para la adopción de planes de contingencia globales frente a eventuales ataques con agentes NBQR (acrónimo que hace referencia a agentes nucleares, biológicos y bacteriológicos, químicos o radiológicos) los cuales pueden instrumentalizarse, convirtiéndose en amenazas para la Seguridad Nacional. Este llamamiento vendría produciéndose sobre todo ante la creciente preocupación de que actores no estatales puedan acceder a los mismos.

Con esto, la proliferación de Armas de Destrucción Masiva (ADM) constituye una amenaza diferenciada en la ESN-2017 tradicionalmente asociada a escenarios de

1 Una enfermedad zoonótica puede transmitirse entre animales y de animales a humanos (antropozoonosis) con origen en bacterias, virus, parásitos y hongos. En la actualidad existen más de 200 tipos de zoonosis conocidas. La zoonosis inversa o antropozoonosis ocurriría cuando un ser humano tiene la capacidad de infectar a un animal. Darwich, L. (julio 2014).

2 Un microorganismo se define como ''toda entidad microbiológica, celular o no, capaz de reproducirse o de transferir material genético''. Instituto Nacional de Seguridad e Higiene en el Trabajo (2014).

3 La pandemia de la COVID-19 habría adelantado la necesidad de redefinir la ESN fuera de la periodicidad general. Conforme a este nuevo paradigma de crisis sanitaria global, la próxima Estrategia ''presentará, presumiblemente, un nuevo escenario estratégico post-COVID-19 en el que las amenazas biológicas adoptarían un papel diferenciado en una escala de riesgos y probabilidad'' Méndez, L. (3 noviembre 2020).

4 Según la información disponible, la nueva Estrategia de Seguridad Nacional (2021) situaría epidemias y pandemias como amenazas en lugar de desafíos. La Estrategia, en la que se vendría trabajando desde hace unos meses, también incluirá la desinformación entre los ámbitos de actuación.

5 Departamento de Seguridad Nacional (2017) Estrategia de Seguridad Nacional. Un proyecto compartido de todo y para todos. Gobierno de España.

conflicto interestatal. Incluyéndose las amenazas biológicas en este espectro, las químicas habrían despertado no obstante hasta el momento mayor interés. En este contexto, organizaciones terroristas de corte yihadista salafista, como *Daesh* y *Al Qaeda,* ya habrían evidenciado el deseo de emplear agentes biológicos a través de su propaganda, amenazas que no habrían sido materializadas pero ejercerían *per se* un efecto desestabilizador por su potencial de peligrosidad.

Partiendo de la premisa de que algunos grupos terroristas podrían tratar de interferir en sectores económicos estratégicos como la agricultura y ganadería en España, en cualquiera de sus fases productivas, sería conveniente revalorizar el estudio del agroterrorismo en el marco de la lucha contra las amenazas biológicas transfronterizas. Conforme a ello, deberían identificarse agentes susceptibles de ser explotados con fines agroterroristas, estudiando las posibilidades de acceso y capacidades técnicas y operativas de estos grupos. Igualmente cabría considerar la proximidad al Magreb[6][7] -en un continente donde existen enfermedades endémicas y condicionamientos que facilitan la permeabilidad de las fronteras-, mientras que la violencia terrorista habría aumentado exponencialmente este último año, alcanzando su punto álgido en toda una década. Ello, sin olvidar que la concentración de esfuerzos dirigidos a la contención de la pandemia en África Occidental ha supuesto una oportunidad para el avance de grupos yihadistas, aumentando significativamente los ataques registrados en el Sahel respecto al año anterior (Díez, 2020)[8].

Con vínculos particularmente intensos con Marruecos en lo relativo a la cooperación antiterrorista y en el plano económico-comercial, la identificación adecuada de brechas relacionadas con el bioterrorismo en España requeriría conocer la actividad productiva en todos los sectores de la industria y sus vulnerabilidades. En este sentido, resultaría necesario estudiar las medidas de bioseguridad adoptadas en empresas agropecuarias españolas, incluidas aquellas deslocalizadas en el país magrebí y cuyos intereses comerciales pudieran verse amenazados por ataques NBQR de naturaleza terrorista, generando impactos negativos para defensa, economía y salud pública.

Esta investigación trata de dar respuestas a algunas Necesidades de Inteligencia (NI) entendiendo que la amenaza del bioterrorismo, -expresada desde el agroterrorismo y el bioterrorismo alimentario-, precisaría de un verdadero enfoque estratégico y un desarrollo normativo e institucional más amplio[9]. Esta amenaza puede ser entendida desde el agroterrorismo (concebido como un medio, en tanto que supone

6 El Magreb siempre ha sido un área de interés para la Política Exterior española. Con Marruecos, el marco general de cooperación tendría su origen en la firma del Tratado de amistad, buena vecindad y cooperación (1991) avanzando en la lucha conjunta contra el yihadismo con la intensificación del diálogo político y diplomático. Pese a un historial de reivindicaciones territoriales no resueltas, este habría facilitado el establecimiento de Consejerías del Interior y Reuniones de Alto Nivel para la puesta en común de cuestiones de interés bilateral, adoptándose acuerdos específicos en otras dimensiones como la policial y judicial. Méndez, L. (2020)

7 La cooperación hispano-marroquí aunque fructífera adolecería todavía hoy de una importante fragilidad. Es decir, la cooperación en todas las dimensiones se asienta en una confianza mutua, muy difícil de reconstruir si se daña. Así se ha evidenciado en acontecimientos recientes como la crisis de Ceuta derivada de la última escalada de tensión diplomática entre ambos países tras el desencuentro por la acogida en España del líder del Frente Polisario.

8 Díez, A. (septiembre 2020).

9 Para más información véase: Cique, A. (8 mayo 2017).

la afectación directa de animales y plantas y la indirecta de las personas) y el bioterrorismo alimentario (basado en la utilización directa de agentes biológicos contra las personas, independientemente del medio)

Las NI se concretarían de la siguiente forma:

- ¿Cómo podemos potenciar dinámicas de colaboración, control y vigilancia en torno a la amenaza bioterrorista y agroterrorista?
- ¿Mediante qué fórmulas es posible desarrollar estrategias de prevención compartidas, redes de investigadores y esquemas de evaluación de riesgos?
- ¿Mediante qué actuaciones podemos concienciar a los agentes de la cadena productiva sobre riesgos y necesidad de impulso a la bioseguridad en instalaciones, plantas de procesamiento y transportes?

El objetivo de este análisis sería contribuir a la ampliación de la cooperación española en el Magreb en seguridad agropecuaria con Marruecos, como país de referencia en el área territorial del Magreb, por lo que se ofrecen conclusiones básicas para la elaboración de un proyecto compartido contra el agroterrorismo, susceptible de consideración una vez se produzcan avances positivos en la normalización de las relaciones. El método de trabajo ha consistido en una revisión bibliográfica (fuentes abiertas secundarias) enriquecidas mediante aportaciones realizadas por expertos (entrevistas en profundidad). Para ello, se ha contado con los perfiles profesionales entrevistados que se citan a continuación:

- Director de Seguridad especialista en amenazas NBQR.
- Técnico Avanzado en Inteligencia y Contrainteligencia y Dirección de Operaciones Psicológicas, experto en comunicación.
- Profesional de la salud especialista en Inteligencia Sanitaria (Medint) Investigación Biosanitaria y Gestión de Crisis Internacionales.
- Técnico Superior en Laboratorio y Análisis Clínico.
- Veterinario militar experto en Enfermedades Emergentes y Reemergentes, Salud humana y Salud animal.

2. LOS AGENTES BIOLÓGICOS COMO AMENAZAS A LA SEGURIDAD

Mientras que el factor biológico no ha suscitado demasiado interés en los estudios de terrorismo -al observarse casi siempre como escenarios de baja probabilidad-, eventos como la pandemia de la COVID-19 podrían cambiar la percepción colectiva frente a la dimensión de incidentes NBQR, vislumbrándose con inquietud la posibilidad, aunque remota, de ataques de naturaleza bioterrorista. De hecho, la *Unión Europea* (UE) alertó en mayo de que el uso de agentes biológicos con motivación terrorista puede ser efectivo, considerando conveniente una respuesta multilateral rápida y coordinada, algo en lo que coincidiría el secretario general de la *Organización de Naciones Unidas* (ONU)[10]. Esto conduciría a reforzar en el mejor de los casos nuestras

10 Council of Europe (2020).

capacidades defensivas, con especial atención a la evolución del terrorismo yihadista de ideología salafista frente a otras categorías residuales.

Pero abordar con éxito la amenaza bioterrorista supone un desafío incluso desde sus fases más tempranas, momentos en los que según autores como Cique (2015) esta suele pasar desapercibida en virtud de su propia naturaleza, siendo vital localizar el foco de infección[11]. En esta línea, sería necesario, tal y como apuntan otros expertos veterinarios como el coronel Martín Otero, "discernir del origen natural y los riesgos de contaminación *in situ* de aquellas contaminaciones y brotes epidémicos intencionados"[12], algo que puede resultar extremadamente complicado, precisamente porque en la determinación de la responsabilidad de un ataque biológico (guerra biológica) suelen producirse cruces de acusaciones estratégicas entre Estados con intereses contrapuestos. A todo esto, el bioterrorismo se caracterizaría precisamente por la magnitud de sus consecuencias, teniendo en cuenta que ''el arma biológica ideal sería aquella capaz de diseminarse rápida y fácilmente en una gran población, que fuese altamente contagiosa, que causara altas tasas de morbilidad y mortalidad y que requiriese de grandes recursos para combatirla'' (Soteras, 2008: 16)[13].

Como una variable del bioterrorismo, el agroterrorismo puede entenderse como "la introducción deliberada de un agente patógeno, ya sea contra el ganado o en la cadena alimentaria, con el fin de socavar la estabilidad social y/o generar miedo" (Cique, 2017: 31), por lo que el potencial de peligrosidad de un ataque de esta naturaleza se incrementaría no solo ante la interdependencia que se da en este sistema, sino también ante el importante papel que representan los productos de origen animal en la alimentación, perfectamente integrados en nuestros hábitos de consumo.

Se calcula que entre el 70-75% de las enfermedades infecciosas emergentes del ser humano tienen un origen animal, pudiendo ello responder tanto a una explicación natural, como accidental o intencionada (King, 2014)[14]. Además, preocuparía que de entre todos los microorganismos considerados como agentes de guerra biológica, un 80% corresponderían a agentes zoonóticos, un porcentaje elevado teniendo en cuenta que la *Organización Mundial de la Salud animal* (OIE)[15] cifra en casi el 1/5 de la población mundial aquella dedicada a la cría, elaboración o comercialización de alimentos de origen animal, grupo que estaría exponiéndose permanentemente a estos como vectores biológicos. Frente a esta realidad, esta organización trataría de

11 Cique Moya es licenciado y doctor en veterinaria, Militar de carrera, Jefe del Departamento de Defensa Biológica de la Escuela del Ejércuto de Tierra, analista del Servicio de Sanidad Ambiental y NBQ de Medicina Preventiva de la Defensa. Se trata de uno de los mayores expertos en este tema en España, contando con una amplia experiencia como formador y numerosas publicaciones relacionadas con la defensa NBQ, de ahí que su trabajo constituya una pieza fundamental en la bibliografía que aquí se ha empleado. Véase Cique, A. (2015).

12 Entrevista personal realizada al coronel Luis Martín Otero, coordinador del Centro de Vigilancia Sanitaria de la UCM (VISAVET) y Red de Laboratorios de Alerta Biológica (RE-LAB) especialista en microbiología, sanidad ambiental y sanidad animal. Su campo de trabajo consiste en las enfermedades emergentes y reemergentes en sanidad animal que puedan afectar a la seguridad nacional e internacional, a 27 de noviembre 2020 (entrevista telemática).

13 Soteras, F. (2008).

14 King, L. (2004).

15 En 2015 se celebró la I Conferencia Mundial sobre la Reducción de Amenazas Biológicas, habiéndose desarrollado hasta el momento el Sexto Plan Estratégico (2016-2020). *Vid.* Organización Mundial de la Sanidad animal, OIE (2019) Informe Anual de Actividad.

garantizar la seguridad sanitaria del comercio internacional de animales y productos de origen animal, una labor imprescindible en la prevención de escenarios epidémicos y pandémicos y ataques con motivación criminal y terrorista.

Sin embargo, para entender la dimensión que estos pueden adquirir, es necesario conocer en primer lugar algunas generalidades en torno a la clasificación de los agentes biológicos. De esta manera, en la industria agropecuaria, aquellos pertenecientes al Grupo 3 implicarían un riesgo especial para trabajadores y consumidores (RD 664/1997) desencadenando transmisión comunitaria[16], mientras que aquellos que pueden ser fácilmente diseminados de persona a persona causarían los mayores impactos en términos de salud pública, mortalidad y conmoción social[17]. Los agentes biológicos más peligrosos (Categoría A) serían así bacillus anthracis, toxina de clostridium botulinum, yersinia pestis, variola major, francisella tularensis y fiebres hemorrágicas virales, filovirus como el ébola y marburg y arenavirus como el lassa y machupo.

Respecto a los antecedentes, cabe precisar que los ataques a los medios de subsistencia y fuentes de alimentación humanas ya estuvieron presentes en la historia desde los imperios clásicos de la antigüedad y reinos medievales euroasiáticos hasta las potencias coloniales occidentales (Soteras, 2006)[18] observando a partir del siglo XX cómo sobre todo los agentes químicos y en menor medida los biológicos han sido empleados con un éxito relativo por parte de actores estatales, adquiriéndose posteriormente numerosas resoluciones alrededor de la prohibición y no proliferación. Así pues, el sistema multilateral de no proliferación y desarme tiene su origen en el Protocolo de Ginebra (1925) que prohíbe el uso de armas físicas y toxinas, mientras que la Convención para la prohibición de las Armas Bacteriológicas y toxinas-CABT (1972) abarcaría la categoría completa de armas biológicas. En este escenario, España se ha comprometido con regímenes de control de exportaciones de tecnologías sensibles y de doble uso y con iniciativas de carácter operativo[19].

Numerosos ejemplos en el marco de conflictos de alta y baja intensidad estarían protagonizados por Estados Unidos, especialmente durante la Guerra de Vietnam con ataques a cultivos de arroz utilizando agentes químicos, herbicidas defoliantes como el agente naranja, que con el tiempo han demostrado capacidad de afectar a nuevas generaciones por su pervivencia en sedimentos en ríos y lagos[20]. También la CIA, en una de las muchas acciones de desgaste tras la revolución cubana, habría utilizado agentes químicos plaguicidas contra la base de la industria agrícola de la isla, tratando también de diseminar enfermedades entre los cultivos de exportación de Nicaragua (Soteras, 2008).

Igualmente existen precedentes por parte de grupos no estatales, actos que han sido catalogados como terrorismo, como el incidente de Matsumoto y el atentado de Tokio en los que se liberó gas sarín, ambos perpetrados por la secta apocalíptica *Aum Verdad Suprema*. Pero si bien este no consistió en un ataque biológico sino químico, la destrucción de vidas humanas demostraría nuestra vulnerabilidad ante enemigos

16 Real Decreto 664/1997, de 12 de mayo, sobre la protección de los trabajadores contra los riesgos relacionados con la exposición a agentes biológicos durante el trabajo.
17 Centers for disease control and prevention, CDC. (N.D).
18 Soteras, F. (2006).
19 Ministerio de Asuntos Exteriores, Unión Europea y Cooperación (s.f).
20 Ray, K.; Wright, L. (2019).

invisibles en el espectro NBQR. Más tarde, tras el 11-S, la crisis del Amerithrat causó un revuelo importante en Estados Unidos, una crisis que consistió en una serie de ataques con cartas que contenían esporas de carbunco enviadas a varios Senadores y medios estadounidenses, atribuyéndose finalmente la autoría a un microbiólogo[21]. Tras este suceso, se comenzaría a debatir en torno a la posibilidad de que la viruela, erradicada desde la década de los 80, pudiese ser empleada en un futuro como arma biológica por parte de grupos terroristas[22].

Precisamente en el año 2001, algunos países impulsaron a iniciativa de Canadá y conjuntamente con la *Organización Mundial de la Salud* (OMS) la *Global Health Security Initiative* (GSHI) orientada a consolidar la preparación y respuesta ante eventuales ataques terroristas NBQR desde la cooperación interestatal. La GSHI se habría ocupado así de algunos eventos como la pandemia de la influenza, el SARS y el accidente en Fukushima. Sin embargo, aunque existan varios grupos de trabajo en el seno de esta iniciativa sobre amenaza química, radio-nuclear y comunicación de crisis, por el momento no habría ninguno que aborde específicamente la amenaza biológica.

Aunque si algo han demostrado las crisis sanitarias más recientes es la necesidad de anticipación, aprender de la experiencia y mejorar la respuesta ante eventuales incidentes biológicos antes de que adquieran carácter global. En esta línea, cabe recordar que la crisis del ébola de 2014 promovió la doctrina *Smart Defense* de la *Organización del Tratato del Atlántico Norte* (OTAN) fundamentada en la búsqueda de soluciones cooperativas, algo que favoreció el proyecto *Rhino* de INTERPOL para abordar brotes infecciosos a gran escala. Con esto, pese a los precedentes citados, parece que un ataque bioterrorista en el corto y medio plazo, y a diferencia de los eventos naturales, sí podría inscribirse en la lógica del *'cisne negro'* (Taleb, 2007) sin que ello implique descuidar la prevención[23]. La nueva *Estrategia de Seguridad Europea 2020-2025* señala, no obstante, que los terroristas estarían tratando de adquirir materiales NBQR añadiendo que "en los últimos dos años se han producido varios casos, tanto en Europa (Francia, Alemania, Italia) como en otros países (Túnez, Indonesia), de ataques con agentes biológicos (generalmente toxinas vegetales)"[24].

3. ESPAÑA ANTE UN EVENTUAL ESCENARIO AGROTERRORISTA

En un contexto de presión creciente sobre los recursos naturales, la necesidad de proteger los servicios ecosistémicos se hace cada vez más palpable, generando oportunidades para la adopción de un enfoque integrador entre biodiversidad y seguridad (León, 2016)[25]. Este aumento de la conciencia medioambiental allanaría previsiblemente el terreno para una mayor sensibilización también ante los riesgos biológicos, incluidos aquellos asociados a ataques al medio rural y producción agropecuaria. Conforme a ello, en la evaluación de riesgos sería preciso identificar su campo

21 US Department of Justice (2010).

22 Actualmente se conservan viales del virus en dos laboratorios en Estados Unidos y Rusia. La negativa a su destrucción se justifica precisamente en este riesgo, pudiendo darse la necesidad en un futuro de desarrollar nuevas vacunas a partir de esas muestras. BBC news mundo (17 septiembre 2019).

23 Taleb, N. (2007).

24 Eur-Lex. (2020).

25 León, M. (2016).

de acción y en qué afectaría a la economía del país y reputación de sus exportaciones, analizando cuáles serían los sectores susceptibles de ser atacados y a través de qué medios. Del mismo modo, deberían definirse las variables que consideraría una organización terrorista en la planificación y ejecución.

Siguiendo esta lógica, preocuparía la vulnerabilidad de los alimentos frente a la contaminación intencional por agentes debilitantes o letales, ya que ‘’las cadenas alimentarias, tanto en su producción, procesamiento y distribución de proteínas como de alimentos y agua, son básicas para el normal funcionamiento de las actuales sociedades de tipo consumista y este servicio es considerado como esencial’’ (Soteras, 2008: 18). Teniendo esto presente, muchos se preguntarán si las principales organizaciones terroristas en la actualidad estarían realmente al alcance de agentes biológicos no complejos para su obtención o generación, procesado, transporte, conservación y uso.

En palabras de Cique (2015) los grupos terroristas podrían llegar a realizar ataques bioterroristas, aunque probablemente a escala reducida, ya que la capacidad real de diseminación estaría limitada todavía a entornos locales, algo en lo que coinciden la mayoría de analistas. Este autor plantea que un ataque de glosopeda (fiebre aftosa) que afectase a nuestro país constituiría una acción *low cost* dado su limitado carácter zoonótico, si bien el terrorista fallecido tras la exposición a cualquier agente sería considerado como un mártir por la organización, en esa modalidad de terrorismo suicida que practica específicamente el yihadismo[26]. Por su parte, en principio métodos como ‘’el envenenamiento de los alimentos y el agua, requieren de conocimientos técnicos limitados’’ (Soteras, 2008: 15), así como algunos materiales tóxicos industriales, aunque los distintos sistemas de alerta estarían diseñados para evitar que ese daño llegue a los hogares, mientras que el acceso a determinados agentes biológicos precisa saber dónde encontrarlos, algo que suele implicar obstáculos insalvables.

En la actualidad *Daesh* ya ha amenazado con el envenenamiento del agua y cultivos de países Occidentales, si bien es cierto que todavía no habría perpetrado ningún ataque de esta tipología, aunque la simple amenaza del uso en la propaganda yihadista es capaz de generar un determinado estado de alarma y opinión, sobre todo en un clima de intercertidumbre y en lugares donde hayan tenido lugar ataques convencionales recientemente. Sin embargo y pese a la amplificación mediática, determinar las capacidades operativas reales requiere realizar análisis mucho más profundo. Aún así, existe el riesgo de que esta y otras organizaciones tratasen de reclutar perfiles que resulten de interés a estos fines, titulados universitarios y expertos en microbiología (Cique, 2014)[27] además de biólogos, ingenieros y veterinarios, quienes conocerían el nivel de bioseguridad necesario para desarrollar un verdadero programa biológico.

Sin embargo, esto no resultaría viable puesto que no se podría contar en principio con una infraestructura de laboratorio que ofrezca garantías superiores a entornos de fabricación casera. En este sentido, parece que las capacidades de los laboratorios estatales no serían reproducibles, a no ser que se establezcan ‘’nuevos santuarios o se negocien acuerdos con algún proveedor estatal’’ (Reinares, 2020)[28].

26 En todo caso, existen una serie de fases dentro del proceso de capacitación de una organización terrorista: adquisición de agentes biológicos, cultivo o procesamiento, improvisación de sistemas de diseminación y finalmente, diseminación. *Vid.* Cique. (2015).

27 Cique, A. (2 mayo 2014).

28 Reinares, F. (2020).

Además, según el coronel Martín Otero, el hecho de que los sectores susceptibles de ser atacados sean aquellos que tienen unos niveles de bioseguridad mayores podría traducirse en una expresión de mayor resiliencia en la salud pública[29] en cualquier caso, dificultando que un plan de estas características pudiese llegar a materializarse en el entorno inmediato.

Conforme a esta idea, la OMS (2003) valora positivamente el hecho de que "la diversidad dietética disponible en muchos países desarrollados también reduce la probabilidad de que todo el suministro de alimentos se contamine y tiende a diluir los posibles efectos sobre la salud"[30], tratándose este de un factor tranquilizador en la ponderación de riesgos. No obstante, es precisamente esta diversidad la que hace complicada la prevención, ya que existirían múltiples fuentes de alimentación que podrían ser agredidas por contaminantes específicos. Los ataques al sistema de producción serán diferentes según el tipo de alimento, generándose por tanto un efecto multiplicador alrededor de los escenarios de riesgo, por lo que parecería razonable segurizar de forma permanente estas industrias en la lógica de la prevención de riesgos.

El terrorismo agropecuario también puede atacar la base de la materia prima, como por ejemplo las principales concentraciones de la cabaña ganadera. Mediante un análisis de la alimentación general de la población en España, observamos que existen productos alimentarios como la carne y preparados a base de esta que se generan de forma masiva, por lo que cabría reforzar nuestros esfuerzos en torno a los que se consumen con cierta regularidad[31]. Según la OMS (2003) el riesgo aumentaría significativamente en aquellos que requieren de procesado, teniendo en cuenta que ‘’en muchos sistemas de procesados de alimentos, el tratamiento de calor constituye una oportunidad para la generación de contaminantes microbiológicos’’(p.14).

Atacar la industria de procesados, ya sea la cárnica o la láctea[32], implicaría por tanto enfrentarnos a escenarios mucho más desfavorables en términos de salud pública y seguridad, ya que la eficiencia del ataque sería mayor si el producto, como por ejemplo la leche, se distribuye de forma masiva en el mercado. En la siguiente tabla se muestra la relación de agentes biológicos[33] presentes en una actividad económica específica -la explotación del ganado bovino para la producción de leche-, los cuales serían además susceptibles de ser empleados con fines terroristas[34].

29 Fuente: coronel Luis Martín Otero. Entrevista personal. (27 de noviembre 2020).

30 Food Department, WHO (2003).

31 En 2017 el aporte del sector primario (agricultura, ganadería, pesca y silvicultura) fue de un 2,7% del PIB, unido al 2,5% de la industria agroalimentaria y actividades indirectas, alcanzando hasta un 10%. Destacaría el volumen de empleo generado por el sector en la cadena de valor y el hecho de que en el segundo trimestre de 2020, el Valor Añadido Bruto (VAB) creció un hasta un 4,4% frente a la caída del PIB nacional. Por tanto, la dimensión real en nuestro país relacionada con la producción y consumo en el sector primario, incluida su industria de transformación, implica que hablemos de un evento con gran potencial desestabilizador, aunque improbable. INE. (2020).

32 *Ibíd.* Los mayores incidentes y mejor documentados incluyen un brote de infección por Salmonella typhimurium en 1985, que afectó a 170.000 personas, debido a la contaminación de leche pasteurizada en una planta lechera en Estados Unidos. VISAVET. (2010).

33 La mayoría de estos agentes patógenos están catalogados dentro del Grupo 3, si bien algunos corresponden al Grupo 2, lo que sugiere una transmisión comunitaria más limitada.

34 Consideraciones extraídas de la Guía desarrollada por la OMS sobre respuestas en salud pública ante armamento químico y biológico. WHO. (2004).

