Cuadernos de Estrategia 201

Límites jurídicos de las operaciones actuales: nuevos desafíos

Instituto Español de Estudios Estratégicos

ieee.es
Instituto Español de Estudios Estratégicos

MINISTERIO DE DEFENSA

Cuadernos de Estrategia 201

Límites jurídicos de las operaciones actuales: nuevos desafíos

Instituto Español de Estudios Estratégicos

ieee.es
Instituto Español de Estudios Estratégicos

MINISTERIO DE DEFENSA

CATÁLOGO GENERAL DE PUBLICACIONES OFICIALES
http://publicacionesoficiales.boe.es/

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

https://publicaciones.defensa.gob.es/

NIPO: 083-19-231-0 (edición papel)
ISBN: 978-84-9091-444-1 (edición papel)

Depósito legal: M-28436-2004

Fecha de edición: diciembre 2019
Maqueta e imprime: Ministerio de Defensa

NIPO: 083-19-232-6 (edición libro-e)

En esta edición se ha utilizado papel 100 % libre de cloro procedente de bosques gestionados de forma sostenible.

ÍNDICE

Introducción

Ángel Serrano Barberán

«El automóvil, indudablemente, ha transformado el mundo, como el cine, como la radio y como otros cuantos inventos de esos transcendentales...». Esto es lo que decía el escritor madrileño don Antonio Díaz Cañabate en su entrañable *Historia de una taberna*, escrita en el ya lejano año de 1944. Y cuanta razón tenía... Esos *inventos transcendentales*, que se han ido incrementando a un ritmo vertiginoso por los adelantos científicos y tecnológicos que se han producido en los últimos tiempos, sin duda alguna han transformado el mundo y la vida de las personas que en él habitan. Han cambiado muchas de sus costumbres, han influido en la forma en que se relacionan las personas y los grupos humanos y han provocado modificaciones sustanciales que han afectado a todos los sectores de la actividad humana, a la medicina, a la industria, al comercio, al mundo de la información... y, cómo no, a las relaciones sociales y a las relaciones internacionales, sean estas amistosas o no. Y de la misma forma que en tantos otros sectores, esa prodigiosa evolución tecnológica y científica de la que hemos sido testigos en los años recientes ha influido también poderosamente en el ámbito militar, dando lugar no solo a la aparición de nuevos medios de combate, es decir, a la aparición de nuevas armas o sistemas de armas cada vez más poderosos y precisos, sino también a nuevos métodos de conducción de las operaciones militares. Y es en este punto donde nos podemos preguntar: estos nuevos medios y métodos de combate ¿son todos admisibles desde una óptica legal?, ¿son todos ellos conformes al derecho internacional? o ¿sería ne-

cesaria una nueva normativa que regulase su uso, limitando o incluso prohibiendo su empleo?

Como es de sobra conocido, la regulación de los medios y métodos de combate en el curso de un conflicto armado, con la finalidad principal de evitar que su uso cause perjuicios y daños innecesarios, especialmente a la población y a los bienes civiles, constituye el objeto de lo que inicialmente se conocía como derecho de la guerra (las *leyes y usos de la guerra* de épocas históricas anteriores) y que hoy en día recibe el nombre de derecho de los conflictos armados o, de una forma más frecuente, derecho internacional humanitario (DIH). También es igualmente sabido que esa rama del derecho internacional público ha sufrido una evolución significativa a partir del último tercio del siglo XIX, dando lugar a un extenso cuerpo normativo en el que destacan los Convenios de Ginebra de 1949 y sus dos protocolos adicionales de 1977, acuerdos internacionales que tienen una extraordinaria importancia, no solo por la aceptación que han merecido por la mayor parte de los Estados que componen la comunidad internacional, sino porque muchas de sus normas (y entre ellas el núcleo esencial de la regulación de los medios y métodos de combate), precisamente por esa aceptación casi general, se consideran hoy parte integrante del derecho consuetudinario, que obliga por igual a todos los Estados y otros actores internacionales (el llamado *ius cogens*). Pero el DIH continua su evolución[1], tratando de adaptarse a la propia evolución de los conflictos armados, que a su vez lo hacen al hilo de la situación política mundial y, adicionalmente, como consecuencia de la influencia que en ellos ejerce el fabuloso desarrollo tecnológico y científico al que hemos hecho más arriba mención.

En efecto, aunque como dice la Doctrina para el empleo de las Fuerzas Armadas españolas[2], la *naturaleza* de los conflictos armados no ha variado, en la medida en que siguen caracterizándose por el uso de la violencia y el uso de la fuerza, sí se he modificado en cierto sentido lo que el propio documento denomina el *rostro* de los conflictos, es decir la forma en que estos surgen y se presentan. Los conflictos armados internacionales, o lo que es lo mismo, los conflictos armados entre Estados o entre Estados y organizaciones internacionales, constituyen hoy en día la excepción, habiendo caído en desuso,

[1] Baste mencionar aquí, como ejemplos de esa evolución, la Convención sobre prohibiciones o restricciones del empleo de ciertas armas convencionales que puedan considerarse excesivamente nocivas o de efectos indiscriminados (10 de octubre de 1980) y sus protocolos; la Convención sobre la prohibición del desarrollo, la producción, el almacenamiento y el empleo de armas químicas y sobre su destrucción (13 de enero de 1993); la Convención sobre la prohibición del empleo, el almacenamiento, producción y transferencia de las minas antipersonal y sobre su destrucción (18 de septiembre de 1997); o la Convención sobre municiones en racimo (30 de enero de 2008).

[2] Doctrina para el empleo de las FAS, *Publicación Doctrinal Conjunta*, PDC-01 (A), promulgada por el jefe del Estado Mayor de la Defensa con fecha 27 de febrero de 2018, p. 18, apartado 015.

además, la declaración formal de guerra. Actualmente, la situación de conflicto armado internacional, que es lo que da pie a la aplicación del DIH que rige tal tipo de conflictos, se genera desde el mismo momento en que hay un recurso a la fuerza armada entre dos Estados, por mínimo que sea. Por el contrario, los conflictos armados de carácter no internacional, conflictos que tienen lugar en el territorio de un Estado entre fuerzas gubernamentales y fuerzas disidentes o grupos armados organizados o entre estos entre sí, son la regla general y aunque están igualmente sometidos a las disposiciones del DIH a ellos aplicables desde el momento en que se considera que el conflicto se produce (cuando las hostilidades alcanzan un mínimo de intensidad), sus normas son más limitadas y están menos desarrolladas. A esta circunstancia de que sean los conflictos armados no internacionales o internos (aunque a veces sus consecuencias se puedan extender a países vecinos) los más frecuentes en el panorama mundial actual se une que, precisamente por las nuevas tecnologías y por el uso que de ellas hacen tanto algunos Estados como actores y grupos no estatales, hay ocasiones en nuestros días en que «la tradicional frontera entre paz y guerra se ha difuminado dificultando la gradación de las respuestas y la identificación del estado final del conflicto con las ideas clásicas de victoria y derrota»[3].

Por otro lado, las nuevas tecnologías, y entre ellas la llamada *revolución digital,* han motivado una ampliación de los ámbitos de las operaciones, dando lugar a que al lado de los ámbitos clásicos (terrestre, marítimo y aeroespacial), se contemplen actualmente también el ámbito ciberespacial y el denominado ámbito cognitivo (aunque este, basado entre otras cosas en el empleo de técnicas de comunicación, realmente haya existido siempre, en mayor o menor medida).

A esta evolución de los conflictos, con predominio de los conflictos armados de carácter no internacional, con una presencia cada vez mayor de grupos armados no estatales que recurren con frecuencia al terrorismo y a métodos de combate poco convencionales (lo que ha dado lugar a la proliferación de los denominados *conflictos asimétricos*), con un acceso cada vez más fácil a nuevas tecnologías y, por último, con la irrupción cada vez mayor de situaciones que se mueven en una zona ambigua entre la normalidad y el conflicto, tratan de dar respuesta los propios Estados y la comunidad internacional científica y doctrinal, interrogándose básicamente si el estado actual del derecho internacional y en concreto del derecho internacional humanitario es suficiente para regular adecuadamente las operaciones militares en los conflictos actuales o, por el contrario, sería necesario proceder a la negociación, elaboración y aprobación de nuevas normas internacionales que establezcan una regulación adecuada para las nuevas situaciones a que se enfrenta hoy en día la comunidad internacional. A esa preocupación responden algunas iniciativas gubernamentales y no gubernamentales y en ese marco

[3] PDC-01 (A). *Doctrina para el empleo de las FAS*, p. 18, apartado 015.

se encuadran también muchas de las propuestas y trabajos doctrinales que han visto la luz en los últimos años y entre las que podemos mencionar, a título de ejemplo en lengua española, los artículos contenidos en la *Revista Internacional de la Cruz Roja* número 886 (2012), bajo el título «Nuevas Tecnologías y Guerra», los artículos dedicados al tema en la *Revista Electrónica de Estudios Internacionales*[4], en la *Revista Española de Derecho Internacional*[5], en la *Revista Española de Derecho Militar*[6], o en algunos de los trabajos publicados por el propio Instituto Español de Estudios Estratégicos del CESEDEN[7].

Y es en esta misma línea en la que se enmarca el presente estudio, efectuado por el grupo de trabajo que he tenido el honor de presidir y que bajo el título *Límites jurídicos de las operaciones actuales: nuevos desafíos,* trata de acercarnos al concepto y a los problemas que desde el punto de vista jurídico pueden plantear algunos de los medios y métodos de combate caracterizados por su novedad y por la influencia que en ellos tienen las nuevas tecnologías. El grupo de trabajo, compuesto por oficiales del Cuerpo Jurídico Militar, profesores universitarios y juristas, todos ellos académicos correspondientes de la Real Academia de Jurisprudencia y Legislación, se ha centrado en la exposición y en el análisis de una serie de aspectos de las operaciones contemporáneas que tienen una notable actualidad y que se han considerado de interés para las Fuerzas Armadas y para el público en general.

El teniente coronel auditor don Mario Lanz Raggio, profundo conocedor y experto en derecho internacional humanitario, autor de numerosas publicaciones y profesor tanto del Centro de Estudios de Derecho Internacional Humanitario de la Cruz Roja española como del Instituto Internacional de Derecho Humanitario de Sanremo (Italia), explica en el primer capítulo, con el expresivo título de «El conflicto en las sombras: aspectos generales y elementos jurídicos de las operaciones en la zona gris», el concepto y los

[4] Como, por ejemplo, el reciente estudio publicado en el número 37, de junio 2019, «Los sistemas de armas autónomos en la Convención sobre ciertas armas convencionales: sombras legales y éticas de una autonomía ¿bajo control humano?», cuya autora es Reyes JIMÉNEZ SEGOVIA.

[5] Ver, sin ir más lejos, GÓMEZ ISA, Felipe. «Los ataques armados con drones en derecho internacional». *REDI,* Vol. LXVII, 1, 2015, pp. 61-92.

[6] En la que, por lo que respecta al ámbito ciberespacial, merece citarse el trabajo conjunto de la profesora Susana De Tomás Morales, miembro de este grupo de trabajo, y Ana Pilar Velázquez Ortiz: «La responsabilidad del mando en la conducción de operaciones durante la ciberguerra: la necesidad de una adiestramiento eficaz», trabajo que fue galardonado con el Premio Defensa José Francisco Querol y Lombardero 2013 y publicado en la *REDM* número 100, 2013, pp. 117-150; y DÓMINGUEZ BASCOY, Jerónimo: «Ciberguerra y derecho. El «ius ad bellum» y el «ius in bello» en el ciberespacio», publicado en el mismo número de la *REDM* citado, pp. 151-198.

[7] De nuevo a título de ejemplo, y sin propósito exhaustivo, MEZA RIVAS, Milton. «Los sistemas de armas completamente autónomos: un desafío para la comunidad internacional en el seno de las Naciones Unidas». *Documentos de Opinión*, 85/2016, 18 de agosto de 2016.

elementos definidores de lo que él denomina ese *espacio intermedio entre dos realidades opuestas, la del conflicto armado y la de situación de paz*, que se ha dado en llamar la «zona gris», en el que no solo los Estados, sino también actores no estatales, realizan todo un elenco de actividades que bordean los límites de la legalidad internacional, aprovechando sus lagunas o resquicios, con una finalidad o propósito hostil, pero sin llegar al uso de la fuerza armada, de manera que permiten alcanzar los objetivos fijados, dificultando las posibilidades de reacción, en el ejercicio de su derecho a la legítima defensa, de quienes sufren esas acciones. Ambigüedad, opacidad, y el uso de métodos o técnicas como la manipulación informativa, la propaganda, la influencia política o económica caracterizan las operaciones en la zona gris y la aproximan a conceptos vecinos como son los de la guerra y la amenaza híbrida, conceptos que son igualmente examinados por el teniente coronel Lanz, analizando sus diferencias y sus similitudes. Siendo una de las notas características de las operaciones en la zona gris la intención de eludir la aplicación normal de las normas jurídicas, el trabajo continúa con un pormenorizado examen de los ámbitos normativos que se ven afectados de forma más relevante por esas operaciones. De los cuatro ámbitos que se analizan me gustaría destacar aquí el relativo al campo del derecho internacional de los derechos humanos, utilizando las mismas palabras del autor del trabajo, para quien ese campo «se ha revelado como un terreno muy fructífero para el desarrollo de operaciones de *lawfare*[8], lo que unido a las posibilidades que ofrece el uso de la propaganda y la manipulación informativa, concede a los actores de zona gris una oportunidad inmejorable para desacreditar las operaciones de las fuerzas armadas del rival y condicionar de este modo su actuación futura». Y, en efecto, la realidad de los conflictos contemporáneos da toda la razón a esa afirmación. Sin ánimo de extendernos más, diremos simplemente que el capítulo examina otras cuestiones jurídicas del máximo interés como son los posibles medios de reacción, haciéndose hincapié en los recursos de naturaleza jurídica, para finalizar con unas muy fundamentadas conclusiones.

El capítulo segundo lleva por título «Las operaciones militares en el ámbito cognitivo: aspectos jurídicos» y su redacción ha sido encomendada a don Rafael José de Espona, doctor en derecho y vocal de la Sección de Derecho Militar de la Real Academia de Jurisprudencia y Legislación. Para quienes no se hayan familiarizados con los conceptos empleados en el planeamiento y conducción de las operaciones militares actuales, la expresión *ámbito cognitivo,* en su relación con el derecho, no es excesivamente conocida, ni siquiera entre muchos juristas. Tampoco son muchos los estudios que, al menos en

[8] A cuyo concepto alude también el autor en su trabajo, pero adelanto ya que el *lawfare*, expresión que deriva del juego entre las palabras del idioma inglés *law* y *warfare*, sin perjuicio de los debates doctrinales que provoca su definición, se puede conceptuar, de forma muy esquemática y algo simplista, como el uso del derecho como arma o como medio para conseguir un objetivo militar.

español, se han dedicado a analizar sus aspectos jurídicos. De ahí el interés de este capítulo, en la medida en que nos aproxima a una serie de conceptos poco difundidos y se analizan sus implicaciones jurídicas tanto en el plano interno como internacional. A nadie se le escapa la importancia que ha adquirido hoy en día la transmisión y la manipulación de la información, debido como sabemos a la revolución digital, a los avances tecnológicos en el campo de la informática, a la presencia de Internet y a la difusión de las llamadas redes sociales. Son todos estos instrumentos que actúan sobre el ámbito cognitivo, o lo que es lo mismo, sobre la capacidad de percepción de las personas, sobre la que, a su vez, se asienta su capacidad para tomar partido por una u otra opción y adoptar decisiones. De ahí su extraordinaria importancia, dado que el uso de la información o desinformación se puede convertir en un arma de guerra potencialmente decisiva en los conflictos actuales. Y de ahí la complejidad de los problemas jurídicos que se pueden plantear en este ámbito, entre otras cosas porque los instrumentos propios de las operaciones militares en el ámbito cognitivo se pueden utilizar fuera de un conflicto armado, en situaciones de normalidad y, por otro lado, si hablamos de estas operaciones en el marco de un conflicto armado, no se puede olvidar que con frecuencia van dirigidas a producir efectos sobre la población civil, que se encuentra bajo la protección del derecho de los conflictos armados, lo que puede afectar al principio de distinción, uno de los principios básicos y esenciales, como sabemos, del derecho internacional humanitario. Y ello aunque estas operaciones tengan un carácter complementario al uso de la fuerza. Al tratamiento de estos y otros relevantes aspectos se dedica este capítulo.

Los capítulos tercero y cuarto han sido desarrollados, respectivamente, por doña Susana De Tomas Morales, profesora de Derecho Internacional Público en la Universidad Pontificia Comillas-ICADE y por don Jacobo de Salas Claver, abogado en ejercicio y teniente auditor reservista. Ambos capítulos se encuentran íntimamente relacionados puesto que los dos se dedican al estudio y al análisis de los aspectos jurídicos de las operaciones en ese nuevo ámbito que se ha añadido a los tradicionales, el ámbito virtual o ciberespacial, aunque examinadas desde dos perspectivas distintas. En el primero de ellos se analizan los límites jurídicos que afectan a la resiliencia, es decir, a la capacidad para resistir, absorber y recuperarse de los efectos de una amenaza, en este caso una ciberamenaza, haciéndole frente mediante operaciones multiámbito, utilizando medios y métodos tanto convencionales como cibernéticos. Mientras que el capítulo cuarto tiene por objeto las implicaciones jurídicas de las operaciones ofensivas en el ciberespacio. Ambos capítulos responden al interés y a la preocupación que han despertado las operaciones en el ámbito ciberespacial como consecuencia del desarrollo tecnológico producido en este terreno y que se han acentuado a raíz de los acontecimientos acaecidos en Estonia en el año 2007, seguidos por los producidos en el conflicto entre Rusia y Georgia en el año 2008, tras la autoproclamación de la independencia de Osetia del Sur. Esta preocupación, incrementada por la conciencia de que el ciberespacio es un ámbito accesible

a cualquier individuo, que no conoce fronteras y que se encuentra expuesto a una enorme vulnerabilidad, con efectos dañinos potencialmente enormes, ha motivado que incluso algunos Estados, entre ellos España, hayan constituido mandos militares específicos para ocuparse de la ciberdefensa[9]. Y ha dado igualmente lugar a debates políticos y doctrinales sobre la adecuación de las normas del derecho internacional a este tipo de operaciones. Dentro de esos debates doctrinales destacan los que, a iniciativa del Centro de Excelencia de Ciberdefensa de la OTAN en Estonia, han dado lugar al *Manual de Tallín*, en sus dos versiones[10], manual que como indica Jacobo de Salas en el desarrollo de su capítulo, constituye en su versión 2.0 probablemente el documento doctrinal sobre operaciones en el ciberespacio de mayor consenso doctrinal. En cualquier caso, los dos capítulos que se incluyen en el presente trabajo contribuyen al enriquecimiento de este debate doctrinal, siendo ambos, en mi opinión, de un elevado nivel intelectual y siendo de destacar que ambos coinciden en las conclusiones: las operaciones en el ciberespacio, en el marco de un conflicto armado, deben quedar sometidas a las normas del derecho internacional humanitario.

Finalmente, el capítulo quinto, redactado por el teniente auditor don Alfonso López-Casamayor Justicia, analiza los aspectos jurídicos de otro tema de gran actualidad: la legalidad del empleo de las armas letales autónomas. Los sistemas de armas autónomos han suscitado muchísima controversia tanto a nivel ético como a nivel jurídico. La posibilidad de que, sin intervención humana, una máquina sea capaz de decidir cuando y contra quién o contra qué puede utilizar la fuerza y además una fuerza que será normalmente de efectos destructivos enormes, genera muchas dudas desde el punto de visto ético y legal. A la exposición y análisis del concepto de armas autónomas y de sus diferentes clases, así como a un detallado examen de los principales aspectos jurídicos a tener en cuenta en relación a ellas se dedica este interesante capítulo, que nos ofrece también una información actualizada sobre los debates más recientes que sobre estas armas se están llevando a cabo tanto en el seno de la reunión anual de las altas partes contratantes del Convenio sobre Ciertas Armas Convencionales, como en el marco del grupo informal de expertos sobre sistemas de armas autónomas letales.

El capítulo quinto, como todos los anteriores, finaliza con unas conclusiones en las que sus autores recapitulan, de forma resumida, los resultados de su estudio y las deducciones de éste. De su lectura es posible comprobar que, en efecto, la aplicación de las nuevas tecnologías al campo de las operacio-

[9] Mando Conjunto de Ciberdefensa creado por Orden Ministerial 10/2013, de 19 de febrero (*Boletín Oficial del Ministerio de Defensa* número 40, de 26 de febrero de 2013).

[10] La primera edición del *Tallinn Manual on the International Law Applicable to Cyber Warfare* data del año 2013. Esta versión ha sido actualizada y ampliada en el año 2017, mediante la publicación del *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Como es posible apreciar, ya el mismo título del Manual es indicativo de la ampliación de su contenido.

nes militares plantea una serie de cuestiones de tipo técnico, ético y legal que deben ser convenientemente abordadas por la comunidad internacional para evitar consecuencias gravemente perjudiciales. Para enfrentarse a ese desafío, que afecta tanto al desarrollo y empleo de nuevas armas y sistemas de armas como a las nuevas tácticas o métodos de conducción de las operaciones resulta necesario, desde un punto de vista legal, que los Estados se esfuercen en cumplir la obligación que les impone el artículo 36 del Primer Protocolo Adicional a los Convenios de Ginebra, de 8 de junio de 1977, según el cual, cuando estudien, desarrollen, adquieran o adopten una nueva arma o nuevos medios o métodos de combate, los Estados deben comprobar que su empleo en ciertas condiciones o en todas las circunstancias no es contrario al derecho internacional, norma esta que, como mantiene el Comité Internacional de la Cruz Roja, es aplicable a todos los Estados con independencia de que hayan ratificado o no dicho Protocolo[11]. Pero, sin duda, no basta con ello. Como bien indica el teniente coronel Lanz en su trabajo, es necesario también reforzar los sistemas de eficacia de las normas del derecho internacional humanitario para evitar que el empleo de esos nuevos medios o métodos de combate haga irrisoria la protección que sus normas ofrecen a las víctimas de los conflictos armados y, en particular, a las personas civiles y a la población civil. Y, como reflexión final, creo que es necesario igualmente potenciar la concienciación de todos los sectores de la sociedad sobre los riesgos que entraña el desarrollo y empleo de esas nuevas armas y métodos de combate si se hace al margen del derecho y, en particular, del derecho internacional humanitario, que contiene en su seno normas suficientes para su regulación, aunque algunos aspectos, como ocurre con cualquier rama del derecho, puedan siempre ser objeto de mejora. A la idea e intención de aportar un granito de arena, fomentando el debate al respecto en el ámbito doctrinal, responde el presente trabajo, con los capítulos que siguen a continuación.

[11] *Guía para el examen jurídico de las armas, los medios y los métodos de guerra nuevos. Medidas para aplicar el artículo 36 del Protocolo Adicional I de 1977*. Ginebra: Comité Internacional de la Cruz Roja, 2006, p. 4.

Capítulo primero

El conflicto en las sombras: aspectos generales y elementos jurídicos de las operaciones en la zona gris

Mario Lanz Raggio

Resumen

Las menciones a las operaciones desarrolladas en el ámbito de la zona gris son cada vez más abundantes en el ámbito de las relaciones internacionales. En el presente trabajo trataremos de abordar el alcance de dicho concepto, con especial referencia a los aspectos jurídicos que presenta, así como a los posibles mecanismos de reacción frente a los actores internacionales que tratan de aprovecharse de las debilidades del sistema normativo internacional.

Palabras clave

Zona gris, guerra híbrida, *lawfare*, buena fe, resiliencia jurídica.

The conflict in the shadows: general aspects and legal elements of the operations in the gray area.

Abstract

References to the operations carried out in the framework of the gray zone are increasingly more extensive in the field of international relations. In this work we are studying the scope of this concept, with special reference to the legal aspects that it presents, as well as to the possible mechanisms to face the growing attempts of some international actors to take advantage of the weaknesses existing in the international law.

Keywords

Gray zone, hybrid warfare, lawfare, good faith, legal resilience.

Introducción

La transformación que han sufrido los conflictos armados en los dos últimos siglos de la historia de la humanidad ha sido absoluta. Los primeros instrumentos jurídicos que en el siglo XIX asumieron el reto de regular los medios y métodos de combate, así como los que trataron de limitar y establecer condiciones al recurso de los Estados a la fuerza, en el marco respectivamente del *ius in bello* y del *ius ad bellum*, tenían como referencia un fenómeno perfectamente definido: el de la guerra. La característica esencial de dicho fenómeno en la época era su carácter formal, lo que determinaba que el supuesto de hecho que pretendían regular tales normas no dependía más que de la existencia de una declaración formulada al efecto por uno o varios Estados y comunicada de forma oficial.

Si bien ese carácter esencialmente formal de la guerra entra en crisis después de la Segunda Guerra Mundial con la aprobación de la Carta de las Naciones Unidas de 26 de junio de 1945 y de los Convenios de Ginebra de 12 de agosto de 1949 (que dan lugar a la introducción del concepto eminentemente material de conflicto armado), lo cierto es que la aplicación de las normas reguladoras del derecho aplicable a las hostilidades sigue fundamentándose en una clara distinción entre la situación de paz y la de enfrentamiento armado.

A pesar de que las normas del derecho de los conflictos armados no han variado sustancialmente desde la aprobación el 8 de junio de 1977 de los dos primeros protocolos adicionales a los Convenios de Ginebra, lo cierto es que la naturaleza de los conflictos ha experimentado una transformación radical, especialmente después del final de la guerra fría, pudiéndose constatar que los clásicos enfrentamientos armados de carácter interestatal han desaparecido prácticamente de la escena internacional, viéndose sustituidos por conflictos armados de carácter interno en los cuales los actores no estatales han alcanzado un protagonismo esencial. Tales conflictos se caracterizan igualmente por su carácter asimétrico, lo que implica que una de las partes es sensiblemente inferior en capacidad militar a su oponente, obligándole a recurrir a medios no convencionales para poder enfrentarse a él con éxito. Otro factor esencial, tal y como señala De Espona en el capítulo segundo de la presente publicación, es el «global y exponencial incremento tecnológico de redes de telecomunicaciones y de digitalización».

Es por ello, que los nuevos conflictos que han ido surgiendo en los últimos años se caracterizan por su carácter desestructurado, por dar lugar a una cantidad cada vez mayor de víctimas civiles y por librarse principalmente a través de medios y métodos no convencionales, entre los que se encuentra el recurso al terrorismo, los ataques cibernéticos, la propaganda, la mani-

pulación de la información, la «guerra informativa», los ataques al sistema económico o financiero o el *lawfare*[1].

En muchas ocasiones algunos actores tratan de obtener sus objetivos mediante el empleo de recursos que no implican el uso de la fuerza armada y que se encuentran al borde de la legalidad internacional, aprovechando las lagunas existentes en las normas jurídicas en beneficio propio y dificultando la identificación de la amenaza y la adecuada reacción por parte del oponente.

Como consecuencia de todo ello, y dada la dificultad de hacer frente a este entramado de actuaciones con referencia a las normas tradicionales que se contienen en el derecho internacional (pensadas sin duda alguna para situaciones absolutamente diferentes) nos debemos plantear si contamos con las herramientas jurídicas necesarias para poderlas contrarrestar eficazmente.

A pesar de que son numerosos los trabajos que se han venido publicando, especialmente en los últimos tres años, sobre la materia, existen pocos autores que se hayan centrado en su estudio desde el punto de vista del derecho. En el presente trabajo trataremos de examinar desde una perspectiva preferentemente jurídica estas nuevas realidades y las posibles vías para hacer frente a los riesgos que comportan.

La llamada zona gris y las amenazas híbridas

Entre estas nuevas realidades que presenta el escenario internacional nos centraremos, por su importancia, en la definición y características de la llamada zona gris, así como en su relación con otros conceptos afines.

El concepto de la zona gris

En los últimos años ha surgido con fuerza en el ámbito de las relaciones internacionales –y, más concretamente, entre los estudiosos de las cuestiones relacionadas con la paz y seguridad– el término «zona gris» para referirse a una serie de dinámicas por medio de las cuales diferentes actores utilizan en su propio beneficio las lagunas e indefiniciones que presenta el ordenamiento jurídico internacional para lograr así la consecución de unos determinados fines de carácter estratégico.

El uso del referido término, sin embargo, no es exclusivo de este ámbito y se encuentra muy extendido en otros campos para referirse a las situaciones en las que se constata la existencia de una realidad de difícil catalogación

[1] El *lawfare* ha sido definido como «un método de guerra que consiste en el uso del derecho como medio para lograr un objetivo militar». DUNLAP, C. J. «Law and Military Interventions: Preserving Humanitarian Values in 21st Century Conflicts». Carr Center for Human Rights, noviembre de 2001.

con arreglo a las reglas que rigen ordinariamente un determinado sector del conocimiento humano. Normalmente dichas referencias se producen cuando, existiendo una clara dicotomía entre dos conceptos opuestos (blanco y negro) se constata la existencia de una tercera categoría que resulta difícil de catalogar en uno u otro, por lo que se sitúa en un lugar incierto e indefinido (zona gris) entre ambos. Se habla así, por ejemplo, de zona gris, para hacer referencia en el ámbito de la política a aquellos espacios que se encuentran en un punto indeterminado entre lo público y lo privado; o, en el de la economía, en lo que se refiere a los supuestos intermedios entre la liberalización y el control estatal de la actividad económica.

En el mundo del derecho, el concepto de zona gris se ha empleado también de forma profusa, haciendo referencia generalmente a aquellos espacios en los que la aplicación de la norma no resulta clara y evidente.

Más específicamente, y ya dentro el ámbito del derecho internacional, la citada expresión ha sido empleada tradicionalmente para referirse a aquellas áreas jurídicas «que se sitúan en las áreas colindantes del derecho de la paz y del derecho de la guerra», y en las que sería procedente «la aplicación acumulativa del derecho de los derechos humanos y el derecho internacional humanitario, garantizando, de ese modo, al menos la aplicación de un mínimo de normas humanitarias»[2].

No obstante, y como se ha indicado anteriormente, el alcance de la expresión en el ámbito de las relaciones internacionales y, más específicamente, del estudio de las nuevas amenazas en materia de seguridad y defensa, se refiere a la existencia de un espacio intermedio entre dos realidades opuestas, la del conflicto armado y la de la situación de paz, cuya delimitación resulta esencialmente incierta. Precisamente las notas de ambigüedad e indeterminación de tales ámbitos son los factores de los que se sirven algunos actores en el plano internacional para utilizar en su beneficio los posibles resquicios de la legalidad internacional, utilizando una variedad de instrumentos alternativos a la fuerza armada (entre otros, de índole económica, legal, o propagandística), con vistas a la consecución de un fin determinado sin el coste que implicaría el recurso a la fuerza militar.

Como ejemplos de estas prácticas, se ha venido señalando las actividades desarrolladas por Rusia en Crimea y en los territorios de Donetsk y Lugansk, el expansionismo de China en el mar de la China Meridional o la estrategia de Irán en Siria, además de las llevadas a cabo por grupos no estatales como Boko Haram o el Dáesh.

Una definición de partida muy útil, por su simplicidad, para empezar a comprender el alcance de este concepto es la empleada por el Mando de

[2] ROSSAS, V. Allan y MERON, Theodor. «Combatting lawlessness in grey zone conflicts through minimum humanitarian standards». *American Journal of International Law*. Vol. 89, n.º 2, 1995, p. 215.

Operaciones Especiales de los Estados Unidos, que la califica como «una interacción competitiva entre un Estado y actores no estatales que se encuentra entre la dualidad tradicional entre la guerra y la paz»[3]. Como se puede ver el elemento central de la definición es la dualidad a la que anteriormente nos hemos referido, entre lo negro y lo blanco, entre la guerra y la paz, elemento este que es una constante en la práctica totalidad de los estudios que han venido realizándose hasta la fecha[4].

Esta definición básica, sin embargo, debe ser completada necesariamente con un conjunto de elementos adicionales que nos permitan una mejor aproximación al concepto, haciendo referencia –por un lado– a los fines que la impulsan, –por otro– a los medios empleados y a su naturaleza y –por último– a los sujetos que protagonizan tales actividades. De esta forma, la definición contenida en el informe de la Junta Asesora en materia de Seguridad Internacional del Departamento de Estado de los Estados Unidos afina más el concepto, precisando que «el término zona gris se caracteriza por el uso de técnicas dirigidas a obtener los objetivos estratégicos de una nación y a frustrar los de sus rivales, empleando instrumentos de poder –a menudo de carácter asimétrico y ambiguo– distintos al uso de las fuerzas militares regulares»[5].

Más completa aún resulta la definición que nos ofrece Brands, quien la conceptúa como «una actividad que, siendo por naturaleza coercitiva y agresiva, se encuentra intencionadamente diseñada para mantenerse por debajo del umbral de los conflictos armados convencionales»[6]. Las actividades desarrolladas en el ámbito de la zona gris son monopolio de lo que se viene a llamar «poderes revisionistas», que buscan alterar algunos de los aspectos que conforman la legalidad internacional, si bien eludiendo, por razones de conveniencia, el recurso a la fuerza militar[7]. De esta forma los referidos actores serían capaces de obtener beneficios estratégicos de distinta naturaleza, según el caso, que serían equivalentes a los que habitualmente se asocian a una victoria militar.

---

3 KAPUSTA, P. «The Gray Zone». *U. S. Special Operations Command White Paper*. Septiembre de 2015, p. 1.

4 VOTEL, Joseph L.; CLEVELAND Charles T.; CONNETT, Charles T. e IRWIN, Will. «Unconventional Warfare in the Gray Zone». *Joint Force Quarterly* 80, enero de 2016; ELKUS, Adam. «Shades of Gray: Why the Gray Wars Concept Lacks Strategic Sense». Informal Institute for National Security Thinkers and Practitioners, diciembre de 2015; o FREIER, Nathan P. «Outplayed: Regaining Strategic Initiative in the Gray Zone». United States Army War College Press, junio 2016.

5 International Security Advisory Board: Report on Gray Zone Conflict, enero de 2017, p. 1.

6 BRANDS Hal. «Paradoxes of the Gray Zone». Foreign Policy Researc Institute, febrero 2016.

7 Estos poderes revisionistas buscan modificar el orden establecido a su conveniencia, pero no pretenden su destrucción, tal y como buscan otros actores que podríamos calificar como radicales (MAZARR, M. «Mastering the Gray Zone: Understanding a Changing Era of Conflict». Carlisle, PA: United States Army War College Press, 2015).

Estos mismos elementos se incluyen en la definición aportada por Hoffman, para quien las actividades propias de este concepto «se caracterizan por su naturaleza encubierta e ilegal, pero que se mantienen debajo del umbral de la violencia armada organizada. Tales actividades, que incluyen la perturbación del orden, la subversión política, las operaciones psicológicas, el abuso del derecho y la corrupción económica, forman parte de un plan elaborado para la consecución de una ventaja estratégica»[8]. Por su parte, para Mazarr, los conflictos que se desarrollan en la zona gris son aquellos en los que un determinado actor se involucra en un nuevo tipo de guerra que busca la alteración del orden internacional, empleando y combinando elementos de poder de mayor o menor intensidad, pero siempre de una forma no convencional, de modo que resulta difícil para el adversario responder adecuadamente[9].

Un elemento, a nuestro juicio, de gran transcendencia para completar el concepto, especialmente a la hora de proceder a su análisis desde un punto de vista jurídico, es el relativo a la incompatibilidad de las acciones que se suceden en la zona gris con el principio de buena fe que rige en las relaciones internacionales. Así, y tal como acertadamente señala Baqués, tales actuaciones se caracterizan por la «presencia de dinámicas de conflicto alejadas de las guerras convencionales que, a su vez no se limitan a las acciones propias de las HW (guerras híbridas), sino que incluyen medidas que ni siquiera contemplan el empleo de la fuerza armada. Medidas que, a pesar de este último dato, difícilmente pueden quedar integradas en la lógica de la *bona fide* que rige en el derecho internacional y en las relaciones internacionales en tiempo de paz»[10].

Por lo que se refiere al ámbito subjetivo de la cuestión, a pesar de que en la definición inicial que se ha planteado como punto de partida se hace referencia únicamente a las actuaciones en la zona gris protagonizadas por actores estatales, la doctrina es pacífica a la hora de estimar que tales actividades pueden ser desarrolladas también por actores no estatales.

Existen autores que sostienen que las operaciones en la zona gris son exclusivas de los anteriormente mencionados Estados y grupos revisionistas. Así, Fitton sostiene que las estrategias de zona gris se emplean exclusivamente por parte de los «Estados no liberales y los actores no estatales de carácter autoritario», que se aprovechan de las dificultades que presentan las sociedades occidentales, basadas en el pluralismo y en el imperio de la ley, para hacer frente a sus acciones[11]. Siguiendo la referida tesis, la des-

---

8 HOFFMAN, F. G. «Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges». *Prism National Defense University*. Vol. 7, n.º 4, noviembre de 2018.

9 MAZARR, M. *Op. cit.,* p. 4.

10 BAQUÉS, J. «Hacia una definición del concepto "Gray Zone" (GZ)». Instituto Español de Estudios Estratégicos, abril 2017, p. 12.

11 FITTON, O. «Cyber Operations and Gray Zones: Challenges for NATO». *Connections: The Quarterly Journal*. Abril de 2016, p. 113.

vinculación de este tipo de Estados con tales principios les permite acoger tales estrategias, a diferencia de lo que ocurre con los Estados occidentales, que se encontrarían prisioneros de su compromiso con las normas éticas y jurídicas que rigen las relaciones internacionales y, especialmente, con los dictados de la opinión pública. Siendo parcialmente cierta tal consideración, en lo relativo a la mayor vulnerabilidad de las sociedades occidentales ante un «conflicto» suscitado en la esfera a la que estamos aludiendo, a nuestro juicio no resulta ni exacto ni realista excluir por definición la intervención activa de los Estados occidentales en estas dinámicas. En efecto, el uso de tales métodos por parte de los países de occidente y, particularmente por los Estados Unidos, ha sido puesto de manifiesto por autores de diferentes tendencias y nacionalidades, como Brooks, que admite que el propio gobierno de los Estados Unidos ha utilizado dichas tácticas a la hora de argumentar la legitimidad de sus acciones armadas contra dirigentes de diversos grupos en el marco de la llamada «guerra al terrorismo», o al sostener la inaplicabilidad de las disposiciones de los Convenios de Ginebra a los detenidos de Al Qaeda y la consecuente legalidad de las medidas de privación de libertad adoptadas contra los mismos[12]. El uso de estas mismas técnicas ha sido igualmente denunciado en el caso del arresto en Canadá, a instancias del gobierno de los Estados Unidos, de la empresaria china Meng Wanzhou, bajo la acusación de haber incumplido el régimen de las sanciones impuestas a Irán[13]. De igual forma, fuentes oficiales rusas han denunciado el uso por parte de Estados Unidos en Siria de las mismas técnicas que –paradójicamente– le han sido imputadas por los norteamericanos en el mismo territorio[14].

Por otro lado, y a pesar de que el término zona gris en la acepción que estamos examinando es –como se dijo– muy reciente, lo cierto es que la utilización por parte de los contendientes de métodos no convencionales de todo tipo para tratar de doblegar la voluntad del adversario es tan antigua como la guerra misma, constituyendo, como afirma James, una regla de la guerra más que una excepción[15]. Lo que sí es innegable es el hecho de que tales medidas y actuaciones, que constituían habitualmente un complemento que coadyuvaba, en mayor o menor medida, a la obtención de los fines estratégicos, reforzando el éxito de las operaciones militares convencionales, se han

[12] BROOKS, R. «Rule of Law in the Gray Zone». Modern War Institute, West Point, julio de 2018, disponible en https://mwi.usma.edu/rule-law-gray-zone/. Fecha de la consulta 23/01/2019. Ver también MATISEK, J. W. «Shades of Gray Deterrence: Issues of Fighting in the Gray Zone». *Journal of Strategic Security*. Volumen 10, n.º 3, 2017, p. 3.

[13] KAI, J. «The Long Arm of the US Law: A New 'Gray Zone' Tool Against China?». *The Diplomat.* Diciembre de 2018.

[14] BĒRZIŅŠ, J. «Gerasimov, the Experience in Syria, and Hybrid» Warfare». *Strategy and Economics Blog.* Marzo de 2016. Además, GOLDSMITH, J. y HATHAEAY, O. «Bad legal Arguments for the Syria Airstrikes». *Lawfar.* Abril de 2018.

[15] JAMES III, Nicholas M. «US Army Forces in Gray Zone conflict». School of Advanced Military Studies, United States Army Command and General Staff, marzo de 2017, p. 3.

convertido hoy en día en un elemento principal, hasta el punto de que, en la mayor parte de las ocasiones, viene a sustituir completamente al uso de la fuerza militar.

Elementos caracterizadores

En la zona gris coexiste un conjunto entremezclado de métodos diversos en su naturaleza y alcance, lo que determina que no sea sencillo clasificar cada caso concreto, o proceder a la fijación de categorías universales que faciliten la catalogación de tales fenómenos y la consecuente adopción de las medidas correspondientes. Por ello, y tal y como sostiene el propio James, debido a la complejidad, ambigüedad y naturaleza emergente de dichos fenómenos, la mejor forma de describirlos es por referencia a las características más destacadas y al contexto en el que se producen[16]. Siguiendo el referido criterio, debemos destacar las siguientes notas definitorias:

Ambigüedad

Es tal vez el elemento más relevante de los que caracterizan las actuaciones propias de la zona gris. En efecto, el sujeto activo de tales actividades busca intencionadamente la ambigüedad en lo relativo a sus fines y a las medidas emprendidas para su consecución, dificultando así de forma muy significativa la posible reacción por parte del oponente y, en muchas ocasiones, anulándola. Matisek ha descrito esta característica como una forma «nebulosa» de actuación que, «sin vulnerar explícitamente el sistema vigente tras la guerra fría ni las normas y valores internacionalmente reconocidos», trata de obtener un beneficio amparándose en tal indeterminación[17].

Por otro lado, se ha señalado con razón, que a pesar de que las actuaciones están preordenadas para no traspasar las «líneas rojas» que legitimarían una respuesta armada por parte del adversario, lo cierto es que para que una situación concreta excediera de lo que es el plano normal y legítimo de las relaciones internacionales y se adentrara en el ámbito de la zona gris se precisaría emplear un cierto «nivel de agresión»[18]. De esta manera, las actividades propias de la zona gris, siendo «coercitivas y agresivas por naturaleza», se disfrazan y se llevan a cabo de forma ambigua para mantenerse por debajo del umbral de respuesta armada[19].

El componente jurídico es uno de los elementos básicos de esta ecuación en lo que se refiere a los caracteres de ambigüedad y opacidad. Las normas,

16 JAMES III, N. M. *Op. cit.,* p. 4.

17 MATISEK, J. W. *Op. cit.,* p. 7.

18 KAPUSTA, P. *Op. cit.,* p. 3.

19 BRANDS Hal. *Op. cit.,* p. 1.

tanto de ámbito nacional como internacional, convencionales o consuetudinarias, se aplican a un supuesto de hecho que se pretende lo más definido y concreto posible, para asociarle a continuación unas determinadas consecuencias jurídicas. Con arreglo al referido esquema, el derecho crea una serie de categorías, procede a su catalogación y les dota de una regulación concreta.

Así, cuando el derecho internacional regula los límites al recurso a la amenaza o al uso de la fuerza armada configura un sistema jurídico en el que asigna a los actos que exceden de los límites impuestos una consecuencia jurídica: la ilicitud de tales actos y la activación de los mecanismos de legítima defensa y de seguridad colectiva.

De igual forma, y si acudimos a un ejemplo propio del *ius in bello*, las disposiciones del DIH contienen un conjunto de disposiciones reguladoras del estatuto del combatiente que determinan la aplicación de un estatuto específico que le autoriza a participar en las hostilidades, con el consiguiente reconocimiento de la condición de prisionero de guerra, a la vez que les impone una serie de obligaciones, como la de distinguirse de la población civil o respetar las leyes y usos de la guerra. Es decir, crea una categoría determinada y le asigna una regulación jurídica propia, en la que normalmente integra un conjunto diverso de derechos y obligaciones que conforman un estatuto específico.

Pues bien, el problema surge cuando de forma intencionada se altera ese equilibrio y se fuerza el contenido de las referidas categorías, tratando de evitar la aplicación de una consecuencia jurídica indeseada mediante técnicas de manipulación, ocultación y engaño que se dirigen a integrar una determinada actuación en una categoría jurídica que no es la apropiada. Mediante las citadas actuaciones se pretende aplicar a las estrategias emprendidas en el ámbito de la zona gris las normas que rigen en las relaciones normales de paz entre los Estados o, en el ejemplo del *ius in bello* anteriormente citado, procurar obtener los beneficios de la categoría de combatientes sin cumplir con alguna o con la totalidad de las obligaciones inherentes a tal condición, o simplemente con el fin ocultar la participación activa de un Estado en un conflicto[20].

Las mencionadas estrategias dan lugar, paralelamente, a que la respuesta del oponente se vea obstaculizada, al no ser capaz de analizar y afrontar la situación mediante la subsunción de los acontecimientos en alguna de las categorías jurídicas previamente establecidas, condicionando y limitando así de forma muy importante su posible reacción. De esta forma, y tal y

[20] Un ejemplo paradigmático de este último supuesto es el despliegue en territorio de Ucrania durante el conflicto que tuvo lugar en 2014 de unidades militar cuyos integrantes, conocidos como los «hombrecillos verdes (*little green men*)» no mostraban distintivo alguno de nacionalidad, existiendo evidencias más que fundadas de que se trataba de tropas regulares rusas pertenecientes a una unidad de operaciones especiales.

como señala Brooks: «Cada vez se hace más difícil la aplicación de conceptos jurídicos básicos relativos a la guerra y al uso de la fuerza de una forma coherente»[21]. En efecto, en las actividades llevadas a cabo en la zona gris normalmente se hace muy difícil determinar qué se puede considerar un medio de combate: ¿un ordenador?, ¿un programa informático?, ¿una emisora de radio?, ¿una noticia falsa?, ¿un avión civil secuestrado? Lo mismo sucede a la hora de identificar una acción hostil, como por ejemplo un ataque cibernético al sistema bancario de un Estado o una acción disimulada en el marco del apoyo a las fuerzas disidentes de otro país. También en el ámbito del *ius in bello* nos encontramos con idénticas dificultades, por ejemplo, a la hora de aplicar el principio de distinción en el ámbito de las operaciones en el ciberespacio o a la hora de determinar si un individuo que está realizando actividades de agitación política o dirigidas a socavar el sistema financiero está participando activamente en las hostilidades.

Este conjunto de situaciones que se caracterizan por su indeterminación constituye el elemento central del que se aprovechan los actores que operan en la zona gris, explotando las lagunas legales existentes para eludir la responsabilidad de sus actos, de conformidad con las consecuencias jurídicas previstas en la norma, y para minimizar las consecuencias políticas, económicas e incluso militares que pudieran derivarse de sus acciones. En el citado contexto, los citados actores «explotan la función estabilizadora de la norma, al objeto de obtener una ventaja militar sobre su adversario»[22]. La forma de proceder de los citados actores se basa en la pretensión de eludir el cumplimiento de las expectativas ordinarias que se derivarían de la interpretación razonable y de acuerdo a la buena fe de las normas y principios legales, y todo ello, a través de una serie de medidas entre las que se encuentra principalmente la instrumentalización de las posibles debilidades o lagunas que puedan hallarse en los marcos normativos existentes, pero que también pueden llegar al incumplimiento frontal de alguna norma internacional. En todo caso, y este es un factor esencial, el responsable de la planificación de las actividades de zona gris, fundamenta su estrategia en la presunción de que sus rivales no van a romper con su línea de fidelidad y respeto al marco normativo establecido.

Por último, un elemento de especial trascendencia que no debemos dejar de tener presente es la especial vulnerabilidad del sistema jurídico internacional frente a los intentos de desestabilización y de aprovechamiento de las debilidades e incertidumbres que presenta. En este orden de cosas, conviene precisar que tanto las normas de derecho internacional como las del derecho interno son susceptibles de convertirse en objeto de manipulación

21 BROOKS, R. *Op. cit.,* p. 3.

22 SARI, A. «Hybrid warfare, law and the Fulda Gap». Complex Battle Spaces (Michael Schmitt, Christopher Ford, Shane Reeves & Winston Williams). Oxford University Press, 2017, p. 165.

interesada y abusiva por parte de los actores de la zona gris. No obstante, el ordenamiento jurídico interno dispone de herramientas mucho más definidas y eficaces para evitar el abuso de sus disposiciones que el sistema normativo internacional. En efecto, la capacidad de resistencia de este último ordenamiento se ve afectado por una característica inherente al mismo y que forma parte de su propia naturaleza, que consiste en la falta de sistemas verdaderamente eficaces de arreglo de las controversias y de mecanismos que permitan imponer coercitivamente sus normas.

De esta forma, el ordenamiento interno dispone de mecanismos administrativos y judiciales para determinar la ley aplicable y establecer las pautas necesarias para la adecuada interpretación de sus disposiciones, a la vez que cuenta con el poder coercitivo del Estado para imponer, en su caso, el cumplimiento forzoso de las normas y las resoluciones que se dicten. En cambio, el derecho internacional es un ordenamiento imperfecto por naturaleza, donde no existen sistemas de eficacia comparables en intensidad a los de ámbito estatal. Además, los mecanismos de los que dispone son de carácter esencialmente reactivo, y no preventivo, por lo que no pueden actuar hasta que se ha producido efectivamente la lesión al bien jurídico.

Todas estas características determinan que el ámbito de las leyes internacionales resulte especialmente vulnerable a los intentos de manipulación del sistema, ya que a todas luces dispone de unos medios de reacción considerablemente limitados en número y en intensidad, y que, además, se encuentran notablemente mediatizados por intereses políticos.

Opacidad

Precisamente, y como se ha señalado anteriormente, la intencionada indefinición de los modos en el actuar del sujeto activo se complementa con el interés de éste en eludir o minimizar su grado de implicación, así como de ocultar las finalidades perseguidas y los métodos de los que se sirve. Así, según Matisek, el actor «busca obtener victorias políticas limitadas», evitando llevar a cabo acciones militares explícitas, «que resultarían más sencillas de identificar y de responder adecuadamente» por parte del adversario[23]. Es por ello por lo que resulta habitual el recurso a operaciones de baja visibilidad, tratando en la medida de lo posible de no dejar rastro o huella alguno[24].

Para favorecer su opacidad las estrategias que se siguen se salen de la esfera convencional, utilizando medios como ataques cibernéticos, propaganda política, agitación social, coacción económica, sabotaje tecnológico, o em-

[23] MATISEK, Jahara W. *Op. cit.,* p. 4.

[24] VOTEL, Joseph L. *Op. cit.,* p. 112.

pleo de fuerzas formalmente ajenas (*proxies*). En este contexto, el empleo de medios militares se rebela como secundario, quedando limitado a un papel «fundamentalmente simbólico, con intención coercitiva, utilizándose para señalar, intimidar y marcar territorios; y excepcionalmente para respaldar a actores que sí recurren a la fuerza y en ocasiones a gran escala en el marco de una guerra por delegación»[25].

Tales medidas casi siempre se encuentran envueltas en procesos de desinformación y enmascaramiento, desarrollándose de forma que se dificulta la identificación del actor que es el responsable final de las mismas[26].

Intencionalidad

Aunque no se trata de una característica señalada de forma específica entre los distintos autores que han abordado el estudio de la materia, no se debe olvidar –especialmente si pretendemos analizar la cuestión desde una óptica jurídica– que la ambigüedad y opacidad de las actuaciones seguidas en la zona gris son circunstancias intencionadamente buscadas por sus responsables, extendiéndose tal elemento volitivo al alcance los resultados pretendidos, es decir, a impedir una respuesta eficaz del adversario y, en última medida, a obtener la finalidad estratégica.

Dentro de este elemento intencional resulta especialmente relevante hacer mención de la importancia del ánimo «fraudulento» que caracteriza la actuación del actor en las acciones de zona gris. Ya hemos señalado con anterioridad al referirnos al concepto, que hay autores como Baqués o Jordán que se refieren explícitamente a la contravención del principio de la buena fe que debe regir en las relaciones internacionales como uno de los elementos relevantes del concepto[27]. Así las cosas, las actuaciones en zona gris, si bien tratan de evitar a toda costa traspasar los límites establecidos, no pueden catalogarse como manifestaciones ordinarias, regulares y legítimas de las relaciones internacionales, siendo precisamente la transgresión del principio de buena fe el elemento que impide otorgarles tal consideración.