AGENTE	ENFERMEDAD	VACUNA DISPONIBLE
Yersinia pestis	Peste	Sí
Bacillus anthracis	Carbunco	Sí
Burkholderia pseudomallei	Melioidosis, no especificada	No
Francisella tularensis	Tularemia	Sí
Brucella species	Brucelosis	No
Coxiella burnetii	Fiebre Q	Sí
Toxoplasma gondii	Toxoplasmosis	No
Salmonella typhimurium	Enteritis debida a Salmonella	Sí
Rickettsia prowazekii	Tifus epidémico debido a Rickettsia prowazekii	No
Chlamydia psittaci	Infección debida a Chlamydia psittaci	No

Tabla 1. Agentes biológicos presentes en un escenario agroterrorista en España. Explotación del ganado bovino para la producción de leche. Fuente. Elaboración propia en base a BIODAT[35] y OMS[36].

Atendiendo a estos resultados, y en comparación con otras actividades productivas, parece que los agentes biológicos patógenos afectarían en especial a la industria agropecuaria, por lo que resultaría necesario asegurar un nivel adecuado de protección para los trabajadores de aquellas ocupaciones relacionadas directamente con la exposición a cada agente, sobre todo cuando no hay disponible una vacuna eficaz ni otras alternativas terapéuticas. En agentes zoonóticos, preocuparían los microorganismos resistentes y cepas para las que no se cuente con un sistema inmune entrenado ni otros mecanismos sanitarios para la prevención y contención de la propagación del patógeno.

Respecto a los precedentes sobre agroterrorismo y bioterrorismo alimentario, si bien estos son escasos, destacarían el del grupo Osho en 1984 en Estados Unidos[37]

35 BioDat es una base de datos del Instituto Nacional de Seguridad y Salud en el Trabajo (INSST). El total de agentes biológicos presentes en esta actividad asciende a 51, si bien solo 10 de estos serían susceptibles de ser empleados como armas biológicas y 5 no dispondrían de vacuna. Para más información, véase Instituto Nacional de Seguridad e Higiene en el Trabajo (s.f).

36 Anexo 3 (Agentes Biológicos) Guía de la OMS (2004) Respuesta de salud pública a armamento biológico y químico, incluyéndose bacterias (rickettsias y clamydias) hongos, virus y protozoos.

37 Este consistió en la contaminación con Salmonella typhimurium de bufetts de ensaladas en varios restaurantes, con el objetivo de enfermar a los vecinos e influir en un proceso electoral en Oregón. Este agente también fue utilizado anteriormente en incidentes menores en Japón. Food Department, WHO (2003).

y otros incidentes en la década de los 90, como el protagonizado por un trabajador de un laboratorio que contaminó deliberadamente productos de repostería con Shigella dysenteria, con el objetivo de enfermar a sus compañeros. Con esto, el brote accidental de hepatitis A asociado al consumo de almejas en Shanghai en 1998 se trataría del mayor incidente de enfermedad transmitida por alimentos de la historia, afectando casi a 300.000 personas. Otro agente presente en la tabla, yersinia pestis, también ha sido empleado en contextos de guerra biológica, al que se refiere Cique a continuación:

"Yersinia pestis es, junto con bacillus anthracis y la toxina ricina[38] uno de los agentes preferidos por Al Qaeda, sus franquicias y sus productos derivados como agentes de terror, por su impacto mediático ante el rumor de que poseen capacidad operacional de diseminación" (Cique, 2018: 17).

Algunas fuentes apuntan a que en 2009 *Al Qaeda del Magreb Islámico* (AQMI) habría liberado este agente en Argelia[39], falleciendo hasta 40 miembros de la organización. Pero sin constancia de que entonces se practicase la investigación epidemiológica forense requerida, existirían dudas en torno a la naturaleza intencional del incidente (Allswede y Binyamin, 2011)[40].

Posteriormente en 2014 varios medios de comunicación hicieron referencia a la localización en Siria "de un ordenador personal que ocultaba información *técnica* relativa a la preparación de Yersinia pestis junto con una *fatwa* del clérigo saudí *Nasir al-Fahd"* (Cique, 2018: 18). Lo realmente preocupante es que dicha *fatwa* puede interpretarse como una justificación de la moralidad del uso de armas biológicas o de destrucción masiva. Mientras que en 1998 Bin Laden ya tenía una *fatwa* para declarar la guerra a EE. UU., una década más tarde su adjunto *Al-Zawahiri* emitió otra para anunciar una posible próxima etapa del conflicto. *Al-Zawahiri* adoptó así textualmente los ejemplos de al-Fahd, el ataque del profeta Mahoma contra la aldea de al-Taif con una catapulta permite el uso de armas de 'destrucción general' ante la incapacidad de distinguir entre civiles inocentes y combatientes[41].

Observamos en este punto la idea de justificación divina ligada a la enfermedad, conforme a la cual esta se consideraría un castigo de Alá a los infieles (*kafir*)[42]. En esta misma línea, las comunicaciones oficiales emitidas en los últimos meses por *Al-Qaeda* y *Daesh* han hecho referencia, -en una muestra de oportunismo durante la pandemia-, a la venganza hacia Occidente y usura de las economías occidentales como causas de la ira de Alá. Este factor religioso contrastaría con otras motivaciones como las de los ecoterroristas y de sectas igualmente fundamentalistas pero no identificadas con la ideología yihadista, con la diferencia de que el yihadismo ha adquirido una dimensión transnacional no atribuible al resto de grupos. Así mismo, una organización terrorista podría, previo al ataque, ''acudir a algún conocido doctrinario salafista que alegaría un

38 ''En el caso del ántrax y la ricina, preocuparía su persistencia ambiental y en superficies como medios de diseminación''. Entrevista personal realizada a Ana E. García. Técnico Superior de Laboratorio y Análisis Clínico del Centro Farmacéutico Canario del Ejército del Aire-CEFARCA, Estado Mayor Formación en Rastreo Covid-19. Experiencia como delegada informadora de Laboratorios Farmacéuticos, a 30 de noviembre de 2020 en Las Palmas de Gran Canaria.

39 Echrouck, The Washington Times y The Sun se hicieron eco de la noticia. Medios de comunicación citados en Cique, A. (5 marzo 2018).

40 Allswede, M.P; Binyamin, T. (25 may 2011).

41 Mowatt-Larssen, R. (november 16 2010).

42 Reinares, F. (2020).

hadiz como prueba literal de que no hay transmisión de enfermedades infecciosas sin permiso de Alá, de que el contagio de una persona sana por otra infectada solo ocurre si es voluntad de Alá'' (Reinares, 2020).

Además, existiría el temor de que otras enfermedades como la influenza aviar de alta patogenicidad y la Peste Porcina Africana (PPA) puedan ser utilizadas por grupos terroristas (Cique, 2015) ya que, si bien esta última no representa un riesgo para la salud humana, sí causa cuantiosas pérdidas económicas[43][44], aunque el carácter eminentemente exportador de España reduce los riesgos asociados a la diseminación de la PPA dentro del territorio nacional. El sector porcino español genera miles de empleos e importa a más de un centenar de países en su condición de territorio libre de PPA, existiendo un programa de vigilancia sanitaria porcina nacional reforzado por el riesgo procedente del Este de Europa.

En cualquier caso, las consecuencias negativas de un ataque aumentarían exponencialmente en un país como el nuestro en el que el sector turístico es la base de la economía nacional, al ser esta una actividad que se alimenta de la producción del sector primario. Por ello, el daño indirecto a la industria turística merece ser considerado en proyecciones de escenarios, una variable que las organizaciones terroristas podrían estudiar con la intencionalidad de causar el mayor daño posible[45].

La introducción de agentes infecciosos en España a través de las exportaciones plantea igualmente un desafío importante, sobre todo si la crisis sanitaria implica el bloqueo comercial de animales, vegetales y productos derivados de estos que estén afectados o sean sospechosos de estarlo, alterándose la confianza del consumidor y hundiéndose el mercado de productos específicos. Respecto a la producción agrícola, esta constituiría también para la OMS (2003) "un área vulnerable ante la contaminación deliberada, debiendo prestarse atención a la posible sustitución de pesticidas con agentes más tóxicos y a la contaminación de la irrigación del agua" (p.13).

Supervisar adecuadamente la calidad e inocuidad del agua destinada al riego y aquella de la que beben los animales o mediante la cual se procesa su comida resulta, por consiguiente, fundamental en la prevención de riesgos biológicos, evitando que esta sea el vector utilizado para cometer actos terroristas[46]. Al mismo tiempo, en los momentos de procesado de alimentos vegetales, los sistemas de ventilación pueden ser medios contaminantes que pasen fácilmente desapercibidos, así como la presencia de químicos tóxicos, pesticidas, metales pesados y químicos industriales, por lo que es aconsejable extremar las precauciones siguiendo las indicaciones de los expertos.

También cabe valorar la posibilidad de que un terrorista, interiorizando la lógica del martirio (terrorismo suicida) pueda infectarse intencionadamente y actuar como

43 Food and Agriculture Oganization. (october 2018).

44 Desde el *Marco mundial para el control progresivo de las enfermedades animales transfronterizas* (GF-TADs) la FAO y la OIE han puesto en marcha una iniciativa contra la PPA. En 2019, nueve países de la UE se vieron afectados por un brote de esta enfermedad. Ministerio de Agricultura, Pesca y Alimentación (30 noviembre 2020).

45 El turismo aporta un 12,5% al PIB nacional, constituyendo la base económica de muchas autonomías como Canarias en las que el dato asciende al 35%. Exeltur (2018).

46 El movimiento keniata Mau Mau desarrolló en la década de los 50 el primer acto de sabotaje agroalimentario moderno concluido con éxito mediante la utilización de toxinas vegetales sobre la cabaña ganadera del país. Soteras, F. (2008).

vector, desplazándose personalmente a un área geográfica concreta, como una zona muy transitada de una gran ciudad. Preocuparía en este sentido que grupos yihadistas como *Boko Haram* y *Daesh* (Cique, 2014) pudiesen utilizar el virus del ébola, temiéndose una posible acción coordinada con mártires infectados. Pero si bien los brotes epidémicos en África facilitarían el acceso a las fuentes infecciosas, sería necesario un nivel de capacitación del que, dadas las actuales condiciones, estos no dispondrían a corto ni medio plazo.

Mientras, ciertos agentes químicos y biológicos y materiales radio-nucleares pueden diseminarse como aerosoles de partículas pequeñas o líquidos volátiles, pero deben cumplirse condiciones atmosféricas muy concretas en ataques contra civiles. En cualquier caso, es necesario asumir que atacar varias líneas de producción de una gran compañía alimentaria de forma coordinada y encubierta respondería a una acción terrorista no visible. Un ataque al sistema agropecuario se movería por tanto en un plano de mayor discreción coincidiendo con el periodo de incubación, tratando en todo caso de sortear los mecanismos de detección y alerta temprana. En este caso, existirían diferencias importantes respecto a los ataques convencionales (con armas de fuego y armas blancas, IEDs y vehículos pesados) cuyo despliegue moviliza rápidamente a los medios, ya que en el escenario descrito la estrategia de los terroristas sería la reivindicación del daño una vez que este estuviese produciéndose, cuando fuese difícil de contener y revertir.

4. LAS RELACIONES CON EL MAGREB EN LA INDUSTRIA AGROPECUARIA ESPAÑOLA

La posición geoestratégica de España como punto de conexión entre África y Europa ha contribuido a definir la historia de sus relaciones y alianzas políticas y económicas. Esta cercanía, sobre todo respecto al sur peninsular y el archipiélago canario, supone sin embargo algunas vulnerabilidades a tener en cuenta. A la existencia en el continente de enfermedades endémicas -muchas de ellas con origen en agentes definidos como arma biológica-, se sumarían condiciones de salubridad deficientes en algunos países, sectores depauperados con poblaciones sin acceso a saneamiento, salud pública y a sistemas médicos y veterinarios adecuados. En este contexto, los desafíos demográficos e impactos asociados al cambio climático influyen en la sanidad animal, sobre todo ante la ausencia de estructuras de salud alimentaria plenamente operativas. De esta forma, los cambios medioambientales podrían propiciar la movilidad de especies animales o vegetales (especies invasoras) de forma natural[47], facilitando ciertas condiciones logísticas.

Junto a algunos agentes biológicos y microorganismos que ponen en riesgo cultivos, como el "virus del mosaico de la mandioca y del rayado común, relacionados con las hambrunas que amenazan la seguridad alimentaria en África" (Cique, 2018: 10), según la European and *Mediterranean Plant Protection Organization* (EPPO)[48]

47 Los vientos desde el Magreb habrían favorecido durante décadas las plagas de langostas en Canarias y en Almería, mientras que de ahora en adelante el cambio climático podría propiciar la llegada de diversas especies de mosquitos. En cualquier escenario, las pérdidas en las cosechas implican caída de la producción, subida de precios y alteración del mercado internacional.

48 EPPO es una organización intergubernamental europea y mediterránea cuyo objetivo es frenar la diseminación de patógenos vegetales (plagas en los ecosistemas) y desarrollar una estrategia internacional contra la introducción y propagación de plagas (incluidas plantas exóticas invasoras) que dañan los ecosistemas agrícolas y naturales.

preocuparía la posibilidad de que grupos no estatales alterasen ecosistemas de forma intencionada, afectando sobre todo a la región del Mediterráneo. Desde el IEEE ya se alertó de la vulnerabilidad de España ante potenciales ataques a la agricultura y ganadería provenientes del Magreb (Cique, 2017), algo que afectaría negativamente a los intereses comerciales de empresas españolas dedicadas a cultivos y cosechas en la región, especialmente en agricultura intensiva, por lo que cabría analizar las relaciones España-Marruecos en búsqueda de oportunidades.

Marruecos ha sido históricamente un competidor de España en la producción agrícola pero desde hace un tiempo este país lleva atrayendo la inversión española, ascendiendo ya al 10% del total de empresas nacionales registradas en el país vecino aquellas que pertenecen a este sector. Pero mientras que la producción computa como marroquí en los mercados exteriores, los productos se venden bajo marca española. Esto se vería favorecido por el abaratamiento de la mano de obra y un suelo más asequible, concentrándose "en la región del Gharb, una fértil llanura entre Tánger y Rabat, y sobre todo el valle del Souss, con capital en Agadir"[49].

La proximidad de España a zonas que no han sido reconocidas como libres de fiebre aftosa[50] también supone un elemento a tener en cuenta desde el punto de vista de la bioseguridad y biodefensa, mientras que el riesgo de un ataque de glosopeda se agudizaría en determinados momentos (Cique, 2017) como la fiesta del sacrificio, con la importación masiva de ganado ovino desde Marruecos hacia Ceuta y Melilla[51][52]. *Aid el Kebir* es una celebración importante para la comunidad musulmana, pero desde 2015 el Ministerio de Agricultura ha aplicado restricciones a la entrada de corderos desde el Norte de África a Melilla debido a brotes de fiebre aftosa en Marruecos.

También la OIE, la FAO e INTERPOL están desarrollando un proyecto a favor de la consolidación de la resiliencia frente al agroterrorismo y la agrocriminalidad. Sus áreas prioritarias son el Norte de África, Sudeste asiático y Oriente Medio, centrándose en "el refuerzo de capacidades de los agentes en el terreno y una mejor coordinación de los sectores de la sanidad animal y de las fuerzas del orden" (OIE, 2019). La lucha contra el terrorismo y el crimen organizado en todas sus formas sigue siendo una cuestión prioritaria para la UE y España, apostando por la mejora de la legislación en materia de seguridad fronteriza y el aprovechamiento de bases de datos y cooperación con países no comunitarios, también en torno a las amenazas transfronterizas graves para la salud.

Expertos como el coronel Martín Otero opinan que "sería interesante ampliar la cooperación en seguridad con países del Magreb en la lucha contra amenazas biológicas"[53] teniendo presente además el ascenso del yihadismo en el Sahel y la habilidad de estos grupos para operar en sus estructuras de oportunidad. En todo caso,

49 Otazu, J. (30 octubre 2020).

50 ''La epidemia más reciente en el Reino Unido en 2001 afectó a más de 2.000 explotaciones, provocando ''graves perjuicios a las comunidades rurales, así como una preocupación generalizada entre el público por la seguridad de la carne de vacuno''. Eur-Lex (2016).

51 La Vanguardia (18 agosto 2019).

52 La introducción de enfermedades con altos índice de contagio desde mercados exteriores se ve minimizada por la Ley de Sanidad Animal con "la regulación de la inspección sanitaria en frontera, como una primera barrera defensiva''(p.2). Ley 8/2003, de 24 de abril, de sanidad animal. BOE-A-2003-8510.

53 Fuente: coronel Luis Martín Otero. Entrevista personal. (27 de noviembre 2020).

teniendo en cuenta que en un mundo globalizado no existe soberanía alimentaria plena, ‘’una acción terrorista tendría un sentido transnacional aunque se actúe de forma local”[54], por lo que esta amenaza requiere ser combatida necesariamente también mediante una estrategia transnacional.

5. EL AGROTERRORISMO DESDE LA PERSPECTIVA DE LA SEGURIDAD FÍSICA Y DIGITAL

5.1. SEGURIDAD FÍSICA

Mientras que la ESN-2017 señala dentro de las infraestructuras críticas al sector de la alimentación como un objetivo vulnerable (Ley PIC 08/2011)[55] el bioterrorismo buscaría romper el eslabón más débil dentro de la cadena de distribución, momentos en los que aumentaría el potencial de contaminación intencional. En este sentido, expertos en amenazas NBQR como el oficial de las Fuerzas Armadas Miguel P. Casas consideran que este sería aquel previo al consumidor, mientras que “las fábricas y las plantas de producción y distribución se tratarían de objetivos demasiado arriesgados, aunque no por ello debemos descartarlos del todo”[56]. Por tanto, una acción de estas características respondería a un objetivo de corto alcance pero de gran impacto económico, mediático y propagandístico.

También desde el punto de vista ofensivo, la diseminación por aerosoles precisaría de medios tecnológicos avanzados, algo que podría llevar a pensar que es factible ejecutar sabotajes directos a instalaciones que percibimos erróneamente más seguras frente a espacios al aire libre[57]. En cualquier caso, desde esta perspectiva es preciso disponer de un Plan de Seguridad, revisando constantemente los procedimientos de la compañía y controlando la seguridad en el entorno, perímetro exterior y acceso, para preservar barreras de seguridad físicas. Respecto a esto último, debería garantizarse sobre todo la adecuada supervisión de personal que tiene acceso a áreas críticas durante las distintas fases de producción, para lo que sería necesario desarrollar códigos de conducta, habilitación de Puntos de Control Críticos (PCI)[58] y contratación

54 Fuente: Entrevista personal realizada a un técnico Avanzado en Dirección de Operaciones de Inteligencia y Contrainteligencia y técnico Avanzado en Inteligencia y Dirección de Operaciones Psicológicas, experto en comunicación, a 2 de diciembre 2020 (entrevista telemática). No se facilita la identificación del entrevistado por razones de confidencialidad.

55 Los centros de almacenamiento y distribución alimentaria están considerados infraestructuras estratégicas y servicios esenciales. Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de infraestructuras críticas. BOE-A-2011-7630.

56 Fuente: Entrevista personal realizada al oficial de las FF.AA. Miguel P. Casas, especialista en CBRN/RNBQ y director de seguridad privada. Experiencia en Unidades de Operaciones Especiales y Unidad Militar de Emergencias. Ha participado en misiones internacionales de la OTAN y ONU en Líbano y Afganistán. Actualmente ejerce como oficial de célula NBQ/CBRN y de protección medioambiental en el Cuartel General del Eurocuerpo en Estrasburgo, a 3 de diciembre 2020 (entrevista telemática).

57 Una infección deliberada mediante la exposición a un agente de transmisión aerógena revestiría mayor peligrosidad para la población civil.

58 La herramienta CARVER de la FDA puede servir de referencia proporcionando apoyo específico al sector agroalimentario para la evaluación de riesgos en torno a contaminaciones intencionadas, estudiando el grado de vulnerabilidad de la compañía e incorporando variables de impacto psicológico y socioeconómico.

de un servicio de seguridad competente. Estos, por su parte, se contemplan dentro de los Planes de Seguridad de los Operadores (PSO) de infraestructuras críticas.

Ante potenciales amenazas, la selección del personal debe evidentemente garantizar que no existen vínculos con organizaciones terroristas ni de criminalidad organizada, investigando, reportando y documentando actividades sospechosas cuando sea necesario. Sin embargo, hay que tener en cuenta la siguiente situación:

"En términos de riesgo, las grandes explotaciones ganaderas o grandes extensiones de cultivos siempre serán más vulnerables a un ataque agroterrorista, ya que 'la concienciación mediante la información y formación son fundamentales para impulsar las medidas de bioseguridad en estas instalaciones" (Miguel P. Casas, 2020)[59].

Por ello, resultaría aconsejable orientar el radar de detección de amenazas "a las instalaciones donde se concentra el ganado de forma permanente o temporal, como por ejemplo una feria de ganado"[60] poniendo el foco en unas condiciones higiénico sanitarias óptimas, también en mataderos y en transportes de animales, sobre todo a larga distancia. Por su parte, las áreas de procesamiento revestirían una especial fragilidad, por lo que es necesario desarrollar medidas que salvaguarden la bioseguridad de los alimentos, como pueden ser la prohibición de introducir pertenencias personales y de realizar fotografías, mientras que el servicio de comida (cadenas alimentarias) o superficies como mercados (mayoristas) estarían altamente expuestos porque en ellos se manipulan los productos. En este sentido, parece aconsejable implementar planes de seguridad alimentaria específicos para cada instalación, contando anticipadamente con detectores de incidentes, alarmas operativas, controles de temperaturas y monitorización de *containers* durante la distribución.

5.2. SEGURIDAD DIGITAL

Respecto a la seguridad digital, es necesario "detectar desencadenantes e indicios de posibles actividades ilícitas relacionadas con el acceso a equipos y material biológico, con su adquisición y con su distribución"[61]. Paralelamente, para los técnicos de Laboratorio resulta vital "proteger los laboratorios, tanto de forma física como digital, en los que estén almacenados agentes biológicos del grupo 3 y 4" (García, 2020)[62] asegurando reservas adecuadas de medicamentos y vacunas. En esta línea, en el año 2019 se renovó el Convenio entre la *Agencia Española de Medicamentos y Productos Sanitarios* (AEMPS) y el *Ministerio de Defensa* en torno a la gestión y custodia de depósitos de medicamentos y productos sanitarios para emergencias y catástrofes, algo esencial también ante eventuales escenarios agroterroristas. Mientras tanto, -al igual que en laboratorios y en espacios donde se almacenan productos biológicos patógenos-, la restricción de accesos a lugares donde se encuentren los equipos informáticos se convertiría en una condición básica, garantizando auditorías de seguridad frecuentes y una protección integral contra ciberataques que busquen el robo de información sensible o favorecer alguna de fase del ataque.

59 Fuente: Miguel P. Casas. Entrevista personal. (3 de diciembre 2020).

60 Ibíd.

61 Estos grupos pueden recurrir de forma ilegal a la red oscura para adquisición, transporte y comunicaciones. Véase Operación Pandora.

62 "La posibilidad de modificar microorganismos mediante técnicas de ingeniería genética supone también un riesgo importante". Fuente: Ana E. García. Entrevista personal. (30 de noviembre 2020).

Un ciberataque a la industria de transformación podría consistir en el hackeo de sistemas informáticos para acceder a instalaciones, por ejemplo, para que la detección por parte del sistema informático fallase, sin alertar de la introducción física de otros productos o de su alteración en la cadena. En este sentido, aunque no específicamente en la industria agropecuaria, recientemente se ha producido un intento de contaminación química del agua que abastece a los hogares de toda una ciudad en el Estado de Florida, Estados Unidos[63].

En cualquier caso, el uso malintencionado del ciberespacio representa cada vez más un problema imposible de ignorar, desde los ataques que han recibido estructuras hospitalarias durante la pandemia de la COVID-19 y los intentos de acceder a las investigaciones y desarrollos de algunas vacunas, hasta otras prácticas que puedan perseguir dañar la salud de las personas. Según INTERPOL, que cuenta con una Unidad de Prevención del Bioterrorismo, los delincuentes estarían explotando canales de comunicación ocultos y anónimos como la red oscura para comunicarse, comprar, vender e intercambiar información, algo que ha sido anunciado en su plataforma web desde el año 2017 y que estaría dotando, aunque lentamente, de un nuevo perfil a esta amenaza. Desde la perspectiva de la biodefensa, además, los medicamentos y vacunas también podrían ser objeto de ataque, por lo que respecto a esta cuestión, la organización aconseja reforzar la vigilancia de la cadena de suministro. En un clima de desinformación, los ciberdelincuentes podrían rentabilizar la falsificación de productos sanitarios y otros de necesidad ante la escasez de suministros, por lo que una rápida actuación es fundamental para evitar una catástrofe sanitaria[64].

A todo esto, la libre difusión del conocimiento en el campo de la biomédica podría servir tanto para las vacunas como para el desarrollo de programas biológicos encubiertos (Cique, 2014), constituyendo una ventana de oportunidad para delincuentes y terroristas. De hecho, el riesgo de que grupos extremistas utilicen indebidamente programas de investigación centró la *Convención de Armamento Biológico de la ONU en 2018*, mencionándose específicamente el peligro del hipotético uso terrorista del ébola en África Occidental. Ante todos estos riesgos, la OIE tendría intención de dotarse de herramientas de seguimiento de datos modernizadas, apostando por "la integración de las biotecnologías en los sistemas alimentarios, el uso de big data, inteligencia artificial o blockchain en la gestión de datos" y cruzarlos entre organizaciones[65].

En un contexto de avances científicos como el descrito, también el rol que desempeña la investigación privada corporativa alrededor de la biotecnología agrícola es controvertido. En un campo donde el poder se concentra en algunas empresas transnacionales, existe el riesgo de que en el futuro "empresas en este campo que pudieran estar dirigidas por individuos simpatizantes o vinculados a organizaciones terroristas podrían proporcionar no solo financiación sino información técnica"[66]. En general, y a la larga, la investigación privada corporativa exenta de vigilancia y regulación podría favorecer el

63 El ciberterrorista habría conseguido penetrar en el sistema informático de una planta de tratamiento con el objetivo de aumentar los niveles de hidróxido de sodio dándole dichas instrucciones determinadas al sistema. El personal pudo percatarse a tiempo sin que se produjese ningún daño, existiendo además un control posterior que presumiblemente habría podido detectar la contaminación en las siguientes 24 o 36h. Agencias Washington (9 de febrero de 2021)

64 Interpol (s.f)

65 Organización mundial de sanidad animal (2019).

66 Fuente: técnico Avanzado experto en comunicación. Entrevista personal. (2 de diciembre 2020).

desarrollo de tecnologías y productos susceptibles de ser empleados con la finalidad de destruir cultivos o provocar hambrunas y conflictos armados (Soteras, 2008).