El citado principio, que se contiene en el artículo 2.2 de la Carta de las Naciones Unidas, y ha sido desarrollado en la Resolución 2625 (XXV) de la Asamblea General y en resoluciones de distintas instancias internacionales, constituye un elemento estructural básico del ordenamiento internacional. Para Carrillo Salcedo «La buena fe [...] es un principio fundamental de todo

---

25 JORDÁN, J. «El conflicto internacional en la zona gris: una propuesta teórica desde la perspectiva del realismo ofensivo». *Revista Española de Ciencia Política*. N.º 48, p. 132, noviembre de 2018.

26 BRANDS Hal. *Op. cit.,* p. 2.

27 BAQUÉS, J. *Op. cit.,* p. 12. JORDÁN, J. *Op. cit.,* p. 132.

sistema jurídico y en derecho internacional lleva a cabo una función de extraordinaria importancia: servir de límite a la discrecionalidad del Estado soberano en el ejercicio de sus competencias, corregir los posibles abusos del Estado en la apreciación del alcance de sus derechos y obligaciones jurídicas internacionales»[28].

En íntima relación con la vigencia del aludido principio se encuentra el concepto de prohibición del abuso de derecho, elemento este que, pese a que su origen ha de situarse en el ámbito del derecho interno, se ha visto extendido al campo del derecho internacional, habiendo sido expresamente recogido en diferentes resoluciones de tribunales internacionales como la expresión negativa del principio de la buena fe[29]. De igual forma, la prohibición ha sido igualmente recogida en distintas normas convencionales, como es el caso del artículo 17 del Convenio Europeo de Derechos Humanos.

Pues bien, el ejercicio abusivo del derecho, buscando de forma interesada la aplicación de categorías y de consecuencias jurídicas distintas a las que se derivarían de la aplicación regular de las normas y principios que rigen el orden internacional, constituye precisamente el fundamento de la actuación de los actores de zona gris.

En otro orden de cosas, cabe señalar que la finalidad perseguida por el sujeto activo puede ser de muy diversa naturaleza: entre otras, la subversión del orden establecido en un país concreto, la anexión de un territorio, el reconocimiento internacional de una situación concreta, o el debilitamiento de las naciones «enemigas». En todo caso, los beneficios estratégicos que se persiguen por esta vía se aproximan a los que podrían derivarse de una victoria en el campo de batalla.

Gradualidad

La forma de consecución de los citados objetivos suele ser gradual, de forma que los actores que explotan la zona gris emplean de forma planificada y secuencial las acciones necesarias mediante «pasos graduales que aseguran la consecución del objetivo estratégico perseguido»[30]. El uso gradual de diferentes instrumentos facilita la consecución de los objetivos propuestos, a la vez que dificulta la reacción del adversario, al que obliga a enfrentarse a un conjunto heterogéneo de actividades hostiles en mayor o menor medi-

[28] CARRILLO SALCEDO, J. A. *Soberanía del Estado y derecho internacional*. Tecnos, 1976, p. 169.

[29] Asunto relativo a «ciertos intereses alemanes en la Alta Silesia polaca y asunto relativo a las zonas francas de la Alta Saboya y del País del Gex».

[30] MAZARR, M. *Op. cit.,* p. 75.

da, pero que individualmente consideradas nunca superan el umbral de la agresión armada.

Relevancia del uso de las nuevas tecnologías

Aunque muchas de las prácticas que se integran en las actividades de la zona gris, tales como la propaganda, la influencia política o económica o la desestabilización son elementos clásicos que se encuentran presentes en el ámbito de los conflictos entre las colectividades humanas desde muy antiguo, resulta evidente que el desarrollo de los sistemas tecnológicos, así como de los medios de comunicación y redes sociales ha creado nuevas vulnerabilidades, incrementando exponencialmente las posibilidades de éxito de las actividades de dicha naturaleza. Y ello no solo porque hayan surgido mecanismos de gran potencial de daño y fácil uso, como pueden ser los ciberataques, sino especialmente porque las nuevas tecnologías en el ámbito social e informativo permiten explotar de forma muy eficaz los resultados de las acciones llevadas a cabo por cualquier otro medio, multiplicando así sus efectos y contribuyendo de forma decisiva al éxito global en la consecución de los objetivos estratégicos pretendidos.

Por otro lado, en este mundo cada vez más inmerso en los recursos tecnológicos, las cuestiones relacionadas con la ciberseguridad han alcanzado particular relevancia. En efecto, la inmensa mayoría de las actividades esenciales que se llevan a cabo en las sociedades modernas (desde la medicina hasta la economía, los transportes, el sistema bancario, los sistemas de seguridad, o los procedimientos electorales) se caracterizan por mantener una altísima dependencia en su funcionamiento respecto de los sistemas informáticos que les prestan servicio, sistemas que además se han rebelado ciertamente vulnerables. Dicha circunstancia ha dado lugar a que la seguridad de tales sistemas ante posibles ataques se haya convertido en una de las principales prioridades de los gobiernos, pese a lo cual es innegable que el ciberespacio se ha convertido en uno de los medios más propicios para el desarrollo de acciones de zona gris.

Desigualdad intrínseca

La desigualdad es una circunstancia que, a la vez que constituye la causa generadora de estas dinámicas, condiciona de forma importante su desarrollo. Así, resulta evidente que los actores que recurren a estos procedimientos se encuentran en una situación de inferioridad frente a sus oponentes, razón esta que les desaconseja acudir al uso de la fuerza, decantándose en su lugar por procedimientos que, aunque de naturaleza más indirecta, les permite obtener unos beneficios suficientes para la consecución de sus fines.

Sentado lo anterior, es igualmente evidente que esta desigualdad se muestra asimismo en un plano radicalmente opuesto y que se centra en el hecho de que los Estados occidentales se encuentran más vinculados por el cumplimiento de las normas tanto nacionales como internacionales, por el posicionamiento de la opinión pública, o por la vigencia de ciertos valores éticos, que otro tipo de Estados, entre los que suele citarse a China o Rusia, o que ciertas organizaciones no estatales. Dicha circunstancia determina que el margen de acción o de respuesta de los primeros resulte mucho más reducido, lo que genera una situación de desventaja en el «enfrentamiento» en zona gris del que indudablemente se benefician los Estados y grupos no estatales que lo promueven. Por esta razón, Schmitt ha acuñado el término *asymetric lawfare* para definir el uso de técnicas de zona gris, que tiene su fundamento en el hecho de que los países comprometidos con la aplicación regular de las normas del ordenamiento jurídico internacional son mucho más reticentes a la hora de aplicar tales estrategias[31].

Dificultad de respuesta

La mayor capacidad militar de un determinado Estado o alianza militar se revela absolutamente ineficaz para poner freno a las amenazas surgidas en este ámbito. Al actuar al margen de la lógica binaria clásica, los poderes revisionistas que impulsan las acciones en zona gris eluden la superioridad militar y tecnológica de sus rivales y les fuerzan a hacer frente a la situación en un ámbito que les causa acusadas incertidumbres en lo relativo a la identificación de la naturaleza de la amenaza y a la definición de las posibles respuestas.

Zona gris, guerras híbridas y amenazas híbridas

Aunque el objeto del presente trabajo no es el de profundizar en las diferencias terminológicas y conceptuales de las nuevas estrategias de conflicto surgidas tras la guerra fría, sino el de analizar la cuestión desde un punto de vista jurídico, sí resulta conveniente precisar la diferencia existente entre la zona gris y otros conceptos de uso generalizado en la doctrina.

En este orden de cosas, también en los últimos años se han incorporado a los estudios elaborados en este ámbito doctrinal los conceptos de guerra híbrida y de amenaza híbrida. El primero de estos conceptos está evidentemente relacionado con el de la zona gris, en la medida en que el actor explota los elementos de opacidad, ambigüedad e indeterminación, llevando a cabo acciones que normalmente se mantienen en el límite del conflicto, pero traspasando ocasionalmente dicho límite.

---

[31] SCHMITT, Michael N. «Grey Zones in the International Law of Cyberspace». *The Yale Journal of International Law*. Octubre de 2017.

La guerra híbrida puede ser así descrita como «la conjunción de actividades planeadas, coordinadas y controladas de forma centralizada, que incluye tanto acciones convencionales como no convencionales, llevadas a cabo por actores militares y no militares, y que se desarrollan en ámbitos como el conflicto tradicional, las operaciones de inteligencia e influencia, la seguridad económica y financiera, la seguridad energética y el ciberespacio»[32]. Por su parte, para Hoffman, los actores de la guerra híbrida combinan medios de guerra convencionales, tácticas irregulares, terrorismo y criminalidad en sus operaciones, de forma que consigue «aunar la alta letalidad y poder destructivo de un conflicto estatal, con el fanatismo y el prolongado fervor de la guerra irregular»[33].

En todo caso, y desde un punto de vista jurídico, el concepto de guerra híbrida implica importantes desafíos especialmente para el derecho internacional, precisamente como consecuencia de la fusión entre medios tradicionales y no tradicionales que implica.

Hay autores como Carment que consideran incluso que los dos conceptos, a pesar de no ser sinónimos, forman parte de la misma estructura, en la medida en que la zona gris haría referencia a los objetivos estratégicos, mientras que la guerra híbrida implicaría la materialización de tales estrategias a nivel táctico, empleando medios preferentemente fuera de la línea de conflicto, pero también, de ser ello necesario, otras medidas que impliquen ya el uso de la fuerza, traspasando dicha línea[34]. Es evidente, así, que aunque la explotación de las zonas grises no requiere específicamente del uso de mecanismos propios de la guerra híbrida, en muchas ocasiones la materialización de los objetivos estratégicos perseguidos aconseja la adopción de tales medidas como complemento a las actividades no convencionales que las han precedido.

En todo caso, y tal y como acertadamente pone de manifiesto Martínez Valera, entre la zona gris y la guerra híbrida existe un común denominador, «en el sentido que ambas comparten capacidades comunes, militares y no militares, que le habilitan para plantear una GZ o una HW, simultáneamente en diferentes escenarios o una como continuación de la otra, en función de la estrategia elegida»[35].

---

32 MORALES MORALES, S. «Quo vadis... la guerra a través de herramientas no convencionales». *Revista general de marina*. Marzo de 2017.

33 HOFFMAN, F. G. «Conflict in the 21st Century: The Rise of Hybrid Wars». Potomac Institute for Policy Studies, 2007, p. 38.

34 CARMENT, D. «War's Future: the risks and rewards of grey-zone conflict and hybrid warfare». Canadian Global Affairs Institute, octubre 2018, p. 1.

35 MARTÍNEZ VALERA, G. «Actores no estatales en zona gris. Las organizaciones de carácter violento y crimen organizado transnacional». Instituto Español de Estudios Estratégicos, octubre 2018, p. 6.

Por otro lado, esta similitud de los medios y tácticas empleados determina que las cuestiones legales que surgen de ambos fenómenos sean sustancialmente iguales, de modo que, tanto en uno como en otro escenario, el adversario «emplea argumentos jurídicos con el fin de legitimar su propio comportamiento y así incrementar su capacidad de acción, a la vez que intenta deslegitimar las acciones de su rival, reduciendo así su libertad de actuación»[36].

«El conflicto híbrido y la guerra híbrida serían así dos categorías específicas dentro de las tácticas híbridas de las que se puede valer un Estado para alcanzar sus objetivos estratégicos»[37]. La diferencia entre las dos categorías se centraría esencialmente en el hecho de que el conflicto híbrido no implica de ningún modo el uso de la fuerza armada, empleándose en su lugar una serie de acciones de carácter político, económico, diplomático o propagandístico, mientras que en el segundo sí se contemplan actuaciones de uso de fuerza, en conjunción con otras de distinta naturaleza como las anteriormente apuntadas.

Es por ello, que debemos entender que las estrategias de zona gris son un elemento que forma una parte esencial en la naturaleza y alcance de las amenazas híbridas, sean estas de la naturaleza que sean. Por tal razón, resulta conveniente adoptar el concepto más amplio de amenaza híbrida como referencia a la hora de estudiar, tanto los espacios donde las referidas estrategias actúan con mayor eficacia, como las posibles medidas de reacción que se pueden emplear para neutralizarlas.

Este mismo enfoque es el seguido en la *Estrategia de Seguridad Nacional de 2017*, que emplea el término acciones híbridas para referirse a las «acciones combinadas 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»[38].

Los ámbitos normativos de actuación de las estrategias de zona gris

Como antes hemos señalado, uno de los elementos esenciales que caracterizan las estrategias de zona gris es la explotación intencionada de las normas y principios internacionales con el fin de alterar su aplicación regular y eludir las consecuencias jurídicas que se asociarían naturalmente a su ac-

[36] SARI, A. «Legal resilience in an era of gray zone conflicts and hybrid threats». *Working Paper* 2019/1. Exeter Centre for International Law, enero de 2019, p. 17.

[37] *At a glance. Understanding hybrid threats*. Servicio de Estudios del Parlamento Europeo, junio de 2015.

[38] Real Decreto 1008/2017, de 1 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2017.

tuación. Es por ello, que las operaciones de zona gris se pueden desarrollar en cualquier ámbito del ordenamiento jurídico, operando tanto en el derecho internacional como en el doméstico. A pesar de la expresada inexistencia de límites de actuación, podemos destacar tres sectores normativos que, por su relación directa con la propia naturaleza de las estrategias de zona gris, o por su relevancia a la hora de disciplinar las posibles acciones de respuesta contra aquellas, resultan más relevantes: el *ius ad bellum*, *el ius in bello* y el derecho de los derechos humanos (en adelante DIDH).

La importancia de estos tres marcos normativos está directamente relacionada con la evidente vinculación que tienen todos ellos con el elemento de dualidad entre el conflicto y la paz que caracteriza el concepto de zona gris. En el referido contexto, las ya de por sí complejas relaciones entre los tres sectores, constituyen un campo abonado para que los actores interesados puedan explotar a su conveniencia las posibles brechas e indefiniciones del sistema.

El ius ad bellum

La trasgresión de las normas reguladoras del uso de la fuerza es, sin duda alguna, el elemento central del concepto de las estrategias de zona gris, en la medida en que el propósito último de las mismas no es otro que el de eludir las consecuencias que se derivarían de la aplicación de sus disposiciones a las actividades que se desarrollan en este ámbito.

Como es sabido, el artículo 2.4 de la Carta de las Naciones Unidas prohíbe expresamente a los Estados recurrir a la amenaza o al uso de la fuerza contra la integridad territorial o la independencia política de otro Estado, prohibición esta que solo admite como excepción el principio de la legítima defensa individual y colectiva, en los términos y condiciones establecidos en el artículo 51 de la propia Carta de San Francisco, así como el ejercicio por parte del Consejo de Seguridad, de los poderes que se le atribuyen en el capítulo VII.

Pues bien, el elemento central que define el concepto de legítima defensa es la existencia previa de un ataque armado, pues sin la concurrencia de este elemento cualquier tipo de acto de respuesta militar contra una actuación concreta de un tercer Estado habría de considerarse contraria a las disposiciones de la Carta y, por tanto, ilegal y no permitida[39]. Es por ello, que las técnicas empleadas en al ámbito de las actividades de zona gris, por definición,

[39] El artículo 51 de la Carta determina que «ninguna disposición de esta Carta menoscabará el derecho inmanente de legítima defensa, individual o colectiva, en caso de ataque armado contra un miembro de las Naciones Unidas...». [Énfasis añadido]. Por otro lado, en la sentencia dictada por el Tribunal Internacional de Justicia en el asunto de las actividades militares y paramilitares en Nicaragua y contra Nicaragua se «reafirma que el derecho a la legítima defensa solo puede ejercerse en respuesta a un ataque armado».

no han de traspasar nunca el límite que implica la existencia de un ataque armado. Por el contrario, sus actividades se mantendrán siempre por debajo de dicho umbral, lo que les permitirá realizar actos que entran de lleno en la amenaza o el uso de la fuerza en sentido amplio, pero al no tener el carácter de ataque armado, no generarán una respuesta militar del oponente, toda vez que el derecho no le reconoce al sujeto pasivo de la acción la facultad de actuar en legítima defensa en las mencionadas circunstancias.

Este problema es particularmente relevante en lo que se refiere a los mecanismos de defensa colectiva, en la medida en que las actuaciones guiadas por el anteriormente citado propósito pueden tener la virtualidad de dejar sin efecto las garantías que para los Estados aliados supone la existencia de los referidos mecanismos. Así, el artículo 5 del Tratado de Washington por el que se crea la Organización del Tratado del Atlántico Norte condiciona de forma expresa la adopción de las medidas de asistencia colectiva a la previa existencia de un ataque armado contra el territorio de este, por lo que si la fuerza empleada contra dicho Estado no sobrepasa dicho umbral, es altamente cuestionable que, además de la puesta en marcha de los mecanismos de consulta previstos en el artículo 4, la Alianza pudiera emprender acción alguna[40]. Tampoco parece una opción posible una eventual enmienda de dicho precepto, no solo a la vista de las dificultades que ello entrañaría a la hora de alcanzar el suficiente consenso entre los aliados, sino especialmente porque cabe entender que la vinculación de las disposiciones del Tratado Atlántico con las normas contenidas en la Carta de Naciones Unidas relativas al uso de la fuerza lo haría por completo inviable.

Por lo que se refiere al ejercicio de la legítima defensa contra los ataques armados de un agente no estatal, parece existir un cierto consenso acerca de que el derecho internacional ampara el derecho a la legítima defensa, con arreglo a las condiciones establecidas en el artículo 51 de la Carta, siempre y cuando tales ataques se produjeran desde el exterior y el Estado territorial desde el que se lanzó se mostrara incapaz de impedirlos o no quisiera hacerlo.

En todo caso, es evidente que se trata de una cuestión que no es pacífica y que es objeto de intenso debate, lo que es un caldo de cultivo perfecto para que los actores que explotan las zonas grises pretendan aprovecharse de tal circunstancia.

[40] El referido artículo dispone en su apartado primero que «Las partes convienen en que un ataque armado contra una o contra varias de ellas [...] se considerará como un ataque dirigido contra todas ellas y en consecuencia acuerdan que si tal ataque se produce, cada una de ellas, en ejercicio del derecho de legítima defensa individual o colectiva, reconocido por el artículo 51 de la Carta de las Naciones Unidas [...] asistirá a la parte o partes así atacadas, adoptando [...] las medidas que juzgue necesarias, incluso el empleo de la fuerza armada...». [Énfasis añadido].

El uso de fuerzas asociadas (*proxy forces*) es otro recurso ampliamente utilizado por los sujetos activos en las actividades de zona gris, en este caso de carácter esencialmente estatal, para eludir su implicación directa en las acciones hostiles y la consiguiente responsabilidad por tales acciones. Aunque el recurso a tales prácticas no es nuevo, y podemos encontrar infinidad de ejemplos, tanto a lo largo de la guerra fría, como con posterioridad, su integración como uno de los mecanismos empleados en las estrategias de la zona gris, en combinación con otro tipo de medidas como la presión política, las acciones de propaganda, o las medidas de carácter económico, multiplica su eficacia.

La utilidad de este tipo de intervención no solo reside en el hecho de que permite eludir la aplicación de las normas prohibitivas del uso de la fuerza entre los Estados mediante la falta de identificación entre tales fuerzas y el Estado que las controla, sino que también puede tener una incidencia decisiva a la hora de determinar el régimen jurídico aplicable al conflicto en sí. De esta forma, el recurso a este tipo de fuerzas puede eludir la internacionalización formal del conflicto, al no poderse afirmar la intervención de un tercer Estado, evitando así la aplicabilidad del régimen jurídico propio de los conflictos armados internacionales.

El derecho de los derechos humanos

Teniendo en cuenta que en la propia esencia de las actividades en zona gris se encuentra el evitar en la medida de lo posible traspasar la línea que da lugar a la existencia de un conflicto armado y a la correspondiente aplicabilidad del DIH, el ámbito normativo que resultará de aplicación a las acciones destinadas a contrarrestar tales acciones por parte de un Estado será normalmente el del DIDH. Ello es así, por el carácter de derecho especial propio de las normas del DIH, que determina que su ámbito material de aplicación se extienda única y exclusivamente a las situaciones en las que exista conflicto armado, por lo que sus disposiciones «únicamente rigen cuando se producen los presupuestos previstos en las mismas normas internacionales humanitarias»[41].

Como consecuencia de ello, tanto las acciones de zona gris que no alcancen la intensidad de la violencia ni, en el caso de los conflictos armados no internacionales, el nivel de organización requerido, como las posibles respuestas planteadas por el oponente, han de ser tratadas necesariamente bajo la óptica del derecho de los derechos humanos. De esta forma, y tal y como se concluye en la Resolución 2217 (2018) del Comité de Asuntos Jurídicos y Derechos Humanos de la Asamblea Parlamentaria del Consejo de Europa, a pesar de

[41] RODRÍGUEZ VILLASANTE Y PRIETO, J. L. «Ámbito de aplicación del derecho internacional humanitario, tipología y delimitación de los conflictos armados». En *Derecho Internacional Humanitario*. Tirant lo Blanch, 2017, p. 119.

las complejidades que presentan las amenazas híbridas y a la difícil atribución de la responsabilidad sobre las mismas, no se puede concluir que los actores que operan en la zona gris actúen en un ámbito sin regulación legal, declarando expresamente que resultarán en todo caso de aplicación las normas, tanto del ordenamiento interno como del derecho internacional correspondientes en función de la materia y, entre ellas naturalmente, las relativas a los derechos humanos. De esta forma, las referidas acciones «deberán examinarse a la luz de la normativa interna en materia penal y, en caso necesario y dependiendo de la situación, de los instrumentos legales internacionales aplicables a la materia (tales como las normas reguladoras del derecho del mar o las que se dirigen a la lucha contra el cibercrimen, el terrorismo, las manifestaciones de odio o el blanqueo de dinero)»[42].

La relevancia de las operaciones en la zona gris en este ámbito es consecuencia precisamente del deseo de sus actores de evitar verse involucrados en acciones que traspasen el límite de la acción armada, lo que –además de enervar la posibilidad de adopción por parte del oponente de medidas de fuerza defensivas– determina que el paradigma aplicable a la regulación material de las acciones sea el propio de las operaciones de seguridad pública y no el de los conflictos armados.

La diferencia entre la actuación en uno u otro ámbito es ciertamente apreciable, toda vez que evidentemente el alcance del uso de la fuerza y las condiciones que rigen su empleo difieren en uno u otro caso. De esta forma, fuera del ámbito propio del conflicto armado el uso de la fuerza se restringe de forma significativa y el alcance de los principios de necesidad y proporcionalidad es muy diferente[43]. Por esta razón, el actor de zona gris no solo obtiene un provecho directo derivado de la imposibilidad de su adversario de usar la fuerza armada en legítima defensa, sino que además consigue que el empleo de medios de menor intensidad se ajuste a unos parámetros mucho más restrictivos.

Por otro lado, la aplicabilidad de las disposiciones del derecho de los derechos humanos (particularmente cuando se trata de misiones llevadas a cabo por las Fuerzas Armadas) se ha revelado como un terreno muy fructífero para el desarrollo de operaciones de *lawfare*, lo que unido a las posibilidades que ofrece el uso de la propaganda y la manipulación informativa, concede a los actores de zona gris una oportunidad inmejorable para desacreditar las

[42] «Legal challenges related to hybrid war and human rights obligations». Resolución adoptada por el Comité de Ministros del Consejo de Europa el 12 de diciembre de 2018.

[43] La proporcionalidad en el marco de las operaciones de seguridad pública se centra en la necesidad del empleo de la fuerza para evitar un mal mayor, mientras que en el ámbito del conflicto armado el cálculo de proporcionalidad se realiza sobre la base de que los daños incidentales no resulten excesivos atendiendo a la ventaja militar que se pretenda obtener (artículo 57 del Protocolo Adicional I).

operaciones de las fuerzas armadas del rival y condicionar de este modo su actuación futura.

En todo caso, las cuestiones más importantes que la dinámica de la zona gris suscita en el campo de los derechos humanos se centran en la naturaleza, intensidad y límites de la respuesta de los Estados que son víctimas de dichas estrategias.

Así las cosas, el propio Consejo de Europa ha manifestado ya su preocupación por algunas medidas adoptadas por algunos Estados que han impuesto limitaciones a algunos de los derechos fundamentales de los ciudadanos como el derecho a la libertad de información o de expresión, a la intimidad personal o a la propia libertad ambulatoria, en el citado ámbito[44].

El ius in bello

Como noción básica, el concepto de zona gris juega en el margen entre la paz y el conflicto, de forma que los actores que intervienen en la misma tratan precisamente de eludir que sus actividades crucen el umbral de intensidad que cualifica la existencia de un conflicto armado. Por esta razón, un desarrollo estricto del concepto nos llevaría necesariamente a concluir que el ámbito de aplicación del DIH sería ajeno por completo a su margen material de actuación.

No obstante, la utilidad de explotar las ambigüedades y debilidades de la norma no se agota únicamente en el referido ámbito conceptual, sino que también puede ser empleado con idéntico éxito para obtener ventajas estratégicas en el marco de aplicación del *ius in bello*. Dentro del aludido marco se pueden distinguir dos líneas diferentes de actuación según la naturaleza y alcance de los intentos de abusar del sistema normativo establecido.

Así, dentro de la primera de dichas categorías, y que se corresponde en mayor medida con la noción general que hemos expuesto sobre la zona gris, podríamos incluir todas las actuaciones dirigidas a explotar las ambigüedades que presenta la norma, todo ello en contra de las exigencias de la buena fe, y al objeto de conseguir el objetivo estratégico perseguido.

Un ejemplo ilustrativo de estas técnicas lo podemos encontrar en la interpretación del concepto de participación directa en las hostilidades. A tal efecto, el DIH protege a las personas civiles contra los efectos de las operaciones militares, «... salvo si participan directamente en las hostilidades y mientras dure tal participación»[45]. Pues bien, la determinación de qué debemos entender por participación en las hostilidades y la naturaleza directa o indirecta

[44] Resolución 1840 (2011), 16 de octubre; Resolución 1954 (2013), de 2 de octubre; y Recomendación 2024 (2013) de 2 de octubre.

[45] Artículo 51.3 del Protocolo Adicional I.

de tal intervención es una cuestión que presenta innumerables problemas interpretativos y con una indudable trascendencia práctica, en la medida en que el civil en quien concurra tal condición perderá su inmunidad frente a los ataques y se convertirá en sujeto pasivo lícito de la acción militar. La existencia de importantes puntos oscuros y de serias incertidumbres en la aplicación de la norma, unida a la ventaja estratégica que puede derivarse del reconocimiento de la eventual inmunidad frente a los ataques de una persona que realice cierto tipo de actividades «fronterizas» entre la participación directa y la indirecta en las hostilidades, constituyen un núcleo perfecto para su explotación por parte de los actores de la zona gris.

Una segunda categoría o línea de actuación está integrada por aquellas acciones que no tratan de explotar directamente las ambigüedades de la norma, sino el mayor compromiso del sujeto pasivo de la acción con su cumplimiento, junto a la superior exposición de este a las críticas que pudiera generar una determinada respuesta por parte de la opinión pública o de la comunidad internacional.

Los ejemplos que podemos utilizar en este supuesto se refieren al uso de los llamados «escudos humanos», o a la intencionada utilización por parte del que participa en las hostilidades de la ventaja que le produce el hecho de rodearse de civiles y confundirse con ellos. El uso de dichas prácticas está muy extendida especialmente entre actores no estatales, y persigue evitar que el enemigo emplee libremente su potencial, al verse coartado en su actuación por la obligación de protección a las personas civiles. Este tipo de actuación explota el ámbito de desigualdad intrínseca o asimetría legal a la hora de cumplir las obligaciones internacionales entre algunos actores no estatales y la inmensa mayoría de los Estados que conforman la sociedad internacional. La citada desigualdad se incrementa de forma significativa en el caso de los países occidentales, no solo por su teórico mayor compromiso con el e*status quo*, sino especialmente por la mayor dependencia que tienen respecto de las críticas públicas que generan sus acciones.

Estas circunstancias condicionan de forma muy significativa la actuación de las fuerzas armadas ante escenarios como los descritos, en la medida en que razonablemente anteponen a las necesidades operacionales, una serie de criterios y líneas de actuación que muchas veces van más allá de lo estrictamente impuesto por las normas, en este caso las del DIH.

La responsabilidad internacional

Como se ha señalado anteriormente, un elemento esencial en la explotación de las ventajas de la zona gris reside en la opacidad de las actuaciones, de tal forma que no sea posible atribuir su autoría al sujeto activo que las promueve. A este respecto, el artículo 2 del Proyecto de Artículos sobre Responsabilidad del Estado por Hechos Internacionalmente Ilícitos establece como

elemento determinante de la responsabilidad internacional de un Estado la existencia de una acción u omisión que, por un lado, sea «atribuible al Estado según el derecho internacional» y, por otro, que implique la «violación de una obligación internacional del Estado»[46]. A este último elemento de carácter objetivo ya nos hemos referido con anterioridad, señalando como uno de los elementos integrantes de las operaciones de zona gris la utilización interesada de las ambigüedades legales para eludir las obligaciones impuestas por el derecho internacional.

Pero también en el ámbito subjetivo de la atribución de la responsabilidad internacional operan las estrategias de zona gris, obteniendo provecho de las indefiniciones y ambigüedades de la normativa reguladora de esta materia. De tener éxito en este campo, las eventuales trasgresiones de las normas reguladoras del uso de la fuerza, del derecho de los conflictos armados, del derecho de los derechos humanos o de cualquier otro sector del ordenamiento jurídico, no podrían ser atribuidas a la parte que las ha generado, por no poder establecerse un nexo claro entre sus actos y las contravenciones detectadas. La mencionada dificultad de atribución resulta especialmente predicable de las operaciones en el ciberespacio, tal y como acertadamente pone de manifiesto De Salas Claver en el capítulo cuarto de la presente publicación.

Al objeto de alcanzar estos fines, los actores de zona gris pueden, o bien simplemente disimular el origen de las actividades de forma que resulte imposible su atribución concreta, o bien actuar por medio de las anteriormente citadas fuerzas asociadas. En este último caso, la atribución de la responsabilidad dependerá de que se pueda acreditar que tales fuerzas asociadas actúan efectivamente bajo la dirección o el control del Estado o siguiendo sus instrucciones[47]. Por otro lado, a la mera existencia de un control sobre las fuerzas subordinadas debe añadirse, como requisito esencial, que el control sea efectivo y que tenga carácter general, lo que sucede cuando interviene en la organización, coordinación o planificación de las actividades del grupo[48].

---

[46] El Proyecto de Artículos sobre Responsabilidad del Estado por Hechos Internacionalmente Ilícitos, que recoge y sistematiza el derecho consuetudinario en la materia, fue adoptado por la Comisión de Derecho Internacional el 9 de agosto de 2001 y remitida a la atención de los Estados miembros por la Asamblea General de las Naciones Unidas, en Resolución 56/83 de 12 de diciembre del mismo año.

[47] El artículo 8 del Proyecto, bajo el epígrafe de «Comportamiento bajo la dirección o control del Estado», dispone que «se considerará hecho del Estado según el derecho internacional el comportamiento de una persona o de un grupo de personas si esa persona o ese grupo de personas actúa de hecho por instrucciones o bajo la dirección o el control de ese Estado al observar ese comportamiento» (énfasis añadido).

[48] El requisito de la efectividad del control estatal se recoge en la Sentencia del Tribunal Internacional de Justicia de 27 de junio de 1986, en el asunto relativo a las actividades militares y paramilitares en Nicaragua y contra Nicaragua (Nicaragua contra los Estados Unidos de América), mientras que el criterio del control general (*overall control*) se puede

Aunque el criterio seguido en el caso Tadic sobre la naturaleza del control ha sido matizada por la Sentencia del Tribunal Internacional de Justicia en el caso Bosnia y Herzegovina contra Serbia, relativo al genocidio de Srebrenica, lo cierto es que la acreditación del elemento del control efectivo no resulta en absoluto sencilla, máxime si tenemos en cuenta que el actor que trata de explotar la zona gris tratará por todos los medios de disimular los mecanismos de control sobre las fuerzas asociadas de los que disponga, evitando toda relación abierta con las mismas[49]. Por ello, la atribución de responsabilidad internacional a un Estado por las acciones cometidas por una persona o grupo de personas está sometida a unas condiciones muy estrictas y requiere la constatación de una serie de elementos de difícil apreciación, lo que determina que las actuaciones realizadas a través de fuerzas interpuestas constituyan un recurso de gran utilidad en las estrategias de zona gris. Es más, la actuación por medio de estas fuerzas interpuestas permite al actor de la zona gris llevar a cabo de forma indirecta todo tipo de acciones, especialmente las que implican el uso de la fuerza armada, lo que implica un grado de fuerza evidentemente muy superior al del resto de las estrategias que se llevan a cabo en este ámbito.

Por lo que se refiere a las posibilidades de una eventual represión penal internacional de los actos derivados de las estrategias de zona gris, las cuestiones que se plantean son muy similares a los que nos hemos referido al tratar la cuestión del uso de la fuerza, toda vez que el umbral que se aplica en el Estatuto de Roma por el que se crea la Corte Penal Internacional es exactamente el mismo al que nos hemos referido al hablar de las disposiciones de la Carta de las Naciones Unidas. De esta forma, aun cuando la Corte Penal Internacional ya ha activado el crimen de agresión como uno de los delitos de su competencia, el umbral que se exige para la concurrencia del referido tipo determina que sea difícilmente imaginable su aplicabilidad en las difusas actividades que componen la zona gris. En efecto, de forma coherente con la naturaleza de la propia Corte y con la vinculación de esta al sistema de Naciones Unidas, para la definición del crimen de agresión que se llevó a cabo en la «Conferencia de Revisión de Kampala», se empleó el concepto de agresión que se desarrolla en la Resolución 3314 (XXIX) de la Asamblea General, de 14 de diciembre de 1974[50]. De esta forma, el apartado 2 artículo 7 bis del Estatuto de la Corte parte del citado concepto, exigiendo

encontrar en la Sentencia del Tribunal Penal para la Antigua Yugoeslavia en el caso Tadic (*Prosecutor v. Dusko Tadic*).

[49] En la sentencia del Tribunal Internacional de Justicia de 14 de febrero de 2017, dictada en la resolución del citado caso, se concluye que el criterio del control general es demasiado amplio y se extiende mucho más allá del alcance consuetudinario del concepto, que exige la existencia de un control efectivo.

[50] El artículo 1 de la Resolución 3314 (XXIX) define la agresión como «... el uso de la fuerza armada por un Estado contra la soberanía, la integridad territorial o la independencia política de otro Estado, o en cualquier otra forma incompatible con la Carta de las Naciones Unidas...» [énfasis añadido].

la existencia de un ataque armado de igual naturaleza e intensidad que la que sería determinante de la concurrencia de una responsabilidad internacional del Estado por el hecho ilícito de la agresión, así como del derecho del atacado a defenderse de tales acciones por medio de la fuerza armada.

Por si las circunstancias anteriormente expuestas no fueran suficientes para certificar la afirmación previamente expuesta sobre la difícil aplicabilidad de los mecanismos de justicia penal internacional a las actividades de zona gris, las condiciones para el ejercicio de la competencia sobre el crimen de agresión que se contienen en el artículo 15 bis y 15 ter del Estatuto, que se encuentran fuertemente condicionadas por la posición adoptada por el Consejo de Seguridad de Naciones Unidas sobre la existencia de una situación de agresión, hacen aún más remota la citada eventualidad, a la vista de las dificultades que entraña su cumplimiento.

Los medios de reacción

La intrínseca indefinición y opacidad de las operaciones en la zona gris determina que sea ciertamente difícil plantear estrategias efectivas de defensa. En todo caso, parece evidente que la eficacia de las medidas de reacción exige que estas contemplen un conjunto de elementos de distinta naturaleza: política, económica, militar y –por supuesto– jurídica. En el presente epígrafe trataremos de sistematizar las más relevantes, con especial referencia a estos últimos:

Las vías de oposición a las estrategias de zona gris

A pesar de lo difuso del concepto y de la muy variada tipología de las acciones que configuran la zona gris, y precisamente por las dificultades que entraña el poder articular una respuesta efectiva, se ha venido proponiendo un conjunto de medidas, esencialmente en el plano político-estratégico, cuya adopción resulta imprescindible para contrarrestar en la medida de lo posible los efectos de dichas actividades. Así, en términos generales, las líneas de oposición más comúnmente invocadas son las siguientes:

La institucionalización de mecanismos encargados de identificar y afrontar las amenazas de zona gris

Para tal fin es preciso, por un lado, el diseño de estructuras multidisciplinares que desde diferentes ópticas sean capaces de ofrecer una respuesta adecuada y eficaz. El aludido carácter multidisciplinar vendría dado, entre otros, por la presencia de analistas políticos, medios de inteligencia, personal militar, técnicos especializados, expertos en comunicación social y, también, de asesores jurídicos.

Paralelamente, resulta imprescindible coordinar a nivel internacional (especialmente en el ámbito de la OTAN y de la Unión Europea) los esfuerzos que se realicen en este campo, al objeto de ofrecer una respuesta unitaria y armonizada a las amenazas.

La referida necesidad de coordinación a nivel internacional de los esfuerzos en la materia ha sido puesta de manifiesto tanto por la OTAN, como por la Unión Europea y el Consejo de Europa. Así, en el punto 13 de la declaración conjunta realizada por los jefes de Estado de los países miembros de la OTAN con motivo de la cumbre celebrada en Gales en el año 2014, se anuncia la disposición para conseguir que la OTAN sea capaz de enfrentarse a las amenazas derivadas de la guerra híbrida, y se advierte que resulta «esencial que la Alianza se procure las herramientas y procedimientos precisos para disuadir y para dar respuesta de forma eficaz a las amenazas híbridas».

Siguiendo el referido concepto, en el año 2015 la OTAN adoptó una estrategia específica para la guerra híbrida, que se centre en la preparación, la disuasión y la defensa como sus tres pilares esenciales. De igual modo, en el punto 21 de la declaración conjunta efectuada por los jefes de Estado tras la cumbre celebrada en Bruselas los días 11 y 12 de julio de 2018, se pone de manifiesto que las naciones aliadas se enfrentan a un creciente número de amenazas procedentes tanto de actores estatales como no estatales, que llevan a cabo actividades de carácter híbrido, al objeto de crear ambigüedad y de borrar las líneas entre la paz, la crisis y el conflicto. Para hacer frente a tales amenazas no descartan los líderes de la OTAN la posibilidad de invocar en su caso el artículo 5 del Tratado Atlántico, sosteniendo la necesidad de aumentar el nivel de resiliencia y la capacidad de disuasión y de defensa, y anunciando la creación de una serie de equipos de apoyo para la lucha contra las actividades híbridas (*Counter Hybrid Support Teams*) que se pondrán a disposición de los países aliados que lo requieran.

La determinación de los objetivos políticos que persigue el adversario

Tal y como apunta Hoffman, un error comúnmente cometido por los Estados Unidos y, por extensión, por el resto de los Estados occidentales, consiste en centrar su atención en la naturaleza de las medidas que adopta su rival y en la forma en que las aplica, prestando escasa atención a las razones últimas que fundamentan tal actuación, es decir en los objetivos que con ello pretende alcanzar[51].

La disuasión

[51] HOFFMAN, F. G. *Op. cit.,* p. 41.

El concepto clásico de disuasión imperante en la guerra fría no parece servir de gran ayuda a la hora de frenar los intentos de los actores de zona gris, especialmente por lo que se refiere a los grupos no estatales, muchos de los cuales no solo no temen al uso coercitivo de la fuerza por parte del adversario, sino que incluso pueden llegar a valorarlo como un elemento favorecedor de sus intereses[52]. Incluso, la adopción de medidas de uso de la fuerza por parte de un Estado puede ser un terreno propicio para la utilización de nuevas estrategias de zona gris que persigan deslegitimizar tales actos en el plano de las relaciones internacionales y en el ámbito de la opinión pública.

Es por ello, que ha surgido con fuerza entre algunos autores un nuevo concepto de disuasión referido específicamente a las actividades de zona gris, que se materializa en el uso del término «disuasión gris *(gray deterrence)*». El citado concepto hace referencia a un conjunto de acciones, entre las que se incluirían –por ejemplo– algunas tan dispares como las de carácter informativo y las operaciones que impliquen el uso de la fuerza militar, que pueden adoptarse para contrarrestar las estrategias de zona gris, fundamentalmente mediante la alteración del análisis coste/beneficio del que parten los actores de tales estrategias al diseñarlas. En todo caso, la naturaleza de las referidas medidas de disuasión debe centrarse predominantemente en el marco político, social o informativo, más que en el militar, habida cuenta de que el objetivo de estas debe orientarse a «minimizar los espacios sociales» de los que se nutre el oponente[53]. De esta forma, el desarrollo de mecanismos de respuesta que sean capaces de identificar las amenazas, analizar los propósitos de los actores implicados y emprender un conjunto variado de acciones que permitan desacreditar y deslegitimizar los intentos de manipulación tanto del sistema normativo internacional como de la opinión pública por parte del «adversario gris», constituye un elemento clave a la hora de contrarrestar las estrategias emprendidas por este tipo de actores.

El desarrollo de políticas de información eficaces

Uno de los «campos de batalla» más importantes en los que se libra la lucha contra las amenazas de zona gris es el de la información, ya que el sujeto que promueve las mismas trata de imponer una «narrativa» que resulta afín a sus intereses, en la que los canales de información tradicionales y, especialmente, los más recientes, cumplen un papel esencial. Por tal razón, el diseño de estrategias que permitan responder con eficacia a tales intentos de distorsión de la realidad resulta absolutamente esencial.

Los recursos de naturaleza jurídica

52 WOOD, G. «What ISIS Really Wants». *The Atlantic*. Marzo de 2015.

53 MATISEK, J. W. *Op. cit.,* p. 14.

En un plano estrictamente jurídico, una adecuada reacción contra las estrategias de zona gris tendría necesariamente que tener en cuenta los aspectos que se señalan a continuación.

El cumplimiento de las normas y el respeto al principio de la buena fe

Debemos tener presente que siempre han existido lagunas, incertidumbres y ambigüedades en las normas que integran el ordenamiento jurídico internacional, normalmente como consecuencia de la necesidad de alcanzar un consenso entre los Estados cuando se trata de aprobar una norma convencional. Para alcanzar dicho consenso, en muchas ocasiones es necesario acudir a una redacción calculadamente ambigua que permita una diferente (y obviamente interesada) interpretación de su contenido. Paradójicamente esta característica de las normas del derecho internacional no solo no es un obstáculo para el normal desarrollo de las relaciones interestatales, sino todo lo contrario, en la medida en que posibilita la adopción de acuerdos consensuados, cuya consecución, en otras circunstancias, resultaría ciertamente compleja.

Esta misma característica se encuentra presente a la hora de permitir la necesaria adaptación a las nuevas realidades que inevitablemente se presentan a lo largo de la vigencia de una norma, permitiendo llevar a cabo una interpretación integradora que constituye una vía imprescindible para la evolución del derecho y para el adecuado desarrollo de las relaciones internacionales.

Las mencionadas características forman parte indudablemente del tradicional juego que confronta los intereses de los Estados y no son producto del surgimiento de las dinámicas de la zona gris. El elemento que caracteriza específicamente las maniobras políticas y jurídicas de los Estados que explotan las ambigüedades de la zona gris es la quiebra del principio de la buena fe, al que ya hemos hechos referencia anteriormente. En efecto, no se trata en esta estrategia de tratar de hacer valer una interpretación favorecedora de un determinado interés nacional, sino de torcer el alcance de una norma o conjunto de normas, alterando así las categorías normativas preestablecidas de tal forma que se consiga eludir la consecuencia jurídica prevista por el ordenamiento jurídico.

Ante estas actuaciones en la zona gris, los Estados afectados, descartada la alternativa de aquietarse a las intenciones del actor que las lleva a cabo, tienen la posibilidad de oponerse con todos los medios a su alcance a esa nueva «interpretación» que afecta a las categorías legales establecidas, haciendo valer sus puntos de vista y evitando así la consolidación de la situación.

Por supuesto, existe también la opción de recurrir a esas mismas técnicas de zona gris, bien para contrarrestar las técnicas del oponente, bien para alcanzar los objetivos estratégicos propios en otras áreas. Ya se ha hecho

antes mención al hecho de que los Estados occidentales han recurrido en ocasiones a estas técnicas, pero, como también se ha puesto de manifiesto, en dicho «campo de batalla» los aliados se encuentran en una situación de franca desventaja, lo que hace aconsejable buscar otros escenarios de confrontación más propicios. Es más, la propia dinámica de la zona gris en el campo de las relaciones internacionales determina que la implicación de un Estado (especialmente del mundo occidental) en tales actividades «pueda deslegitimar» sus intentos de contrarrestar las llevadas a cabo, a su vez, por otros Estados o grupos no estatales ante la comunidad internacional. Se ha sostenido, en este sentido, que las naciones realmente comprometidas con el orden instaurado tras la segunda Guerra Mundial no se pueden permitir responder a las amenazas híbridas con la adopción de los mismos medios y métodos de sus adversarios, sin contribuir a la decadencia de dicho orden[54]. Con arreglo a dicha circunstancia, y desde este punto de vista jurídico, la mejor opción para un Estado comprometido con el orden internacional imperante es la de respetar escrupulosamente el principio de la buena fe en las relaciones internacionales, velando por el estricto cumplimiento de las normas en toda ocasión. En esta confrontación de orden jurídico, los Estados no deberían traspasar la línea roja que separa la lógica defensa de sus intereses mediante una interpretación razonable y coherente de las normas y principios que conforman el ordenamiento jurídico internacional, de las posiciones dirigidas a forzar la alteración de las categorías jurídicas que forman parte de este con vulneración de las exigencias de la buena fe.

Este mismo punto de vista ha sido expuesto por algunos autores como Brooks o Mazarr, habiendo señalado este último que la respuesta más efectiva a las técnicas de la zona gris no pasa por la consecución de un conjunto de capacidades de la misma naturaleza que las puedan contrarrestar, sino la «reafirmación y el fortalecimiento de las normas, reglas e instituciones que integran el orden internacional»[55].

También desde el punto de vista institucional se ha mantenido idéntica postura, y así en el ámbito europeo, la anteriormente citada resolución del Consejo de Europa de 12 de diciembre de 2018 ha exhortado a los Estados miembros a evitar el uso de tales medidas en las relaciones internacionales, así como a «respetar de forma incondicional las normas contenidas en el derecho internacional, con arreglo al objeto y finalidad de las mismas, absteniéndose de explotar de forma abusiva las lagunas y ambigüedades que pudieran existir».

En todo caso, dicha posición que podríamos llamar «institucionalista» no implica que haya que negar toda posible evolución de las normas que ri-

[54] HOFFMAN, F. G. «Further thoughts on hybrid threats». *Small Wars Journal*. Marzo de 2009.

[55] MAZARR, M. J. «Struggle in the gray zone and world order». *War on the rocks*. Diciembre 2015.

gen las relaciones internacionales en la actualidad. En efecto, el sistema de principios y normas básicas, que rigen el orden internacional tras el fin de la Segunda Guerra Mundial, se revela insuficiente para hacer frente a las nuevas realidades y amenazas surgidas en los últimos años, siendo deseable que se busque un consenso internacional que pudiera permitir una mejor adaptación del derecho, de tal forma que permita ofrecer respuesta a estas situaciones que se producen en la zona fronteriza intermedia entre la paz y el conflicto.

Además, resulta conveniente señalar que esta línea de actuación de respeto a la legalidad y al orden establecido coadyuva de forma muy importante al éxito de las estrategias defensivas de disuasión a las que nos hemos referido con anterioridad, en la medida en que resulta imprescindible a la hora de exteriorizar un mensaje coherente que ponga en entredicho los actos del adversario y refuerce la legitimidad de la propia posición. Partiendo de dicha circunstancia, se puede considerar recomendable incluso ir un poco más allá en el cumplimiento de las obligaciones internacionales, especialmente en el terreno del DIH y de los derechos humanos. Efectivamente, habida cuenta de la del peso que la «guerra de la propaganda» alcanza en las estrategias de zona gris, extremar las medidas de protección de las personas y bienes que pudieran resultar afectadas directa o indirectamente por la acción militar y adoptar incluso mecanismos y modos de actuación que excedan de lo estrictamente impuesto desde un punto de vista jurídico, resulta una vía particularmente efectiva, en la medida en que contribuye, por un lado, al mejor cumplimiento de las obligaciones internacionales y, por otro, refuerza la legitimidad de los actores que actúan conforme a dichos criterios, a la vez que mejora su imagen pública.

Las contramedidas

La ausencia en el ámbito de las relaciones internacionales de un poder coercitivo equiparable al ejercido por el Estado en el ámbito interno determina que, en el caso de que se verifique la existencia de un hecho internacionalmente ilícito atribuible a un tercer Estado, en las condiciones a las que nos hemos referido con anterioridad, aquel Estado lesionado en su derecho a causa de tal actuación pueda legítimamente adoptar de forma unilateral las medidas necesarias para hacer cumplir el derecho internacional. Siguiendo a González Campos, el referido concepto responde a una doble caracterización:

- En atención a su ejercicio, las contramedidas constituyen «una manifestación de la autotutela o autoprotección por un Estado del propio derecho cuando ha sido lesionado por otro u otros Estados».

- En atención a su finalidad, «presuponen la existencia de una medida anterior de otro Estado, constitutiva de un hecho ilícito, frente a la que reacciona el Estado lesionado»[56].

Como consecuencia de ello, las contramedidas son actuaciones unilaterales emprendidas por un Estado como reacción a un hecho internacionalmente ilícito cometido por otro, y con la finalidad de imponer coercitivamente el respeto de su derecho. Tales contramedidas, que deben respetar las disposiciones generales limitativas del uso de la fuerza en las relaciones internacionales, consisten generalmente en la ruptura de relaciones diplomáticas, la suspensión de los efectos de ciertos tratados bilaterales, los embargos, la adopción de medidas económicas, las retorsiones o el ejercicio de represalias no armadas.

En todo caso, y con arreglo a lo establecido en la Resolución del Instituto de Derecho Internacional de 1989, la legitimidad de estas medidas unilaterales se encuentra sometida al cumplimiento de las siguientes condiciones:

1) «Requerimiento previo (salvo caso de extrema urgencia) al Estado infractor para que cese en su conducta criminal».
2) «Limitación de la medida al Estado infractor».
3) «Proporcionalidad de la medida a la gravedad de la infracción».
4) «Consideración de la incidencia de la medida sobre el nivel de vida de las poblaciones afectadas, los intereses de los particulares y de los Estados terceros».

Por todo ello, y siempre dentro del citado marco limitativo, una de las vías más eficaces para hacer frente a las acciones de zona gris que impliquen la comisión de hechos internacionalmente ilícitos es la adopción de contramedidas por parte de los Estados afectados contra el infractor. Tales contramedidas pueden incluso implicar la adopción de medidas que –en condiciones normales– estarían prohibidas por el ordenamiento jurídico internacional, si bien se consideran lícitas por haber sido adoptadas legítimamente en respuesta a un previo hecho ilícito, configurándose así, como represalias admisibles con arreglo al derecho internacional.

El *lawfare* defensivo

Desde otro punto de vista, y teniendo en cuenta que el objetivo principal del impulsor de las actividades de zona gris no es otro que el de crear y mantener un escenario legal artificialmente construido que permita el desarrollo óptimo de las medidas que ha planeado y, a la vez, disminuya o anule la

[56] GONZÁLEZ CAMPOS, Julio D.; SÁNCHEZ RODRÍGUEZ, Luis I.; ANDRÉS SAENZ DE SANTAMARÍA, Paz. *Curso de Derecho Internacional Público*. Thomson Cívitas, 2004, p. 403.

capacidad de respuesta de su adversario, la vía para afrontar las amenazas que plantean las referidas actividades pasa ineludiblemente por el desarrollo de medidas preventivas que permitan identificar las amenazas y contrarrestarlas de forma efectiva.