6. INTEGRACIÓN DE CAPACIDADES CIVILES Y MILITARES Y RESPUESTA ANTE CRISIS

Al igual que la segurización física y digital, la integración de capacidades civiles y militares debe estar motivada por una voluntad política definida y un adecuado respaldo financiero y presupuestario. En 2001, la OMS aprobó la *Resolución WHA54.14, Alerta y respuesta ante epidemias,* permitiendo la revisión del *Reglamento Sanitario Internacion*al (RSI) conforme a la evolución de las necesidades en salud pública[67], la lucha contra el tráfico ilegal de plantas y animales y el reforzamiento del control aduanero y la vigilancia permanente. Pero si bien el RSI autoriza a la OMS a denunciar públicamente infracciones de Estados, -reacción tardía o negación de brotes epidemiológicos-, para asegurar la transparencia y el correcto flujo de la información, la organización está sujeta al principio de no injerencia política, por lo que en la práctica sus movimientos contemplan limitaciones significativas.

Con ello, la asignación eficiente de partidas presupuestarias a proyectos es fundamental para obtener resultados positivos. No obstante, la disponibilidad de financiación privada podría estar condicionada a dedicar esos recursos a investigaciones específicas conforme a un particular interés, teniendo en cuenta además el peso de las grandes potencias y más recientemente también de China en el proceso de toma de decisiones. También en ese mismo año se creó la *Red de Laboratorios de Alerta Biológica* (RE-LAB)[68] que, en palabras del coronel Martín Otero, uno de sus impulsores, "cubriría la eficiencia de detección y comunicación al ser activada, algo que no siempre sucede"[69].

Cabe mencionar igualmente algunas iniciativas de cooperación intraestatal beneficiosas en la lucha contra el agroterrorismo y bioterrorismo alimentario como el proyecto *PlantFoodSec*, que puso sobre la mesa por primera vez la preocupación por la seguridad del suministro europeo de alimentación ante posibles ataques[70]. Creado por la UE en 2016, consistió en una red virtual de especialistas en seguridad alimentaria y cultivos, desarrollando una herramienta de evaluación de riesgos rigurosa (análisis de posibles escenarios agroterroristas probado en distintos supuestos representativos).

Pero lo cierto es que más allá de iniciativas con un limitado recorrido como el Cuerpo Médico Europeo[71] -asociadas a la logística y gestión y a otros proyectos compartidos

67 España forma parte de una estructura multilateral que buscaría la prevención de enfermedades zoonóticas, la detección (mediante acciones de vigilancia en tiempo real) y una respuesta rápida multisectorial (con despliegue de personal y contramedidas médicas) Global Health Security Agenda (s.f).

68 La RE-LAB "desempeña sus funciones en el ámbito de la seguridad biológica, en especial en todo lo relacionado con la detección e identificación de agentes biológicos (…) Actualmente está formada por 12 laboratorios de referencia con instalaciones de alta seguridad biológica y por un laboratorio colaborador". Instituto Carlos III (s.f).

69 Fuente: coronel Luis Martín Otero. Entrevista personal (27 de noviembre 2020).

70 Comisión Europea (2016)

71 Reserva de equipos médicos de emergencia y laboratorios móviles de bioseguridad para el desarrollo de capacidades de evacuación médica y despliegue de personal especializado. Hasta la fecha han realizado dos misiones de apoyo internacional.

en bioseguridad-, no existen verdaderos Sistemas de alerta rápida conjuntos multilaterales, aunque la última Estrategia de Seguridad Europea plantea la conveniencia de impulsar algo similar contra los ciberataques. España participa en la acción conjunta EMERGE, -cuyo objetivo es crear una red europea de laboratorios de diagnóstico de bioseguridad de nivel 3 y 4-, en la UE SHIPSAN ACT, la red EPISOUTH y EPISOUTH PLUS, mientras que otro proyecto, *EQuaTox*, estableció laboratorios especializados en toxinas, algo positivo en la lucha contra el bioterrorismo. Sería interesante estudiar si esto es trasladable a la industria agropecuaria de los países de la UE para una gestión de crisis más eficiente, a través de canales de comunicación seguros en torno al *Centro de Coordinación de Alertas y Emergencias Sanitarias* (CCAES)[72].

En ese ámbito, además, es esencial contar con todo el potencial científico industrial y militar de una sociedad, algo con lo que estarían familiarizados médicos y enfermeros militares, así como farmacéuticos y veterinarios (Cique, 2020), pese a que estos últimos todavía no están considerados como una profesión sanitaria dentro del Sistema Nacional de Salud. Por otro lado, a nivel intraestatal existe *una Estrategia nacional de protección civil,* así como un *Plan de Biocustodia* -en este caso enfocado a la amenaza nuclear y no a la biológica-, pero la responsabilidad correspondería al Ministerio de Sanidad, Consumo y Bienestar social, "donde las capacidades militares y el Sistema de Protección Civil se integran de forma explícita en la respuesta" (Cique, 2020: 33)[73].

Aunque se han producido avances, parece que las capacidades para detectar acciones biodelictivas, tanto a nivel nacional como europeo, son todavía modestas. Respecto a los Sistemas de respuesta, no solo debe darse una profilaxis adecuada sino una política de comunicación que ponga en valor las fuentes oficiales, en un esfuerzo por despolitizar su contenido y proporcionar información técnica accesible. Solo así se transmitirá la sensación de solvencia y credibilidad necesarias, algo fundamental para asegurar una mínima estabilidad durante el desarrollo del incidente, clave para ejercer un control efectivo de la situación. Una política de comunicación equilibrada se fundamentaría por tanto en la ponderación del riesgo, ya que esto repercute en una menor alarma social. También se obstaculizaría mucho menos el trabajo de las Fuerzas y Cuerpos de Seguridad del Estado y profesionales en salud humana y animal, contrarrestándose acciones de desinformación y pseudociencia.

Teniendo esto presente, los expertos coinciden en valorar como deficiente el nivel de concienciación de la sociedad general, así como de los agentes del sistema agropecuario en cuanto a riesgos biológicos. El coronel Martín Otero considera que "el estado de investigación en materia de bioseguridad de cultivos y alimentos podría

72 El CCAES es competente en la elaboración de planes de prevención y respuesta ante amenazas a la salud pública en España, coordinando la *Red Nacional de Vigilancia Epidemiológica* (RENAVE). En una situación epidemiológica también actuaría el *Sistema de Alerta Precoz y Respuesta Rápida* (SIARP) los servicios de vigilancia de las Comunidad Autónomas y el *Centro Nacional de Epidemiología* (CNE) del Instituto de Salud Carlos III. El SIAPR se habría incorporado al CCAES con el objetivo de disponer de una red de comunicación permanente ante Eventos de Salud Pública de Importancia Nacional e Internacional, su seguimiento y evaluación.

73 También existe un acuerdo entre Sanidad Militar y Ministerio de Sanidad para la vigilancia entomológica en instalaciones de Defensa que resulta interesante a la hora de prevenir la entrada natural o intencionada de especies invasoras como "mosquitos y otros dípteros hematófagos" que generarían plagas en España. Cique, A. (2020).

ser mejorable, para lo que sería necesario aumentar el presupuesto"[74]. Mientras, el oficial de las Fuerzas Armadas Miguel P. Casas añade que "es preocupante el desconocimiento general de la sociedad y en particular, en muchos casos, de las Fuerzas y Cuerpos de Seguridad del Estado, protección civil y bomberos sobre la realidad de la amenaza NBQR"[75]. En este contexto, la Inteligencia Sanitaria (MEDINT) podría resultar de apoyo para autoridades civiles en aspectos logísticos, en tanto que ''la creación de doctrina y planes operativos, así como sistema de vigilancia y monitoreo son son esenciales en futuras amenazas, existiendo herramientas informáticas de big data para realizar inferencia y prospectiva de los parámetros de salud pública" (Castillejo, 2020)[76].

7. AMPLIACIÓN DE LA COOPERACIÓN ESPAÑOLA EN EL MAGREB EN SEGURIDAD AGROPECUARIA

La lucha contra amenazas biológicas transfronterizas constituye un bien público mundial, por lo que se necesitaría una colaboración formalizada y debidamente coordinada entre Estados en base a la suma e integración de capacidades. En este sentido, se ha considerado necesario el desarrollo de la iniciativa *One Health*, la cual se basa en un enfoque que engloba sanidad animal, salud pública y seguridad, adecuado ante desafíos de salud pública globales, incluido el agroterrorismo. Al mismo tiempo, España mantiene una vocación de cooperación estable con países del Magreb como Marruecos también en el ámbito de la seguridad y especialmente en el desarrollo de un modelo de lucha contra el terrorismo que ha registrado resultados positivos, por lo que parece conveniente actualizarlo conforme a amenazas emergentes como el bioterrorismo y agroterrorismo.

Para ello, primero debemos conocer el riesgo real en la actualidad y los escenarios de riesgo plausibles, identificando debilidades y fortalezas respecto a la lucha contra amenazas biológicas en cada país, para lo que podrían desarrollarse consultorías o asistencias técnicas concretas. Posteriormente cabría adoptar Estrategias generales y específicas, así como Protocolos de colaboración que materialicen dichas líneas estratégicas en sectores en los que dependemos mutuamente y donde existen intereses compartidos. En este caso, nos interesaría fomentar la coordinación a partir de ejercicios conjuntos para determinar el nivel real de comunicación y desempeño entre responsables y organismos homólogos, así como fortalecer la armonización de regulaciones, por ejemplo, en medidas básicas fitosanitarias.

También resultaría conveniente desarrollar programas de sensibilización en torno a esta problemática a través de la difusión de información sanitaria y zoosanitaria, haciendo accesible el conocimiento de los mecanismos de prevención y respuesta en todos los niveles territoriales. El apoyo a la formación especializada supondría incluso el despliegue de personal sanitario en crisis reales y simulacros junto con otros profesionales (equipos de intervención ante incidentes biológicos), asegurando inversiones

74 Fuente: Entrevista personal (27 de noviembre 2020).

75 Fuente: Entrevista personal (3 de diciembre de 2020).

76 Fuente: Entrevista personal realizada a Sergio Castillejo Pérez. Licenciado en Medicina. Especialización en Medicina Tropical, Inteligencia y Seguridad Internacional, y Gestión Internacional de Crisis. Ha sido Capitán Médico en el Cuerpo Militar de Sanidad y en el Instituto Mixto de Investigación Biosanitaria de la Defensa, a 14 de diciembre de 2020 (entrevista telemática)

suficientes para la correcta implementación de planes de contingencia e intervención entre ambos. El simulacro más reciente ante escenarios NBQR, de carácter intraestral, tuvo lugar en Santander en el III Congreso Internacional de Sanidad Militar[77]. Este contó con la participación de servicios de emergencias, protección civil y policía que participaron en un escenario de ataque con gas sarín contra un objetivo turístico.

La corrección de deficiencias de sistemas de salud, enfocado a la reducción de desigualdad entre recursos, debe acompañarse de mejoras en las capacidades de diagnóstico laboratorial y de los sistemas de trazabilidad de contactos, minimizando los impactos de crisis transnacionales. Surgiría así la posibilidad de conformar un grupo de trabajo internacional abierto a la participación de terceros sobre bioseguridad, estableciendo una periodicidad adecuada para encuentros complementarios a reuniones de Alto Nivel. A todo esto, resultaría imprescindible mantener relaciones de buena vecindad con un país con el que a lo largo de la historia se han producido desencuentros y etapas de desgaste en las relaciones bilaterales[78]. En el marco de una acción solidaria, España prestaría su apoyo a un Plan regional de bioseguridad en el área del Magreb que pueda trasladarse al Sahel a largo plazo, -desarrollando una cooperación triangular con África Subsahariana-, con especial atención a la evolución del terrorismo yihadista en la región. El fortalecimiento de los servicios de aduanas e inmigración, reforzando a su vez zonas especiales de vigilancia en puertos y aeropuertos con efectivos entrenados en la detección de amenazas NBQR, contribuiría a la reducción del riesgo bioterrorista en nuestras fronteras[79].

Finalmente, la recuperación tras incidentes bioterroristas se centraría en el apoyo a la investigación policial y una correcta recogida de pruebas forenses en los focos de infección, poniendo a prueba el nivel de competencia de ejercicios de simulación[80]. En España ya se ha realizado un simulacro de escenario bioterrorista con fiebre aftosa en una explotación en el que participó el Cuerpo Nacional de Policía, Guardia Civil, RELAB y Servicios Veterinarios del Ministerio y CCAA. Con esto, la adopción de un Plan de Defensa alimentario compartido estaría orientado a “proveer alimentos sanos y seguros libres de contaminantes añadidos de forma intencionada con objetivo criminal o terrorista” (Cique, 2014: 1) por lo que España y Marruecos podrían, una vez superada la crisis diplomática, impulsar conjuntamente proyectos que beneficiarían al Norte de África y Flanco Sur europeo. Conforme a esto, la iniciativa ALERT de la FDA podría ser un modelo para la implementación efectiva de Planes de Defensa alimentarios también en un escenario compartido como este.

77 Departamento de Seguridad Nacional (24 febrero 2018).

78 España ha cooperado tradicionalmente con Marruecos en ámbitos diversos que van desde la gestión de los flujos migratorios hasta la lucha contra el yihadismo, el crimen organizado y los tráficos ilícitos. Con el inicio de una nueva etapa en las relaciones desde 2004 hasta la actualidad, interrumpida con la crisis de Ceuta, entre ambos se han desarrollado operaciones policiales conjuntas antiterroristas y otras iniciativas. Marruecos está dentro del V Plan Director de la Cooperación Española (2018-2021).

79 El regreso de combatientes terroristas extranjeros (CTE) podría suponer la transmisión de medios y conocimientos basados en la experiencia también en este ámbito específico, poniendo igualmente sobre la mesa una cuestión no exenta de polémica como la repatriación de yihadistas occidentales, sobre todo mujeres y menores, que se unieron al Califato en Siria e Irak, actualmente en el limbo de campos como al-Roj custodiados por milicias kurdas.

80 Este simulacro buscaba la evaluación de capacidades de coordinación, adecuación en la comunicación y transferencia de pruebas y eficacia de los planes de contingencia. Organización Mundial de Sanidad animal (2016).

8. CONCLUSIONES

La salud humana depende de la salud animal y de la salud medioambiental, una realidad que en un mundo globalizado afectaría a todas las sociedades independientemente de su nivel de desarrollo. Si bien las condiciones higiénico sanitarias y la falta de regulación efectiva en torno a la seguridad de cultivos y de la sanidad animal favorecen la evolución y el incremento de los agentes biológicos patógenos, la ausencia de soberanía alimentaria en sociedades consumistas implica la necesidad de mantener relaciones comerciales estables agrícolas y ganaderas que protejan la industria alimentaria.

Las enfermedades epidémicas de origen natural han demostrado una elevada capacidad de impacto en el desarrollo de la historia. Sin embargo y más allá de las prácticas desarrolladas en contextos de guerra biológica, existen precedentes en cuanto al uso de agentes químicos y biológicos por parte de grupos no estatales contra la población civil, sectas y ecoterroristas que podrían inscribirse en la lógica general del biocrimen, agroterrorismo y bioterrorismo alimentario, acciones que no siempre precisan de recursos económicos ilimitados.

Organizaciones yihadistas como *Daesh* y *Al Qaeda* habrían expresado interés en torno al armamento NBQR, si bien contarían con dificultades para desarrollar su propio programa biológico ante los distintos retos tecnológicos, operativos y logísticos que pueden surgir sobre todo a gran escala. La capacidad de influencia de estos, en cambio, aconsejaría observar su evolución y en ningún caso descuidar las medidas de bioseguridad y biodefensa, especialmente en las relaciones con países del continente africano. Con esto, el sector agropecuario tendría un rol esencial en el sostenimiento del desarrollo vital de una nación, ya que este constituye nuestra fuente de alimentación real.

En su condición de infraestructura crítica, el sector precisa de una adecuada protección física y digital, mientras que la cuantificación del nivel de peligrosidad de esta amenaza dependerá de una correcta medición del riesgo asociado a esta y de la construcción de escenarios de riesgo fiables. Un ataque de naturaleza bioterrorista afectaría a todos los sectores de actividad, mientras que en España el turismo, que depende del sector primario para su sostenimiento, resultaría especialmente perjudicado. Por tanto, mientras este sea considerado como un escenario de baja probabilidad, mayor será el margen de maniobra de las autoridades competentes en la prevención y preparación ante una crisis de impactos multidimensionales.

Debe realizarse en cualquier caso una apuesta clara por la excelencia científica, desarrollando investigaciones responsables y evitando prácticas dañinas para el estatus sanitario de nuestro país y del entorno europeo. Para ello, es imprescindible concienciar a la población del peligro real que supone el empleo deliberado de patógenos, aprovechando las lecciones aprendidas tras incidentes epidémicos globales, si no se cuenta con un sistema de coordinación eficiente que integre capacidades civiles y militares propias de cada especialidad. Si bien el riesgo cero no existe, las dinámicas de colaboración repercuten de manera directa en el aumento de los niveles de bioseguridad y bioprotección. Superar acuerdos simbólicos y declaraciones de intenciones vacías resulta clave para poner en marcha medidas vinculantes, abogando por una cooperación nacional e internacional estable entre autoridades y estructuras sanitarias. Esto implica la necesidad de superar las tensiones recientes con Marruecos puesto que la cooperación sería prioritaria para España, en tanto que permitiría liderar y coordinar esfuerzos en antiterrorismo el Magreb y Sahel.

BIBLIOGRAFÍA

Agencias Washington (9 de febrero de 2021) Un hacker intenta envenenar el agua del grifo de una ciudad de Florida. La Vanguardia. Tecnología. Extraído a 10 de febrero de 2021. https://www.lavanguardia.com/tecnologia/20210209/6233589/hacker-envenenar-agua-grifo-florida.html

Allswede, M.P; Binyamin, T. (25 may 2011) The Potential Terrorist Possession of Weaponized Plague in North Africa: A Forensic Epidemiology Case Study and Discussion of Principles in Tizi Ouzou, Algeria. *Prehospital and Disaster Medicine (PDM)-Cambridge University Press*, 26 (1). Extraído a 25 de noviembre de 2020. https://www.cambridge.org/core/journals/prehospital-and-disaster-medicine/article/p123-the-potential-terrorist-possession-of-weaponized-plague-in-north-africa-a-forensic-epidemiology-case-study-and-discussion-of-principles-in-tizi-ouzou-algeria/6796DD11A7CDC0BCA7BF2A4522C547C8

BBC news mundo (17 septiembre 2019) Viruela: ¿por qué todavía se guardan dos muestras del virus que produce una de las enfermedades más letales de la historia? Redacción. Extraído a 3 de diciembre de 2020. https://www.bbc.com/mundo/noticias-49734898

Centers for disease control and prevention, CDC. (N.D) Bioterrorism Agents/Diseases (Category A). Emergency Preparedness and Response CDC. Extraído a 22 de noviembre de 2020. https://emergency.cdc.gov/agent/agentlist-category.asp

Cique, A. (2 mayo 2014) Defensa alimentaria: un reto para el sector agroalimentario. Documento MARCO IEEE 06/2014. Instituto Español de Estudios Estratégicos. Extraído a 3 de diciembre de 2020. http://www.ieee.es/temas/cambio-climatico/2014/DIEEEM06-2014.html

Cique, A. (2015) Capacidad biológica del Daesh: querer no es poder. Documento de Opinión IEEE 130/2015. Instituto Español de Estudios Estratégicos. Extraído a 25 de noviembre de 2020. http://www.ieee.es/contenido/noticias/2015/12/DIEEEO130-2015.html

Cique, A. (8 mayo 2017) Preparación y respuesta frente al agroterrorismo. Documento de Opinión IEEE 50/2017. Instituto Español de Estudios Estratégicos. Extraído a 27 de noviemnbre de 2020. http://www.ieee.es/contenido/noticias/2017/05/DIEEEO50-2017.html

Cique, A. (5 marzo 2018) Reducción de amenazas biológicas. Documento Marco IEEE 06/2018. Instituto Español de Estudios Estratégicos. Extraído a 4 de diciembre de 2020. http://www.ieee.es/contenido/noticias/2018/03/DIEEEM06-2018.html

Cique, A. (2020) Capacidades sanitarias especializadas en escenario bioterroristas. Documento de Opinión IEEE 68/2020. Instituto Español de Estudios Estratégicos. Documento Marco IEEE 06/2018. Instituto Español de Estudios Estratégicos. Extraído a 5 de diciembre de 2020. http://www.ieee.es/Galerias/fichero/docs_informativos/2020/DIEEEI05_2020ALBCIQ_SanidadMilitar.pdf

Comisión Europea (2016) Final Report Summary - PLANTFOODSEC (Plant and Food Biosecurity) CORDIS, Resultados de Investigaciones de la UE. Extraído a 2 de diciembre de 2020. https://cordis.europa.eu/project/id/261752/reporting/es

Council of Europe (2020) The Council of Europe continues working to enhance international co-operation against terrorism, including bioterrorism.Counter-terrorism

Newsroom. Extraído a 1 de diciembre de 2020. https://www.coe.int/en/web/counter-terrorism/-/covid-19-pandemic-the-secretariat-of-the-committee-on-counter-terrorism-warns-against-the-risk-of-bioterrorism

Darwich, L. (julio 2014) Panorama. Introducción a las zoonosis: conceptos básicos. Revista de Divulgación científica del Centro de Investigación en Sanidad Animal, CReSA. (6) 4-8. Extraído a 16 de noviembre de 2020. http://www.cresa.cat/cresa3/modulos/actividades/cresapiens/pubs/cresapiens06.pdf

Departamento de Seguridad Nacional (2017) Estrategia de Seguridad Nacional. Un proyecto compartido de todo y para todos. Gobierno de España.

Departamento de Seguridad Nacional (24 febrero 2018) Nacional-Simulacro Antiterrorista. Actualidad. Seguridad Nacional. Extraído a 1 de diciembre de 2020.https://www.dsn.gob.es/gl/actualidad/seguridad-nacional-ultima-hora/nacional-simulacro-ataque-bioterrorista

Díez, A. (septiembre 2020). Yihadismo en el Sahel Occidental: Una amenaza creciente y compartida. Documentos. Departamento de Seguridad Nacional-DSN. Extraído a 27 de noviembre de 2020. https://www.dsn.gob.es/es/documento/yihadismo-sahel-occidental-una-amenaza-creciente-compartida

Entrevista personal realizada al coronel Luis Martín Otero, Coordinador del Centro de Vigilancia Sanitaria de la UCM (VISAVET) y Red de Laboratorios de Alerta Biológica (RE-LAB) especialista en microbiología, sanidad ambiental y sanidad animal. Su campo de trabajo consiste en las enfermedades emergentes y reemergentes en sanidad animal que puedan afectar a la seguridad nacional e internacional, a 27 de noviembre 2020 (entrevista telemática).

Entrevista personal realizada al Oficial de las FFAA Miguel P. Casas, Especialista en CBRN/RNBQ y Director de seguridad privada. Experiencia en Unidades de Operaciones Especiales y Unidad Militar de Emergencias. Ha participado en misiones internacionales de la OTAN y ONU en Líbano y Afganistán. Actualmente ejerce como Oficial de célula NBQ/CBRN y de protección medioambiental en el Cuartel General del Eurocuerpo en Estrasburgo, a 3 de diciembre 2020 (entrevista telemática).

Entrevista personal realizada a un Técnico Avanzado en Dirección de Operaciones de Inteligencia y Contrainteligencia y Técnico Avanzado en Inteligencia y Dirección de Operaciones Psicológicas, experto en comunicación, a 2 de diciembre 2020 (entrevista telemática). No se facilita la identificación del entrevistado por razones de confidencialidad.

Entrevista personal realizada a Ana E. García. Técnico Superior de Laboratorio y Análisis Clínico del Centro Farmacéutico Canario del Ejército del Aire-CEFARCA, Estado Mayor. Formación en Rastreo Covid-19. Experiencia como Delegada Informadora de Laboratorios Farmacéuticos, a 30 de noviembre de 2020 en Las Palmas de Gran Canaria.