Es en este ámbito donde adquiere mayor relevancia el concepto anteriormente aludido de *lawfare*, especialmente por lo que se refiere a los aspectos «defensivos» del uso del derecho como arma. Efectivamente, el *lawfare* guarda una evidente relación con las dinámicas de la zona gris, hasta el punto de que alguna de las definiciones que de dicho concepto nos han ofrecido algunos estudiosos de la materia muestran un alto porcentaje de elementos coincidentes. Así, Kittrie señala que dicho concepto consiste en el «uso del derecho para obtener los mismos o similares efectos que se obtendrían por medio de una acción militar convencional, siempre que la parte que utilice el derecho de esta forma actúe impulsada por la intención de destruir o debilitar a su oponente», definición esta que encajaría con la que hemos adoptado para caracterizar las acciones de zona gris[57].

De igual forma, otro de los elementos esenciales del *lawfare*, que surge de la evolución del concepto inicialmente planteado es el del abuso del derecho, de forma que a la definición original que apunta sencillamente al uso del derecho como arma, habría que añadirle la dimensión intencionalmente vulneradora de la norma[58]. Este elemento subjetivo, relacionado con el propósito de instrumentalizar el derecho, forma igualmente parte esencial del concepto de zona gris, tal y como hemos señalado al hacer referencia a sus características definitorias.

A pesar de la similitud entre ambos conceptos, lo cierto es que el de *lawfare* tiene un alcance más restringido, en la medida en que debe reducirse al ámbito de la acción hostil, mientras que las actividades de zona gris tienen un alcance multidimensional y afectan no solo a tales acciones, sino a cualquier ámbito del ordenamiento jurídico internacional que ofrezca a los actores que las promuevan una posibilidad de explotación de las incertidumbres legales que pueda presentar.

En todo caso, es innegable que el uso del derecho como arma es un elemento importante de las estrategias de la guerra híbrida, por lo que la puesta en funcionamiento de mecanismos dirigidos a contrarrestar los eventuales intentos de uso de tales tácticas se revela como una parte esencial del sistema de respuesta que necesariamente ha de plantearse. De hecho, se ha

[57] KITTRIE, O. F. *Lawfare: Law as a Weapon of War*. Oxford University Press, enero de 2016, p. 8.

[58] De esta forma el propio Dunlap, se vio obligado a redefinir el concepto inicial que hemos expuesto al inicio del trabajo, sosteniendo que el *lawfare* se corresponde con la estrategia tanto de uso como de abuso del derecho como un medio que sustituye al tradicional uso de la fuerza para obtener la consecución de un fin estratégico determinado: Dunlap, C. J. «Lawfare Today: A Perspective». *Yale Journal of International Affairs*. 2008, p.146.

señalado expresamente al *lawfare* como una «técnica específica de la guerra híbrida»[59].

Desde este punto de vista, el concepto de *lawfare* y el diseño de estrategias defensivas inspiradas en este concepto ofrecen una base muy interesante para la puesta en marcha de mecanismos e iniciativas destinadas a contrarrestar las operaciones de los actores que operan en la zona gris. Esta concepción, además, conecta directamente con el cumplimiento de las normas con arreglo a las exigencias de la buena fe a la que nos hemos referido en el apartado anterior.

La adopción de medidas extraordinarias

En muchos casos, la intensidad de los actos de agresión del adversario puede hacer precisa la adopción de medidas que supongan una limitación de las libertades de los ciudadanos. El Consejo de Europa en la anteriormente citada Resolución ha expresado ya su preocupación por ciertas decisiones adoptadas por países europeos en casos puntuales, subrayando la necesidad de que el Estado afectado proceda formalmente en tales circunstancias a la expresa derogación de las obligaciones derivadas del Convenio que se vean afectadas por las medidas de protección que se aprueben. A tal efecto, el artículo 15 del Convenio Europeo de Derechos Humanos permite la citada derogación en los supuestos en que concurra una gravísima amenaza para la propia supervivencia del Estado, como es el caso de un conflicto armado, con la excepción de los derechos reconocidos en los artículos 2 (derecho a la vida, con la excepción de las muertes ocasionadas por actos lícitos de combate), 3 (prohibición de la tortura), 4.1 (prohibición de la esclavitud y trabajos forzados) y 7 (principio de legalidad penal). El citado procedimiento permitiría a los Estados parte de Convenio dejar en suspenso las obligaciones asumidas con relación a la garantía de los derechos y libertades de los ciudadanos, siempre y cuando se cumplan cuatro presupuestos básicos:

- Que las medidas adoptadas sean adoptadas de conformidad con la legislación interna del Estado.
- Que respondan a una situación de tal gravedad que amenace a la propia existencia de la nación.
- Que dichas medidas no contravengan las restantes obligaciones del Estado en virtud del derecho internacional.

[59] MUÑOZ MOSQUERA, A. y BACHMANN, S. D. «Lawfare in Hybrid Wars: The 21st Century Warfare». *Journal of international humanitarian legal studies*. N.º 7. 2016, pp. 63-87.

- Que el Estado concernido comunique oportunamente al secretario general del Consejo de Europa la naturaleza de las medidas y su ámbito temporal de aplicación[60].

La aplicación de estas medidas podría amparar la adopción de medidas restrictivas de la libertad de los ciudadanos, de la libertad de expresión, de la libertad de reunión y de asociación, entre otras. En todo caso, el elemento de hecho que justifica la adopción de las referidas actuaciones se reserva para situaciones ciertamente extremas, de tal forma que el propio artículo 15 del Convenio (que de forma reveladora lleva por título el de «Derogación en caso de estado de excepción») pone como ejemplo comparativo la existencia de un acontecimiento tan grave como es un conflicto armado. Por ello, cabe entender que la citada derogación expresa de obligaciones resulta una medida extrema que no se corresponde ni resultaría proporcionada para responder a la inmensa mayoría de las amenazas que se derivan de las actuaciones de zona gris.

Sin perjuicio de ello, la posibilidad de limitación del ejercicio de alguna de las libertades a las que hemos hecho referencia, fuera de los casos extremos que justifican la derogación, ha sido expresamente reconocida por el Consejo de Europa y el propio Tribunal Europeo de Derechos Humanos en los casos en que así lo impongan las exigencias de la seguridad nacional o de la seguridad pública. De esta forma, en las situaciones en las que las amenazas derivadas de las acciones en la zona gris den lugar a una amenaza para la seguridad nacional, el Estado afectado podrá limitar el ejercicio de ciertos derechos y libertades de los ciudadanos para tratar de neutralizar la amenaza, todo ello, naturalmente, con sujeción a unos elementales principios de legalidad y proporcionalidad. Tales restricciones permitirían, por ejemplo, adoptar medidas limitativas de la libertad de movimientos, del derecho a la intimidad, de la libertad de expresión, de la libertad ambulatoria o de las garantías establecidas en los procedimientos de expulsión de extranjeros.

Con arreglo a lo expuesto, la adopción de medidas restrictivas o limitativas de los derechos y libertades de los ciudadanos, si bien es una posibilidad que no resulta en sí mismo ilícita, siempre que se cumplan los presupuestos para su adopción, no parece ser una opción admisible para los Estados occidentales, salvo en casos extremos. En efecto, las exigencias del Estado de derecho y una consolidada cultura que impone el escrupuloso respeto por parte de los gobernantes a las libertades ciudadanas son elementos que determinan que la limitación excepcional de las mismas haya de considerarse siempre como la última acción posible, después de agotar todos los recursos disponibles para neutralizar la amenaza.

[60] No obstante, tal y como ha declarado el Tribunal Europeo de Justicia en la sentencia dictada con fecha 16 de septiembre de 2014, en el asunto «Hassan contra el Reino Unido», la citada comunicación no resulta preceptiva en los casos en los que resulten de aplicación las disposiciones del DIH.

La resiliencia jurídica

Tal como se ha señalado anteriormente, el uso de técnicas de zona gris da lugar a una suerte de «asimetría jurídica» que permite que el adversario pueda emplear, en la práctica, medidas de fuerza contra otro sin que este último pueda oponer el recurso a la fuerza armada en legítima defensa. Desde un punto de vista legal, y siguiendo a Sari, la definición de un sistema para contrarrestar los efectos de la referida asimetría pasa necesariamente por tres etapas:

- El desarrollo de una definición de las dinámicas jurídicas que conforman las amenazas híbridas.
- La determinación de las posibles vulnerabilidades legales.
- El fortalecimiento de las medidas de prevención, de disuasión y de defensa en el ámbito jurídico[61].

Precisamente, uno de los cuatro principios rectores de la política de seguridad nacional recogidos en la *Estrategia de Seguridad Nacional de 2017* es el de resiliencia, que tiene por objeto «fortalecer la capacidad de recuperación ante posibles crisis, manteniendo la estabilidad necesaria para garantizar la continuidad en la acción del Gobierno dirigida a la protección de los ciudadanos y la provisión de los servicios esenciales, para retornar al estado de normalidad en el menor tiempo posible, de modo que se minimicen las consecuencias negativas sobre la seguridad y el bienestar de los ciudadanos»[62].

Pues bien, ese mismo principio general resulta aplicable en su integridad a las dinámicas legales que se derivan de lo que hemos descrito como asimetría jurídica. De esta forma, el concepto de *legal resilience* o resiliencia jurídica ha surgido con fuerza en la doctrina para aplicarse a la capacidad de resistir los intentos de desestabilización del sistema jurídico. Sari define el concepto como la «resistencia de los sistemas jurídicos a los cambios y su capacidad de adaptación frente a los intentos de desestabilización»[63]. Desde este punto de vista, la resiliencia jurídica de un sistema normativo vendría dada por la medida en que es capaz de superar los vacíos, lagunas e indeterminaciones y por la posibilidad de adaptarse a las nuevas circunstancias y desafíos que presenta la realidad fáctica que pretende regular.

En cualquier caso, la base de la efectividad de la resiliencia jurídica se encuentra en la posibilidad de conseguir que el sistema de normas en su conjunto o un aspecto específico del mismo sea capaz de resistir los intentos de

61 SARI, A. *Op. cit.,* p. 26.

62 El concepto, naturaleza y características de la resiliencia, en particular, en lo relativo a su aplicación al ámbito de las operaciones en el ciberespacio, se abordan de forma clara y detallada en el capítulo 3 de esta publicación, a cargo de la De Tomás Morales, por lo que nos remitimos a lo allí expuesto.

63 SARI, A. *Op. cit.,* p. 20.

manipulación y desestabilización sin perder el objeto y finalidad que le es propio. Con arreglo a este principio, el citado mecanismo resulta de aplicación tanto en el plano de la resiliencia de las normas domésticas, como en el de las normas internacionales. De hecho, esta última perspectiva es la que resulta de mayor utilidad, en la medida en que, tal y como expone Shea, la adopción de una estrategia de resiliencia en el ámbito internacional permite el intercambio de diferentes puntos de vista y aunar esfuerzos en el fortalecimiento de las normas internacionales y del *status quo*[64].

En definitiva, la resiliencia jurídica ofrece una base común a partir de la cual resulta posible aunar esfuerzos a la hora de categorizar las distintas amenazas contra la integridad del sistema normativo internacional y de hacer frente a las mismas de forma más eficiente.

Conclusiones

La proliferación de acciones que explotan las ambigüedades de la zona gris ha sido constante en los últimos años y cabe esperar, a la vista de la evolución política internacional, que tales acciones cobren aún mayor importancia en los años venideros. Tal y como se ha señalado a lo largo de este trabajo, el recurso a tales estrategias no solo lo podemos observar en las acciones de los Estados revisionistas o de los agentes no estatales, sino que implica también a las potencias defensoras del *status quo* internacional. En todo caso, resulta igualmente evidente que los Estados occidentales son más vulnerables a estas amenazas precisamente por su mayor vinculación con el orden internacional establecido y por su mayor exposición a factores tales como la opinión pública o la crítica internacional.

Por tal razón, cabe entender que la posición que deben adoptar los países de nuestro entorno ante estos fenómenos debe ser esencialmente la de actuar en defensa de la legalidad internacional, fomentando y apoyando el cumplimiento de las obligaciones de los Estados con arreglo a los dictados de la buena fe. Otro modo de actuar, diferente al apuntado, que tendiera a la explotación interesada y manipuladora de las ambigüedades del sistema, además de contribuir a deslegitimar sus acciones, colocaría a los países de nuestro entorno en una posición de enfrentamiento en un terreno, como el de la zona gris, en el que se encuentra en franca inferioridad frente a sus posibles oponentes. Como consecuencia de ello, se hace imprescindible apostar inequívocamente por la defensa de las normas y principios que integran el ordenamiento jurídico internacional, así como por el desarrollo ordenado de los mismos con vistas a poder afrontar las nuevas realidades y desafíos que se presentan en el orden mundial. En este orden de cosas, compartimos plenamente la opinión expresada por De Tomás Morales en el capítulo tercero de esta publicación, al señalar que «... el hecho de que los autores de

[64] SHEA, J. «Resilience: a core element of collective defence». *NATO Review Magazine*. 2016.

los ciberataques se aprovechen de las vulnerabilidades que presenta este espacio virtual como campo de batalla no debe ser una justificación para que las operaciones de las FAS se sirvan de las mismas vulnerabilidades de esa zona gris, separándose del cumplimiento de los principios y valores que iluminan esas operaciones en los espacios físicos».

El gran reto que se nos presenta es, por tanto, el de fortalecer la eficacia de las normas de derecho internacional, adoptando nuevas normas que se adapten a las dinámicas que presentan las nuevas amenazas y reforzando en la medida de lo posible los medios de resolución de las controversias. Desde el primero de los citados puntos de vista, parece necesario regular algunos aspectos de las actividades que tienen lugar en ese campo intermedio que hemos tratado de definir entre la guerra y la paz, como es el caso de las actividades cibernéticas o de las normas sobre responsabilidad internacional de los Estados.

De igual forma, se hace necesario trabajar juntamente con los Estados aliados para poner en marcha mecanismos que permitan identificar y hacer frente de forma efectiva a las amenazas derivadas del uso de estrategias de zona gris, así como –en el ámbito interno– integrar adecuadamente en esta tarea los esfuerzos de los distintos órganos de la Administración que resulten competentes, junto a diferentes actores de la sociedad civil.

En suma, solo una adecuada concienciación sobre las amenazas que se pueden derivar de las acciones en zona gris, una implicación activa de toda la sociedad y una adecuada cooperación con los países aliados pueden dotarnos de la capacidad de resiliencia necesaria para afrontar con garantías de éxito los retos a los que nos enfrentamos en este campo.

Capítulo segundo

Las operaciones militares en el ámbito cognitivo: aspectos jurídicos

Rafael José de Espona

Resumen

El ámbito cognitivo del campo de acción de las Fuerzas Armadas se ha definido de manera específica por la doctrina de defensa española al mismo tiempo que se ha desarrollado la aplicación práctica del concepto de «amenaza híbrida» en el entorno internacional del conflicto y su «zona gris». Asimismo, ello ha coincidido con el desarrollo de la función de integración militar denominada comunicación estratégica (STRATCOM, por su acrónimo en inglés), que es idónea para la acción cognitiva. El propósito del presente estudio consiste en dilucidar si existen nuevos límites jurídicos a las operaciones militares en el **á**mbito cognitivo y, de haberlos, cuáles son y cómo se aplican.

Palabras clave

Ámbito cognitivo, comunicación estratégica, STRATCOM, «zona gris» del conflicto, amenaza híbrida, límites jurídicos, operaciones militares.

Abstract

The cognitive sphere of the scope of action of the Armed Forces has been specifically defined by the Spanish defense doctrine at the same time that practical Implementation of Hybrid Threat concept has been developed in the international environment of the conflict and its «grey zone». Likewise, this has coincided also with the development of the military integrated function called Strategic Communication (STRATCOM), which is suitable for cognitive action. The purpose of the present study is to elucidate if there are new legal limits for military operations in the Cognitive Sphere and, if so, what they are and how to implement them.

Keywords

Cognitive sphere, strategic communication, STRATCOM, grey zone of conflict, hybrid threat, legal limits, military operations.

Introducción

Configuración del actual teatro de operaciones en el ámbito cognitivo. Sociedad de la información, amenaza híbrida y STRATCOM

El ámbito cognitivo del campo de acción de las FAS (Fuerzas Armadas) se define específicamente en la doctrina de defensa española coincidiendo con la aplicación práctica del concepto de amenaza híbrida en el entorno internacional del conflicto, así como con el desarrollo de la función de integración militar denominada STRATCOM, idónea para la acción cognitiva. Ello plantea la cuestión de si existen nuevos límites jurídicos a las operaciones militares en dicho ámbito.

La guerra y las modalidades del combate han cambiado mucho respecto de la concepción clásica, tras el proceso de la década precedente conocido como RAM (revolución en asuntos militares), con la aparición de los *conflictos de IV generación* –que implica combatir+estabilizar, integrando en el planeamiento los efectos previstos y sus repercusiones en medios de comunicación– y la mayor importancia de la llamada *guerra asimétrica* junto a un global y exponencial incremento tecnológico de redes de telecomunicaciones y de digitalización. Todo ello facilita las operaciones encubiertas, irregulares, de bandera falsa y decepción, la ciberguerra, la guerra de información y otras actividades hostiles insidiosas efectuadas por quienes se sustraen de los cauces formales y convencionales de los conflictos bélicos. Así, la moderna doctrina de la *guerra hí*brida contempla la agresión no formalmente declarada, de amplio espectro incluyendo la esfera económica y la desestabilización social, con frecuente empleo de INFOOPS y PSYOPS[1]. Esto forma parte de la realidad de la guerra y los conflictos contemporáneos y futuros, además, claro está, del clásico combate cinético con tropas uniformadas (aunque solo sea a efectos de disuasión). Si bien el factor psicológico es consubstancial a toda acción humana –y se ha explotado para influir, amenazar, hostigar y agredir a lo largo de la historia– las PSYOPS estructuradas según la metodología moderna poseen un recorrido iniciado en la I Guerra Mundial[2] que llega hasta las avanzadas técnicas actuales, apoyadas en los avances de la neurociencia[3].

---

[1] NATO STRATCOM CoE. ***Hybrid Threats. A Strategic Communications Perspective***. Riga, 2019, pp. 12, 13 y 20.

[2] MOUTON, Francois; PILLAY, K. y VAN`T WOUT, M. C. «The Technological Evolution of Psychological Operations Throughout History». En CLARKE, N. l. y FURNELL S. M. (editors). *Proceedings of the Tenth International Symposium on Human Aspects of Information Security & Assurance* (HAISA 2016 Frankfurt). Plymuth: ed. Plymouth University, 2016, pp. 266-278.

[3] U. S. ARMY. *From PSYOP to MindWar: The Psychology of Victory by Colonel Paul E. Vallely, Commander, with Major Michael A. Aquino, PSYOP Research & Analysis Team Leader*. Head-

Como señala la vigente *Doctrina para el empleo de las FAS* los ámbitos de operación militar son los espacios físicos y no físicos, que condicionan las aptitudes y procedimientos de los medios, fuerzas y capacidades que deben operar en ellos. Dichos ámbitos son el físico –desglosado en el terrestre, el marítimo y el aeroespacial–, el cognitivo y el ciberespacial[4].

La acotación doctrinal concreta del ámbito cognitivo describe que «es un ámbito intangible inherente al ser humano, considerado de forma individual, socializada u organizada, y es consustancial a su capacidad de juicio y de toma de decisiones», el cual alcanza a las voluntades de todas las personas afectadas por el conflicto y a los sistemas de inteligencia artificial, por lo que impregna al resto de ámbitos. Su principal limitación es que, para operar en él, se manejan aspectos intangibles y de difícil evaluación, como los valores, las percepciones, la conciencia, las actitudes y los prejuicios. [...] Este ámbito permite a las FAS alcanzar objetivos que quedan fuera del alcance de otros, mediante el empleo de técnicas de comunicación, la ciencia psicológica y otras ciencias sociales»[5], a los que debemos añadir los avances científicos aplicados a la ingeniería social[6]. De estos tres ámbitos, siempre han existido el físico y el cognitivo; el ciberespacial es contemporáneo y requiere la implantación de redes de telecomunicaciones y sistemas de computación (que no dejan de ser parte del ámbito físico terrestre, submarino y espacial radioeléctrico). El ámbito físico cambia su dinámica por las modernas prestaciones de las plataformas, comunicaciones y medios tecnológicos; el cognitivo también –sobre todo por el alcance masivo y en tiempo real de las acciones cognitivas sobre la población– y constituye un ámbito que impregna a los demás, puesto que las mentes humanas actúan sobre los planos físico y cibernético y los efectos de la actividad en dichos ámbitos alcanzan a lo propiamente cognitivo.

Lo que caracteriza al ámbito cognitivo contemporáneo es la accesibilidad masiva de la tecnología aplicada a las telecomunicaciones y a la gestión de información, la superabundancia informativa y de canales de difusión y terminales individuales de recepción puestos asequiblemente al alcance de la masa social. Con la difusión de computadores interconectados se aumenta el volumen de procesamiento de información –en tiempo real– y la interacción hombre-máquina (en creciente desarrollo, debido a las mejoras en sistemas operativos orientados al usuario, el lenguaje computacional y los dispositivos de *interface*). Por lo tanto, la dinámica del ámbito cognitivo contemporá-

quarters, 7th Psychological Operations Group, United States Army Reserve, Presidio of San Francisco, CA, 1980.

4 *Publicación Doctrinal Conjunta PDC-01 (A). Doctrina para el empleo de las FAS*, párrafo n.º 300, 2018, p. 79.

5 *Publicación Doctrinal Conjunta PDC-01 (A) Doctrina para el empleo de las FAS,* párrafo n.º 308, 2018, p. 81.

6 AVERY, Thomas. «Popper on "Social Engineering": A Classical Liberal View». *Reason Papers*. Vol. 26, Summer 2000, pp. 29-38.

neo es distinta cuantitativa y cualitativamente respecto del histórico, debido a que hoy día se impregna de la llamada sociedad de la información, concurrente con la sofisticación de las técnicas de ingeniería social aptas para la modelación de amplios segmentos de población.

Esta sociedad de la información se perfila actualmente por los siguientes 5 factores: saturación y desatención, empleo de metodologías analíticas irreflexivas, premisas epistemológicas implícitas simples, difusión de información asociada a ingeniería social, y soporte electrónico creciente con digitalización e *internet de las cosas.*

Respecto de la saturación informativa y desatención por sobrecarga de estímulo, se aprecia que el entorno de la información en la sociedad actual supone que, debido a la superabundancia de información disponible y a la alta frecuencia de difusión de nuevos contenidos, las audiencias se encuentran sobrecargadas. Así, su percepción se debilita en tanto que se produce una desatención sobre la información, bien porque se obvia buena parte de ella o porque, aun captándola, no se asimila en su totalidad o en su correcto sentido.

La forma en la que la información se percibe depende en gran parte de la manera en la que se procesa, incluyendo el método de análisis del proceso intelectivo consciente (reflexión) o inconsciente (intuición). Considerando que el adiestramiento y la costumbre previa respecto de las mecánicas de análisis condicionan el procesamiento de la información, el rápido y masivo flujo de información en medios de comunicación propicia el análisis simplista y poco reflexivo. Como tendencia de futuro basada en datos clínicos ya disponibles, surge en la población un crónico déficit de atención (por uso abusivo de dispositivos telemáticos) y una reducción del horizonte temporal en el análisis de la realidad (el hedonismo cultural reduce la capacidad de sacrifico, tolerancia a la frustración y perseverancia del esfuerzo), de modo que el potencial de análisis informativo humano –en general– se verán mermado, empleándose metodologías analíticas irreflexivas.

Las premisas epistemológicas implícitas simples refuerzan el factor anteriormente descrito. Las categorías de pensamiento, conceptos predeterminados, dogmática científica, paradigmas y tópicos culturales operan como premisas que condicionan el procesamiento de la información en todo su recorrido. El lenguaje periodístico o tertuliano preponderante (propiciado por la reducción de contenidos en humanidades en los planes de estudio escolar) incorpora elementos simplificadores implícitos sobre la construcción de los conceptos asociados a los términos empleados reiteradamente en la semántica de los medios de comunicación (i. e. uso frecuente de parámetros de reduccionismo binario, como la categorización progresista-retrógrado).

Entre la maraña del ruido informativo, se vislumbra la difusión de información asociada a vectores de ingeniería social. En la relación entre sociedad e información, opera un vector de doble sentido: aquella genera información y

también la recibe. En este orden, las aportaciones informativas configuradas adecuadamente –en sus contenidos/silencios, forma de exposición, canales de difusión y cronología– son susceptibles de modelar la sociedad en términos metodológicos de ingeniería (lo que se ha venido en denominar *ingeniería social*, en expresión de Karl Popper[7]). Debido a las distintas capacidades, percepción y estructura social de la población y las élites (de distinto tenor –político, científico, religioso o plutocrático– y alcance decisorio), las técnicas de ingeniería social y la instrumentalización de la información serán diferentes, aunque operando en un plano común.

Por último, cabe considerar el soporte electrónico de la información creciente, unido al fenómeno de digitalización y aparición de la llamada *internet de las cosas.* Es una tendencia de futuro la transferencia de soportes de información clásicos (papel) a electrónicos (archivos informáticos), favorecida por el proceso de digitalización en la industria, el comercio y el tratamiento del *marketing*. Las innovaciones industriales incorporan crecientemente componentes avanzados de electrónica de control, de uso generalizado (i. e. domótica) y conectados a redes telemáticas, de modo que desarrollarán la denominada *internet de las cosas*. Todo ello contribuye al fortalecimiento de los procesos de inteligencia artificial, que pueden ir restringiendo el ámbito de toma de decisiones humanas.

Las capacidades militares integradas para actuar sobre el ámbito cognitivo han devenido en la función denominada comunicación estratégica o STRATCOM[8], cuya evolución desde la doctrina norteamericana hasta su implantación en la OTAN ha llegado hasta la inclusión de STRATCOM como función directiva en los estados mayores (no como un mero coordinador externo) englobando INFOOPS, PSYOPS y asuntos públicos[9]. En nuestro estudio se parte de la definición española STRATCOM según la *Doctrina para Empleo de las FAS 2018*, que considera la comunicación estratégica como «la integración de todas las capacidades de comunicación, técnicas y funciones de información, con otras actividades militares, para comprender y modelar el entorno de la información, en apoyo del logro de los objetivos de la defensa

[7] AVERY, Thomas. «Popper on "Social Engineering": A Classical Liberal View». *Reason Papers*. Vol. 26, 2000, pp. 29-38.

[8] El acrónimo se debe a la influencia de la terminología anglosajona «Strategic Communication». En OTAN se entiende como una función de integración, empleándose desde 2009 (promulgación de la *Military Policy MC0628*, en 2017).

[9] SILVELA DÍAZ-CRIADO, Enrique. En Diego Mazón Born (coord.). La comunicación estratégica: «Comunicación estratégica: origen y evolución del concepto». *Documento de Seguridad y Defensa* n.º 72. IEEE-CESEDEN, 2017, pp. 13-34. U. S. ARMY. *From PSYOP to MindWar: The Psychology of Victory by Colonel Paul E. Vallely, Commander, with Major Michael A. Aquino, PSYOP Research & Analysis Team Leader*. Headquarters, 7th Psychological Operations Group, United States Army Reserve, Presidio of San Francisco, CA, 1980.

nacional»[10]. Si bien está militarmente definido el concepto STRATCOM, su doctrina se encuentra en proceso de elaboración. Al implicar la integración de INFOOPS, PSYOPS, inteligencia y contrainteligencia, asuntos públicos, comunicación externa y CIMIC, se maximiza la potencia del combate cognitivo. La función integrada militar STRATCOM, concurrente con otras funciones militares, opera en el mismo ámbito cognitivo sobre el que se proyecta la comunicación estratégica del Estado. Conviene distinguir la modalidad de acción militar en el **á**mbito cognitivo –sea monitorización, protección, influencia o agresión–, la adecuación a audiencias propias o adversarias, así como sus instrumentos. Respecto de la situación final deseada y líneas de acción estratégica, STRATCOM debe partir de una armonía en la relación entre la orientación política y la dirección militar estratégica.

Constituye un reto complejo la acotación del ámbito cognitivo a efectos jurídicos y –más concretamente– desde la óptica militar, al respecto de operaciones y potenciales conflictos sobre aquel. A diferencia de los ámbitos físicos y ciberespacial, el ámbito cognitivo es totalmente intangible (y, al mismo tiempo, la interrelación de este con los demás ámbitos –especialmente el ciberespacial– es necesaria para la coherencia operativa de la acción cognitiva). Considerando que STRATCOM es una función de coordinación que integra capacidades para las operaciones militares en el ámbito cognitivo, la concordancia de efectos con los medios de acción sobre los ámbitos físico y cibernético introduce elementos que requieren la armonización jurídica entre los distintos tipos de operaciones militares concurrentes.

Los límites a la acción militar en el ámbito cognitivo pueden ser estructurados en torno al derecho y la ética. Para concretar aquellos, se plantean varias cuestiones jurídicas de partida ante el estado de la cuestión sobre la delimitación y marco jurídico de las operaciones militares en el ámbito cognitivo. Siendo STRATCOM un concepto reciente y con una doctrina militar en elaboración, adolece además de un alto grado de desregulación, incluso aunque entre sus funciones integradas se encuentran algunas ya antiguas (i. e. INFOOPS y Contrainteligencia). El ordenamiento jurídico, además, suscita frecuentemente confusión con la *Lex Artis* militar, realidad que evoluciona mucho más rápido que la normativa (i. e. proceso RAM, guerra híbrida), dado que el derecho tiene una cadencia mayor. Asimismo, ha de tenerse presente la llamada *lawfare* –neologismo anglosajón que fusiona terminológicamente los términos ley (*law*) y guerra (*warfare*)– en tanto que constituye un cauce de indebida limitación o lastre jurídico (hostilmente inducidos) de las capacidades propias. Por último, respecto de la cooperación cívico-militar, ha de tenerse presente que, en el ámbito cognitivo, a diferencia de los demás ámbitos, los medios y recursos necesarios para actuar son cuantitativa y

[10] *Publicación Doctrinal Conjunta PDC-01 (A) Doctrina para el empleo de las FAS*, párrafo n.º 433, 2018, p. 106.

cualitativamente superiores en el sector civil respecto del militar[11], motivo por el cual la contribución del apoyo civil y la articulación de adecuados cauces de cooperación público-privada resultan imprescindibles.

La doctrina conjunta de las FAS españolas establece principios morales y legales, determina como se ejecuta la acción conjunta y la combinada con aliados, así como la integrada con los demás instrumentos de poder del Estado. Parte de una descripción del entorno y el espacio de las operaciones, añadiendo a los ámbitos físicos tradicionales, el ciberespacial y el formado por la información y las percepciones. Según esta doctrina, «de entre los intereses nacionales de seguridad, se consideran vitales los que España está dispuesta a proteger y, llegado el caso, a defender ante cualquier agresión por poder llegar a afectar a su supervivencia como nación. Esto es, preservar intactos la soberanía, la independencia, la integridad territorial y el ordenamiento constitucional como elementos constitutivos del Estado, así como la libertad, la vida y la prosperidad de los españoles, dentro y fuera del territorio nacional»[12].

El propósito del presente capítulo consiste en dilucidar si existen nuevos límites jurídicos a las operaciones militares en el ámbito cognitivo y, de haberlos, cuáles son y cómo se aplican. Para ello, partiremos del análisis del marco jurídico de las operaciones, enfocando las implicaciones jurídicas de la acción de los poderes estatales de defensa nacional en dicho espacio y considerando especialmente la trascendencia jurídica de los medios militares para la acción cognitiva, planeada desde la función STRATCOM. El objeto se centra en el empleo de las FAS en operaciones militares, atendiendo al marco normativo vigente y al contexto jurídico en que se encuentran, en orden a discernir cuáles son los límites existentes (y su eventual novedad), tomando en consideración las modernas tecnologías disponibles y los procedimientos operativos actuales. Nuestro enfoque está orientado por la *Doctrina Conjunta para el Empleo de las FAS* –PDC-01(A)– que contempla los ámbitos cognitivo y virtual además del clásico físico que abarca el terrestre, el marítimo y el aeroespacial. Nuestra atención se dirige al *ius in bello*[13], al *ius ad bellum* y al derecho en tiempo de paz tanto en condiciones de normali-

11 MANDELBLIT, Avihai. «Lawfare: the Legal Front of the IDF». *Military and Strategic Affairs*. Vol. 4, n.º 1, abril 2012, pp. 51-57.

12 *Publicación Doctrinal Conjunta PDC-01 (A) Doctrina para el empleo de las FAS*, párrafo n.º 044, 2018, p. 23.

13 Como es sabido, la apreciación de la licitud en el marco legal del conflicto se discierne a partir de 3 principios: de distinción (de la población civil respecto de los combatientes), de proporcionalidad y de limitación de la acción hostil. ALIA PLANA, Miguel. «Reglas de enfrentamiento (II): gestión de blancos (*targeting*)». *Cuaderno Práctico* n.º 8. Escuela Militar de Estudios Jurídicos, julio-diciembre 2016, pp. 7-49.

dad como de crisis interna, ponderando las particularidades operativas que la acción cognitiva requiere en cada caso[14].

Además de la intrínseca complejidad jurídica de una materia que trata sobre la intangibilidad de la dimensión cognitiva (agravada por la obsolescencia conceptual en la literatura jurídica doctrinal sobre asuntos militares, que propicia confusión y malinterpretación sobre los medios y efectos cognitivos de la acción militar), se presentan obstáculos prácticos adicionales, habida cuenta la falta de doctrina militar STRATCOM tanto nacional como OTAN y la desregulación específica de la acción militar en el ámbito cognitivo; además, la acción operativa estructurada y desarrollada es todavía incipiente.

Nuestra metodología expositiva procede a explicar la acción militar en el ámbito cognitivo desde la óptica que permita apuntar los aspectos jurídicos clave para, finalmente, concentrar una reflexión sobre el marco legal. Se precisa que los límites jurídicos de la acción militar en el ámbito cognitivo son considerados en el contexto del *Sistema de Seguridad Nacional*, la cual está compuesta por la defensa nacional, la seguridad pública y la acción estatal exterior[15]. Metodológicamente, a la luz de los elementos que definen al ámbito cognitivo desde la óptica doctrinal del empleo de las FAS vigente[16], el análisis delimitativo desde la ley, la costumbre y los principios generales del derecho requiere tomar en consideración la analogía respecto de la acción militar en el ámbito físico –que se encuentra más desarrollada jurídicamente– así como referentes clásicos plenamente aplicables en la actualidad (i. e. la desmoralización militar provocada).

Tipología del conflicto en el ámbito cognitivo

Desde la perspectiva militar, se considera conflicto la situación de confrontación –real o potencial– que afecta a la seguridad nacional, e implica a colectividades organizadas contendientes (las cuales no necesariamente han de encontrarse reconocidas por el derecho internacional) que, cuando emplean medios de combate para imponer voluntades, generan un conflic-

[14] VV. AA. «Analysis of Risk Communication Strategies and Approaches with At-Risk Populations to Enhance Emergency Preparedness, Response and Recovery». Final Report RAND, 2008, p. 20.

[15] Según define art. 9 de la Ley de Seguridad Nacional: «Se consideran componentes fundamentales de la seguridad nacional a los efectos de esta ley la defensa nacional, la seguridad pública y la acción exterior, que se regulan por su normativa específica. Los servicios de inteligencia e información del Estado, de acuerdo con el ámbito de sus competencias, apoyarán permanentemente al sistema de seguridad nacional, proporcionando elementos de juicio, información, análisis, estudios y propuestas necesarios para prevenir y detectar los riesgos y amenazas y contribuir a su neutralización».

[16] *Publicación Doctrinal Conjunta PDC-01 (A) Doctrina para el empleo de las FAS*, párrafo n.º 308, 2018, p. 81.

to armado[17]. La secuencia desde el riesgo potencial y la amenaza, hasta la agresión, perfila el tipo de conflicto.

La agresión producida y los medios de combate utilizados requieren una adecuada identificación, tanto para su planificación como para el análisis jurídico asociado a su empleo. Los nuevos tipos de armas actualmente disponibles y los efectos perjudiciales producidos mediante técnicas sofisticadas abren un elenco de posibilidades entre las que se encuentra la agresión al ámbito cognitivo y la lesión de sus componentes, así como los medios que podemos denominar «de agresión cognitiva» si su finalidad es análoga o generan efectos parejos a los del armamento convencional (como disuadir, agredir, neutralizar, conquistar o rendir). Si los espacios clásicos –tierra, mar, aire– y el ciberespacial pueden recibir la acción militar que conduzca a la supremacía militar, lo mismo debe ocurrir en el ámbito cognitivo.

El conflicto en o sobre el ámbito cognitivo posee elementos diferenciales por el campo y entorno de la acción y las aplicaciones técnicamente posibles: imprevisibilidad, transversalidad, insidiosidad, dinamismo y proyección, e interacción con el ámbito del ciberespacio.

En tanto que el ámbito cognitivo de las operaciones supone una dimensión transnacional, suprafronteriza y difusa sobre la que se generan y proyectan efectos de difícil predicción (inesperados por su contenido o alcance, prolongado o efímero), en un entorno de saturación informativa e irresponsabilidad o ignorancia de los posibles efectos adversos involuntarios (i. e. desde los medios de comunicación masiva e industria del entretenimiento se construyen patrones de referencia de consecuencias perniciosas), se causa una alta imprevisibilidad. Por otra parte, aunque se generen vectores de acción cognitiva desde el ámbito militar para actuar solo sobre el sector militar o elementos de índole bélica, su proyección es susceptible de extenderse sin fácil contención a otros sectores o a la sociedad en su conjunto, de forma transversal.

La acción militar cognitiva no necesariamente ha de ser invasiva ni lesiva desde la perspectiva de una agresividad manifiesta, sino que será incluso más efectiva si genera intoxicación informativa, desestabilización o influencia negativa del adversario, de ahí su carácter insidioso.

El aludido dinamismo del conflicto tiene relación directa con las prestaciones tecnológicas en los medios de comunicación, transmisión y difusión informativa, los cuales han revestido a las operaciones militares y de otros poderes públicos de unos parámetros que, por su complejidad y rapidez, para ser plenamente efectivos requieren anticiparse al conflicto y –llegado este– una precisa sincronización con el *tempo* de la guerra; además, su

[17] *Publicación Doctrinal Conjunta PDC-01 (A) Doctrina para el empleo de las FAS*, párrafo n.º 013, 2018, p. 18.

capacidad de proyección genera efectos de gran alcance, susceptibles de usurpación por terceros (i. e. el programa de influencia cultural de la URSS).

Respecto de la interacción con el ámbito del ciberespacio, este tiene una relación estrecha con el ámbito cognitivo, por cuanto que es cauce propicio para la acción sobre la dimensión cognitiva, simultaneada con la ciberguerra y la guerra electrónica (i. e. diseminación de contrainformación, inducción de fenomenología del tipo *fake news* y *Wikileaks*)[18].

En el ámbito cognitivo surge la cuestión de si el conflicto se considera armado. El medio de agresión cognitiva o de provocación cognitiva de la agresión física («arma cognitiva» sería una figura retórica algo forzada, pero semánticamente ilustrativa) aplica su acción sobre el ámbito cognitivo de forma que pueda generar efectos tangibles al desencadenar la violencia física y provocar el uso de armamento (i. e. propiciando una rebelión armada o contienda civil). Por lo tanto, en las operaciones militares sobre el ámbito cognitivo no puede excluirse del horizonte –en la escalada del conflicto– el uso concurrente, derivado o indirecto, del armamento, ni los efectos destructivos humanos o materiales.

Respecto del contexto de la acción militar en el ámbito cognitivo, se plantean tres posibles estadios. En primer lugar, la situación de conflicto armado. En esta se incluye la guerra en estadio formal y permite aplicar el *ius in bello.* El conflicto –su mera existencia o su originación– entraña una intrínseca relación con la información de modo que, cuando el conflicto es subyacente, subrepticio o todavía en potencia, la comunicación de los elementos que lo evidencian puede operar como un coadyuvante o un retardante del propio conflicto, según el sentido de empleo. A este respecto, las acciones que conformen el medio de agresión cognitiva pueden generar sobre el adversario una desestabilización social o crear incluso un estado subversivo interno previos incidiendo sobre las percepciones y las actitudes, bien como apoyo a otros vectores hostiles o como acción unívoca independiente (los conflictos en el ámbito ciberespacial plantean una problemática similar en varios aspectos). Teóricamente, cabría debatir en qué medida un conflicto es solo o preponderantemente cognitivo, aunque es indudable que la acción hostil cognitiva puede ser la primera manifestación del conflicto.

A su vez, en esta situación de conflicto cabe distinguir, por una parte, el conflicto circunscrito al **á**mbito cognitivo. Es clara su delimitación en cuanto al ámbito de acción, pero compleja la acotación de sus efectos extensivos al ámbito físico. Por otra, se presenta el conflicto producido en el **á**mbito físico o ciberespacial[19], que trasciende implícitamente al **á**mbito cognitivo por los

[18] LEWIS, James A. «Cognitive Effect and State Conflict in Cyberspace». CSIS, 2018. NATO STRATCOM CoE. «The Black Market for Social Media Manipulation». NATO STRATCOM CoE–SINGULAREX, 2018.

[19] CCN-CERT. *Desinformación en el ciberespacio*. CCN-CERT / BP 13. Febrero 2013.

efectos que las acciones en aquellos generan en este. En virtud de los medios de acción y la forma de aplicarlos, y según las operaciones militares (que serán fundamentalmente de carácter encubierto, con la consubstancial dificultad probatoria de la misma) que se desarrollen en el **á**mbito cognitivo, considerando los efectos negativos sobre este –sean injerencia, desestabilización, subversión cognitiva o agresiones de baja intensidad– podemos distinguir diferentes tipos de conflicto[20]. A efectos jurídicos, creemos conveniente destacar este aspecto en lo concerniente al cálculo de la proporcionalidad de la respuesta. Ello es así porque la reciprocidad de la acción ha de ser delimitada según se intervenga en el **á**mbito cognitivo de otro Estado modelándolo sin lesividad (i. e. configurando la percepción, la interpretación analítica, la construcción de narrativas o la inoculación de conceptos y términos semánticos), se provoque una alteración de los parámetros de equilibrio del **á**mbito cognitivo del adversario, se genere una modificación en actitudes y percepciones en sentido opuesto al deseado por este (pero que en sí mismo no conlleva más efectos directos ni es aprovechado para otras acciones) o se causen efectos lesivos de distinto alcance y área de aplicación, a partir de las agresiones al **á**mbito cognitivo en sí mismo considerado (i. e. provocar pánico social) o cursando a través de este hacia otros ámbitos (i. e. crear revueltas sociales).

En segundo lugar, la situación de ausencia de conflicto. Ello obliga a actuar fuera del *ius in bello*, bajo unos parámetros jurídicos de paz formal. Estos pueden ser modulados al respecto de tres tipos de intervenciones de índole militar sobre el ámbito cognitivo, en tareas de prevención y protección, vigilancia y alerta temprana, y disuasión. Con ello aludimos a la motivación, todavía en tiempo de paz, de las posibles operaciones permanentes o de reacción que hubieran de activarse posteriormente.

Por último, encontramos la zona gris del conflicto, se entiende por esta la parte del espectro de los conflictos en la cual predominan acciones al margen del principio de buena fe entre Estados (o entidades en posición análoga) las cuales, aunque socavan la paz, no incurren en supuestos formalmente considerados como constitutivos de respuesta armada. Esta zona gris se perfila en base a las lagunas normativas o el exacerbado garantismo legal, debilidades sociopolíticas, rigidez institucional en la gestión de conflictos y compleja toma de decisiones, entre otros factores. Las actividades a desarrollar en la zona gris –con distinto grado de clandestinidad, ambigüedad y visibilidad– tienden a mantenerse en un entorno de baja intensidad para confundir, desestabilizar y debilitar al adversario, minando su capaci-

[20] Particularmente estimamos lo que sería una campaña autónoma mediante medios susceptibles de ser calificados como «medios de agresión cognitiva» (que incorporan máximas capacidades derivadas de la neurociencia aplicada), una acción integrada en operaciones convencionales en los ámbitos físico y ciberespacial, actuando los medios de acción cognitiva como multiplicador de efectos de la fuerza de combate, o una contribución militar a la acción de otros instrumentos del Estado, para objetivos no militares.

dad de respuesta. Dichas actividades abarcan los sabotajes, los disturbios subversivos y otros[21]. La amenaza híbrida es propicia sobre la zona gris del conflicto. A este respecto, Lanz destaca la reciente institucionalización de mecanismos encargados de identificar y afrontar las amenazas producidas en esta zona en tanto que, frecuentemente, se presentan actores quienes –empleando recursos al margen del uso de la fuerza armada y al borde de la legalidad internacional– aprovechan maliciosamente las lagunas normativas y dificultan la identificación de la amenaza y la reacción adecuada del adversario. Este tipo de acciones en la zona gris del conflicto conculcan principio de buena fe que rige en las relaciones internacionales y entrañan para el oponente agredido una dificultad de respuesta (de hecho, la mayor capacidad militar de un Estado o alianza militar es ineficaz, o al menos ineficiente, para afrontar dichas amenazas) puesto que, bajo el artículo 2.4 de la Carta de las Naciones Unidas –que prohíbe a los Estados el recurso a la amenaza o al empleo de la fuerza armada contra la integridad territorial o la independencia política de otro Estado (con la excepción el principio de la legítima defensa individual y colectiva)– no es viable salvar la limitación que implica la existencia real de un ataque armado[22].

La cuestión se complica en cuanto a la propia entidad jurídica de los sujetos implicados, por cuanto que el adversario es (cada vez más) de composición compleja o difícil identificación. De este modo cabe considerar –junto a los clásicos potenciales adversarios, Estados y organizaciones multinacionales– la presencia de otros entes sujetos a distinta regulación jurídico-internacional (i. e. organizaciones terroristas, criminales, grupos paramilitares, apátridas) o incluso indeterminados[23]. Dado que, frecuentemente, las amenazas, riesgos y agresiones sobre el ámbito cognitivo se desenvuelven en la zona gris del conflicto, no ha de darse por supuesto que el enemigo actúe con respeto al marco legal al que se sujeta la actuación de las FAS, ni que estime análogamente los criterios de legitimidad o fundamentación moral que sirvan para respaldar su acción.

A medida que se desglosan los componentes de la acción hostil sobre el ámbito cognitivo, se va ampliando el espectro de la singular problemática de trascendencia jurídica, incluso sobre la mera existencia del conflicto y su génesis subyacente. Sobre esto, se señalan dos aspectos de especial relevancia: la percepción de la amenaza o agresión, y la atribución de la acción.

---

21 *Publicación Doctrinal Conjunta PDC-01 (A) Doctrina para el empleo de las FAS*, párrafos n.º 363-365, 2018, p. 18.

22 LANZ RAGGIO, Mario. «El conflicto en las sombras: aspectos generales y elementos jurídicos de las operaciones en la zona gris», en la presente monografía. BAQUÉS, Josep. «Hacia una definición del concepto "Gray Zone" (GZ)». *Documento de Investigación 02/2017*. Instituto Español de Estudios Estratégicos, 2017.

23 *Publicación Doctrinal Conjunta PDC-01 (A) Doctrina para el empleo de las FAS*, párrafo n.º 017, 2018, p. 19.

En cuanto a la percepción de la amenaza o agresión producida sobre el ámbito cognitivo, o de los medios cognitivos utilizados para canalizar los ataques potenciales o efectivos, estimamos que para ello se requiere el conocimiento de técnicas especiales analíticas y un adiestramiento previo por parte del personal militar (i. e. metodologías de ingeniería social inversa). Doctrinalmente, «se entiende por percepción la interpretación subjetiva, elaboración personal o representación mental, fruto de la interiorización de la información y los estímulos recibidos del entorno»[24]. Ahora bien, la evidenciación taxativa y formal, para encajar completamente en los tipos jurídicos categorizados del *casus belli*, será difícil cuando no imposible. Es similar a la problemática que acontece al respecto de la percepción de un ciberataque.

La adecuada atribución de la acción o vector cognitivo hostil conlleva conocer la causa última, la responsabilidad en la elección en los medios empleados y la verificación de la intencionalidad agresiva. La constatación de una amenaza o agresión se basa en lo que podemos denominar indicadores y señales (siendo los primeros espontáneos y los segundos deliberados). Ambos sirven al sujeto receptor como elementos reactivos. La atribución es distinta según quién perciba la situación, puesto que la sociedad –compuesta por la población y su élite– enfoca la realidad de forma disímil. Confirmada la percepción efectiva de la amenaza o agresión en el campo de la energía, se plantea de inmediato el problema de la atribución de esta, en base a la cual se relaciona esta con un determinado agente causal adversario, sea porque puede ser definido explícitamente o porque se le desenmascara. En este último supuesto, ello se produce frecuentemente con un considerable grado de incertidumbre que, a veces, motiva divisiones internas en los estamentos rectores reacios a reconocer una amenaza o agresión realmente producida, o su atribución concreta. En todo caso, esta siempre habrá de ser comprobada con rigor para evitar ser víctima de engaño (decepción). De acuerdo con SALAS –tratando dicha problemática desde la perspectiva de la acción en el ámbito ciberespacial, que es análoga al ámbito cognitivo a estos efectos[25]–, la atribución de la acción hostil, para un adecuado *targeting* (tanto en respuesta como en disuasión) es regla básica del derecho internacional humanitario que las operaciones militares se dirigirán únicamente contra objetivos militares (artículo 48 del Protocolo I Adicional a los Convenios de Ginebra de 1949). Así, la necesidad militar requiere que los objetivos sean únicamente aquellos que realicen una contribución directa al esfuerzo bélico del enemigo, o que su destrucción o daño produzca una ventaja militar al atacante por su naturaleza, localización, propósito o uso[26].

---

[24] *Publicación Doctrinal Conjunta PDC-01 (A) Doctrina para el empleo de las FAS*, párrafo n.º 308, 2018, p. 81.

[25] LIBICKI, Martin C. *Cyberdeterrence and Cyberwar*. Santa Mónica: RAND, 2009, pp. 41-51.

[26] SALAS, Jacobo de. «De la flecha al ratón. Consideraciones jurídicas de las operaciones ofensivas en el ciberespacio» en la presente monografía. MOORE, Daniel. «Targeting Technology: Mapping Military Offensive Network Operations». En Minárik, T., Jakschis, R.,

La trascendencia de estas cuestiones en el plano del derecho internacional público lleva a complejas **c**onsideraciones jurídicas sobre el *ius ad bellum* y los posibles ajustes para delimitar una adecuada respuesta en cuanto a su justificación, homogeneidad y proporcionalidad.

Sobre la justificación, destacamos que, en el ámbito cognitivo, puede estar produciéndose un conflicto, pero no encontrarse revestido de los parámetros conformadores que permitan su evidenciación y prueba diáfana para justificar la respuesta, en términos de percepción y/o atribución (máxime cuando la sofisticación de las operaciones militares en el ámbito cognitivo a menudo solo permite su apreciación por parte de analistas expertos). Esto conlleva implicaciones jurídicas ante terceros que puedan disentir de la mera existencia de tal conflicto, no solo de la comunidad internacional sino de orden interno estatal, de modo que se provoquen disensiones internas entre las instituciones y poderes del Estado.

En cuanto a la homogeneidad o concordancia de medios o plano de acción en la reacción, se plantea en un doble sentido: como respuesta al ataque cognitivo con medios cognitivos o bien físicos o cibernéticos, o como respuesta al ataque físico o cibernético con medios cognitivos. En principio, no parece que sea procedente una respuesta heterogénea en el primero de los supuestos, salvo que se restringa al máximo la acción física o cibernética con medios violentos (i. e. destrucción puntual de la instalación desde la que se lanzan ataques cognitivos, sin daños personales). En el segundo supuesto, la ausencia de homogeneidad parece plenamente admisible. En todo caso, la combinación de aspectos cuantitativos y cualitativos junto a la limitación de efectos permitirá ponderar si la heterogeneidad de la respuesta es jurídicamente aceptable.

Por último, al respecto de la proporcionalidad, dado que el conflicto en el ámbito cognitivo tiene una larga «cadena hostil» hasta la guerra cognitiva total –en distintos grados–, la respuesta defensiva homogénea puede actuar de forma proporcional en cuanto a la gradación de la agresividad o la acotación del sector del ámbito cognitivo de que se trate (i. e. no es lo mismo alterar la percepción social sobre riesgos económicos que provocar una guerra civil).