Entrevista personal realizada a Sergio Castillejo Pérez. Licenciado en Medicina. Especialización en Medicina Tropical, Inteligencia y Seguridad Internacional, y Gestión Internacional de Crisis. Ha sido Capitán Médico en el Cuerpo Militar de Sanidad y en el Instituto Mixto de Investigación Biosanitaria de la Defensa, a 14 de diciembre de 2020 (entrevista telemática)

Eur-Lex (2020) Comunicación sobre la Estrategia de la UE para una Unión de Seguridad. COM (2020) 605 final. EUR-LEX home. Extraído a 3 de diciembre de 2020. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52020DC0605

Eur-Lex (2016) Lucha contra la fiebre aftosa. EUR-LEX (2003). Directiva 2003/85/CE del Consejo relativa a medidas comunitarias de lucha contra la fiebre aftosa. EUR-LEX home. Extraído a 4 de diciembre de 2020. https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=LEGISSUM%3Af83003

Exeltur (2018) Impactur Canarias. Estudio del impacto económico del turismo sobre la economía y el empleo de las Islas Canarias. Alianza para la Excelencia Turística (Exeltur) y Gobierno de Canarias. Extraído a 23 de noviembre de 2020. https://www.exceltur.org/wp-content/uploads/2019/12/IMPACTUR-Canarias-2018.pdf

Food Department, WHO (2003) Terrorist Threats to Food. Guidance for Establishing and Strengthening Prevention and Response Systems. Food Safety Issues. Extraido a 1 diciembre de 2020. https://apps.who.int/iris/handle/10665/42619

Food and Agriculture Oganization (october 2018). Joint FAO-OIE Evaluation of the Global Framework for Transboundary Animal Diseases (GF-TADs). Office of Evaluation. Project evaluation series, OIE. Extraído a 1 de diciembre de 2020. http://www.fao.org/publications/card/es/c/CA1957EN/

Global Health Security Agenda (s.f) Zoonotic Disease. Home. Extraído a 4 de diciembre de 2020. https://ghsagenda.org/zoonotic-disease/

Instituto Carlos III (s.f) Red de Laboratorios de Alerta Biológica. Presentación.Extraído a 1 de diciembre de 2020. https://eng.isciii.es/eng.isciii.es/QuienesSomos/CentrosPropios/relab/Paginas/default.html

Instituto Nacional de Seguridad e Higiene en el Trabajo (s.f) BioDat. Ministerio de Trabajo, Migraciones y Seguridad Social. Extraído a 7 de diciembre de 2020. http://biodat.insht.es/

Instituto Nacional de Seguridad e Higiene en el Trabajo (2014) Evaluación y Prevención de Riesgos relacionados con la Exposición a Agentes Biológicos. Guía Técnica INSST. Extraído a 16 de noviembre de 2020. https://www.insst.es/documents/94886/96076/agen_bio.pdf/f2f4067d-d489-4186-b5cd-994abd1505d9

Interpol (s.f) Interpol alerta del interés de la delincuencia organizada por las vacunas contra la COVID-19. Noticias. Extraído a 2 de diciembre de 2020. https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2020/INTERPOL-alerta-del-interes-de-la-delincuencia-organizada-por-las-vacunas-contra-la-COVID 19#:~:text=Las%20notificaciones%20naranjas%20de%20INTERPOL,comportamientos%20delictivos%20de-predadores%20y%20oportunistas

King, L. (2004) Enfermedades zoonóticas emergentes y reemergentes: desafíos y oportunidades. 76ª Sesión General.Comité Internacional París-OIET. Extraído a 22 de noviembre de 2020. https://www.oie.int/doc/ged/D696.PDF

La Vanguardia (18 agosto 2019) Festividades del Islam. Miles de musulmanes celebran en Melilla Aid El Kebir o Fiesta del Sacrificio. Redacción. Extraído a 2 de diciembre de 2020. https://www.lavanguardia.com/vida/20190812/464008913606/miles-de-musulmanes-celebran-en-melilla-aid-el-kebir-o-fiesta-del-sacrificio.html

León, M. (2016) Medio ambiente, biodiversidad y seguridad. Revista de Pensamiento Estratégico y Seguridad CISDE, 2 (1). Extraído a 3 de diciembre de 2020. http://ua-journals.com/ojs/index.php/cisdejournal/article/view/144

Ley 8/2003, de 24 de abril, de sanidad animal. BOE-A-2003-8510. https://www.boe.es/buscar/doc.php?id=BOE-A-2003-8510

Ley 8/2011 de 28 de abril, por la que se establecen medidas para la protección de infraestructuras críticas. BOE-A-2011-7630. https://boe.es/buscar/pdf/2011/BOE-A-2011-7630-consolidado.pdf

Méndez, L. (3 noviembre 2020) Reservas de inteligencia compartidas en el nuevo panorama estratégico. Documento de Opinión IEEE 139/2020. Instituto Español de Estudios Estratégicos. Extraído el 20 de noviembre de 2020.http://www.ieee.es/publicaciones-new/documentos deopinion/2020/DIEEEO139_2020LAUMEN_inteligencia.html

Méndez, L. (2020) Inteligencia contra el yihadismo y el crimen organizado: oportunidades en la cooperación hispano-marroquí. Santa Cruz de Tenerife, España. Ediciones Idea, Colección Idea Global.

Ministerio de Agricultura, Pesca y Alimentación (30 noviembre 2020) Situación de la Peste Porcina Africana. DG Sanidad de la Producción Agraria. DG Sanidad e Higiene Animal y Trazabilidad (Gobierno de España). Extraído a 2 de diciembre de 2020. https://www.mapa.gob.es/es/ganaderia/temas/sanidad-animal-higiene-ganadera/informeppa_2021-01-13_tcm30-437584.pdf

Ministerio de Asuntos Exteriores, Unión Europea y Cooperación (s.f) La política española de no proliferación y desarme. Gobierno de España. Extraído a 1 de diciembre de 2020. http://www.exteriores.gob.es/Portal/es/PoliticaExteriorCooperacion/DesarmeyNoProliferaci%C3%B3n/Paginas/Inicio.aspx

Mowatt-Larssen, R. (november 16 2010) Argument. Al Qaeda's Nuclear Ambitions. Ayman al-Zawahiri promises to make his next smoking gun a mushroom cloud. Foreign Policy (FP). Extraído a 6 de diciembre de 2020. https://foreignpolicy.com/2010/11/16/al-qaedas-nuclear-ambitions/

Organización Mundial de Sanidad animal (2016) Ejercicio de simulacro: Amenaza biológica por terrorismo - Fiebre aftosa en España. El Sistema Mundial de información Sanitaria (web). Extraído a 1 de diciembre de 2020. https://www.oie.int/es/sanidad-animal-en-el-mundo/el-sistema-mundial-de-informacion-sanitaria/ejercicios-de-simulacro/detalle/article/simulation-exercise-biological-terrorism-threat-foot-and-mouth-disease-in-spain/

Organización Mundial de la Sanidad animal, OIE (2019) Informe Anual de Actividad.'Su sanidad, nuestro futuro'. Extraído a 21 de noviembre de 2020. Publicaciones OIE. https://www.oie.int/rapport2018/wp-content/uploads/2019/05/OIE-RAPPORT-ANNUEL-ES-WEB.pdf

Otazu, J. (30 octubre 2020) Marruecos, el discreto destino de la agricultura española. Agrodiario. Extraído a 2 de diciembre de 2020. https://www.agrodiario.com/texto-diario/mostrar/2142994/marruecos-discreto-destino-agricultura-espanola

Ray, K.; Wright, L. (2019) Long-Term Fate of Agent Orange and Dioxin TCDD Contaminated Soils and Sediments in Vietnam Hotspots. Open Journal of Soil Science, (9)

1. Extraído a 3 de diciembre de 2020. https://www.scirp.org/journal/paperinformation.aspx?paperid=90675

Real Decreto 664/1997, de 12 de mayo, sobre la protección de los trabajadores contra los riesgos relacionados con la exposición a agentes biológicos durante el trabajo. Extraído a 3 de diciembre de 2020. BOE-A-1997-11144. https://www.boe.es/buscar/act.php?id=BOE-A-1997-11144

Reinares, F. (2020) COVID-19 y bioterrorismo. Comentario Elcano 9/2020 - 23/3/2020. Real Instituto Elcano. Extraído a 4 de diciembre de 2020. http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/comentario-reinares-covid-19-y-bioterrorismo

Soteras, F. (2006) Seguridad biológica. Trabajo Programa de Doctorado Paz y Seguridad Internacional. Instituto Universitario General Gutiérrez Mellado-UNED. Extraído a 1 de diciembre de 2020. https://iugm.es/wp-content/uploads/2016/07/Seguridad_Biologica_Fernando_Soteras.pdf

Soteras, F. (2008) Agroterrorismo. La nueva amenaza emergente para las sociedades d consumo. Boletín de Información- Centro Superior de Estudios de la Defensa. (304) 15-24. Biblioteca del Ministerio de la Presidencia. Extraído a 2 de diciembre de 2020. https://mpr.bage.es/cgi-bin/koha/opac-detail.pl?biblionumber=169334

Taleb, N. (2007) El cisne negro: el impacto de lo altamente improbable. Madrid, Paidós Ibérica.

US Department of Justice (2010) Amerithrax Investigative Summary. DOJ Reports. Extraído el 5 de diciembre de 2020. https://www.justice.gov/archive/amerithrax/docs/amx-investigative-summary.pdf

VISAVET (2010) Nuevas amenazas terroristas del siglo XXI. II Jornada sobre Bioterrorismo. Terrorismo alimentario. Universidad Complutense de Madrid. Extraído a 3 de diciembre de 2020.https://www.visavet.es/es/congresos/jornada_bioterrorismo_amenazas_siglo_xxi_seguridad_defensa.php

World Health Organization (2004) Public health response to biological and chemical weapons. Who Guidance. Extraído a 5 de diciembre de 2020. https://www.who.int/csr/delibepidemics/biochemguide/en/

STABILITY POLICING CONCEPT: A MUST FOR THE ALLIANCE, AN OPPORTUNITY FOR THE SPANISH ARMED FORCES

JORGE JUAN PÉREZ RODRÍGUEZ

LTCOL (OF-4) SPANISH GUARDIA CIVIL
RESEARCHER IN TRAINING AT THE INTERNATIONAL DOCTORAL SCHOOL OF THE UNED
DOCTORAL PROGRAM IN EUROPEAN UNION

Fecha de recepción: 02/03/2021. Fecha de aceptación: 04/06/2021

ABSTRACT

SP (Stability Policing) is defined as the 5th function of NATO (North Atlantic Treaty Organization) MP (Military Police). Despite that and as a result of the last lessons learnt from NATO Operations, SP should be treated as a new independent discipline in NATO Doctrine due to the relevant impact of its activities in the operations. These are aimed at managing the transition from a situation of war or instability to a stable situation, filling the security gap that exists after the completion of military operations, until the deployment of civilian security forces is possible.

This article simply intends to highlight the need to enhance the capabilities of the military forces in order to lead the transition from a post-war situation generated after a military intervention, to a situation of stability that allows the participation of civilian capabilities. All this, in light of the negative results observed after the latest NATO operations. Without a change in this regard, it does not seem possible to face new missions with guarantees of success, at a time when large regions of the world are demanding the need for help to improve their stability as the first factor whose consolidation is essential for social progress in other areas.

The SP concept could be a useful tool to fill the existing aforementioned gap and contribute to achieve the final target of the operations: the establishment of a secure situation that facilitates the progress of societies.

SAF (Spanish Armed Forces) should take advantage of the excellent capabilities of Guardia Civil in order to perform SP tasks in military operations and benefit from its participation, making it possible to assume a leading position in NATO operations.

Keywords: Stability, military, police, civil-military, operations, strategy, security, Guardia Civil, Gendarmerie, investigation, NATO.

1. THE RELEVANCE OF STABILIZATION IN NATO OPERATIONS

Terrorists, organized crime syndicates, warlords, and petty criminals have all found a suitable habitat to develop their illegal activities in states and regions in conflict. During the last decades, these activities have been favored by the development of new technologies linked to the Internet, economic globalization, and the increase in

fanaticism. Civil society has been the victim that suffered the effects of the evolution of these unstable environments[1].

Following the opinion of the USIP (United States Institute of Peace), the only effective possible response to this situation should group together all the actions required for the stabilization of each of the different sectors, in which it is necessary to act, assigning them to specialized organizations and serving as a basis for the establishment of a sustainable long-lasting peace[2].

In a generic way, the USIP's Guiding Principles for Stabilization and Reconstruction defines the concept of stabilization as *"ending or preventing the recurrence of violent conflict and creating the conditions for normal economic activity and non-violent politics[3]".*

In the field of defense, NATO defines stabilization[4] as *"an approach used to mitigate crisis, promote legitimate political authority, and set the conditions for long-term stability by using comprehensive civilian and military actions to reduce violence, re-establish security, and end social, economic, and political turmoil."*

During the last decades, NATO members have launched various initiatives aimed at stabilizing conflict zones in diverse countries such as Afghanistan, Iraq, or Somalia. It has also developed other initiatives oriented to the fight against terrorism, with characteristics similar to stabilization programs across the Middle East. In all of them, no matter what the solution is called, stabilization is a necessity whose achievement is essential, and it cannot be addressed by the military forces alone. The use of force should not and cannot be the only tool to be used in these initiatives, nor is it the most effective.

Although NATO's ability to stabilize conflict zones has increased in recent years, considering the lessons learnt from the failures of the last operations, it could be considered that it has not yet reached the desirable levels of development that will ensure the success of operations. NATO members face an increasingly complex and uncertain global environment in which many of their adversaries show instability and take advantage from it. Protracted conflicts provide a suitable habitat for violent extremists and criminals to expand their dominance of the area. Because of this, it is necessary for NATO to redouble its efforts and carry out stabilization missions adequately.

Following the Report of the SIGAR (Special Inspector General for the Afghanistan Reconstruction) *"Stabilization: Lessons from the U.S. Experience in Afghanistan[5]"* stabilization military missions should have into account, among other insights, the following recommendations highlighting the need for complementing military contingents

1 *"Guiding Principles for Stabilization and Reconstruction". USIP (2009). Washington. ISBN 978-1-60127-033-7. Section 1: INTRODUCTION, 1.0 Context, page 1-2*

2 Idem 1

3 Ibid 1. Appendix E: Acronyms and Glossary of Selected Key Terms, page 11-232.

4 NSO (NATO Standardization Office). Allied Joint Publication AJP-3.4.5 *"Allied Joint Doctrine for the military contribution to stabilization and reconstruction", Edition A Version 1, December 2015, Chapter 1, Section 1, par 102*

5 SIGAR. *"Stabilization: Lessons from the U.S. Experience in Afghanistan", May 2018* https://www.sigar.mil/pdf/lessonslearned/SIGAR-18-48-LL.pdf , EXECUTIVE SUMMARY, RECOMMENDATIONS, Executive Branch, page xiii, consulted 28th Feb 21

with the civilian capabilities necessary to undertake them:

> "1. State should take *the lead in laying out a robust whole-of-government stabilization strategy, USAID (United States Agency for International Development) should be the lead implementer, and US DOD (Department of Defense) should support their efforts.*
>
> *(…)*
>
> *6. DOD should ensure it has a sufficient number and mix of civil affairs personnel with the right training and aptitude for the next stabilization mission.*
>
> *7. State and USAID should designate a new civilian response corps of active and standby civilian specialists* who can staff stabilization missions".

2. STABILIZATION AND STABILITY POLICING

According to the USIP, the Strategic Framework for Stabilization and Reconstruction offers a comprehensive look at the complexity of stabilization missions. This framework recognizes that *"the end states and their associated conditions cannot be pursued independently of one another[6]".* One of these end states necessary to achieve it is a SASE (Safe and Secure Environment), *"in which the population has the freedom to pursue daily activities without fear of politically motivated, persistent, or large-scale violence[7]".*

A key action in this field is the SSR (Security Sector Reform), necessary to build host nation ownership and capacity. Following NATO Doctrine[8], *"SSR involves reforming security institutions so that they can play an effective and accountable role in providing internal and external security. SSR is focused on establishing the conditions for meeting longer term governance and development; however, it also contributes to establishing a SASE and restoring public security"*.

SP (Stability Policing) is one of the pillars of the SSR process envisaged in AJP (Allied Joint Publication)-1 (e)[9] and in AJP-3[10] doctrinal series. SP involves reforming security institutions so that they can play an effective and accountable role in providing internal and external security, including maintaining local law and order until appropriate civil authorities can take over their tasks.

According to AJP-3.22[11], SP is defined as "*police related activities intended to reinforce or temporarily replace the indigenous police in order to contribute to the restoration and/or*

6 *"Guiding Principles for Stabilization and Reconstruction". USIP (2009). Washington. ISBN 978-1-60127-033-7. Section 2 The Strategic Framework for Stabilization and Reconstruction, page 2-8*

7 Ibid, Section 6 Safe and Secure Environment, page 6-38

8 NSO. Allied Joint Publication AJP-3.4.5 *"Allied Joint Doctrine for the military contribution to stabilization and reconstruction", Edition A Version 1, December 2015, Chapter 1, Section 1, para 108*

9 NSO. Allied Joint Publication AJP-1(e) *"Allied Joint Doctrine", Edition E Version 1, February 2017. Type of operations, 2.45 Crisis response, Military contribution to stabilization and reconstruction. Type of operations, page 2-22*

10 NSO. Allied Joint Publication AJP-3 *"Allied Joint Doctrine for the conduct of operations", Edition C Version 1, February 2019. Section 5 – Types of operations, Military contribution to stabilization and reconstruction, page 1-31*

11 NSO. Allied Joint Publication AJP-3.22 *"Allied Joint Doctrine for stability policing", Edition A Version 1, July 2016, Part II - TERMS AND DEFINITIONS, LEX-2*

upholding of the public order and security, rule of law, and the protection of human rights." SP focuses on the needs of the civil populace through supporting and, when necessary, temporary replacing of the local police forces when the latter are either unable or unwilling to perform the function themselves. It is performed in unstable areas/fragile States where NATO is engaged, throughout the spectrum of conflict, ranging from peace to high-intensity conflict. However, it is conceptually framed within the stabilization and reconstruction of post-conflict processes.

3. MILITARY POLICE AND STABILITY POLICING

According to AJP-3.21[12], MP (Military Police) forces are defined as *"designated military forces with the responsibility and authorization for the enforcement of the law and maintaining order, as well as the provision of operational assistance through assigned doctrinal functions. MP provide operational assistance through five doctrinal functions."* These functions are:

1. Mobility support: MP facilitates and allows freedom of movement of military forces throughout the area of operations. It contributes to movement control activities through the control and regulation of military traffic during planned movement operations. It also assists with the security of basic military route networks, supporting the movement and coordination, among others, of stragglers, dislocated civilians, internally displaced people, and refugees, to ensure the routes remain clear for military traffic.
2. Security: MP can contribute to the protection of the force through the establishment and maintenance of a safe and secure environment within which to operate. This function includes activities such as area, physical and personal security, crowd and riot control, convoy escort, close protection, and information security.
3. Detention: MP must be prepared to capture, detain, retain, or hold individuals for a wide variety of reasons. This may include members of their military, a foreign or adversary force, civilians, or other people for specified operational reasons.
4. Police: MP forces must be responsible for the enforcement of discipline and the conduct of investigations, especially for the alleged commission of military crimes.
5. SP: defined before.

MP can be intended as both a set of functions (mobility support, security, detention, police and stability policing) and as the organization/personnel that carry them out. This practical usage of the term MP typically causes confusion over the actual terms of discussion concerning the relationship between the latter and SP.

In terms of functions, MP and SP are different military functions. This diversity is conceptual and it is based on their relevant aims and "target audience". While MP

12 NSO. Allied Joint Publication AJP-3.21 *"Allied Joint Doctrine for military police", Edition A Version 1, February 2019. CHAPTER 1, INTRODUCTION, Military Police Definition, page 1-2*

focuses on marshalling the troops, ensuring discipline, providing combat support[13][14] and conducting enabling tactical activities[15], SP focuses on providing a police service to the local population and building up the national ordinary police (it is irrelevant whether the national police possess military or civilian status) capacity and capabilities.

SP is an operational set of activities different from combat (nor is it a combat-light function), contributing to the military effort of stabilization and reconstruction of the Host Nation.

The aim of SP is to establish a SASE, restore public order and security, and contribute to the creation of the conditions for effective governance. Throughout the spectrum of conflict, the initial goal of SP is to re-establish and maintain sufficient security for the local populace; afterwards, to re-establish law and order, enforce the law and, eventually, reinforce the local security institutions. SP engages an adversary, which is not a conventional enemy, through tailored-to-the-need procedures, equipment, and forces, in order to contribute to the achieving of the mission objectives and the planned end-state. Even though SP focuses on civilians and ordinary police, it is not a civil function: it is a military function performed by the deployed military Force. Taking as a basis the NATO agreed term for SP, described above, a possible way to explain the actual essence of SP is an ordinary policing military function.

In terms of organizations/personnel, while the MP function can only be performed by the MPs (therefore it is an exclusive function), SP can be performed by a wide array of assets, despite the contrary criteria maintained by various NATO state members that will be explained in section 6 of this document, including the MP forces, based on the complexity of the tasks and on the required level of police skills as well as the police abilities and expertise owned by the potential "SP enforcers" (therefore it is an inclusive function). The more tasks are typically associated with ordinary police, the more ordinary police skills come to play.

That said, it becomes clear why we must be careful not to mix up functions and organizations when talking about MP and its relationship with SP.

The doctrinally assigned 5ft function SP to the overall function MP is, in fact, the contribution of the MP organizations/personnel (better to say MPs to mark the difference from MP as a function) to the broader SP function. In other terms, SP is a function for the MPs, not an exclusive function of the latter. The wider function SP embraces the 5th function for the MP; the first can be performed by GTFs (Gendarmerie-Type Force) (GTF) / PFMSs (Police Force with Military Status), MP forces and conventional military forces. SP can be performed by a multipurpose asset as part of the assigned tasks or by a dedicated specialized asset, called SPU (Stability Policing Unit).

There is some misconception about SP as an exclusive MPs function based on a misinterpretation of AJP-3.21 as the doctrine setting the framework for the overall SP function, while the reference doctrine for SP is AJP-3.22. As a matter of fact, AJP-3.21 regulates the MPs contribution to the wider SP function, not the wider SP function itself.

13 NSO. Allied Joint Publication AJP-3.2 *"Allied Joint Publication for land operations", Edition A Version 1, March 2016, paragraph 0167*

14 NSO. Allied Tactical Publication ATP-3.2.1 *"Allied Land Tactics", November 2009, paragraph 3006*

15 bid 13, paragraph 0167

Marking the conceptual point about SP as a function for the MPs and not of the MPs is one of the utmost importance for several practical reasons. One prominent practical reason is that not all GTFs / PFMUs can perform MP tasks (or other military tasks), in accordance with their national laws/regulations: for the latter, SP may be the only possibility to contribute to military operations. Insisting on considering SP as an exclusive function of the MPs may exclude some GTFs / PFMSs from NATO Operations, thus resulting in a waste of capabilities and skills.

4. NATO STABILITY POLICING CONCEPT

According to AJP-3.22, the NATO Strategic Concept, *"describes the requirement for the Allies to develop the capability to train and develop local forces (police forces included) in crisis zones, so that local authorities are able, as quickly as possible, to maintain security without international assistance[16]".* This requirement demands the need to substitute and, if necessary, support local police forces, *"as part of NATO's contribution to a comprehensive approach, has been underscored in recent operations in Kosovo, Iraq, and Afghanistan[17]".* In this regard, *"while the Military Committee (MC) has undertaken effort to develop a Security Force Assistance concept (SFA Concept) to address the need to train and develop indigenous military security forces, the need to address local police forces remains unfilled[18]".* That is why the necessity to adopt a SP Concept is in the collective interest of the Alliance.

The rationales described above require to be conceptualized, and a SP capability needs to be established: the mere fact that it needs to be explained highlights the gap that calls for being filled. *"NATO lacks a precisely defined SP capability that is properly acknowledged within the NATO Defence Planning Process (NDPP) and targeted to Nations. This means that during a force generation process Nations can provide SP contributions that lack police expertise and experience, likely resulting in disastrous consequences: this is why adopting an SP concept is the opportunity for the Alliance to fill this gap[19]".*

A formal SP capability is needed in an effort to formally bring this police expertise within NATO, and to develop a reference capability requirement to support the creation of a minimum capability requirement for NATO Operations. Doctrine is not sufficient for this purpose.

This does not entail the establishment of new units or enlarging the NCS (NATO Command Structure[20]); it just means that there is a need to establish a SP capability package that can be plugged into the force, when required. Some nations may

16 NSO. Allied Joint Publication AJP-3.22 *"Allied Joint Doctrine for stability policing", Edition A Version 1, July 2016, PREFACE, paragraph 2, page VII*

17 Idem

18 Idem

19 De Magistris, Guiseppe., Bergonzini, Stefano. (2020), Gendarmerie in international environment, "*STABILITY POLICING: A GOLDEN OPPORTUNITY FOR NATO".* Romanian Gendarmerie, June 2020, page 26, https://www.nspcoe.org/wp-content/uploads/2020/11/Stability-Policing-a-golden-opportunity-for-NATO.pdf

20 *"The NATO Command Structure", NATO. Factsheet, February 2018,* https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_02/1802-Factsheet-NATO-Command-Structure_en.pdf : *"NATO's Command Structure (NCS) is the backbone of NATO. It is composed of permanent multinational headquarters at the strategic, operational and component levels of command, distributed geographically and commonly funded".*

contribute with their GTFs / PFMSs, others with their MPs or properly trained and equipped conventional forces; some other would not contribute as they may lack the required capabilities: no additional costs will be borne by NATO, nor by Nations other than those the latter want to bear on voluntary basis.

Adopting the SP Concept is also in the interest of GTFs / PFMSs and MPs themselves so they can plan and develop their capabilities supported by a clear conceptual framework. It is not about bearing more expenses, it is about improving and using the capabilities that are already in place.

In addition, nothing in the Concept calls for the establishment of a SP Advisor within the NCS. However, it is pivotal to establish a network of SP SMEs (Subject Matter Experts) throughout the staffs, at least at a strategic and operational level, but also at a LC (Land Component) level, to professionally manage SP during the planning and execution of Operations and exercises, as well as in the doctrine and lessons learned cycles. SP SMEs positions may be double-hatted and covered by GTFs / PFMSs, MPs, and conventional military forces personnel: it is not important who manages SP, but rather that it is managed in a professional manner.

5. STABILITY POLICING UNIT (SPU)

As described in the previous section, SP may be conducted by a wide range of military forces. Since it requires a civil-oriented mindset and a specialist approach to meet the needs and expectations of the civil population in order to succeed, the best suitable forces are the GTFs / PFMSs. In fact, SP is a function also for the MP, together with its traditional four functions. Nevertheless, when the MP are called to perform SP duties, they are not conceptually performing MP activities, but civil police activities.

SPUs are specialized units with specialized policing skills[21] generated for the specific purpose of conducting SP. Major international organizations, such as NATO, EU and UN, have set up varying types of Stability Police Units (SPUs), namely MSU[22] (Multinational Specialized Unit), IPU[23] (Integrated Police Unit) and FPU[24] (Formed Police Unit).

NATO created the MSU to cover the need for the Alliance to be endowed with a military capability of civil police SFOR operation in Bosnia and Herzegovina in 1997[25].

21 NSO. Allied Joint Publication AJP-3 *"Allied Joint Doctrine for the conduct of operations", Edition C, Version 1, February 2019, Chapter 1, Section 5, para 1.66d*

22 NSO. Allied Tactical Publication ATP-3.2.1.1 *"Guidance for the conduct of tactical stability activities and tasks", Edition B Version 1, March 2014, PREFACE, paragraph 194, page 1-38: "A MSU is a military asset with specific capabilities at the operational level designed to guarantee a safe and secure environment through a Combat Bridging (CB) function. Combat Bridging is an enabling function utilizing Tactics Techniques and Procedures focused on the security requirements of an environment transitioning from the combat phase to the Stabilisation and Reconstruction phases. The MSU provides the Commander with a specialized asset ideally suited to bridge the gap between high intensity combat and stabilisation until the local Police and other institutions are capable of assuming these duties".*

23 EU. Concept for rapid deployment of police elements in an EU-led substitution mission. Council of the European Union. 8508/2/05 REV 2 RESTREINT UE/EU RESTRICTED, 31 May 2005, 1.3.1. INTEGRATED POLICE UNIT (IPU), page 4

24 *"FORMED POLICE UNITS (FPUS)", United Nations Police,* https://police.un.org/en/formed-police-units-fpus , consulted 6th June 2021

25 *"About NATO Stability Policing", NATO Stability Policing Center,* https://www.nspcoe.org/about-us/about-stability-policing/ , consulted 6th June 2021

Ever since then, some more experience was gained, and NATO currently considers that *"stability policing forces must be robust, flexible, interoperable, and rapidly deployable and provided with adequate logistic capacity. This means that Stability Policing Units (whose structure will be defined in a future tactical publication) will be most suitable to be deployed in these circumstances*[26]*"*.

GTFs / PFMSs are military forces that possess a unique set of ordinary police skills and expertise since they perform ordinary police tasks in their home countries daily as their core business, in addition to their military tasks. For this uniqueness, which represents their center of gravity, GTFs / PFMSs are the logical first choice to run and staff a SPU[27], but not the only solution: this is also aligned with real NATO Operations (SFOR, KFOR) and Coalition Operations (Iraq) where the MSU[28] have been staffed mainly by GTFs / PFMSs, integrated, little by little, by MPs and conventional military forces.

Therefore, a SPU can hypothetically be staffed by GTFs / PFMSs, MPs, a combination of the two, and integrated by conventional forces, bearing in mind that a SPU is not a civil police asset, but a military asset performing ordinary police tasks in the area of operations.

Regarding the command and control on SP activities, a distinction must be made between the following situations:

1. Absence of a deployed SPU

   When no dedicated SPU of whatever size is deployed, it is reasonable to consider using the MPs to perform SP activities, as MP assets are always embedded in the deployed Force and they represent the most suitable available asset. The Provost Marshal would advise the Force Commander in this regard and, if double-hatted as the MP Commander, he would also command and control the activities.

   Presence of a deployed SPU

   When a dedicated SPU of whatever size is deployed, a general or specific need for SP is acknowledged by the Alliance. In this case, SP is led and chiefly performed by the SPU without excluding the possibility for other actors to conduct SP activities as well, depending on mission mandate. The SPU Commander would be subordinated to the Force Commander and would advise the latter on SP matters. The SPU Commander and the Provost Marshal would coordinate for cross-cutting issues and would keep reciprocally informed.

6. HOW IS STABILITY POLICING IMPLEMENTED IN NATO COUNTRIES?

Based on whether or not the SP is exclusively considered as an MP function, there are two large groups of member states whose characteristics are detailed below.

26 NSO. Allied Joint Publication AJP-3.22 "Allied Joint Doctrine for stability policing", Edition A Version 1, July 2016, paragraph 0225, page 2-9

27 Idem 9, para. 2.6.3

28 NSO. Allied Joint Publication AJP-3.4.1 *"Allied Joint Doctrine for the military contribution to peace support", Edition A, Version 1, December 2014, NATO Standardization Office, paragraph 0441, page 4-19*

6.1. SP AS A NON-EXCLUSIVE MP FUNCTION

This position is mainly defended by Italy and France, which have GTF / PFMS (Italian Carabinieri[29] and French Gendarmerie[30]) capable of developing, in addition to the MP functions, regular police public security functions in the benefit of the civilian population within the framework of their own territory, and whose armed forces also lack other specific military police different from the mentioned police Corps. In both cases, these corps are not considered MP forces.

AJP-3.22 is, for both countries, the only doctrinal reference for SP, while AJP-3.21 simply addresses the aspects related to the contribution of the MP to the SP. This stance is based on the next arguments:

- Some other NATO GTF / PFMS, such as the Romanian Gendarmerie[31], which have already participated in recent years in NATO operations carrying out SP activities with excellent results, can only develop, according to the Romanian national legal framework, this type of function lacking the status of MP[32]. These functions are developed by specific MP forces, that are part of the Romanian Armed Forces. Considering SP as an exclusive MP function would make it impossible to integrate Romanian Gendarmerie into NATO operations.
- The forces responsible for carrying out SP activities must possess the professional experience and necessary expertise in performing police functions in their respective member states, exercising their authority over civilian population. Only in this case can it be assured that SP forces have the technical capability necessary to correctly develop SP tasks and contribute to achieve the operation objectives. This condition is not usually met by a large part of the MPs, whose authority is generally limited to military personnel.

6.2. SP AS AN EXCLUSIVE MP FUNCTION

Broadly speaking, the group of countries in favor of this position includes those member states that do not have GTF / PFMS. Among them are the Nordic countries, such as Sweden[33] and Denmark[34], as well as USA[35], Germany[36] and the

29 ITALY. LEGGE 31 marzo 2000, n. 78. Delega al Governo in materia di riordino dell'Arma dei carabinieri, del Corpo forestale dello Stato, del Corpo della Guardia di finanza e della Polizia di Stato. Norme in materia di coordinamento delle Forze di polizia. GAZZETTA UFFICIALE DELLA REPUBBLICA ITALIANA n.º 79, 4 de abril de 2000, articule 1, paragraph 2

30 FRANCE. LOI n° 2009-971 du 3 août 2009 relative à la gendarmerie nationale. Journal officiel de la République française n°0180 du 6 août 2009, art 1, 3º

31 ROMANIA. LEGE nr. 550 din 29 noiembrie 2004, privind organizarea și funcționarea Jandarmeriei Române. Publicat în MONITORUL OFICIAL nr. 1175 din 13 decembrie 2004, art 1 (1)

32 ROMANIA. LEGEA nr. 346 din 21 iulie 2006, privind organizarea și funcționarea Ministerului Apărării Naționale. Publicat în MONITORUL OFICIAL nr. 867 din 2 noiembrie 2017, art 5 (36)

33 *"FÖRSVARSMAKTENS MILITÄRPOLISENHET",* FÖRSVARSMAKTEN, https://www.forsvarsmakten.se/sv/organisation/livgardet/forsvarsmaktensmilitarpolisenhet, consulted 3rd JUN 21

34 *"Hærens Militærpoliti"* Militærpolitisektionen, Hærens Logistikskole, Aalborg Kaserne. Norrensundby, Denmark. http://www.militarypolice.dk/hls/HRN_MP_2003.pdf, III. MILITÆRPOLITI OPERATIONER

35 USA. FM 3-39 "MILITARY POLICE OPERATIONS", Headquarters, Department of the Army, Washington, DC, April 2019 https://fas.org/irp/doddir/army/fm3_39.pdf, ANNEX A

36 *"German Military Police", NATO MILITARY POLICE CENTRE OF EXCELLENCE,* https://mpcoe.org/GERMANY, consulted 22nd October 2020

United Kingdom[37], whose MP forces are legally authorized to carry out most of the functions and activities included in AJP-3.21, according to their national legal framework. Among them are the police investigation of certain crimes with similar powers to those assigned to the civilian police forces. Because of this, these member states do not accept that the SP can be separated from MP and merge as a new discipline for NATO.

7. STABILITY POLICING IN SPANISH ARMED FORCES

7.1. MP TAKS ACCORDING TO SPANISH REGULATION

According to the content of the SAF (Spanish Armed Forces) Security Decree[38] the military, naval or air police units (all of them considered as MPs) are those equipped with adequate weapons and equipment, organized, and trained to fulfill the next tasks[39] in Spanish territory:

1. Carry out the surveillance, custody, escort and regulation of military convoys and transports, as well as the protection of members of the SAF.
2. Identify personnel and vehicles in military compounds.
3. Ensure order, discipline, and uniformity of the military personnel.
4. Control the traffic within the military compound. Outside the military compounds, MPs may perform this activity in the absence of traffic police officers or with their support, always after having obtained authorization from the civilian traffic authorities.
5. Guard and safekeep prisoners and detainees in military penal prisons and establishments, as well as carry out security and order maintenance inside these establishments.
6. Assist military prosecutors and judges when required.
7. Make reports for the benefit of the security in their specific scope of action.

In addition to the described tasks, the SAF Security Decree enables MP to also perform the two following tasks:

1. Security services in military compounds[40].
2. Support to security forces, at their request, exclusively performing their proper functions and within the limits of their powers.

Outside the Spanish territory, MP is only allowed to develop the described tasks and always in accordance with the provisions of the corresponding international agreements.

37 *"Royal Military Police", The British Army,* https://www.army.mod.uk/who-we-are/corps-regiments-and-units/adjutant-generals-corps/provost/royal-military-police/, consulted 04th June 2021

38 SPAIN. Real Decreto 194/2010, de 26 de febrero, por el que se aprueban las Normas sobre seguridad en las Fuerzas Armadas. BOE núm. 64, de 15 de marzo de 2010, páginas 25324 a 25334, art 29

39 Ídem 11, art 30

40 Ídem 11, art 15

7.2. SPANISH MP ORIGIN AND NATURE

In addition to the MP forces (military, naval and air police units) composed by military personnel from to the SAF, but with different origin, Spanish Guardia Civil may also be part of the Spanish MP, in compliance with the military missions that can be entrusted to this corps, based on the military nature and police formation, as established in paragraph a).1º, article 3, of the Decree on military missions of Guardia Civil [41]. During these missions, the members of Guardia Civil will be subjected to compliance with the Penal Military[42] and Disciplinary[43] Laws and will depend on the SAF chain of command, in the same conditions of the rest of the contingent. In fact, and at any effects, Guardia Civil can be considered as part of the SAF contingent in similar conditions to the rest of their components, providing the force a technical capacity based on specific skills.

7.3. SPANISH MP REGULATION VS. NATO DOCTRINE

The development of the five doctrinal functions defined in the Allied Joint Doctrine (AJD) for the MP notably transcends the kind of tasks that can be carried out by Spanish MP in accordance with the provisions of Spanish regulations reflected above. In fact, there is a more than evident lack of correlation among the tasks assigned to the Spanish MP with those provided for the AJD. In short, the situation goes as follows:

- Some of the tasks included in the AJP correspond to those assigned by the Spanish legislation to the MP.
- On the other hand, some others do not correspond to them but can be carried out through the participation of other capacities of the SAF.
- Lastly, there is a third group of tasks for which the personnel of the SAF do not have the necessary legal authorization.

Regarding the normative value of the AJD, the Spanish Supreme Court ruled[44] that the NATO Standardization Agreements (STANAGS's) do not have any normative or legal value either in international law or in Spanish domestic law, since they are only procedures developed for the homologation or standardization of the actions and operations of the armed forces regarding the different member states of the Alliance. Consequently, AJP-3.21[45] and AJP-3.22[46] must be interpreted and applied in a way that does not cause conflict with Spanish law. This situation is valid both in Spanish territory and abroad, based on the criteria established by the Constitutional Court in its

41 SPAIN. Real Decreto 1438/2010, de 5 de noviembre, sobre misiones de carácter militar que pueden encomendarse a la Guardia Civil. Boletín Oficial del Estado núm. 269, de 06/11/2010, páginas 93269 a 93271.

42 SPAIN. Ley Orgánica 14/2015, de 14 de octubre, del Código Penal Militar. Boletín Oficial del Estado núm. 247, de 15/10/2015, páginas 95715 a 95746

43 SPAIN. Ley Orgánica 8/2014, de 4 de diciembre, de Régimen Disciplinario de las Fuerzas Armadas. Boletín Oficial del Estado núm. 294, de 5/12/2014, páginas 100151 a 100191

44 SPAIN. Tribunal Supremo (Sala de lo Militar, Sección 1ª). Sentencia núm. 5789/2008, de 3 de noviembre (ECLI:ES:TS:2008:5789), Fundamento de Derecho CUARTO, página 23

45 The agreement of nations to use this publication is recorded in STANAG 2296

46 The agreement of nations to use this publication is recorded in STANAG 2616

Declaration 1/1992[47], by which it is established that *"Spanish public powers are no less subject to the Constitution when they act in international or supranational relations than when exercising ad intra their attributions."* This statement declares that the mandatory subjection of Spanish public powers in general, and among them the SAF in particular, to abide by the provisions of the Spanish constitutional framework, even when they perform their services abroad[48].

For all these reasons, the Commander of the SAF has stablished in its Resolution[49] the implementation of the AJD of MP the following reservation: *"Spain agrees with the general aspects and tasks to be carried out by MP units set out in AJP-3.2.3.3 (currently AJP-3.21). However, in accordance with paragraph 0002 of the prologue, Spain will determine, case by case, the tasks that the MP units contributed may or may not carry out depending on their different origin and nature".*

By means of this reservation, it is indirectly recognized that although the SAF can cover all five doctrinal functions included in the AJD for MP, not all of them can be carried out by the MP units composed by SAF military personnel. The position adopted by Spain in this regard advocates for the consideration of MP from a functional point of view: some functions can be covered by the referred MP Units, but others cannot and must be assigned to other kind of units or resources.

Specifically, after having analyzed the AJD of MP, it can be concluded that Spanish MP units (composed by SAF military personnel) are limited to perform only the next activities in relation with the first four MP functions:

1. Mobility support: activities related to civilian traffic control are limited to the absence or the support of the traffic civilian police. Besides that, MPs can exclusively make reports when an accident involving military vehicles occurs, but these reports are not for legal use due to the lack of authorization of MPs to investigate possible criminal responsibilities of military personnel, neither administrative responsibility of civilians in case. This needs to be investigated by traffic police.

2. Security: Spanish MP's are not allowed to do many of the activities required to Close Protections Teams (CPT) outside military compounds. Among them belong the identification of civilians or the delimitation of a secured area around the people escorted, reserved to the security forces. These restrictions generate huge limitations in MP CPT services. By contrast, they can be responsible for the security of the military bases.

3. Arrests: in peacetime Spanish MP's are only allowed to practice arrests in case they witness flagrant crimes, in the same conditions for any other people. Arrests in other cases are reserved to judicial police, always after

47 SPAIN. Tribunal Constitucional (Pleno). Declaración de 1 de julio de 1992. Requerimiento 1236/1992 del Gobierno de la Nación en relación con la existencia o inexistencia de contradicción entre el art. 13.2 de la C.E. y el art. 8 B, apartado 1 del Tratado Constitutivo de la Comunidad Económica Europea, en la redacción que resultaría del art. G B, 10, del Tratado de la Unión Europea. Boletín Oficial del Estado núm. 177, de 24/07/1992, Fundamento Jurídico 4, página 6

48 Liñán Nogueras, Diego J., Roldán Barbero, Javier. (2008), EL ESTATUTO JURÍDICO DE LAS FAS EN EL EXTERIOR. Madrid: Ed. Plaza y Valdés, página 309

49 SPAIN. Resolución 200/14804/13 del JEMAD por la que se implanta el Acuerdo de Normalización OTAN STANAG 2296 "Doctrina conjunta aliada de Policía Militar–AJP-3.2.3.3". Boletín Oficial de Defensa núm. 212, de 29/10/2013, página 25054

their investigations. This changes in wartime, when the arrests of war prisoners are foreseen by military personnel, and especially Special Operations Forces (SOF) members.

4. Police: Spanish MP forces are responsible for the enforcement of discipline, but they are not allowed to conduct investigations for the alleged commission of any kind of crime. According to Spanish Law, activities developed during criminal investigations are strictly reserved to judicial police. The generic functions of the judicial police are determined in the article 126 of the Spanish Constitution[50]: *"the judicial police depends on the Judges, the Courts and the Public Prosecutor's Office in their functions of investigating the crime and discovering and detaining the offender, in the terms established by law."* Derived from the constitutional mandate, the Judicial Power Law[51] establishes in the same terms in its article 547 that *"the function of the Judicial Police includes assisting the courts and tribunals and the Public Prosecutor's Office in the investigation of crimes and in the discovery and detaining of offenders. This function will be the responsibility, when required, to all members of the Security Forces and Corps, whether they depend on the central government, the autonomous communities or local entities, within the scope of their respective competencies".*

7.4. THE SPANISH JUDICIAL POLICE

The specific activities reserved to Spanish judicial police are described in different articles of the Criminal Process Law. Among others, they are the following ones:

- Arrest of alleged criminals when it can be inferred as a result of their investigations that they have committed a crime.
- Entry and registration at addresses without authorization of their residents.
- Control, checking and access to postal and telegraphic mails.
- Interception and access to phone conversations and electronic communications.
- Conversation, sound and image recording by means of electronic devices.
- Remote access to mass storage of information.
- Remote access to computer equipment.

The limitation of fundamental rights recognized in the Spanish Law required by the judicial police for the practice of investigations demands, with mandatory character, an express regulation carried out by means of a Norm with the character of Organic Law, enabling specific corps, agencies or public services to perform these sensitive activities in accordance with the provisions of article 81.1 of the Spanish Constitution: *"Organic laws are those relating to the development of fundamental rights and public liberties."*

50 SPAIN. Constitución Española, de 29 de diciembre de 1978. Boletín Oficial del Estado núm. 311, de 29/12/1978, páginas 29313 a 29424

51 SPAIN. Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial. Boletín Oficial del Estado núm. 157, de 02/07/1985, páginas 20632 a 20678

Article 283, of the Criminal Process Law[52] (an Organic Law), defines the corps, agents or public employees authorized to carry out judicial police functions. Spanish Guardia Civil members are specifically included in the list. However, the members of SAF are not included in it. Taking this into account, it is not possible to attribute the character of judicial police to the members of the SAF based on the following:

- They are not included in the article 283 of the Criminal Process Law.
- There is also no other legal statement with normative rank of Organic Law in which this character is expressly assigned to them.

After this reasoning, it is necessary to think about the scope of the specific activities that the Spanish MP's can carry out to aid the organs and prosecutors of the military jurisdiction and try to define them. The answer to this question is found in the article 81 of the Military Jurisdiction Authority and Organization Law[53], in which it is defined the general limits to which the work of auxiliary personnel extends: *"in all military judicial courts there will be the necessary auxiliary personnel who, under the direction of the corresponding Secretary, will carry out the work entrusted to them in relation to the dispatch and processing of the procedures that are followed."* Therefore, it can be possible to identify the tasks included within the term assistance as those related to the administrative processing of the procedures. Those activities are far different from those reserved to judicial police in the framework of the criminal investigation, also defined in art 82 of the referred Law, which consist of investigating the crimes, discovering, and detaining the offenders. All this respecting the military judicial courts and the military judicial prosecutors.

7.5. SPANISH SP IMPLEMENTATION

In the same way the Commander of the SAF has ruled in its Resolution[54] to implant the JAD for the SP that *"Spain agrees with the SP general aspects and tasks to be carried out by MP Units set out in that publication. However, Spain will determine case by case the activities and tasks that the MP Units may or may not carry out depending on their different origin."*

Regarding this aspect, it does not appear that SP activities are included, in any case, among the tasks assigned to the Spanish MP in the SAF Security Decree 194/2010. Moreover, considering the nature of SP tasks oriented to reforming, training, advising and assisting the local security forces, including the complete substitution of them in order to provide the necessary public security services, it would be more than convenient, due to the complexity that this entails, to deploy police officers experienced in carrying out of these kind of tasks on a daily basis. That is, specialists in maintaining citizen security endowed with extensive professional expertise, in addition to the specific training and equipment required in this area.

52 SPAIN. Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal. Boletín Oficial del Estado núm. 260, de 17 de septiembre de 1882

53 SPAIN. Ley Orgánica 4/1987, de 15 de julio, de la Competencia y Organización de la Jurisdicción Militar. Boletín Oficial del Estado núm. 171, de 18/07/1987, páginas 22065 a 22079

54 SPAIN. Resolución 200/17595/17 del JEMAD por la que se implanta el Acuerdo de Normalización OTAN STANAG 2616 "Doctrina conjunta aliada para policía de estabilización – AJP-3.22, Edición A". Boletín Oficial de Defensa núm. 239, de 12/12/2017, página 29493

The Spanish MP is not a member of the Spanish security forces, defined in the Spanish Security Forces Law[55], in which, on the other hand, Guardia Civil plays a relevant role. Therefore, it goes without saying that according to Spanish Law, it is not possible to assign MP forces to those missions related to the maintenance of the public security. Besides that, Spanish Criminal Process Law MP's are not allowed to carry out criminal investigations and activities exclusively reserved for the judicial police.

This situation differs from that existing in those Allied state members, such as the US, the UK, Germany, or the Nordic countries, where MP forces may perform certain criminal investigations, although mainly related to military crimes, or those other countries that lack specific MP forces, such as Italy or France.

That is why the Spanish approach to SP operations is described in the mentioned Resolution of the Commander of the SAF, by which the NATO STANAG 2616 is implemented, that establishes a model based on the assignment of SP tasks to the MP Forces, based on their nature and origin, due to the two different existing provenances: SAF or Guardia Civil. In other words, it recognizes that those MP forces composed exclusively by members of the SAF will not be the most suitable to carry out those SP tasks, which require the technical police specialization they lack and for which they are not legally authorized in Spain. These tasks should be assigned to MP forces composed by members of Guardia Civil.

As a guide, these tasks are related to training the local security forces in the practice of procedures reserved for the judicial police, that is, in actions related to the criminal investigations. It is not appropriate for the SAF personnel to oversee training local police corps in aspects related to the planning and execution of the service and, in general, of specific police techniques. SAF personnel are also not the most suitable to substitute local security forces in public security missions.

On the other hand, they are perfectly prepared for training local forces in transversal matters characterized by their generic nature, which can be shared between armed forces and security forces, especially in those environments where the degree of insecurity is very high, such as basic security techniques, movement of personnel, vehicles and convoys, use of firearms, signals, human resources management, logistics, budged and financial management or computers use and networks, among many others.

8. CONCLUSIONS

In conclusion, the arguments presented highlight the need for the integration, in the Allied contingents, of experts in maintaining law and order with professional experience in carrying out their police duties daily. Mentoring, training, advising and reconstructing local security forces cannot be assigned to personnel without prior professional experience in the field. The lack of professional expertise could be one of the causes that explain the negative results of the last allied operations.

To try to solve this problem, GTFs / PFMSs are the best suitable resources due to the professional background of their members acquired in the daily work as public

55 SPAIN. Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad. Boletín Oficial del Estado núm. 63, de 14/03/1986, páginas 9604 a 9616, artículo 2

security agencies in their own countries. For those allied countries that lack of GTFs / PFMSs, such as the US, it should be crucial to try to find the best solution in order to provide an adequate response to the operational demands. In this regard, it does not seem appropriate assigning SP responsibilities to MP forces without previous experience in this field.

In the case of the SAF, the most suitable option is to take advantage of the capabilities of Spanish Guardia Civil, a PFMS with exceptional police skills, that can be completely integrated in the SAF contingents and their chain of Command, reinforcing the support of this Corps to the Spanish National Defense, since it has the necessary expertise to carry out police tasks on benefit of the civilian population, as showed in previous NATO operations. Consequently, SAF must be aware of the qualitative advantage of having such a valuable resource as a means to consolidate their position as a relevant actor in the framework of NATO operations.

BIBLIOGRAPHY

"Guiding Principles for Stabilization and Reconstruction". USIP (2009). Washington. ISBN 978-1-60127-033-7.

SIGAR. *"Stabilization: Lessons from the U.S. Experience in Afghanistan"*, May 2018 https://www.sigar.mil/pdf/lessonslearned/SIGAR-18-48-LL.pdf, consulted 28th Feb 21.

USIP. *"Guiding Principles for Stabilization and Reconstruction: Safe and Secure Environment"*, https://www.usip.org/guiding-principles-stabilization-and-reconstruction-the-web-version/safe-and-secure-environment, consulted 9th Feb 21.

De Magistris, Guiseppe., Bergonzini, Stefano. (2020), Gendarmerie in international environment, *"STABILITY POLICING: A GOLDEN OPPORTUNITY FOR NATO".* Romanian Gendarmerie, June 2020.

"The NATO Command Structure", NATO. Factsheet, February 2018, https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_02/1802-Factsheet-NATO-Command-Structure_en.pdf

EU. *"Concept for rapid deployment of police elements in an EU-led substitution mission".* Council of the European Union. 8508/2/05 REV 2 RESTREINT UE/EU RESTRICTED, 31 May 2005.

"FORMED POLICE UNITS (FPUS)", United Nations Police, https://police.un.org/en/formed-police-units-fpus

"About NATO Stability Policing", NATO Stability Policing Center, https://www.nspcoe.org/about-us/about-stability-policing/

"FÖRSVARSMAKTENS MILITÄRPOLISENHET", FÖRSVARSMAKTEN, https://www.forsvarsmakten.se/sv/organisation/livgardet/forsvarsmaktensmilitarpolisenhet

"Hærens Militærpoliti" Militærpolitisektionen, Hærens Logistikskole, Aalborg Kaserne. Norrensundby, Denmark. http://www.militarypolice.dk/hls/HRN_MP_2003.pdf

USA. FM 3-39 *"MILITARY POLICE OPERATIONS",* Headquarters, Department of the Army, Washington, DC, April 2019 https://fas.org/irp/doddir/army/fm3_39.pdf

"German Military Police", NATO MILITARY POLICE CENTRE OF EXCELLENCE, https://mpcoe.org/GERMANY

"Royal Military Police", The British Army, https://www.army.mod.uk/who-we-are/corps-regiments-and-units/adjutant-generals-corps/provost/royal-military-police/

Liñán Nogueras, Diego J., Roldán Barbero, Javier. (2008), *EL ESTATUTO JURÍDICO DE LAS FAS EN EL EXTERIOR*. Madrid: Ed. Plaza y Valdés.