La acción militar en el ámbito cognitivo y sus implicaciones jurídicas

Las implicaciones jurídicas de la acción militar en el ámbito cognitivo han de tenerse presentes con suficiente antelación, a fin de ajustar el marco normativo y configurar los elementos operativos con la adecuada concordancia jurídica. Al respecto de la ineficiencia normativa, en el derecho comparado

Lindström, L. (eds.). *CyCon X: Maximising Effects - 2018 10th International Conference on Cyber Conflic*t. Tallin: NATO CCD COE Publications, 2018, pp. 89-108.

Torres Soriano –quien recuerda un axioma elemental: «la voluntad de combate del Ejército [...] no solo depende de la moral de sus tropas y cuadros de mando, sino que orbita en torno a la percepción de su ciudadanía»- señala que la vigente ley federal norteamericana Smith-Mundt Act (promulgada en 1948) tenía como propósito la fundamentación jurídica de la contrapropaganda durante la Guerra Fría, e introdujo la salvaguarda democrática de la prohibición expresa de la distribución doméstica de instrumentos propagandísticos confeccionados para audiencias-objetivo extranjeras. De este modo, «los equipos jurídicos del Ejército [US Army] temen que la puesta en marcha de acciones eminentemente persuasivas en Internet, puedan ser interpretadas como una violación de esta disposición, debido al hecho de que este medio invalida la distinción entre audiencia doméstica y extranjera. Este rigor legal ha reducido considerablemente la oposición que el discurso insurgente encuentra en Internet, ya que su contestación proviene casi de manera exclusiva de entes no gubernamentales, con diversos y contrapuestos resultados». Por ello, concluye que «cuando se trata de librar conflictos asimétricos la poderosa maquinaria burocrática del Estado es más un obstáculo que una fuerza», de modo que, en la dimensión informativa del conflicto, se llega a producir una pérdida del control sobre los flujos de información que alcanza al interior de la propia fuerza combatiente[27].

Por lo tanto, a fin de no incurrir en errores de inadecuación jurídica normativa e interpretativa, conviene señalar las principales implicaciones jurídicas teóricas de la acción militar en el ámbito cognitivo, de acuerdo con su espectro de aplicación práctica y recorrido operativo.

La acción del Estado sobre el ámbito cognitivo supera, por medios y alcance, a la estrictamente militar, pero no actúa con su avanzada metodología polemológica ni dispone de la capacidad de sincronización integrada con medios bélicos cinéticos. Los instrumentos de poder de una nación para afrontar un conflicto son aquellos propios del Estado junto con la aportación social más allá de la estructura administrativa. Los instrumentos diplomáticos, de información, militar y económico son parte del poder de cualquier actor relevante en un conflicto. En el ámbito cognitivo se hace especialmente patente que, en los conflictos actuales, es necesario superar la mera interacción cívico-militar aplicando a las operaciones el principio de unidad de acción, que supone para las FAS la integración de la acción conjunta (y combinada, en su caso) con los demás instrumentos de poder del Estado, contando con los tres componentes: moral (voluntad de vencer y capacidad de sacrificio); intelectual; y físico de la capacidad de combate de las FAS[28].

---

[27] TORRES SORIANO, Manuel R. «Los límites de la guerra de la información. Lecciones aprendidas tras los conflictos de Iraq y Afganistán». *Revista Ejército*. N.º 818, junio 2009, pp. 14-22.

[28] STRATCOM ha de ser función directiva, no un coordinador externo, por lo que requiere integración de alto nivel. Tiene una utilidad plena y permanente, aplicable en formato bélico convencional, híbrido o en tiempo de paz, incluyendo la gestión de crisis.

Según el contexto formal de conflicto, paz o crisis, la acción difiere. En tiempo de conflicto armado, así como los medios de fuerza de combate son potestad exclusiva del Estado el cual encomienda su empleo a las FAS, la STRATCOM debe actuar armónicamente junto con las capacidades confluyentes desde distintos órganos del Estado para acción en el ámbito cognitivo. En tiempo de paz, STRATCOM se armonizará sin generar interferencias o conflictos con otros medios bajo dirección no militar, pero con libertad de acción para sus propios cometidos permanentes de vigilancia, disuasión, alerta temprana, defensa, prevención y protección. La gestión de crisis abarca distintos marcos jurídicos, desde la situación de normalidad a los escenarios atípicos jurídicamente diferenciados, como la situación de interés para la seguridad nacional y los estados de alarma, excepción y sitio, y la debida limitación de la transparencia administrativa en favor del secreto de seguridad nacional.

Al respecto de la potencial acción militar enemiga en el ámbito cognitivo propio, las FAS disponen de capacidad para detectar los indicadores de dicha acción (alerta temprana y análisis prospectivo), de modo que se puedan activar las acciones de protección, identificando la influencia o agresión enemigas y desarrollando acciones para contrarrestarla, la monitorización. En estas tareas se han de considerar los efectos jurídicos probatorios de las evidencias detectadas –sean vectores, indicadores (espontáneos) o señales (inducidas)– así como la *Lex Artis* de las técnicas empleadas (i. e. métodos de ingeniería social inversa), para una adecuada percepción y atribución. En todo caso, la protección del ámbito cognitivo (i. e. para neutralización de vectores cognitivos hostiles y *vacunación cognitiva*) deberá evitar colisionar con el derecho a la libertad de expresión y salvaguardar en todo caso el bien de cuantos integran la Nación española, en uso de su soberanía, en el marco de los principios y libertades y derechos fundamentales dimanantes de la Constitución Española.

Respecto de la acción militar en el ámbito cognitivo exterior, la posible influencia es de espectro amplio –ello no siempre constituye una injerencia internacional– y se deslinda claramente de la agresión, la cual puede afectar a aspectos diversos como actitudes y percepciones sobre la realidad de la conciencia situacional, a la estabilidad interna, a la paz social, al vigor de protección de la soberanía, etc. A este respecto, recordamos lo afirmado sobre el *ius ad bellum* e, aplicándolo tanto al enfoque bélico preventivo como reactivo; sobre las cuestiones de *ius in bello*, profundizaremos posteriormente. En cuanto a las misiones de paz, se añaden los aspectos jurídicos internacionales humanitarios en cuanto a los cuales consideramos procede destacar que el hecho de considerar audiencia-objetivo a la población civil no vulnera el principio de distinción por cuanto que la acción cognitiva a ellos destinada no genera efectos lesivos.

En el proceso de planeamiento, se presentan varias cautelas, partiendo de la definición de audiencias-objetivo con una cuidadosa delimitación para minimizar los posibles efectos negativos colaterales sobre la población civil

del adversario (i. e. generación de pánico en una operación de decepción)[29]. En cuanto a la elaboración de narrativas, las líneas de acción a desarrollar han de conducir a una situación final deseada la cual –pudiendo incluir la aspiración de alcanzar el dominio del ámbito cognitivo o bien centrarse en efectos específicos– en todo caso ha de ser acorde con los principios morales y valores éticos propios del mandato político de la misión y su marco jurídico aplicable, afirmación genérica que se aplica en el caso concreto de las narrativas con los contenidos semánticos de estas (i. e. sería indebido, para disuadir a la población de acciones contrainsurgentes, transmitir la idea de que los gobernantes de los países de la OTAN que intervienen en la misión internacional pretenden instaurar una dictadura).

En cuanto a los medios, estos incluyen sistemas de gestión, transmisión y difusión masiva de información, e incluso aquellos dispositivos que suelen denominarse como «armamento no letal» (i. e. cañones de microondas o dispositivos acústicos LRAD), si bien estos últimos solo cabrían ser utilizados en condiciones bélicas. En todo caso, es propicia la concurrencia con los medios militares de combate que sean menos cruentos (i. e. guerra de mando y control, guerra electrónica, ciberguerra). En condiciones de paz, cabría emplear medios de acción STRATCOM y cauces comunes o análogos a los utilizados en los gestores de la comunicación social, en plano de concurrencia con medios privados (i. e. agencias de publicidad, gestores de redes, demoscopia).

Los elementos subjetivos son, básicamente, el actor y el destinatario de la acción cognitiva. El sujeto activo son las FAS, por sí solas o en coordinación junto a otros poderes del Estado (cuestión imprescindible para evitar el entrecruzamiento y anulación/distorsión mutua de vectores de acción cognitiva, así como para garantizar la coherencia y concordancia de las narrativas y acciones[30]). Su legitimación activa se fundamenta en la misión jurídico-constitucional que se les encomienda. El sujeto pasivo es la audiencia-objetivo, bien connacional (en el caso de misiones de protección del ámbito cognitivo nacional, en tiempo de paz o de guerra) o foránea (en el supuesto de misiones de paz internacionales o en guerra, así como en apoyo aliado en tiempo de paz), cuestión que supone distintos contextos jurídicos. Sobre el sujeto pasivo, el principio de distinción ha de atenuarse en el marco de un conflicto, pues tanto combatientes como población civil comparten el ámbito cognitivo. También ha de tenerse en cuenta que, colateralmente, en muchas ocasiones tanto terceros como elementos propios se verán de alguna manera afecta-

[29] En el ámbito cognitivo, la acción es concurrente con otros emisores masivos –medios de comunicación, corporaciones, partidos políticos, agentes sociales, ONG y activismo social–, en un entorno de ruido informativo, saturación y *fenomenología viral en redes*. Por ello, la mutabilidad o volatilidad de los efectos cognitivos puede llegar a ser muy alta.

[30] SANTOS RODRÍGUEZ, Felipe. «La comunicación estratégica (STRATCOM) en los conflictos modernos: el caso de Afganistán». *Revista del Instituto Español de Institutos Estratégicos*. N.º 2, 2013.

dos por las acciones en un ámbito cognitivo común. Según se ha indicado, se requiere la protección –de acuerdo con la narrativa de los mensajes– de la audiencia propia (población, combatientes, decisores) y, en especial, de determinados segmentos sociales (i. e. infancia y colectivos vulnerables) que componen en parte o se relacionan con la audiencia-objetivo.

Los efectos generados por la acción militar en el ámbito cognitivo pueden tener una gran proyección, en tanto que la situación final deseada en el proceso de planeamiento, a nivel político, puede llegar a potenciar la fortaleza internacional del Estado y su solidez nacional. Aparte de los efectos pretendidos, la proyección espontanea de otros sobre el ámbito cognitivo es inherente a toda comunicación expresa o implícita a las acciones u omisiones; así, aun no siendo deliberada, aquella ha de ser tenida en cuenta por la STRATCOM. Además, es posible que los resultados de la acción cognitiva causen efectos colaterales favorables o adversos (i. e. percepción indebida por la propia fuerza), incluyendo daños colaterales al adversario o a terceros. Por lo tanto, para la planificación de efectos y ejecución de la acción cognitiva acorde, se requieren mecanismos de control y cautelas para una acción debida, jurídicamente definidos, articulados desde el principio de prudencia aplicado a la planificación y a la ejecución mediante las reglas de enfrentamiento (ROE, del inglés *Rules of Engagement*), y desde el principio de distinción respecto de la modulación de efectos sobre la audiencia-objetivo sea combatiente o no (i. e. provocar que los efectivos disparen contra sí, pero no contra sus propios civiles). Dichos filtros cautelares conllevan dos evaluaciones preliminares: de un lado, el análisis jurídico del contenido de las narrativas (considerando las implicaciones jurídicas de los mensajes, y su potencial tergiversación jurídica por el adversario) enemigas; de otro, el análisis neurocientífico de los posibles efectos probables, desde la óptica del derecho de la responsabilidad, por daños. En el caso de negligencia, se podrían llegar a plantear cuestiones de responsabilidad del Estado por daños causados a las personas[31].

Los aspectos técnicos-metodológicos, aun siendo adecuados al sentido e intención de una acción cognitiva legitimada, plantean cuestiones prácticas complejas sobre sus consecuencias. Constituyen perfidia los actos que traicionan la buena fe del adversario a la que apelan, pero no las estratagemas como las que entrañan las PSYOPS[32]. Los avances actuales en neurociencia y técnicas de modelación psicológica social facilitan la disponibilidad de tecnologías y métodos invasivos y dañinos de las capacidades de atención y percepción, del proceso intelectivo y memorístico, la fisiología del sistema

[31] En particular, se protegerán segmentos sociales vulnerables. Contra audiencias-objetivo cualificadas (i. e. élites decisoras, analistas de la comunidad de inteligencia, grupos de presión) el uso de narrativa arcana permite efectos lesivos restringidos a ellas.

[32] ALIA PLANA, Miguel. «Reglas de enfrentamiento (II): gestión de blancos (*targeting*)». *Cuaderno Práctico* n.º 8. Escuela Militar de Estudios Jurídicos, julio-diciembre 2016, pp. 7-49.

nervioso y el equilibrio mental (pudiendo forzar la asimilación de contenidos o inducir actitudes, decisiones y emociones gravemente perjudiciales para los individuos y la sociedad, capaces de desencadenar psicopatologías)[33]. Su insidiosidad depende del conocimiento multidisciplinar sobre los factores de percepción de la audiencia-objetivo: sus premisas epistemológicas, paradigmas conceptuales, interpretación de la narración del mensaje en el orden ético, metafísico y humanístico, incluyendo los canales no semánticos (arte, música[34], pintura, escultura/arquitectura, cine y estética). Procede, por lo tanto, definir los límites de empleo de tecnologías o métodos para no dañar la salud mental e integridad psicológica de las audiencias, de acuerdo con el marco jurídico interno de salud pública y el DIH. Tal delimitación depende del *estado del arte* de los medios tecnológicos y de los estudios realizados sobre su aplicación, en orden a predeterminar los posibles resultados de su empleo (lo que califica la prudencia debida del mando), y de una precisa segmentación de los grupos sociales que componen las audiencias-objetivo, para acotar mejor el principio de distinción (i. e. no sería temerario dirigir ciertos mensajes que infundieran temor a una parte de la población civil potencialmente insurgente, para disuadirla de su entrada en combate).

La participación activa del sector privado como apoyo a los medios de las FAS en la actividad en el ámbito cognitivo es una tendencia de futuro, apreciada en el contexto OTAN STRATCOM. La colaboración público-privada puede ser ocasional o permanente (contando incluso con una reserva civil especializada). La aplicación del principio jurídico de cooperación público-privada, destacado en las últimas disposiciones normativas y estratégicas de seguridad nacional *(Ley de Seguridad Nacional de 2015, Estrategia de Seguridad Nacional de 2017, Estrategia de Ciberseguridad Nacional 2019)* plantea, en la práctica, cuestiones de armonización jurídico-administrativa y jurídico-mercantil (todavía no concretadas en su solución por la normativa o la jurisprudencia), para evitar conflictos de interés y conculcar normativa empresarial, del libre mercado y competencia.

Entre ellas destacamos, *a priori*, dos posibles escenarios que son elocuentes: en primer lugar, en el caso de actuar sobre el **á**mbito cognitivo propio en una gestión de crisis, los fines de interés general que iluminan la acción militar (protección del **á**mbito cognitivo) facultan al medio privado de comunicación –que eventualmente colabore apoyando acciones STRATCOM– a emplear medios públicos (i. e. sistemas de telecomunicación militar, en un supuesto de fallido técnico de la red civil) que, en caso contrario, no serían para él accesibles, pero –al mismo tiempo– el uso de dichos medios le per-

[33] KRISHNAN, Armin. «From Psyops to Neurowar: What are the Dangers?». *ISAC-ISSS Conference*. Austin, November 2014.

[34] JUSLIN, Patrik y VASTFJALL, Daniel. «Emotional responses to music: The need to consider underlying mechanisms». *Behavioral and Brain Sciences*. N.º 31, 2008, pp. 559-621. LOVEGROVE, Kitty. «The acoustic world on influence: how Musicology illuminates Strategic Communications». *Defence Strategic Communications*. Vol. 5, otoño 2018, pp.13-49.

mite desarrollar simultáneamente otras actividades corporativas ajenas a la misión en tareas indisociables a las requeridas para la acción de apoyo (i. e. comunicar datos de gestión).

En segundo lugar, en caso de una operación militar sobre el **á**mbito cognitivo foráneo con apoyo de un medio de comunicación privado connacional que contribuye a la acción cognitiva, se plantea en qué medida existe conflicto de interés de este último cuando aprovecha su conocimiento anticipado y detallado de las narrativas para implementar lucrativamente una campaña publicitaria comercial. Sobre la complejidad de la procedimentación jurídica de la interacción público-privada, Sánchez Benítez recomienda reforzar los mecanismos de comunicación estratégica del Estado, elaborando un mapa de recursos comunicativos susceptibles de ser empleados a nivel estratégico[35]. La conducción de operaciones militares con apoyo privado o sincronizadas con este en plano cooperativo, requiere una reglamentación que armonice fines de interés general con otros particulares, lo cual deviene complejo por la asimetría jurídica público-privada y respecto de la capacidad de intervención en el ámbito cognitivo (i. e. transparencia de actividades, uso de información clasificada).

El ámbito cognitivo siempre estará ocupado por algo, incluyendo posibles elementos deseados por distintos actores que son en buena parte inciertos, desde los cuales –por prudencia defensiva– debe suponerse se generan potenciales acciones divergentes (cuando menos) de los efectos deseados por los poderes públicos nacionales. Por esta razón, se requiere una conciencia situacional permanente y sostenible, anticipada al conflicto y con capacidades prospectivas y de alerta temprana en el ámbito cognitivo.

Existen ciertas especificidades de trascendencia jurídica de las operaciones militares según actúen sobre el ámbito cognitivo propio o ajeno.

Respecto del ámbito cognitivo propio, conviene presuponer que la gestión enemiga de la STRATCOM oponente puede integrar metodologías de ingeniería social, incluso de gran alcance, que afecte al ámbito cognitivo objeto de nuestra protección; por ello, se requiere contar técnicas de ingeniería inversa para contrarrestar aquella y poder identificar las evidencias que, llegado el caso, sirvan como prueba de un posible *casus belli* convencional o híbrido a efectos jurídico-internacionales. En las operaciones de contribución militar a la acción del Estado, la acción cognitiva militar es decisiva especialmente en gestión de crisis, protección civil en condiciones de desestabilización o catástrofe[36], incluso por el simple hecho de que la visibilidad de tropas uni-

[35] SÁNCHEZ BENÍTEZ, Sergio. «La comunicación estratégica como política pública». *Documento de Opinión* n.º 21/2011. IEEE, 2011

[36] HERAS DURÁN, José Manuel de. «Marco jurídico de las funciones, no de defensa, de las Fuerzas Armadas en tiempo de paz». En Corrales Elizondo (coord.). *El marco jurídico de las Misiones de las Fuerzas Armadas en tiempo de paz. Cuaderno de Estrategia* n.º 116. Madrid: IEEE, 2002, pp.175-223.

formadas crea una inmediata percepción de gravedad situacional en la población. Junto a las acciones cognitivas cohesivas y de protección, en ciertos casos (i. e. subversión, terrorismo) se pueden requerir concurrentemente acciones cognitivas agresivas *ad-intra*, estrictamente acotadas al marco regulatorio nacional de seguridad nacional y estados de crisis con todos los mecanismos delimitativos propios del estadio que en concreto se trate, sea situación de interés para la seguridad nacional, estado de alarma, de excepción o sitio, y un criterio de máxima restricción en cuanto a medios, tiempo y alcance, según establece el art. 1 de la L. O. 4/1981: «Las medidas a adoptar [...] serán en cualquier caso las estrictamente indispensables para asegurar el restablecimiento de la normalidad. Su aplicación se realizará de forma proporcionada a las circunstancias».

En cuanto al ámbito cognitivo de acción externo (del Estado o área donde eventualmente se proyecte el potencial conflicto), la acción cognitiva orientada a prevenir el conflicto, en tiempo de paz, supone la preparación sostenible de la audiencia-objetivo exterior foránea para hacerla más receptiva a acciones cognitivas de presumible aplicación en caso de producirse el conflicto, incrementando su eficacia; aunque formalmente se desenvuelven en tiempo de paz, ante el riesgo de incurrir en acciones de tipo híbrido que desencadenen una escalada de conflicto, deben atenerse a los límites del derecho internacional público tanto en el fondo como en la forma. En las misiones exteriores de mantenimiento de paz, la acción cognitiva en este caso requiere, de un lado, una adecuación al entorno autóctono propio de la audiencia-objetivo local (i. e. contexto cultural, tipo de percepciones) y, de otro, la concordancia de acción con las demás fuerzas aliadas concurrentes (i. e. sinergia o compatibilidad de narrativas). Activadas en virtud del mandato OTAN, UE u ONU, son reguladas por el por el derecho internacional de los derechos humanos (DIDH) y, en ocasiones, por el DIH y, desde la normativa nacional militar, requiere dotar a la fuerza desplegada de un marco jurídico operativo lo más armonizado posible con las demás fuerzas internacionales, para facilitar una eficaz acción combinada, concretamente mediante ROE de índole cognitivo.

El desconocimiento técnico de la *Lex Artis* de las operaciones militares en el ámbito cognitivo puede provocar un tratamiento jurídico desenfocado sobre el tema. Este, desde un excesivo garantismo jurídico distorsionado (al que la doctrina para el empleo de las FAS alude al tratar de la magnitud de la zona gris del conflicto[37]), podría incurrir en el error de negar de raíz la legalidad e incluso legitimidad moral de la acción militar en dicho campo. El infundado temor a una supuesta injerencia militar sobre la autonomía de la voluntad de la sociedad civil, o a una hipotética extralimitación de funciones, pueden socavar la aplicación o eficacia de las operaciones militares en el ámbito

[37] *Publicación Doctrinal Conjunta PDC-01 (A) Doctrina para el empleo de las FAS*, párrafo n.º 364, 2018, p. 91.

cognitivo. Por lo tanto, para salvaguardar el pleno ejercicio de la libertad de la sociedad contando con la protección de su ámbito cognitivo, la eficacia de funciones militares como STRATCOM requiere resolver la problemática jurídica e interacción práctica concreta respecto de su incidencia en la conducción de las operaciones militares en el ámbito cognitivo, incluyendo medidas de cultura de defensa que evidencien la estricta legalidad de estas.

La inseguridad jurídica constituye un primer problema, de gran alcance. La insuficiente conceptuación jurídica del ámbito cognitivo respecto de la acción militar se aprecia en que el reflejo en el derecho de la moderna terminología relativa a las capacidades y operaciones a desarrollar en el ámbito cognitivo puede llevar a confusión debido a lagunas del ordenamiento jurídico, desregulación y cierta obsolescencia jurídica conceptual sobre la defensa y el conflicto armado respecto del empleo de las FAS en el ámbito cognitivo. Esto resulta patente en el neologismo STRATCOM pues, semánticamente, los términos «comunicación estratégica» pueden interpretarse como alusivos a las transmisiones (aunque el debate esté zanjado en el plano doctrinal militar, no así puede acontecer con el jurista profano)[38]. Además, existen asimetrías en las categorías jurídicas subjetivas que se perfilan en la actualidad de los conflictos (i. e. agentes clásicos de la guerra y entidades actoras en la «zona gris» o de tipo híbrido). Dado que la literatura jurídica y la normativa aplicable están concebidas originariamente para el medio físico y, recientemente, también para el ciberespacial –apenas para el cognitivo– se dificulta el recurso a la analogía entre los ámbitos y medios de índole físico y cognitivo. Esto puede complicar la adecuada interpretación de las ROE. A mayor abundamiento, en caso de plantearse procesos judiciales respecto de la licitud de determinadas acciones militares cognitivas, la dificultad de comprensión del complejo ámbito cognitivo y los medios neurotécnicos podría desembocar en debates sobre cuestiones de filosofía jurídica e interpretación normativa difusa de la *ratio legis* relacionada con conceptos de libertad individual y antropología sobre la autonomía de la voluntad, todo lo cual repercute en la debida seguridad jurídica que ha de revestir a los mandos de las operaciones militares.

Asimismo, junto a lo anterior, encontramos un alto grado de inconcreción jurídica en lo relacionado con la actividad sobre el ámbito cognitivo. La acción en este ámbito presenta varios aspectos difusos, heterogéneos y que adolecen de imprecisión a la hora de delimitar campos de acción, estimación de efectos a generar y verificación de la relación causal entre la acción y las posibles consecuencias negativas indeseadas, así como la valoración del *quantum* de los efectos e intensidad tanto de las acciones como del entorno

[38] Por nuestra parte, para un entendimiento jurídico generalista, consideramos más adecuada la expresión acción cognitiva militar, o guerra cognitiva en caso de estadio bélico, terminología empleada en la doctrina israelita: SIBONI, Gabi. «The First Cognitive War». En Kurz, A., Brom, S. (eds.). *Strategic Survey for Israel 2016-2017*. Tel Aviv: Institute for National Security Studies, 2016.

(grado de oposición o agresividad cognitiva presente en zona de operaciones). Asimismo, es complicado precisar la correlación entre el teatro, zona y área de operaciones en sentido físico y sus correspondientes segmentos del ámbito cognitivo, así como la identificación detallada de los centros de gravedad cognitivos. Todo ello conlleva dificultades de evaluación –a efectos jurídicos– de la proporcionalidad en uso de la fuerza y la adecuación de la asignación de medios a fines por parte del mando y su órgano de apoyo. En este orden, mencionamos el supuesto hipotético de que, ante un adversario que realiza acciones de hostilidad cognitiva media en apoyo a ataques armados pero de baja intensidad (i. e. se infunde temor social con narrativas desmoralizadoras, acompañado de pequeños sabotajes de infraestructuras), se realice en respuesta una oleada de acciones cognitivas altamente agresivas –aunque sin parejas acciones violentas en el medio físico– orientadas a provocar grandes daños personales y materiales en el adversario (i. e. desencadenar un enfrentamiento interno o guerra civil).

Delimitación del empleo de las FAS: las operaciones militares en el ámbito cognitivo

En nuestra opinión, sobre las operaciones militares en el **á**mbito cognitivo se presentan actualmente nuevos límites jurídicos principalmente en dos contextos: [1] la intervención en el **á**mbito cognitivo exterior foráneo en virtud de la legítima respuesta, en los prolegómenos del conflicto, con la finalidad de evitar la escalada del conflicto o, si no es posible, realizar los preparativos oportunos; y [2] la protección del **á**mbito cognitivo connacional en tiempo de paz. Ambas novedades jurídicas limitativas son, según nuestro parecer, extensivas, de manera que permiten un mayor margen de acción.