SPAIN. Tribunal Supremo (Sala de lo Militar, Sección 1ª). Sentencia núm. 5789/2008, de 3 de noviembre (ECLI: ES:TS:2008:5789).

SPAIN. Tribunal Constitucional (Pleno). Declaración del 1 de julio de 1992. Requerimiento 1236/1992 del Gobierno de la Nación en relación con la existencia o inexistencia de contradicción entre el art. 13.2 de la C.E. y el art. 8 B, apartado 1 del Tratado Constitutivo de la Comunidad Económica Europea, en la redacción que resultaría del art. G B, 10, del Tratado de la Unión Europea. Boletín Oficial del Estado núm. 177, de 24/07/1992, páginas 2 a 7.

NATO STANDARDS

NSO. Allied Joint Publication AJP-1(e) "Allied Joint Doctrine", Edition E Version 1, February 2017.

NSO. Allied Joint Publication AJP-3 "Allied Joint Doctrine for the conduct of operations", Edition C Version 1, February 2019.

NSO. Allied Joint Publication AJP-3.2 "Allied Joint Publication for land operations", Edition A Version 1, March 2016.

NSO. Allied Tactical Publication ATP-3.2.1 "Allied Land Tactics", November 2009.

NSO. Allied Joint Publication AJP-3.21 "Allied Joint Doctrine for military police", Edition A Version 1, February 2019.

NSO. Allied Joint Publication AJP-3.22 "Allied Joint Doctrine for stability policing", Edition A Version 1, July 2016.

NSO. Allied Joint Publication AJP-3.4.1 "Allied Joint Doctrine for the military contribution to peace support", Edition A, Version 1, December 2014, NATO Standardization Office.

NSO (NATO Standardization Office). Allied Joint Publication AJP-3.4.5 "Allied Joint Doctrine for the military contribution to stabilization and reconstruction", Edition A Version 1, December 2015.

SPANISH LEGAL REFERENCES

SPAIN. Constitución Española, de 29 de diciembre de 1978. Boletín Oficial del Estado núm. 311, de 29/12/1978.

SPAIN. Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial. Boletín Oficial del Estado núm. 157, de 02/07/1985.

SPAIN. Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad. Boletín Oficial del Estado núm. 63, de 14/03/1986.

SPAIN. Ley Orgánica 4/1987, de 15 de julio, de la Competencia y Organización de la Jurisdicción Militar. Boletín Oficial del Estado núm. 171, de 18/07/1987.

SPAIN. Ley Orgánica 8/2014, de 4 de diciembre, de Régimen Disciplinario de las Fuerzas Armadas. Boletín Oficial del Estado núm. 294, de 5/12/2014.

SPAIN. Ley Orgánica 14/2015, de 14 de octubre, del Código Penal Militar. Boletín Oficial del Estado núm. 247, de 15/10/2015.

SPAIN. Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal. Boletín Oficial del Estado núm. 260, de 17/09/1882.

SPAIN. Real Decreto 194/2010, de 26 de febrero, por el que se aprueban las Normas sobre seguridad en las Fuerzas Armadas. BOE núm. 64, de 15/03/2010.

SPAIN. Real Decreto 1438/2010, de 5 de noviembre, sobre misiones de carácter militar que pueden encomendarse a la Guardia Civil. Boletín Oficial del Estado núm. 269, de 06/11/2010.

SPAIN. Resolución 200/14804/13 del JEMAD por la que se implanta el Acuerdo de Normalización OTAN STANAG 2296 “Doctrina conjunta aliada de Policía Militar–AJP-3.2.3.3”. Boletín Oficial de Defensa núm. 212, de 29/10/2013.

SPAIN. Resolución 200/17595/17 del JEMAD por la que se implanta el Acuerdo de Normalización OTAN STANAG 2616 “Doctrina conjunta aliada para policía de estabilización – AJP-3.22, Edición A”. Boletín Oficial de Defensa núm. 239, de 12/12/2017.

LEGAL REFERENCES FROM OTHER COUNTRIES

Italy. LEGGE 31 marzo 2000, n. 78. Delega al Governo in materia di riordino dell’Arma dei carabinieri, del Corpo forestale dello Stato, del Corpo della Guardia di finanza e della Polizia di Stato. Norme in materia di coordinamento delle Forze di polizia. GAZZETTA UFFICIALE DELLA REPUBBLICA ITALIANA n.º 79, 4 de abril de 2000.

FRANCE. LOI n° 2009-971 du 3 août 2009 relative à la gendarmerie nationale. Journal officiel de la République française n°0180 du 6 août 2009.

ROMANIA. LEGE nr. 550 din 29 noiembrie 2004, privind organizarea și funcționarea Jandarmeriei Române. Publicat în MONITORUL OFICIAL nr. 1175 din 13 decembrie 2004, art 1 (1).

ROMANIA. LEGEA nr. 346 din 21 iulie 2006, privind organizarea și funcționarea Ministerului Apărării Naționale. Publicat în MONITORUL OFICIAL nr. 867 din 2 noiembrie 2017, art 5 (36).

LA INVESTIGACIÓN A TRAVÉS DE DEEP WEB Y DARK WEB: UN ESTUDIO EXPLORATORIO EMPÍRICO

CARMEN SÁNCHEZ PÉREZ

CONSULTORA DE CIBERSEGURIDAD Y COLABORADORA DE LA UNIVERSIDAD CAMILO JOSÉ CELA

CARMEN JORDÁ SANZ

PROFESORA DEL DEPARTAMENTO DE CRIMINOLOGÍA Y SEGURIDAD DE LA UNIVERSIDAD CAMILO JOSÉ CELA

Fecha de recepción: 12/03/2021. Fecha de aceptación: 04/06/2021

RESUMEN

Sin duda, internet ha transformado nuestras rutinas digitalizando conductas, incluidas las constitutivas de delitos. Pero existen espacios específicos que ofrecen ventajas especiales para la comisión de delitos, tal es el caso de la Deep Web y la Dark Web. Este escenario especialmente anonimizado supone un auténtico reto global en términos de persecución policial. Este estudio exploratorio pretende identificar las características principales de las investigaciones policiales de los delitos cometidos en la Deep Web y la Dark Web a partir del estudio de sentencias españolas (n=44): conocer cómo son los delitos a los que se enfrentan nuestras FCSE, cuál es el resultado de la investigación y qué elementos procesales son clave en la persecución de estos delitos son los principales objetivos del presente análisis.

Palabras clave: Deep Web, Dark Web, ciberdelitos, sentencias judiciales.

ABSTRACT

The internet has undoubtedly transformed our routines by digitising behaviour, including criminal behaviour. But there are specific spaces that offer advantages for the commission of crimes, such as the Deep Web and the Dark Web. This particularly anonymised scenario poses a real global challenge in terms of law enforcement. This exploratory study aims to identify the main characteristics of police investigations of crimes committed on the Deep Web and the Dark Web based on the study of Spanish judgments (n=44): what are the crimes faced by our police forces, what is the outcome of the investigation and what procedural elements are key in the prosecution of these crimes are the main goals of this analysis.

Keywords: Deep Web, Dark Web, cybercrimes, court sentences.

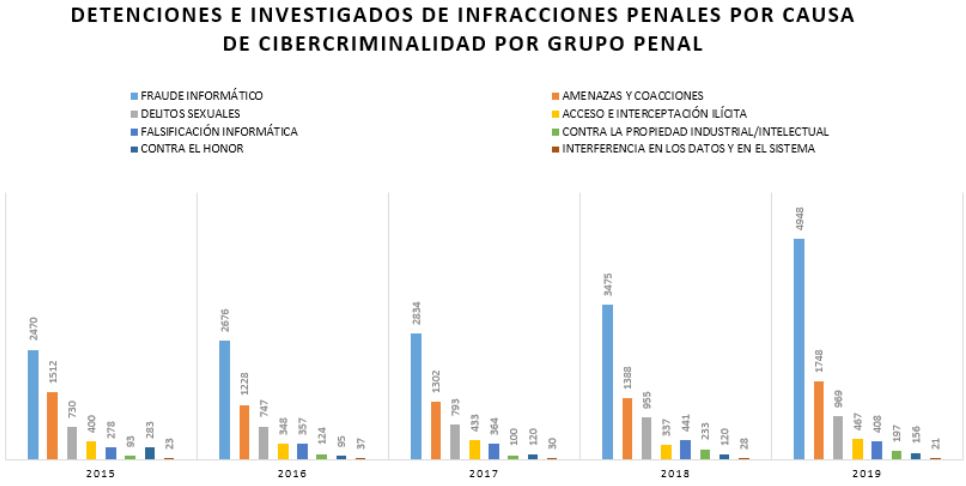
1. MARCO TEÓRICO

A modo de inicio en la materia objeto de estudio del presente trabajo, será necesario abordar una serie de conceptos y elementos primordiales que permitan asentar unas

bases teóricas estables mínimas; esto incluye constatar superficialmente la evidente migración delictiva del entorno físico al virtual, la conceptualización básica de la Deep Web y la Dark Web y la identificación de los fenómenos criminológicos asociados a ellas[1] dadas sus claras ventajas de uso.

1.1. CONCEPTO DE CIBERDELINCUENCIA

El desarrollo de las Tecnologías de la Información y las Comunicaciones, en adelante TIC, ha trasladado muchas de nuestras rutinas al plano digital; y ello ha llevado inevitablemente aparejado el aumento de delitos a través de la red, pues los delincuentes han incorporado las herramientas que estas ofrecen a su modus operandi. Una evidencia de ello es la identificación de los riesgos tecnológicos como una de las mayores preocupaciones sociales (WEF, 2019, 2020), al mismo tiempo que ponen de manifiesto el déficit de gobernanza tecnológica existente actualmente, por tanto, cabe considerarlo como una tendencia al alza. En este sentido, el número de tipologías delictivas perpetradas a través de la red ha aumentado de forma exponencial, siempre por delante de la legislación existente, como es normal en la materia jurídica, si bien en este ámbito la diferencia entre la conducta y el nacimiento de la ley es acuciante. Esto está ocasionado por la naturaleza de la ciencia informática en sí, caracterizada por ser una disciplina en constante evolución (Espinosa, 2019; Barrio, 2017).



Gráfica 1 Detenciones e investigados de infracciones penales relacionadas con cibercriminalidad por grupo penal (2015-2019). Fuente: Ministerio del Interior.

Para ilustrar el incremento de delitos informáticos mencionado, en la gráfica se pone de manifiesto el impacto que las TIC han supuesto en la evolución de la tasa de criminalidad española en base a los datos aportados por el Ministerio del Interior. Se ha tenido en cuenta el periodo comprendido entre 2019, último año con datos disponibles, hasta 2015, año en el que fueron incorporados los datos de todas las comunidades, ya que anteriormente no se disponía de los datos de la Ertzaintza ni de

1 En el presente estudio no se pretende de ninguna manera criminalizar estas fórmulas de navegación, pero sí se asume que una mayor anonimización, por ejemplo, supone un factor de atracción para determinadas actividades delictivas; lo cual no viene a significar en ningún caso que el empleo de Deep Web o Dark Web se haga exclusivamente con fines delictivos, pues aporta también, por continuar con el ejemplo, una mayor privacidad al usuario, ventaja absolutamente respetable.

los Mosos d'Esquadra. En este sentido, cabe destacar el número de Detenciones e investigados de infracciones penales relacionadas con cibercriminalidad desglosado por grupo penal durante el periodo comprendido entre 2015 y 2019, ambos inclusive.

Para abordar esta problemática los expertos en la materia establecieron el término delito informático, derivado de la denominación anglosajona *computer crime* y acuñado por primera vez en los años 80 por varios autores (Espinosa, 2019; Barrio, 2017). El concepto de "delito informático" es bastante amplio y contempla principalmente dos vertientes. Por un lado, las amenazas sobre bienes jurídicos tradicionales que han incorporado el uso de las nuevas tecnologías a su evolución y, por otro, aquellos que atentan sobre las tecnologías propiamente dichas y que amenazan contra el correcto funcionamiento de estas, circunstancia de la cual derivan los riesgos asociados. En este sentido, es posible enumerar algunas de las tipologías delictivas clásicas que en mayor medida han incorporado el uso de las TIC en su comisión; fraude, terrorismo, suplantación de identidad, pornografía infantil o delitos contra la salud pública entre otros. De otro lado, y para facilitar el conocimiento de esta nueva vertiente delictual, se mencionan tipologías como intrusiones no autorizadas a sistemas o ataques de denegación de servicio (DoS). Por su parte, persiguiendo el fin de lograr abordar la ciberdelincuencia de una manera efectiva, el Convenio sobre la Ciberdelincuencia (2001) establece una serie de tipologías delictivas que deberán ser abordadas por las legislaciones vigentes en los diferentes países miembros del Consejo de Europa.

Aparejado a este ámbito nació el concepto de ciberseguridad, que trata de abordar la necesidad de brindar la seguridad requerida a las TIC (Espinosa, 2019). Sin embargo, resulta un reto especialmente difícil para las legislaciones de los países por ser una fenomenología que abarca conductas de carácter transnacional principalmente, siendo singularmente complejo establecer el lugar de comisión del delito o, cuanto menos, establecer una trazabilidad fiable, lo que implica coordinación internacional en materia de jurisdicción penal (Barrio, 2017) y entorpece las labores de detección e investigación. En este sentido, en el año 2001 en Budapest, el Consejo de Europa elaboró el Convenio sobre la Ciberdelincuencia (CETS No.185), siendo este el primer tratado de carácter internacional, posteriormente ratificado en 2010, cuyo objetivo primordial es "aplicar, con carácter prioritario, una política penal común encaminada a proteger a la sociedad frente a la ciberdelincuencia, entre otras formas, mediante la adopción de la legislación adecuada y el fomento de la cooperación internacional" (Consejo de Europa, 2001).

Asimismo, cabe destacar la figura del agente encubierto cibernético, basado en la figura del agente encubierto contemplada en el artículo 282 LECrim que, en el año 2015, con el objetivo de ampliar el campo de actuación, derivó en la creación del agente encubierto cibernético recogida en los apartados 6 y 7 del artículo 282 bis LECrim, por la que se regula la atribución de una "identidad supuesta en comunicaciones mantenidas en canales cerrados de comunicación con el fin de esclarecer alguno de los delitos" previstos e, incluso, contempla la posibilidad de "intercambiar o enviar por sí mismo archivos ilícitos por razón de su contenido", todo ello con el fin de lograr la identificación tanto de los archivos como de los autores. En este sentido, la figura del agente encubierto cibernético nace como una línea de acción que pretende abordar el objetivo específico tercero de la Estrategia de Ciberseguridad Nacional de 2013 de "potenciar las capacidades de prevención, detección, respuesta, investigación y coordinación frente a las actividades del terrorismo y la delincuencia en el ciberespacio

respecto del ámbito judicial y policial", al igual que pretende dar cabida al tercer eje de actuación previsto en la Estrategia Nacional contra el Crimen Organizado y la Delincuencia Grave 2019-2023, mediante la cual se pretende "intensificar las acciones contra la venta de drogas online y su distribución, mejorando el control de la web profunda y las empresas de mensajería, así como potenciar el uso del agente encubierto informático en la red" (Ruiz, 2021).

Si bien no fue hasta 2015 que se dio cobertura legal a esta figura de uso profuso en la investigación de la ciberdelincuencia, existen algunas referencias a su empleo por parte de las Fuerzas y Cuerpos de Seguridad del Estado avaladas por la jurisprudencia. "Así en la STS 236/2008, de 9 de mayo, (Ponente: Excm. Sr. Don José Ramón Soriano Soriano), señala que los rastreos utilizados por el equipo de delitos telemáticos de la Guardia Civil en internet sin resolución judicial mediante, en la cual se accedió a los hash de archivos que contenían pornografía infantil, se encontraba dentro de las competencias propias de la Policía Judicial en relación con la prevención del delito" (Ruiz, 2021, p.33).

Teniendo en cuenta el brevísimo repaso al actual contexto en cuanto a ciberdelincuencia se trata, es pertinente realizar una sucinta aproximación teórica al ámbito o escenario donde ocurren los delitos objeto de estudio, esto es, Deep Web y Dark Web.

1.2. APROXIMACIÓN TEÓRICA A LOS CONCEPTOS CLEARNET, DEEP WEB Y DARK WEB

Tal y como se ha expuesto anteriormente, la ciberdelincuencia contempla un amplio número de tipologías delictivas (Espinosa, 2019) por ello, dada la amplitud, este trabajo se centrará en aquellas que transcurren o para cuya perpetración es necesario acudir a Deep Web o Dark Web, por lo que resulta conveniente realizar una aproximación teórica a estos conceptos.

En primer lugar, con el propósito de explicar brevemente el esquema de internet, se realizará una aproximación a través de la metáfora del iceberg (Bergman, 2001), no exenta de controversias en la materia. De acuerdo con lo expuesto por esta amenaza, internet estaría compuesta a rasgos generales por tres particiones en cuanto a perceptibilidad se refiere. En este sentido, y entendiendo Internet como una gran infraestructura de red que alberga y conecta entre si a millones de sistemas a nivel global, permitiendo las conexiones entre estos sistemas, siempre y cuando cuenten con una conexión a internet, cabe presentar el concepto de *clearnet* (Chertoff & Simon, 2015) que abarca la superficie o parte visible, siendo esta el área de internet comúnmente utilizada y conocida por los usuarios. Si bien esto tan solo sería una mínima parte de internet, existe otra parte, que se estima es 500 veces mayor (He, Patel, Zhang & Chang, 2007) que la web visible a la que los usuarios tienen acceso a través de motores de búsqueda que indexan contenido estático, conocida como Deep Web y Dark Web, las cuales se abordan en lo sucesivo (Chertoff & Simon, 2015).

Antes de profundizar en estos términos de forma concreta, conviene explicar cómo funcionan los motores de búsqueda tradicionales, tales como Google, Yahoo!, Bing, entre otros. Un motor de búsqueda, o también denominado Search Engine, es un sistema informático que utiliza rastreadores o indexadores, referidos tradicionalmente como *crawlers*, para ubicar archivos o sitios web disponibles en internet, de manera que permiten

establecer una especie de índice que facilita su búsqueda. Aunque existen diversos tipos, todos ellos tienen en común que disponen de un determinado número de sitios web estáticos indexados a los que tienen acceso. Estos motores de búsqueda cuentan con una gran limitación y es que dependen de una serie de requisitos para poder registrar los sitios web, tales como ser reportados directamente desde los autores de los sitios web o bien porque son rastreados por sus *crawlers* a partir de enlaces de hipertexto que, a su vez, conducen a otros enlaces. Es, ciertamente, esta limitación la que marca la diferencia entre *clearnet* y Deep Web, abarcando esta última todo sitio web disponible pero que no es indexado por los motores de búsqueda tradicionales, por lo que su accesibilidad se ve, cuanto menos, limitada. Si bien, el hecho de que la accesibilidad se vea dificultada y, por ende, no sea posible tener una visión real de la envergadura de lo que la Deep Web abarca, tan solo pone de manifiesto que esta se extiende en realidad a unos confines mucho mayores de lo que los motores de búsqueda habituales son capaces de albergar. Según un estudio realizado veinte años atrás por Michael K. Bergman (2001), al que se le atribuye la creación del término, Deep Web sería 500 veces más grande que la Web superficial. De este modo, teniendo en cuenta el desarrollo exponencial de Internet desde entonces, se estima que esta cifra se ha visto incrementada hasta aproximadamente el 90% (GL, 2018).

No obstante, las características de la Deep Web anteriormente expuestas no implican que necesariamente todo lo que se escapa a los motores de búsqueda tradicionales implique una denotación ilegal. En su mayoría está compuesta por sitios web restringidos por ser, por ejemplo, de pago, por tratase de bases de datos o archivos empresariales protegidos alojados en la nube, o para cuyo acceso es necesario el uso de servidores proxy o VPN (GL, 2018).

Ahora bien, existe una parte de la Deep Web, conocida como Dark Web que cuenta con una característica que la diferencia de lo anterior y es la capacidad de anonimización que ofrece. El término Dark Web acapara la parte de la Deep Web inaccesible a través de los motores de búsqueda tradicionales, cuyo acceso tan solo es posible a través de un software específico, que incluye técnicas de cifrado que enmascaran las direcciones IP en aras de garantizar la privacidad y evitar la monitorización (Chertoff & Simon, 2015; Gehl, 2014). Mientras que la Deep Web abarca el 90% de Internet, se estima que la Dark Web tan solo supone el 0,1% de esta (GL, 2018).

El contenido disponible en Dark Web se encuentra alojado en lo que se conoce como Darknet, una red a la que solo es posible acceder a través de un software específico. Los más populares son la red TOR, i2p, Freenet o ZeroNet, entre otras. De esta forma, el término Darknet hace referencia a cada una de las redes mencionadas anteriormente, mientras que Dark Web sería el concepto general que incluye a todas estas.

Teniendo en cuenta su uso extendido entre los usuarios, se explicará de forma concisa cómo funciona una de las Darknets más populares. TOR, o The Onion Router, facilita el acceso de forma anónima a sitios.*onion* empleando un sistema de cifrado que hace prácticamente imposible rastrear tanto a los visitantes como a los anfitriones de estos sitios web[2].

2 En su sitio web oficial, el Proyecto TOR se define a sí mismo como “una red conformada por un grupo de servidores operados por voluntarios que permite a las personas mejorar su privacidad y seguridad en Internet. Los usuarios de TOR emplean esta red conectándose a través de una serie de túneles virtuales en lugar de hacer una conexión directa, lo que permite que tanto las organizaciones como las personas compartan información a través de redes públicas sin comprometer su privacidad”. Por

Como bien reconocen sus propios desarrolladores, la anonimización ofrecida por el proyecto TOR presenta una contrapartida, y es que, al igual que otorga garantías en aras de comunicación segura a aquellos que lo requieren, también ofrece a personas criminalmente motivadas una serie de elementos que hacen más factible la comisión de actos delictivos, por lo que su empleo resulta una práctica ampliamente extendida entre delincuentes. De este modo, a fin de abordar la problemática objeto de estudio, se realizará una breve revisión teórica con el propósito de identificar las principales fenomenologías delictivas vinculadas a Deep Web y Dark Web de manera que sirva como sustento de la investigación empírica sobre esta materia.

1.3. FENOMENOLOGÍA DELICTUAL ASOCIADA A DEEP WEB Y DARK WEB

Aunque en un primer acercamiento pudiese parecer todo lo contrario y, a priori, sea susceptible de solaparse con las bases del presente trabajo, Deep Web y Dark Web no son sinónimos de delincuencia per se. Como se incluye con anterioridad, las premisas bajo las que se constituyen proyectos similares a TOR son las de brindar al usuario la privacidad necesaria para explorar Internet y así promover los derechos humanos, tal y como se expone en el punto anterior. Ahora bien, es innegable que resulta un medio óptimo para la perpetración de actos delictivos (Lovejoy, 2020), tales como:

- Delitos contra el patrimonio y contra el orden socioeconómico (Barrera, 2019; Díaz, 2019; Europol, 2020).
- Delitos contra la salud pública (Díaz, 2019).
- Delitos de organizaciones y grupos terroristas (Europol, 2020; Lovejoy, 2020).
- Pedofilia (Requião y otros, 2020).
- Prostitución y explotación sexual (Díaz, 2019).
- Tráfico de armas (Cámara, 2020).

En este sentido, cabe señalar que Deep Web y Dark Web involucran en gran medida la comisión de hechos delictivos, siendo principalmente promovido a través de redes de contacto (Requião, y otros, 2020; Europol, 2019). Esto se refiere a que las Darknets están principalmente organizadas en foros, que es donde transcurre la mayor parte de la actividad. En muchos de los casos, estos foros son de carácter cerrado y son exigidos una serie de requisitos a los usuarios para poder acceder al contenido que incluyen, sobre todo en aquellos delitos que involucran abusos infantiles y terrorismo. En otros casos, son foros en los que tan solo es necesario registrarse, más en los fenómenos criminales que involucran el tráfico de armas, delitos contra la salud pública y delitos contra el patrimonio y contra el orden socioeconómico (Lovejoy, 2020). En cualquier caso, variará pero, por lo general, cuanto más grave sea el delito

su parte, el proyecto TOR fundamenta su desarrollo en la necesidad de brindar la libertad y privacidad necesarias al usuario, pretendiendo servir a activistas, medios de comunicación y militares, entre otros (Gehl, 2014), ya que “en cuanto están dispuestos a quebrantar la ley, los criminales ya pueden hacer muchas más cosas malas de las que pueden llegar a hacer en base a la privacidad ofrecida por TOR”; por lo que pretende, “brindar protección a la gente común que quiere seguir la ley” para que así esta posibilidad no quede únicamente disponible para criminales.

perpetrado a través de Deep Web o Dark Web mayores protecciones tratarán de auto brindarse los usuarios implicados. Teniendo en cuenta lo anterior, y a efectos de definir la intervención de la figura del agente encubierto cibernético anteriormente descrita, resulta necesario aludir a la diferencia existente entre lo que es considerado "canal de comunicación cerrado" y "canal de comunicación abierto", pues la LO 13/2015 en su exposición de motivos determina que "en los canales abiertos, por su propia naturaleza no es necesaria (autorización judicial)". Así, de acuerdo con Valverde (2016), la diferencia reside en "la participación activa y voluntaria del interlocutor al consentir la admisión en su círculo de contactos a quien pretende intervenir en dicho canal, (…) consecuentemente se considerarán canales cerrados aquellos que sí precisen que el sospechoso activamente autorice o consienta la inclusión del perfil del agente investigador entre sus contactos" (Ruiz, 2021, p.41).

En adición a lo anterior, cabe mencionar que el empleo de criptografía en las comunicaciones de cibercriminales resulta una tendencia a la alza y uno de los aspectos más destacados según el informe anual de Europol sobre el Análisis del crimen organizado en internet (IOCTA), en el que se recogen las principales amenazas y tendencias relacionadas con el cibercrimen en 2020, año especialmente relevante en este ámbito, en tanto ha supuesto una evolución del modus operandi de cibercriminales, adaptándose a las circunstancias derivadas de la crisis suscitada por la pandemia COVID-19. De forma concreta, el informe IOCTA 2020 contempla el uso de Dark Web en términos criminales como una sección individual. En esta sección se hace referencia al contenido esencialmente volátil de los mercados que operan a través de Dark Web, sin que haya llegado a destacar ninguno de ellos tras los notables esfuerzos dedicados a la interrupción de la actividad de muchos de estos mercados en 2019, circunstancia que evidencia la efectividad que la cooperación supone en esta materia. Otro de los aspectos puestos en el foco en el informe de IOCTA 2020 ha sido el incremento de operaciones con criptomonedas, lo que resulta realmente preocupante, tanto para el ámbito financiero en sí mismo como para el aspecto más puramente criminal, ya que permite realizar intercambios sin que sea posible establecer una correcta trazabilidad. En este sentido, cabe resaltar que este informe pone de manifiesto la constante permutabilidad del cibercrimen y privacidad aparejada como uno de los principales retos a los que se enfrentan las Fuerzas y Cuerpos de Seguridad.

A este respecto, tal y como pone de manifiesto el informe de IOCTA 2020, las legislaciones de los diferentes países, así como sus FCSE se han visto obligadas a enmendar los instrumentos empleados en la lucha contra el cibercrimen, en general, y aquella fenomenología delictiva que transcurre a través de Deep Web y Dark Web.

1.4. BREVE MENCIÓN AL CONTEXTO DE ACTUACIONES CONTRA LA CIBERDELINCUENCIA

En un plano internacional, los países se han visto abocados a renovar su legislación en materia de ciberseguridad para así poder hacer frente al notable incremento de la delincuencia perpetrada o para cuya consecución es necesario el uso de internet, circunstancia que se ha visto incrementada a raíz de la pandemia suscitada por la COVID-19.

En este contexto, son incontables los países que han aumentado los fondos estatales destinados a ciberseguridad. Cabe resaltar la reciente orden ejecutiva firmada el pasado 12 de mayo de 2021 por Joe Biden, actual presidente de los Estados Unidos, la cual establece estándares de ciberseguridad que tienen como objetivo fortalecer la ciberseguridad del país mediante la creación de una junta para investigar los incidentes de seguridad integrado por el Departamento de Seguridad Nacional, el Departamento de Justicia, el Pentágono y entidades del sector privado[3]. Esta preocupación queda evidenciada en una hoja informativa publicada por la Casa Blanca en la que se indica que "La ciberseguridad es uno de los desafíos más importantes de nuestro tiempo, por lo que el presidente Biden ha hecho del fortalecimiento de las capacidades de ciberseguridad de Estados Unidos una máxima prioridad".

Por su parte, Europa también ha definido como objetivo clave lograr responder a la evolución del panorama de las ciberamenazas. En consecuencia, en diciembre de 2020, la Comisión Europea y el Servicio Europeo de Acción Exterior (SEAE) presentaron una nueva Estrategia de Ciberseguridad de la UE. El objetivo de esta estrategia es reforzar la resiliencia de Europa frente a las ciberamenazas y garantizar que todos los ciudadanos y empresas puedan beneficiarse plenamente de servicios y herramientas digitales seguros y fiables. De igual manera, en abril de 2021, el Consejo dio luz verde a la creación de un Centro de Competencia en Ciberseguridad que tiene como objetivo poner en común las inversiones en investigación, tecnología y desarrollo industrial en materia de ciberseguridad. De esta forma, la coordinación entre los Estados miembros se instaura como un requisito indispensable, ya que este Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad trabajará de forma conjunta con una Red de Centros Nacionales de Coordinación designados por los Estados miembros, así como organizaciones académicas y de investigación, industrias y otras asociaciones de la sociedad civil, y, sobre todo, queda prevista la cooperación con la Agencia de la UE para la Ciberseguridad (ENISA).

Además, para facilitar en mayor medida el acceso transfronterizo a las pruebas electrónicas para los procesos penales, la Unión Europea se encuentra en proceso de negociación de:

- Un acuerdo con Estados Unidos, el país en el que se encuentran la mayoría de los proveedores de servicios, y cuya comunicación se ve en ocasiones entorpecida principalmente por la protección de datos personales y que requiere una profunda deliberación que, por motivos de envergadura, no puede ser tratada en detalle en el presente trabajo.
- El segundo protocolo adicional del Convenio de Budapest mencionado en el primer punto del presente trabajo.

De esta forma, los países han intentado abordar la problemática que la ciberdelincuencia y la fenomenología delictual asociada plantean actualmente, de manera que estas ofrezcan las bases jurídico-legales necesarias para que los diferentes

3 President Signs Executive Order Charting New Course to Improve the Nation's Cybersecurity and Protect Federal Government Networks (12 de mayo de 2021). The White House. Recuperado de: https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/12/fact-sheet-president-signs-executive-order-charting-new-course-to-improve-the-nations-cybersecurity-and-protect-federal-government-networks/

organismos y fuerzas del orden competentes puedan abordar estos aspectos desde una perspectiva práctica efectiva. El EC3 de EUROPOL, el CCN-Cert del Centro Criptológico Nacional (CCN), el Mando Conjunto del Ciberespacio (MCCE) del Estado Mayor de la Defensa (EMAD), así como el Grupo de Delitos Telemáticos (GDT) de la Guardia Civil y la Unidad de Investigación Tecnológica (UIT) de la Policía Nacional son solo algunos ejemplos del proceso de especialización que se está llevando a cabo para hacer frente a las complejas investigaciones tecnológicas en la lucha contra la delincuencia, las dificultades en el análisis de evidencias digitales y la ya innegable necesidad de cooperación internacional.

2. OBJETIVOS

El presente trabajo tiene como principal objetivo:

- Identificar los principales modus operandi empleados por los cibercriminales que operan a través de la Deep Web y Dark Web.

De manera adicional, se tratará de:

- Analizar las características particulares de los delitos perpetrados o para cuya consecución es necesario acudir a Deep Web o Dark Web dentro del marco de la justicia española.
- Estudiar el nivel de detectabilidad que los delitos perpetrados o para cuya consecución es necesario acudir a Deep Web o Dark Web dentro del marco español.
- Determinar la eficacia probatoria de los indicios digitales detectados a partir de Deep Web y Dark Web dentro del marco de la justicia española.
- Reseñar la capacidad de resolución de fenómenos delictivos que involucran Deep Web y Dark Web dentro del marco de la justicia española.
- Describir propuestas de mejora para la investigación de esta fenomenología delictiva.

3. METODOLOGÍA

Para lograr alcanzar los objetivos anteriormente descritos, se determinó que la metodología que mejor se adecuaba era la empírica.

Se trata de un estudio exploratorio consistente en un análisis de sentencias, que constituyen los casos objeto del presente artículo.

En cuanto al procedimiento de selección de casos, es decir, la recopilación de sentencias que involucran Deep Web y Dark Web, este proceso siguió unas pautas previamente establecidas. En primer lugar, las búsquedas se focalizaron en la base de datos de jurisprudencia del Centro de Documentación Judicial (CENDOJ). Para lo cual, se establecieron una serie de criterios de búsqueda, que consistieron en seleccionar la lista de palabras clave que se muestra a continuación.

“Deep Web”, “Dark Web”, “Darknet”, “Dark net”, “red oscura”, “hidden Web”, “TOR”, “I2P”, “web”, “red anónima”, “internet”.

Una vez seleccionadas las palabras clave, se comenzó la búsqueda de estos términos de manera individual y combinados, aplicando como filtro que los resultados se encontraran enmarcados dentro de la jurisdicción penal. De esta forma, se lograron recabar un total de 44 sentencias, que fueron tratadas como estudio de casos, por la preponderancia del valor cualitativo sobre el cuantitativo.

Posteriormente, se procedió a recopilar la información relevante de las sentencias en base al interés del trabajo, para ello se elaboró una tabla a modo de base de datos organizada según tres dimensiones que contienen las siguientes variables:

1. Contenido procesal. Esta dimensión involucra todos los aspectos relativos al proceso judicial propiamente dicho, es decir, las variables relativas al procedimiento, tipo de resolución, órgano que emite el juicio, fallo y fechas de comisión de los hechos y de resolución.

2. Contenido criminalístico y problemas probatorios. Este ámbito constituye el aspecto más relevante, ya que en él se abordaba el análisis del contenido criminalístico, entendiendo por contenido criminalístico la extracción de evidencias mediante métodos y técnicas científicas, con el objetivo de recabar los indicios digitales necesarios que serán tenidos en cuenta en la resolución del caso, es decir, trata de valorar la capacidad probatoria de las evidencias digitales asociadas a Deep Web y Dark Web.

3. Características criminológicas. Esta dimensión hace referencia a los aspectos puramente fenomenológicos, con el objetivo de recabar toda la información criminológica relevante posible que permita identificar patrones en aras de mejorar la prevención, tales como el estudio de delincuentes, hechos delictivos, víctimas y contexto social, entre otros aspectos.

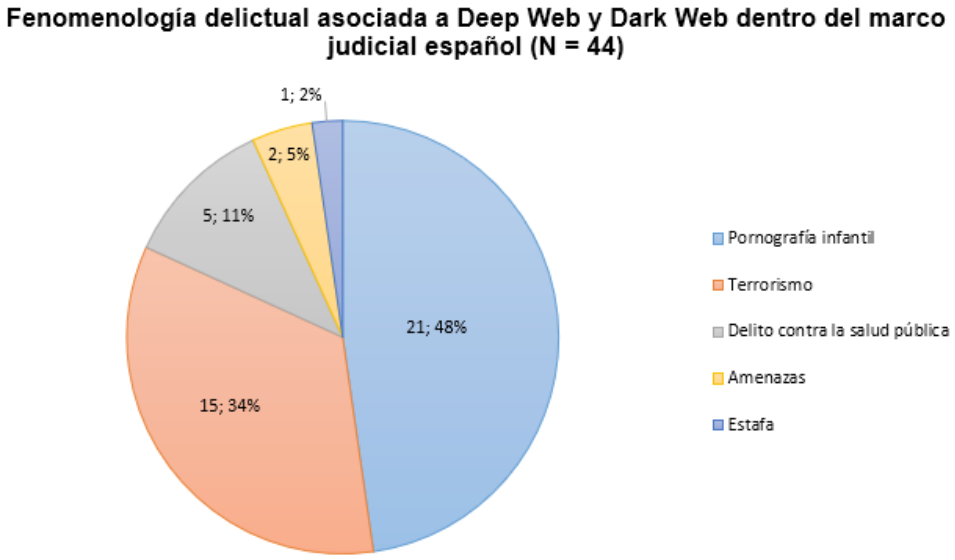
No obstante, la metodología adoptada cuenta con una gran limitación pues, además de ser una muestra muy limitada, el empleo de sentencias como casos implica que solo se tienen en cuenta los hechos conocidos por los juzgados y tribunales de justicia españoles. Dada la particular naturaleza del entorno, en el que predomina el anonimato, existen multitud de hechos que se escapan al conocimiento de los órganos de justicia, lo que supone un sesgo en los resultados obtenidos que fue tenido en cuenta en la interpretación y puesta en contexto de dichos resultados. Este sesgo es lo que se conoce como “cifra oscura” en criminología. Si bien, desde otra perspectiva, es precisamente este sesgo el que permite identificar las características específicas de los delitos relacionados con Deep Web y Dark Web conocidos por el sistema judicial español, poniendo en evidencia cuáles son sus peculiaridades y qué relevancia tienen estas, tanto de cara a la identificación del hecho delictivo y su autor como de cara a la resolución del proceso judicial aparejado.

4. RESULTADOS

Tras realizar una aproximación empírica al objeto de estudio, siendo este, de manera muy generalizada, la actividad criminal que transcurre o para cuya perpetración es necesario acudir a Deep Web y Dark Web, tomando como referencia los hechos conocidos por órganos y tribunales de justicia españoles, se obtuvieron los resultados que se describen a continuación.

En cómputo, se identificaron y analizaron 44 resoluciones judiciales, recabadas a partir de fuentes oficiales, en las que, de una manera u otra, se detectó la presencia de Deep Web y Dark Web. De esta forma, con la finalidad de dotar a estos resultados de una mayor accesibilidad, seguidamente se exponen, de forma gráfica, algunos de los aspectos más relevantes susceptibles de interpretación cuantitativa válida, cuyo análisis pormenorizado será desarrollado a continuación.

En primer lugar, en cuanto al fenómeno delictual asociado a cada una de las resoluciones judiciales identificadas, tal y como se muestra en la Gráfica 2, el fenómeno delictual asociado a Deep Web y Dark Web que mayor presencia obtuvo dentro del marco judicial español fue la Pornografía Infantil, el cual involucró el 48% de los casos identificados; le sigue muy de cerca el fenómeno delictual de Terrorismo, el cual acaparó el 34% de los casos detectados; y, en tercera posición, se encuentra el fenómeno delictual de Delito contra la salud pública, con el 11% de los casos analizados. En las últimas posiciones se encuentran las fenomenologías delictuales de Amenazas, con el 5% de los casos, y la fenomenología de Estafa, que se ha involucrado el 2% de los casos identificados.



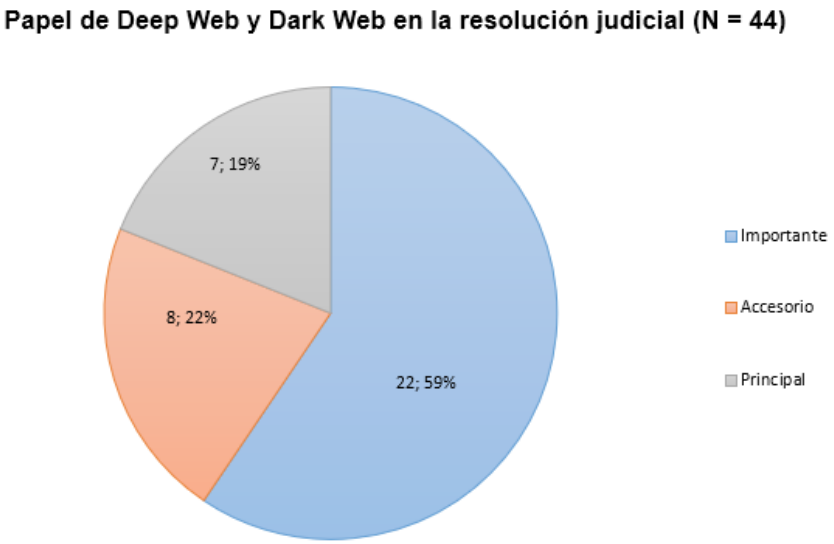
Gráfica 2 Fenomenología delictual asociada a Deep Web y Dark Web dentro del marco judicial español (N=44).

En otro orden de ideas, para tratar de satisfacer la necesidad de conocer el papel que la Deep Web y Dark Web tuvieron dentro de la resolución judicial, se establecieron tres niveles, siendo estos Accesorio, Importante y Principal, ilustrados a través de la siguiente gráfica.

Ordenados de menor a mayor relevancia, el nivel accesorio se asignó a aquellos casos que involucraban Deep Web y Dark Web pero no supusieron una circunstancia de peso en la resolución; en cuanto al nivel importante, hace referencia a aquellos casos en los que la presencia de Deep Web y Dark Web tomó relevancia en la determinación de la resolución en confluencia con otros hechos probados adicionales; por último, el nivel principal se asignó a los casos en los que se tuvo conocimiento

del/los hecho/s delictivos a partir de la investigación de los entornos de Deep Web y Dark Web, o bien la motivación de la resolución estaba basada principalmente en indicios digitales recabados a partir de Deep Web o Dark Web.

Tal y como se puede observar en la Gráfica 3, en el 50% de los casos el papel que Deep Web y Dark Web tuvieron en la resolución judicial fue importante, mientras que en el 34% este papel fue accesorio y, en el 16% restante, el papel fue principal.



Gráfica 3 Papel de Deep Web y Dark Web en la resolución judicial (N=44).

Los resultados plasmados anteriormente permiten realizar un primer acercamiento al objeto de estudio, si bien tal y como se ha descrito en la metodología, dado que se trata de un ámbito de carácter especialmente misceláneo, para comprender la realidad de la fenomenología delictual asociada a Deep Web y Dark Web se consideró necesario abordar esta problemática desde una perspectiva cualitativa, atendiendo a las características reseñables de los diferentes casos de manera más individualizada y así poder extraer conclusiones fructíferas.

4.1. CONTENIDO PROCESAL

Con el propósito de contextualizar las resoluciones judiciales identificadas, se acudió a los aspectos relativos al procedimiento judicial.

En primer lugar, cabe señalar que en el 100% de los casos el fallo fue condenatorio, contra los cuales se interpusieron un total de 14 recursos.

En adicción a lo anterior, y con el propósito de contextualizar las fenomenologías delictuales involucradas, en cuanto al órgano judicial que emitió el juicio fue la Audiencia Nacional en el 25% de los casos, la Audiencia provincial en el 50%, el Tribunal Supremo en el 16%, el Tribunal Superior de Justicia y la Sala de Apelación de la Audiencia Nacional en el 4,5% y, finalmente, el Juzgado de Instrucción en el 2% restante.

4.2. CONTENIDO CRIMINALÍSTICO Y PROBLEMAS PROBATORIOS

Con el fin describir el papel que Deep Web y Dark Web ocuparon en los hechos sentenciados, se realizó un acercamiento más próximo al entorno objeto de estudio en función de cada fenomenología delictiva identificada.

- Pornografía infantil

Dentro de la fenomenología de Pornografía infantil, más aún teniendo en cuenta que se trata de la fenomenología que en un mayor volumen de casos se vio implicada, es decir, el 48% de las detecciones, conviene señalar el papel que ocuparon Deep Web y Dark Web en la resolución judicial, siendo este papel importante en el 38% de los casos, principal en el 33% y accesorio en el 29% de casos restantes. En este sentido, es reseñable el hecho de que todos los casos identificados a partir del análisis global de sentencias en los que el papel de Deep Web y Dark Web fue principal son relativos a la tipología de pornografía infantil, es decir, esto pone de manifiesto que es la única tipología en la que el autor fue detectado como fruto de una investigación policial en Dark Web, ya sea de carácter internacional o nacional, tales como la operación Trojan, DOWNFALL2 Operación FERAS, en las que intervinieron unidades especializadas en esta fenomenología delictiva como INTERPOL, EUROPOL, FBI o el Grupo de Protección a la infancia de la Brigada Central de Investigación Tecnológica.

La circunstancia anteriormente descrita está a su vez relacionada con el funcionamiento de los foros de pornografía infantil en los que su acceso está estipulado de acuerdo con una serie de fases y privilegios, siendo necesario contar con una serie de requisitos para poder acceder a cierto contenido, como puede ser que los usuarios suban contenido al menos una vez al mes o de lo contrario serán desactivados, por lo que no sería posible descargar archivos si no se distribuye contenido. Este aspecto resulta realmente interesante, sobre todo en los casos en los que el sujeto es identificado a través de su participación en un foro de Dark Web, pues, aun desconociéndose su actividad, el mero hecho de ser integrante de un foro de este tipo, más aún si el usuario goza de un nivel de privilegios elevado, es indicativo de que su actividad implica el consumo y la distribución, quedando constatada la capacidad probatoria de este hecho.

Asimismo, dentro de la determinación de la capacidad probatoria, se detectó otro caso de uso habitual, que consistió en aquellas detecciones en las que, a consecuencia de la entrada y registro en el domicilio, se detectó el almacenamiento de contenido de carácter pedófilo en los dispositivos digitales investigados, así como la presencia del navegador TOR instalado en el dispositivo, siendo esto suficiente para que quedasen constatados los hechos probados en relación a los delitos de tenencia y distribución de pornografía infantil.

- Terrorismo

En cuanto a la tipología de Terrorismo, es decir el 34% de los casos identificados, de cara a conocer el papel que Deep Web y Dark Web ocupó en la resolución, en el 53% de los casos este fue accesorio, mientras que en el 47% de los casos restantes el papel fue importante. Para contextualizar las cifras anteriormente descritas, es necesario tener en cuenta que este tipo de resoluciones judiciales implican extensas investigaciones que abarcan multitud de acciones por parte de los condenados, o acusados, por lo que en su mayoría Deep Web y Dark Web constituyen un medio más

a partir del que poder desarrollar su actividad delictiva, observándose un mayor uso de las redes sociales y sistemas de mensajería instantánea, es decir fuentes abiertas de información, con el objetivo de llegar a los usuarios con los que se estrechará la comunicación en una fase ulterior.

En cualquier caso, a partir de la revisión de resoluciones relativas a la fenomenología Terrorismo que implicaron el uso de Deep Web y Dark Web, queda constatado que estas son elementos esenciales en la distribución y propagación. En este sentido, se pone de manifiesto las altas capacidades de adaptación de esta fenomenología delictiva, que no solo se nutre de las ventajas de las nuevas tecnologías, sino que optimizan su empleo mediante la incorporación de softwares de anonimización y criptodivisas, para así desarrollar las actividades delictivas en entornos seguro que entorpezcan la investigación policial y evadir la detección.

Finalmente, cabe destacar, de forma similar a lo acaecido en la tipología de Pornografía infantil, la existencia de cuerpos de seguridad focalizados en su investigación, tales como Unidad de Policía Judicial para delitos de terrorismo (TEPOL) o el Grupo de Información de la Guardia Civil, que intervinieron en operaciones conjuntas de carácter internacional.

- Delito contra la salud pública

Dentro de la tipología de Delito contra la salud pública, que constituye el 11% de las resoluciones identificadas, se determinó que el papel que ocuparon Deep Web y Dark Web en la resolución judicial fue importante en el 100% de los casos, en tanto que este era el medio que los implicados utilizaban para distribuir las sustancias, ya fuesen sustancias estupefacientes o medicamentos sin contar con la acreditación necesaria, por tanto era una parte muy importante en su modus operandi. A pesar de que en ninguno de los casos la detección fue a consecuencia de investigar directamente Deep Web o Dark Web, el hecho de que la compra y posterior distribución se realizase a través de sitios de Dark Web queda sufientemente constatado en los hechos probados de cara a la motivación del fallo.

A raíz de lo anterior, cabe destacar el uso de pagos mediante monedas virtuales, en estos casos Bitcoin, ya que resultan un medio óptimo para evadir la identificación, tanto de receptor como emisor de las transacciones, ampliamente utilizado en entornos de Dark Web.

De igual manera, resulta reseñable la labor de investigación llevada a cabo por las Fuerzas y Cuerpos de Seguridad, que cuentan con unidades específicas para la materia, tales como el Equipo de Delincuencia Organizada Antidroga (E.D.O.A.).

- Amenazas

Dada la baja incidencia de la fenomenología Amenazas, siendo esta del 5% de las detecciones, los casos detectados no han sido considerados representativos del objeto de estudio. En el primero de ellos el proceso comienza a raíz de la recepción de un correo de contenido amenazante a través de un cliente de correo de Dark Web, aunque finalmente su investigación no aportó ningún peso a la resolución judicial. De otro lado, en el segundo caso, la referencia se basa en amenazar con el anonimato que TOR en el contexto de una disputa entre una expareja.

- Estafa

Aunque a priori pudiese parecer lo contrario, dada la baja incidencia -el 2% de casos-, resulta una fenomenología realmente interesante para el objeto de estudio, en la que la totalidad de las detecciones Deep Web y Dark Web ocuparon un papel importante.

De manera concreta, el caso identificado versa sobre la modalidad de estafa cibernética denominada *carding*, siendo Deep Web y Dark Web un requisito necesario para su consecución, pues a partir de los hechos constatados puede extraerse que el condenado obtuvo los datos asociados a tarjetas a partir de esta fuente, sin que en ningún momento se indicase que el sujeto contaba con avanzados conocimientos de informática que le permitiesen llevar a cabo las acciones necesarias para obtener la información vinculada a las tarjetas bancarias por sí mismo, siendo más plausible que lograse obtenerlas mediante un mercado de Deep Web o Dark Web.

4.3. CARACTERÍSTICAS CRIMINOLÓGICAS

Finalmente, atendiendo a los aspectos criminológicos más destacables de las diferentes fenomenologías delictivas, de manera que faciliten un mejor conocimiento del objeto de estudio y favorezcan la labor de investigación y detección de estos fenómenos, se tuvieron en cuenta aspectos relativos al autor y, siguiendo a Herrera (2018), investigadora pionera dentro del ámbito de la Victimología española, a la víctima, que tan solo se ve reflejada en la tipología de Pornografía infantil.

En cuanto a las características del autor en la tipología de Pornografía infantil, se descubrió que la totalidad de ellos fueron varones, habiéndose detectado una notable tasa de implicados que contaban con antecedentes penales previos. Por su parte, las características de la víctima, que comprende aquellos casos en los que el implicado llevó a cabo o bien abusos sexuales o elaboración de contenido, existía una estrecha relación entre el autor y la víctima, así como en aquellos casos en los que se identificó la figura del testigo, este formaba parte del círculo cercano.

De otro lado, en cuanto a las características aparejadas al autor en la tipología Terrorismo, cabe destacar un alto porcentaje de implicados de nacionalidad extranjera.

Por otra parte, teniendo en cuenta las circunstancias de los implicados en la tipología de Delitos contra la salud pública, es reseñable la existencia de coautoría.

En cuanto al resto de tipologías, dada la escasa representatividad de estas, se eludirá la alusión a las características criminológicas.

5. DISCUSIÓN Y CONCLUSIONES

A modo de conclusión, extraídas a partir del estudio realizado, se incluyen una serie de enunciados que tratarán de solventar las necesidades planteadas, de forma que justifiquen la realización del presente trabajo poniéndolas en concordancia con lo establecido por los diferentes autores que han venido abordando esta miscelánea materia objeto de estudio.

En primer lugar, aunque ya se ha comentado anteriormente, cabe destacar el escaso número de resoluciones judiciales dentro del ámbito jurídico español que involucran

el uso de Deep Web y Dark Web, circunstancia que evidencia la existencia de la cifra oscura en cuanto a ciberdelincuencia se refiere relacionada con Deep Web y Dark Web.

En otro orden de ideas, tal y como han venido reflejando diferentes estudios sobre las fenomenologías delictivas asociadas a Deep Web y Dark Web, existen determinadas tipologías que se benefician especialmente de las características que estas ofrecen, incorporándolas en gran medida a sus particulares modus operandi. De esta forma, se ha podido comprobar que las principales fenomenologías delictivas reflejadas por las bases teóricas asentadas sobre la materia, es decir delitos contra el patrimonio y contra el orden socioeconómico, delitos contra la salud pública, delitos de organizaciones y grupos terroristas, pedofilia y explotación sexual, y tráfico de armas, realmente son las que componen el grueso de las principales actividades criminales vinculadas a este ámbito. En este sentido, a partir de la revisión sistemática de resoluciones judiciales extraídas del ámbito español que involucran el uso de Deep Web y Dark Web, se obtuvo como resultado que, de mayor a menor relevancia, Pornografía infantil, Terrorismo, Delitos contra la salud pública, Amenazas y Estafa fueron las fenomenologías más destacadas. Dentro de los actos delictivos enmarcados en la categoría de delitos contra el patrimonio y el orden socioeconómico, se encuentran la fenomenología de Estafa en particular y, de forma indirecta, todos aquellos actos que involucran el empleo de criptodivisas. A su vez, como es obvio, dentro de los hechos delictivos asociados a delitos contra la salud pública, se encuentra enmarcada la fenomenología que ha sido denominada de la misma forma. Por su parte, los actos que envuelven delitos de organizaciones y grupos terroristas acaparan la fenomenología aquí referida como Terrorismo. En cuanto a los actos delictivos de índole sexual, es decir, pedofilia y prostitución y explotación sexual, se encuentra enmarcada la fenomenología Pornografía infantil. Con respecto a los actos que involucran el tráfico de armas, a pesar de que no se ha detectado una relevancia específica tal que permita establecer una fenomenología específica, estos actos han tomado especial relevancia dentro de la fenomenología Terrorismo. Finalmente, cabe mencionar que no se identificaron estudios que avalen el empleo de Deep Web y Dark Web para perpetrar la fenomenología de Amenazas, detectada a partir de la revisión de resoluciones judiciales; esto es porque, tal y como se ha reflejado en los resultados, se trata de detecciones aisladas que poco aportan al estudio de esta materia, sin que sea posible considerar que Deep Web y Dark Web constituyan un medio especialmente significativo para su perpetración, siendo tan importante como cualquier otro.

De forma particular, se han identificado variables significativas en el modus operandi en función de la fenomenología delictiva. Aunque a grandes rasgos son aparentemente similares, pues en todas ellas, Pornografía infantil, Terrorismo, Delitos contra la salud pública, Amenazas y Estafa, los autores acuden a Deep Web y Dark Web para poder perpetrar la actividad ilícita en cuestión sin ser detectados, cuyo flujo transcurre en foros, o markets en su caso, a los que es difícil acceder si no se tiene conocimiento de la dirección URL o IP concreta, información acotada a un círculo de conocedores de la materia en cuestión, es decir, a lo que la literatura se refiere como redes de contacto.

En la fenomenología de Pornografía infantil, el entramado para acceder a los foros en los que transcurre la actividad es especialmente robusto, llegando a existir incluso

un sistema según el cual se determina el nivel de acceso al contenido. Esto es a su vez entorpecedor, por el evidente hecho de que la actividad se encuentra particularmente encubierta, al mismo tiempo que provechoso para la labor investigativa, pues en el momento en el que se logre irrumpir en algunos de estos foros e identificar a una persona quedará suficientemente constatada su participación en la distribución de contenido pedófilo, ya que para ganar el acceso es requisito indispensable aportar contenido de calidad cada cierto tiempo. Esta circunstancia justifica el hecho de que Pornografía infantil fuese la única fenomenología en la que se lograse identificar a los sujetos a través de operaciones policiales encaminadas a la persecución de estos delitos a través de Deep Web y Dark Web. Además, justifica la necesidad de regulación de la figura del agente encubierto cibernético, ya que su labor es especialmente relevante en esta materia, por tanto es esencial que esta figura cuente con todas las garantías legales posibles, de manera que revistan tanto el proceso de investigación como los resultados obtenidos de todos los requerimientos jurídicos necesarios.

Mientras que en otras fenomenologías se ha comprobado que fue más difícil constatar la actividad a través de Deep Web y Dark Web y se acepta que estas tuvieron implicación en los hechos, en cuanto el autor contaba con el software necesario instalado o, en algunas ocasiones, contenido procedente de Darknets o enlaces de acceso, pero por sí mismos estos descubrimientos probablemente no habrían bastado para detectar los hechos delictivos.

En este sentido, se ha observado que en el caso de la fenomenología delictiva de Terrorismo se destinaron grandes recursos dentro de la investigación a la investigación de fuentes abiertas mediante técnicas OSINT. Esto pone de manifiesto la relevancia que las fuentes de información abiertas ocupan dentro del marco de investigación de hechos delictivos que involucran las TIC y, por ende, Deep Web y Dark Web, observándose así la importancia que el ciclo de extracción de inteligencia supone. Este hecho está basado en las particulares dificultades de detección de uno y otro medio. Mientras que monitorizar la actividad que transcurre a través de Deep Web y Dark Web, así como identificar a un sujeto mediante su actividad en este medio resulta realmente dificultoso, si se emplean las herramientas y técnicas adecuadas en la investigación de fuentes abiertas propiamente dichas, tales como redes sociales, altamente empleadas en esta fenomenología delictiva para la difusión y propaganda, resulta relativamente asequible acceder y monitorizar el contenido e identificar a sus autores, si así fuese necesario en base a la gravedad de los delitos y la ausencia de otros medios menos lesivos para obtener la información que se pretende.

Por su parte, en el caso de las fenomenologías de Delitos contra la salud pública y Estafa, aunque en ningún caso se llegase a identificar al autor por su actividad en Deep Web y Dark Web, es evidente que esta integra un parte esencial en su modus operandi y, al contrario que en el caso de la fenomenología de Pornografía infantil, en estos foros o principalmente markets el acceso se ve dificultado en menor medida por los condicionantes requeridos para ser integrantes, lo que podría beneficiar las labores de investigación, aunque en muchos casos existe un sistema de reputación similar. Otro asunto sería el lograr identificar al sujeto en cuestión, es decir, identificar una dirección IP a través de la cual se pueda llegar a la identidad de su propietario, así como su dirección física. Aunque, sobre todo, la escasa incidencia dentro del ámbito jurídico español de estas fenomenologías minoritarias, Delitos contra la salud pública, Amenazas y Estafa, podría deberse a los recursos dedicados a la investigación de las

mismas, que serían menores que en los delitos vinculados con las fenomenologías de Pornografía Infantil y Terrorismo, en los que se observó una mayor especialización de las unidades policiales que intervienen y mayor implicación internacional a nivel de operaciones, o también a la tendencia recogida por Europol en su informe de Análisis del Crimen Organizado en Internet (IOCTA), correspondiente al año 2020, que pone de manifiesto los buenos resultados derivados de los notables esfuerzos dedicados en 2019 a la interrupción de la actividad de numerosos mercados que operan a través de Dark Web.

Desde otra perspectiva, a raíz del estudio de las características relativas a los autores de las diferentes fenomenologías delictivas, se ha identificado una serie de variables específicas que podrían favorecer la investigación. En primer lugar, en los casos de Pornografía infantil se observó que la reincidencia es un hecho habitual. De otro lado, cabe destacar que, en los casos relativos a la fenomenología Terrorismo, la mayor parte de los autores no era de nacionalidad española, lo cual resulta plausible en base a las características específicas de esta tipología delictiva. Finalmente, destacó el hecho de que en la fenomenología Delitos contra la salud pública la participación implicase en un alto grado la coautoría, circunstancia totalmente loable dado que suelen involucrar la existencia de una organización.

Pese a la escasa detectabilidad de los fenómenos delictivos que transcurren a través de Deep Web y Dark Web, cabe resaltar que, a grandes rasgos, en los casos en los que se detectaron indicios digitales, estos tuvieron una gran implicación en la resolución judicial, por lo que cabe atribuirles una buena eficacia probatoria dentro del marco de la justicia española. En muchos de los casos, la detección del software TOR instalado en el dispositivo del autor ya tuvo una implicación importante en el dictamen de la sentencia, esto está basado en las particulares características que reviste este software que implican altas capacidades de anonimización, tal y como se expone en la breve aproximación al concepto de TOR llevada a cabo en el presente trabajo. En relación con la eficacia probatoria, quedó demostrado a través del estudio de casos que los fenómenos delictivos fueron resueltos con fallo condenatorio en la mayoría de ellos, por lo que se considera satisfecha la capacidad de resolución de hechos que involucran Deep Web y Dark Web. Esta circunstancia deriva principalmente del tratamiento del indicio digital, ya que, en el marco de la justicia española, este ha de contar con un determinado protocolo en lo que a su investigación y obtención de la evidencia propiamente dicha se refiere. En este sentido, la investigación e incautación de indicios en los propios equipos no deja de ser sino una verdadera prueba material del hecho delictivo, siempre y cuando cumpla los debidos requisitos de cadena de custodia, así como otros de carácter técnico, necesarios como cualquier otra investigación/inspección ocular.

Asimismo, cabe destacar un correcto entendimiento generalizado de la materia por parte de los órganos de justicia españoles, acudiendo a los términos de manera cierta y reflejándolo de forma accesible en la sentencia, lo cual es esencial para abordar de forma correcta esta problemática. En este sentido, cabe mencionar que la Cámara de Delegados de la Asociación de Abogados del Estado de Nueva York (“NYSBA”) aprobó, a comienzos de septiembre, un informe proponiendo que el Comité Ejecutivo de NYSBA recomiende a la Junta de Educación Legal Continua del Estado de Nueva York que se modifique el requisito de CLE bienal para requerir un crédito en ciberseguridad en el desarrollo de la práctica jurídica. Aunque hasta la fecha en España no se

ha detectado ningún movimiento de propuesta similar, es previsible que pueda surgir en cualquier momento, ya que esta circunstancia es una evidencia más del impacto que el desarrollo de las TIC ha supuesto en el mundo físico y sobre todo jurídico, poniendo de manifiesto la necesidad de optimizar su resolución.

En definitiva, se trata de un ámbito de estudio realmente complejo por sus peculiares características de privacidad y anonimización, lo cual no quiere decir que unas correctas pautas de investigación no deriven en la consecución de resultados favorables. Tal y como se ha expuesto hasta ahora, resulta evidente que la dedicación de esfuerzos en la lucha contra la ciberdelincuencia es esencial, avalada por los buenos resultados obtenidos cuando esta circunstancia fue puesta en práctica. En consecuencia, como se expone al comienzo del presente trabajo, al tratarse la ciberdelincuencia de una fenomenología que se extiende al ámbito internacional, la elaboración de convenios y tratados internacionales tales como el Convenio sobre la Ciberdelincuencia de Budapest de 2001, que buscan crear un marco legal común que sirva como base a las diferentes naciones en la lucha contra el cribercrimen, resultan primordiales dentro de la actual coyuntura socioeconómica. Necesidad que se ha visto incrementada a raíz de la pandemia de la COVID-19, que ha acelerado el proceso de digitalización y desarrollo de las Tecnologías de la Información y las Comunicaciones.

BIBLIOGRAFÍA

Barrera, S (2019). Ciberpol. Metodología para la investigación del cibercrimen. Universidad Internacional de la Rioja (UNIR), Logroño.

Bergman, M. K. (2001). The Deep Web: Surfacing Hidden Value. Journal of Electronic Publishing, Volume 7. https://quod.lib.umich.edu/j/jep/3336451.0007.104?view=text;rgn=main

Barrio, M. (2017). Ciberdelitos: Amenazas Criminales del Ciberespacio. Adaptado reforma Código Penal 2015 (pp. 9-30). REUS, Madrid.

Best, R. A., & Cumming, A. (2008). Intelligence Issues and Developments. En T. M. Paulson, & T. M. Paulson (Ed.), Open Source Intelligence (OSINT): Issues for Congress (75-79). New York: Nova Science Publishers, Inc.

Cámara, S. (2020). Estudios criminológicos contemporáneos (IX): La Cibercriminología y el perfil del ciberdelincuente. Derecho y cambio social, 498.

Chertoff, M., & Simon, T. (2015). The Impact of the Dark Web on Internet Governance and Cyber Security. Global Commission on Internet Governance, Paper Series nº 6, 2-7.

Consejo de Europa (2001). Convenio de Budapest sobre la ciberdelincuencia. 23 de noviembre de 2001, ratificado el 17 de septiembre de 2010. https://www.boe.es/diario_boe/txt.php?id=BOE-A-2010-14221

Consejo General del Poder Judicial (s.f.). Centro de documentación judicial (CENDOJ). http://www.poderjudicial.es/search/indexAN.jsp

Díaz, M. (4 de abril de 2019). Persecución de delitos en la Darknet: un análisis de la jurisprudencia española. Click Jurídico. https://clickjuridico.es/delitos-deepweb-jurisprudencia-espana/

Espinosa, J.F (2019). Ciberdelincuencia. Aproximación criminológica de los delitos en la red. La razón histórica. Revista hispanoamericana de Historia de las Ideas, nº 44, 153-173. ISSN 1989-2659.

European Union Agency for Law Enforcement Cooperation (2019). Internet Organised Crime Threat Assessment (IOCTA) 2019. https://www.europol.europa.eu/sites/default/files/documents/iocta_2019.pdf

Internet Organised Crime Threat Assessment (IOCTA) 2020. https://www.europol.europa.eu/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2020.pdf

Gehl, R. W. (2014). Power/freedom on the dark web: A digital ethnography of the Dark Web Social Network. SAGE Journals, Volume 18(7), 1219-1235.

GL, J. (2018). Técnicas OSINT para investigación en Internet. Manual para investigadores.

Metodología OSINT para investigar en Internet (2020).

He, B., Patel, M., Zhang, Z., & Chang, K. C.-c. (2007). Accessing the Deep Web. Communications of the ACM, 50(5), 95-101.

Herrera, M. (2018). "Las víctimas en el sistema penal y su derecho a los derechos" reflexiones a propósito de "derecho de las víctimas a tener derechos", de José Luis Eloy Morales Brand. Revista Electrónica de Estudios Penales y de la Seguridad: REEPS, Nº. 3.

Lovejoy, G. (2020). Inside the Dark Web. Security and Society in the Information Age, Vol. 2, 124-145.

Ministerio del Interior (s.f.). Portal Estadístico de Criminalidad. https://estadisticasdecriminalidad.ses.mir.es/publico/portalestadistico/portal/datos.html?type=pcaxis&path=/Datos5/&file=pcaxis

National Security Agency Center (NSA) (2013). Untangling the Web: An Introduction to Internet Research.

Orden PCI/161/2019, de 21 de febrero, por la que se publica el Acuerdo del Consejo de Seguridad Nacional, por el que se aprueba la Estrategia Nacional contra el Crimen Organizado y la Delincuencia Grave. BOE núm.46. https://www.boe.es/diario_boe/txt.php?id=BOE-A-2019-2442

Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional. BOE núm.103. https://www.boe.es/eli/es/o/2019/04/26/pci487

Ramos, L. (6 de mayo de 2018). STS 173/2018, de 11 de abril, el agente encubierto digital. Rodríguez Ramos Penal & Compliance. https://www.rodriguezramos.es/2018/05/06/conclusiones-del-abogado-general-m-campos-sanchez-bordona-presentadas-el-12-de-septiembre-de-2017-asunto-c

Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal. 17 de septiembre de 1882. BOE núm.260. https://www.boe.es/buscar/act.php?id=BOE-A-1882-6036

Requião, B., MacCarron, P., Passold, J., Walmocyr, L., Oliveira, K., & Gleeson, J. (2020). Assessing police topological efficiency in a major sting operation on the dark web. Natureresearch: Scientific Reports.

Retenaga, A. M. (28 de mayo de 2014). OSINT - La información es poder. INCIBE-CERT. https://www.incibe-cert.es/blog/osint-la-informacion-es-poder

Roop, J. E. (1969). Chapter 1 - Early Beginnings. En J. E. Roop, Foreing Broadcast Information Service History. Central Intelligence Agency.

Ruiz, T. (2021). "Las Nuevas Diligencias de Investigación Electrónicas".

TOR Project (s.f.). Documentation: Abuse FAQ. https://2019.www.torproject.org/docs/faq-abuse.html.en

World Economic Forum (2019). The Global Risks Report 2019. Insight Report. 14th Edition.

(2020). The Global Risks Report 2020. Insight Report. 15th Edition.

AUTOS Y SENTENCIAS

SAN-2196-2020

SAP-C-1656-2020

SAP-CC-811-2020

SAP-IB-145-2020

SAP-TF-1071-2020

SAP-VA-842-2020

STS-3448-2020

SAN-5286-2019

SAN-633-2019

SAN-1447-2019

SAN-5421-2018

SAN-3383-2019

SAN-4717-2019

SAP-C-1383-2019

SAP-MA-2751-2019

SAP-P-337-2019

SAP-PO-2479-2019

STS-1535-2019

SAN-4611-2018

SAN-2472-2018

STS-2205-2019

SAP-B-13263-2018

ATS-11793-2018

SAP TF-284-2018

STSJ-ICAN-1961-2018

SAP-TF-1900-2018

SAP-V-3858-2018

SAN-2462-2018

SAN-2750-2018

SAN-4993-2018

STS-1385-2018

SAP-LU-471-2017

STS-4554-2018

SAP-CC-819-2017

ATS-12884-2017

STSJ-ICAN-981-2017

SAP-TF-500-2017

SAN-3016-2017

SAP-C-1461-2017

SAP-GC-2515-2017

SAP-M-6587-2017

DATOS SOBRE LOS AUTORES DE ESTE VOLUMEN POR ORDEN ALFABÉTICO

Balbino Espinel es comandante de la Guardia Civil perteneciente a la LXII promoción de la Academia General Militar. Tras haber desarrollado la mayor parte de su carrera en la Jefatura de Información en la actualidad está destinado en el Estado Mayor de la Guardia Civil. Diplomado en Estado Mayor, posee el Máster Universitario en Política de Defensa y Seguridad Internacional por la Universidad Complutense de Madrid.

Carmen Jordá Sanz es doctora en Derecho, Gobierno y Políticas públicas por la Universidad Autónoma de Madrid (UAM), donde se licenció en Psicología y en Derecho en 2012; posee también un Máster Oficial en Criminología y Delincuencia Juvenil por la Universidad de Castilla -La Mancha, un Máster en Evidencias Digitales y Lucha contra el Cibercrimen del Centro Nacional de Excelencia en Ciberseguridad y un Máster en Análisis e Investigación Criminal por el Instituto de Ciencias Forenses y de la Seguridad (UAM). En este Instituto ha realizado proyectos de investigación para la Comisión Europea y para distintos ministerios españoles y europeos. Actualmente es profesora en distintos centros formativos, dirige el Departamento de Criminología y Seguridad de la Universidad Camilo José Cela y es responsable de la Oficina de Inteligencia y Prospectiva de Prosegur.

Laura Méndez García es graduada en Ciencia Política y Administración Pública por la Universidad de Salamanca (2013-2017). Máster en Operaciones de Inteligencia y Contrainteligencia por la Universidad a Distancia de Madrid y el Campus Internacional para la Seguridad y Defensa de España (2017-2018) por el que recibió el diploma honorífico a mejor expediente académico. Miembro de la red de jóvenes investigadores (RJI) Observatorio Internacional de Estudios sobre Terrorismo (OIET), colabora habitualmente en medios de comunicación del Grupo Prensa Ibérica (La Provincia, El Día, El Levante) con artículos de análisis y opinión; con Podcast (Sierra Delta) y Televisión (RTVC). Ha colaborado con think tanks como el IEEE (DO 'Reservas de inteligencia compartidas en el nuevo panorama estratégico') Autora del libro de investigación 'Inteligencia contra el terrorismo y el crimen organizado. Oportunidades en la cooperación hispano-marroquí' de Ediciones Idea. Ha participado en el Congreso 'Inteligencia artificial y Defensa' (USAL y CESEDEN) en 2020 publicando un capítulo ('Yihad 3.0 Vigilancia, monitorización y redes de cooperación') en un monográfico de Aranzadi. Ha participado como miembro del Foro de la Mujer en Seguridad, Defensa y Emergencias, constituido con motivo de la próxima Feria Internacional de Galicia Abanca-, en la redacción del ideario y como moderadora en un seminario de inteligencia sanitaria (Medint). Anteriormente dirigió un proyecto de investigación, en Observatorio Canario de Seguridad y Defensa, coordinando actividades divulgativas y académicas para promover el interés en cuestiones relacionadas con la Seguridad y la Defensa. Analista y Consultora independiente de inteligencia, contrainteligencia y asuntos públicos.

Jorge Juan Pérez Rodríguez es teniente coronel de la Guardia Civil en la Zona de Castilla y León. En su trayectoria profesional ha tenido diversos destinos en el GAR, la Compañía de Getafe, el GRS de León, en Estado Mayor o en Información de la Zona de Castilla y León, entre otros. En el año 2013 se graduó como ingeniero técnico en

informática de sistemas en la UNED y en 2015 obtuvo el título de graduado en derecho en la Universidad Nebrija. Su formación también abarca diferentes cursos profesionales, como el Curso de Operaciones Especiales de la Policía Nacional de Colombia (COPES) y el Curso de Adiestramientos Especiales (ADE) de la Guardia Civil. También el Curso de Policía Judicial y el Curso Superior de Especialistas en Información o el Curso de Estado Mayor de las FAS y el de Planeamiento Estratégico de Misiones Civiles de la Unión Europea. Asimismo, realizó el Curso de Operaciones de Paz de las FAS y el Curso de Misiones Internacionales de la Guardia Civil, dada su experiencia internacional, donde destaca su paso por Afganistán, como asesor del Ministerio de Interior Afgano en Kabul, en el año 2013, en el marco de la National Training Mission for Afghanistan (NTM-A). En este mismo ámbito internacional, con motivo de su paso por el MOPS del EMAD, participó como representante de la Guardia Civil en el Panel para la redacción de la Doctrina aliada conjunta de policía militar (MP Panel), en la Conferencia de jefes de policía militar (MP Chiefs Conference), en el Provost Marshall Forum y en el Clúster de policía militar, todos ellos organizados por la OTAN.

Carmen Sánchez Pérez es graduada en Criminología con mención especial en Ciencias Forenses por la Universidad de Sevilla, formación a través de la cual realizó una experiencia del programa Erasmus en la Universidad de Coventry (Reino Unido), y posee también un Máster Oficial en Criminología, Investigación Criminal y Escena del Crimen por la Universidad Camilo José Cela (UCJC). Actualmente desempeña su actividad laboral como Consultora de Ciberseguridad en el departamento de Technology Consulting de EY, en el que lleva a cabo servicios de consultoría para la definición e implementación de planes estratégicos en materia de ciberseguridad.

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, AUTORÍA Y AFILIACIÓN. En la primera página constará el título, en mayúsculas y negrita, y, debajo, el nombre del autor (en mayúsculas), indicando puesto de trabajo y profesión.

Se adjuntará adicionalmente breve CV del autor de 10 o 15 líneas y dirección de correo electrónico.

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 "Keywords".

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. Arial 12 puntos. Las notas y afiliación serán de la misma letra, tamaño 10 puntos.

CUADROS Y FIGURAS. Serán numerados e incluirán una breve titulación.

PÁRRAFOS. Sangrado de 5 espacios. Espacio sencillo.

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 de la página de forma numerada.

ACCESIBILIDAD. Será necesario comprobar la accesibilidad del documento.

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. Además se tendrá en cuenta la accesibilidad del documento y de las imágenes. 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, previo paso por Turnitin. 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.

CENTRO UNIVERSITARIO GUARDIA CIVIL

Marco Legal

- Ley 39/2007 de la Carrera Militar
- Real Decreto 1959/2009 de creación del Centro Universitario de la Guardia Civil (**CUGC**)
- Orden PRE /422/2013 de servicios centrales de la DGGC
- Ley 29/2014 de Régimen de Personal de la Guardia Civil

Capacidades

- Titularidad del Ministerio del Interior a través de la Dirección General Guardia Civil.
- Ente público diferente de la Administración General del Estado.
- Adscrito a una o varias universidades públicas que expiden titulos oficiales universitarios del EEES: Actualmente UC3M y UNED (pendiente de desarrollo).
- Impartir titulaciones universitarias oficiales (grado, máster, doctor) y desarrollar líneas de investigación de interés para la Guardia Civil.
- Acuerdos de cooperación con otras instituciones a nivel nacional e internacional.

Oferta Académica

Actualmente el CUGC está adscrito a la Universidad Carlos III de Madrid (UC3M) e imparte las Titulaciones Académicas oficiales de:

- Máster en Dirección Operativa de la Seguridad.
- Máster en Seguridad Vial y Tráfico.
- Máster en Alta Dirección en Seguridad Internacional.
- Grado en Ingeniería de la Seguridad.
- Grado en Gestión de Seguridad Pública.
- Curso experto universitario en reconstrucción de siniestros viales.
- Curso de experto universitario en Investigación de la Ciberdelincuencia.
- Curso de experto universitario en Investigación interna.

- Curso de experto universitario en Delitos medioambientales.

Para prestar un mayor apoyo en las asignaturas y facilitar el contacto con los alumnos, el CUGC dispone de un Aula Virtual cuyo acceso se realiza desde la página web (www.cugc.es).

Además desarrolla otras actividades:

- Apoyo institucional para desarrollo de doctorados.
- Investigación Académica.
- Línea Editorial del CUGC.
- Extensión Universitaria.
- Reconocimiento Carta Erasmus 2021-2027.