Sobre las operaciones militares de intervención en el ámbito cognitivo exterior foráneo en virtud de la legítima respuesta –con fines neutralizadores o preparatorios de ulteriores hostilidades armadas– en los prolegómenos del conflicto, esto lo hemos tratado previamente, a lo cual añadimos ahora que, en España, según la inspiración doctrinal OTAN, se introduce un criterio interpretativo favorable, ajustado a las nuevas modalidades de la amenaza híbrida y la zona gris del conflicto. No parecería prudente limitar la operatividad de las FAS y aumentar la vulnerabilidad esperando a que se resuelva (si ello es posible) el debate jurídico internacional abierto sobre las nuevas modalidades de conflicto: en el seno del Consejo de Europa se ha apuntado recientemente (2018) que no hay una definición universal acordada sobre lo que es la «guerra híbrida» y, por lo tanto, no existe un derecho de la guerra híbrida. No obstante, es común opinión que el principal elemento de dicho fenómeno bélico es la asimetría jurídica y legal que encarna, en tanto que sus actores implicados explotan las lagunas normativas y la complejidad jurídica de determinadas acciones, y operan a lo largo de las zonas limítrofes de las categorizaciones jurídico-normativas, evitando incurrir directamente

en los supuestos, tipos y campos de acción regulados respecto de la guerra y los conflictos, generando confusión, ambigüedad y fraude de ley para enmascarar sus hostilidades. La respuesta a este tipo de amenazas y agresiones requerirá una combinación de medios jurídicos, diplomáticos, militares y de contrainteligencia[39]. Pudiendo conocerse la intervención indebida del adversario en nuestro **á**mbito cognitivo sin la evidencia de conflicto incluso (aunque esta acción puede generarlo), la acción preconflicto cognitiva exterior en justa reciprocidad es factible; de este modo, en tanto en cuanto la atribución de la acción adversaria es más difícil de acreditar en el plano de la guerra híbrida, pueden activarse acciones militares cognitivas con mayor anticipación que las físicas, ya que sus efectos son incruentos y con considerable grado de reversibilidad.

En cuanto a los límites jurídicos a las operaciones militares de protección del ámbito cognitivo connacional interno en tiempo de paz, el primer aspecto delimitativo de las operaciones en este tiempo (así como también en guerra) se presenta por su propia razón de ser, que no es otra que la defensa del **á**mbito cognitivo nacional y la acción en este (u otros ámbitos foráneos, si procede) en virtud del artículo 8 de la CE, para salvaguarda de los derechos y libertades fundamentales constitucionales. Este mandato constitucional no puede cumplirse sin una adecuada conciencia situacional del ámbito cognitivo[40]. Por una parte, las acciones de comunicación estratégica llevadas a cabo por el gobierno del Estado son esenciales para la seguridad nacional si bien, por otra, las leyes que garantizan los derechos de los ciudadanos parecen contrarrestar la eficacia de dichas operaciones. Segell concluye que cuando los intereses protegidos por las PSYOPS corresponden cualitativamente a un nivel de seguridad nacional, ello tendrá prioridad (ocasionalmente) sobre el íntegro cumplimiento del marco de derechos de la ciudadanía[41]. Esta lógica parece ser subyacente a la normativa española relativa a los estados de alarma, excepción y sitio, en la cual se contempla la restricción temporal del ejercicio de los derechos y deberes fundamentales de la ciudadanía en virtud de dicha *ratio legis*. Sin embargo, no es solo en situación de crisis cuando procede actuar. La vulnerabilidad de la sociedad de la información ante las amenazas híbridas requiere un cierto incremento de la capacidad

[39] COUNCIL OF EUROPE – Parliamentary Assembly Committee on Legal Affairs and Human Rights. «Legal challenges related to the hybrid war and human rights obligations» report. Council of Europe, marzo 2018.

[40] Sobre el marco jurídico clásico de la acción en el ámbito cognitivo, WINGFIELD consideraba ya en 2005 que los aspectos clave para configurar el análisis jurídico relativo a las INFOOPS ofensivas (que en su estudio se relacionaba con el ámbito aeroespacial) deben sustentarse en torno a la definición del tipo de operación de que se trata en concreto, y si implican el uso de fuerza o efectos análogos al empleo de esta. WINGFIELD, Thomas C. «Legal Aspects of Offensive Information Operations in Space». US Department of Defense, 2005.

[41] SEGELL, Glen. «National Security Priority over the Rights of Citizens in PSYOP». *London Security Policy Study*. Vol. 8, n.º 2, julio 2013, pp. 3-10.

de acción cognitiva militar en situación de normalidad, para poder proteger permanentemente el ámbito cognitivo interior[42]. La cuestión del alcance de dicha capacidad es clave para contenerla en sus justos límites, propios de un Estado social y democrático de derecho, y es donde el derecho constitucional acota tanto la extralimitación de las fuerzas armadas en sus funciones como la insuficiencia en la aplicación del principio de transparencia administrativo, así como los contenidos insertos en las acciones cognitivas en tanto puedan conculcar las libertades y derechos fundamentales de los ciudadanos y la integridad de autonomía de la voluntad.

Estimamos que, en España, existe una doble delimitación de las operaciones militares en el ámbito cognitivo –implementadas de forma integrada con STRATCOM, o mediante capacidades específicas– que es de índole jurídica y ética. De ello dimana el marco de la acción cognitiva en el exterior y en el interior, con las diferencias consubstanciales a la aplicación, en el primer caso, del derecho internacional público:

Respecto del marco jurídico, este internamente comprende fundamentalmente la regulación española pivotando sobre la CE1978, en particular el *corpus* normativo de *Seguridad Nacional y Defensa* (incluyendo las ROE, como desarrollo de este). Se añaden, respecto de la acción exterior, las disposiciones de derecho internacional de los conflictos armados y del derecho humanitario ratificado por España. La doctrina jurídica jurisprudencial e interpretativa y el marco doctrinal militar son esenciales para aplicar el derecho según la *Lex Artis* militar. En el derecho interno y en el entorno OTAN impera un enfoque eminentemente ius positivista propio del Estado social y democrático de derecho.

Los límites éticos abarcan la deontología institucional militar –dentro de la tradición de honor de las FAS españolas–, los principios morales y valores éticos aplicables, los cuales se suelen inspirar en consideraciones consuetudinarias y en un ius naturalismo de índole racionalista (con el referente contemporáneo de la Carta Internacional de los Derechos Humanos de la ONU). En todo caso, tanto en el exterior como interior, son respetados.

Tal como se indicó inicialmente en nuestra Introducción[43], tomamos en consideración la analogía con relación a la acción militar en el ámbito físico, en tanto que metodológicamente nos permite suplir las lagunas normativas al respecto del ámbito cognitivo.

---

[42] En todo caso, se cuidará la confianza de los ciudadanos hacia las instituciones en todas las fases de la acción cognitiva (i. e. narrativas cohesivas). KAVANAGH, Jennifer y RICH, Michael D. *Truth Decay. An Initial Exploration of the Disminishing Role of Facts and Analysis in American Public Life*. Santa Mónica: RAND, 2018, pp. 191-206.

[43] *Publicación Doctrinal Conjunta PDC-01 (A) Doctrina para el empleo de las FAS*, párrafo n.º 308, 2018, p. 81.

El marco jurídico interno

Para delimitar jurídicamente el empleo de las FAS en todo ámbito, incluyendo el cognitivo, ante todo se requiere ajustarlo a los principios de legalidad y legitimidad establecidos en la CE 1978, en la legislación nacional y en los acuerdos internacionales suscritos por España (especialmente la Carta de las Naciones Unidas), partiendo de que las misiones generales de las FAS se encuentran definidas en la CE1978 y en la LO 5/2005 de la Defensa Nacional, pudiendo actuar en aplicación de la legislación nacional –en misiones permanentes o activadas, en condiciones de normalidad o estados de alarma, excepción o sitio–, en ejercicio del derecho a la autodefensa ante un ataque armado (art. 51 Carta de las Naciones Unidas), en virtud de un mandato de la ONU, de compromiso con la OTAN o la UE; a petición del legítimo Gobierno de un Estado foráneo; o para evacuar ciudadanos residentes en el extranjero.

En el derecho constitucional, encontramos que la CE1978 fue elaborada bajo un concepto clásico de la guerra y la milicia, en tiempos en los que en España no se plasmaba en la doctrina militar un desarrollo específico de la acción en el ámbito cognitivo (todo lo más, se estimaban las PSYOPS a nivel táctico u operacional, como potenciador de la fuerza). Sin embargo, la acción militar cognitiva planteada actualmente es plenamente admisible dentro del marco constitucional. El Estado social y democrático de derecho, en virtud de los arts. 8, 30, y 104 CE que proclaman los principios de seguridad, defensa y orden público y encomiendan su salvaguarda específicamente a las FAS (aunque no exclusivamente) –garantizando la soberanía e independencia de España, su integridad territorial y ordenamiento–, confía también con ello la protección del ámbito cognitivo (que es parte de la integridad de los ciudadanos) a las FAS, y a fuerzas y cuerpos de seguridad del Estado. Consideramos implícita dicha encomienda de protección del ámbito cognitivo porque este es indisociable de las mentes de los ciudadanos; así, el Centro Criptológico Nacional (CCN) ha señalado las consecuencias negativas que puede tener en los ciudadanos la pérdida de confianza en las instituciones públicas y en la soberanía por causa de ataques cognitivos de desinformación[44]. Con relación al grado de vigilancia sobre el ámbito cognitivo que correspondería a las FAS, encontramos una clara analogía con el ámbito aeroespacial pues, en este, se requiere una cobertura permanente para garantizar la detección, interdicción y neutralización de vectores hostiles, asimismo, ya se han señalado las concomitancias con el ámbito ciberespacial por el cual cursan en buena parte las acciones cognitivas. Se permite legalmente la limitación del derecho de acceso a la información y la transparencia administrativa sobre la base de secreto de Estado y de defensa, los cuales son compatibles con la salvaguarda de las libertades y derechos fundamentales, como la intimidad, la dignidad y la libertad de expresión (la privacidad y protección de datos

[44] CCN-CERT. *Desinformación en el ciberespacio*. CCN-CERT / BP 13. Febrero 2019, pp. 11-16.

personales se ven reforzados por el GDPR UE 2018). En contextos legales atípicos propios de las crisis, los estados de alarma, excepción y sitio (L. O. 4/1981) permiten la restricción temporal del ejercicio de libertades y derechos fundamentales, a diferencia de la situación de interés para la seguridad nacional (Ley de Seguridad Nacional de 2015). La posible contribución militar en actividades cognitivas de Estado puede obstaculizarse debido a la heterogeneidad conceptual jurídica relativa a la acción en el ámbito cognitivo respecto de otros órganos estatales, generando discordancia operativa interinstitucional, de manera que la eficacia de la acción se puede resentir; por lo tanto, conviene que la doctrina militar sobre acción en el ámbito cognitivo sirva adecuadamente a los poderes constitucionales para una verdadera acción integrada llegado el caso.

La Ley 36/2015 de 28 de septiembre de Seguridad Nacional introduce un marco normativo actual, propicio para la acción militar en el ámbito cognitivo interno en tiempo de paz, tanto en situación de normalidad como de crisis. Dicha norma ha sido fruto de una orientación de estrategia de Estado que ha facilitado el desarrollo normativo e institucional del Sistema de Seguridad Nacional, iniciado por la primera *Estrategia de Seguridad Española* (2011) de visión generalista y programática, desarrollado por la segunda *Estrategia de Seguridad Nacional* (2013) pormenorizada en objetivos y líneas de acción concretas y sistematizadas, y consolidado por la tercera *Estrategia de Seguridad Nacional* (2017) en un complejo contexto –como ha señalado Milosevich-Juaristi– de desestabilización territorial subversiva en el que se evidenció la injerencia cognitiva internacional de origen ruso (empleando la metodología de difusión abierta conocida como *fake news*)[45]. La Ley 36/2015 de Seguridad Nacional fue avalada por la STC 3/11/2016 frente al recurso de inconstitucionalidad de la Generalidad de Cataluña (contrario a la figura denominada *Situación de Interés para la Seguridad Nacional*). Otorga un marco normativo completo que no afecta a los derechos y libertades fundamentales de los ciudadanos, establece un *Sistema de Seguridad Nacional* (título II), que abarca la defensa + seguridad pública + acción exterior y define la *Situación de Interés para la Seguridad Nacional* (art. 23) que fija un estadio a nivel estatal que faculta para intervenir en materia de gestión de crisis y solución de incidencias asociadas actuando los resortes de dicho sistema.

A nuestro juicio, la Ley de Seguridad Nacional 2015 facilita las operaciones permanentes de monitorización y protección del ámbito cognitivo interno por cuanto que, aun no mencionándolo explícitamente (al igual que acontece con otros ámbitos, como el terrestre), se encuentra implícito tal como se desprende de las recomendaciones de seguridad cognitiva a la ciudadanía impartidas a inicios de 2019 desde el Centro Criptológico Nacional[46]. Ade-

[45] MILOSEVICH-JUARISTI, Mila. *La «combinación», instrumento de la guerra de la información de Rusia en Cataluña*. ARI 86/2017. Real Instituto Elcano, 7 de noviembre de 2017.

[46] CCN-CERT. ***Desinformación en el ciberespacio***. ***Op. cit.***

más, los campos de especial interés para la seguridad nacional se definen en el art. 10 la Ley de Seguridad Nacional como «aquellos que requieren una atención específica por resultar básicos para preservar los derechos y libertades, así como el bienestar de los ciudadanos» (entre los que, lógicamente, no puede obviarse el ámbito cognitivo), y establece un criterio de *numerus apertus*, al ser «entre otros, la ciberseguridad, la seguridad económica y financiera, la seguridad marítima, la seguridad del espacio aéreo y ultraterrestre, la seguridad energética, la seguridad sanitaria y la preservación del medio ambiente» (art. 10). El hecho de haber explicitado la ciberseguridad como una de las áreas concretas, incide en uno de los ámbitos de especial interacción con la acción cognitiva.

En este sentido, se apunta a la orientación de la acción cognitiva integrada por los medios del Sistema de Seguridad Nacional del Estado (entre los que se encuentran destacadamente los militares) de carácter constante, en favor de la resiliencia del ámbito cognitivo, puesto que «los principios básicos que orientarán la política de Seguridad Nacional son la unidad de acción, anticipación, prevención, eficiencia, sostenibilidad en el uso de los recursos, capacidad de resistencia y recuperación, coordinación y colaboración» (art. 4.2 | 2), y todo ello no puede alcanzarse, respecto del ámbito cognitivo, sin una proyección plena incluyendo el tiempo de paz. En todo caso, garantiza la transparencia y conciencia social de la actividad de seguridad nacional que abarca las operaciones en el ámbito cognitivo, al establecer medidas de cultura de seguridad para el conocimiento y la sensibilización de la sociedad acerca de sus requerimientos, de los riesgos y amenazas susceptibles de comprometerla, así como del esfuerzo de los actores y órganos implicados en su salvaguarda, subrayando la conveniencia de informar –sin menoscabo de la debida seguridad de la información– sobre las «medidas de anticipación, prevención, análisis, reacción, resistencia y recuperación respecto a dichos riesgos y amenazas» (art. 5.2 | 2). Esta Ley también facilita la interacción con entidades privadas que disponen de medios para una acción cognitiva coadyuvante con fines de interés general propios de la seguridad y la defensa, en tanto que fomenta la cooperación público-privada al disponer que «el sector privado participará en la contribución de recursos a la seguridad nacional» (art. 27.5 | 5). El principio de colaboración privada se resalta al disponer que «las entidades privadas, siempre que las circunstancias lo aconsejen y, en todo caso, cuando sean operadoras de servicios esenciales y de infraestructuras críticas que puedan afectar a la seguridad nacional, deberán colaborar con las Administraciones públicas», y que «en función de las necesidades, podrán asignarse cometidos a otros organismos y entidades, de titularidad pública o privada» (art. 18.2 | 2). Esto se proyecta a otros niveles administrativos, puesto que» el Gobierno, en coordinación con las comunidades autónomas, establecerá cauces que fomenten la participación del sector privado en la formulación y ejecución de la política de seguridad nacional» (art. 7).

Consecuentemente con lo señalado, los documentos estratégicos de seguridad nacional que han aprobado sucesivos gobiernos apuntan, en la práctica, a las aplicaciones mencionadas. La Estrategia de Seguridad Nacional de 2017, promulgada por el R. D. 1008/2017 de 1 de diciembre, incide en la cooperación con el sector privado, pues «pretende potenciar la colaboración público-privada en el ámbito de las amenazas a servicios esenciales como son las comunicaciones, puesto que la mayoría de estos servicios se prestan por operadores privados». Resalta la necesidad de contar con capacidades de monitorización y alerta temprana: «En cuanto a la gestión de crisis, la *Estrategia de Seguridad Nacional 2017* establece que dicha gestión comporta varias fases en un arco temporal que abarca desde la alerta temprana hasta la respuesta. Es importante fomentar un enfoque preventivo y anticipatorio, para el que cobran particular relevancia el seguimiento permanente del entorno de seguridad y sus constantes cambios, los sistemas de inteligencia e información, el desarrollo de metodologías de análisis de riesgos y de instrumentos que contribuyan a la protección contra la desinformación», involucrando «a las empresas estratégicas, los operadores de infraestructuras críticas, los centros de investigación o prospectiva y la sociedad civil en su conjunto». Al referirse a la resiliencia social y al mantenimiento de la estabilidad, se alude al daño cognitivo a la población: «El fomento de la resiliencia de la sociedad y de las Administraciones adquiere una importancia esencial. Se trata de fortalecer la capacidad de recuperación ante posibles crisis, manteniendo la estabilidad necesaria para garantizar la continuidad en la acción del Gobierno dirigida a la protección de los ciudadanos y la provisión de los servicios esenciales, para retornar al estado de normalidad en el menor tiempo posible, de modo que se minimicen las consecuencias negativas sobre la seguridad y el bienestar de los ciudadanos». La *Estrategia de Ciberseguridad Nacional de 2019*, publicada por Orden PCI/487/2019, de 26 de abril, considera el ciberespacio como un ámbito que es cauce estratégico para la acción cognitiva, y destaca la importancia de la resiliencia cognitiva, fomentando la preparación al respecto. Así, en su introducción dispone que «se debe tener en cuenta la concepción del ciberespacio como un vector de comunicación estratégica, que puede ser utilizado para influir en la opinión pública y en la forma de pensar de las personas a través de la manipulación de la información, las campañas de desinformación o las acciones de carácter híbrido. Su potencial aplicación en situaciones muy diversas, donde se incluyen los procesos electorales, genera un elevado grado de complejidad». La guía *Desinformación en el ciberespacio* (publicada en febrero de 2019), del CCN-CERT del Centro Nacional de Inteligencia, incide en esta relación entre el ciberespacio y el ámbito cognitivo, recomendando pautas y metodologías para luchar permanentemente contra la intoxicación informativa deliberada y otros ataques al ámbito cognitivo producidos en todo tiempo.

La L. O. 5/2005, de 17 de noviembre, de la Defensa Nacional resalta la importancia estructural de las FAS en el conjunto del Estado y su acción unitaria, proclamando que «las FAS son el elemento esencial de la defensa y consti-

tuyen una entidad única que se concibe como un conjunto integrador de las formas de acción específicas de cada uno de sus componentes: el Ejército de Tierra, la Armada y el Ejército del Aire» (art. 10). Al fijar, entre sus cometidos, la garantía de la integridad nacional, a nuestro juicio se comprende con ello el ámbito cognitivo interno, según explicamos al describir el marco jurídico-constitucional, puesto que no puede dejarse al margen la protección de la integridad cognitiva de los ciudadanos. Consideramos que ello acontecerá en todo tipo de escenario, especialmente en situaciones de crisis: «Las FAS, de acuerdo con el artículo 8.1 de la Constitución, tienen atribuida la misión de garantizar la soberanía e independencia de España, defender su integridad territorial y el ordenamiento constitucional [...]. Las FAS, junto con las instituciones del Estado y las Administraciones públicas, deben preservar la seguridad y bienestar de los ciudadanos en los supuestos de grave riesgo, catástrofe, calamidad u otras necesidades públicas, conforme a lo establecido en la legislación vigente» (art. 15). La acción sobre el ámbito cognitivo interno, que es de la ciudadanía connacional a las FAS, se reviste de las garantías que suponen las reglas de comportamiento del militar (fijadas por la L. O. 9/2011, de 27 de julio, de derechos y deberes de los miembros de las FAS), por las que todo militar español «ajustará su conducta al respeto de las personas, al bien común y al derecho internacional aplicable en conflictos armados. La dignidad y los derechos inviolables de la persona son valores que tienen obligación de respetar y derecho a exigir. En ningún caso los militares estarán sometidos, ni someterán a otros, a medidas que supongan menoscabo de la dignidad personal o limitación indebida de sus derechos» [...]. El respeto a la ciudadanía y al ordenamiento interno son absolutos, de modo que «si las órdenes entrañan la ejecución de actos constitutivos de delito, en particular contra la Constitución y contra las personas y bienes protegidos en caso de conflicto armado, el militar no estará obligado a obedecerlas y deberá comunicarlo al mando superior inmediato de quien dio la orden por el conducto más rápido y eficaz» (art. 6).

Tratando en concreto sobre las reglas de enfrentamiento (ROE) fijadas por el mando, en tanto que órdenes de carácter general –directivas, en la doctrina OTAN– que determinan el modo de empleo de los medios y fuerza de combate durante una operación militar (estableciendo cuándo, dónde, contra quién y cómo)[47], planteamos su aplicación específica a la acción cognitiva. Recordemos que las ROE se utilizan para el empleo gradual de la fuerza, según las diferentes

[47] Las ROE se recogen en la Ley 39/2007, de 19 de noviembre, de la Carrera Militar, cuyo art. 4 (sobre las «reglas de comportamiento militar») establece que «en el empleo legítimo de la fuerza, hará un uso gradual y proporcionado de la misma, de acuerdo con las reglas de enfrentamiento establecidas para las operaciones en las que participe». Además, las ROE son explícitamente mencionadas en las Reales Ordenanzas para las FAS, aprobadas por R. D. 96/2009, de 6 de febrero, arts. 84, y 94: donde se establece que «en el empleo legítimo de la fuerza, el militar hará un uso gradual y proporcionado de la misma, de acuerdo con las reglas de enfrentamiento establecidas para las operaciones en las que participe. Las ROE, refieren a un aspecto concreto del servicio muy acotado –en el tiempo y espacio, respecto a

situaciones que pueden acontecer a lo largo del desarrollo de una operación militar, y constituyen un mecanismo fundamental para que el mando decida cuándo se debe desplegar una unidad y cuánta fuerza puede emplear. Fijan el grado y las modalidades de aplicación de la fuerza, así como los límites dentro de los cuales actúa el comandante de la operación. Cabe promulgar ROE para restringir acciones concretas, o para ampliar los límites de una acción; conforman un sumatorio de varios factores e incluyen el marco jurídico de la operación, las instrucciones políticas y las consideraciones operativas inherentes a la propia misión. Aplicadas a las operaciones militares en el ámbito cognitivo –teniendo presentes los riesgos asociados al lastre operativo que suponen unas ROE restrictivas en exceso–, surge la cuestión de en qué medida se configuran diferencialmente para la acción cognitiva y constituyen una limitación, lo cual condicionará el proceso de *targeting* para designación de blancos y el posible daño colateral. En primer lugar, debemos señalar que, en su aplicación práctica en misiones exteriores, las ROE suelen desenvolverse en un ámbito cognitivo foráneo impregnado de un componente cultural y una idiosincrasia social extraña, por lo que la percepción, interpretación y efectos de las acciones cognitivas puede diferir mucho, y lo que en España supondría un daño cognitivo (o podría desencadenar situaciones de violencia física), bien pudiera no serlo allí. Por lo tanto, el primer factor a considerar es el ajuste del grado de hostilidad cognitiva, acorde con el tipo de audiencias-objetivo y su contexto. En segundo lugar, creemos que conviene un análisis jurídico comparado (dado que, a fecha de hoy, no hay registros de operaciones combinadas en el ámbito cognitivo, habría de realizarse sobre ejercicios o simulaciones) para la armonización jurídica de las ROE españolas con las fuerzas concurrentes en operaciones combinadas (especialmente de la OTAN) actuando sobre el ámbito cognitivo. Ello permitiría que, llegado el caso de tal tipo de operaciones, se pudiese garantizar que las FAS españolas no se encontrarán en situación operativamente disminuida respecto de su capacidad de acción cognitiva en comparación con sus aliados; asimismo, respecto de las ROE en las acciones cinéticas sobre el ámbito físico, se requiere dicha armonización en favor de la concordancia de los hechos (acciones militares físicas) con las narrativas. Es claro que, en la práctica, las ROE propiciarán una narrativa acorde con los valores OTAN, y restringirán la acción cognitiva maliciosa, con autorrestricción técnica psicológica para no lesionar capacidades mentales ni inducir psicopatologías, actitudes, decisiones o emociones gravemente perjudiciales, según el principio de distinción.

Por último, la doctrina militar y la doctrina jurídica jurisprudencial e interpretativa resultan imprescindibles para poder aplicar eficazmente el derecho de acuerdo con la *Lex Artis* militar que incluye las innovaciones técnicas y operativas en el arte de la guerra y los medios de acción militares. Por ello, la consideración de los aspectos innovadores que supone la nueva dinámica

las condiciones, contexto, métodos y medios para el uso de la fuerza– carecen de rango ni valor normativo independiente, en derecho internacional y en derecho español.

del ámbito cognitivo requiere un esfuerzo de actualización doctrinal concordante en todas las disciplinas y tareas de aplicación.

Al derecho español se añaden, como es bien sabido, las disposiciones del *corpus* de derecho internacional de los conflictos armados y del derecho internacional de los derechos humanos ratificado por España, cuyos aspectos problemáticos sobre el ámbito cognitivo, la zona gris del conflicto y la homogeneidad y proporcionalidad de la respuesta bélica hemos mencionado anteriormente respecto de consideraciones de *ius in bello* y *ius ad bellum*. En el plano jurídico-internacional, destacamos el Tratado del Atlántico Norte en un doble sentido: por una parte, en tanto que las operaciones combinadas en misiones OTAN requieren la armonización de criterios operativos en el ámbito cognitivo; por otra, en el sentido de que la agresión enemiga sobre el ámbito cognitivo de España repercute en el espacio OTAN y, por los cauces de proyección de los vectores transnacionales que expanden los efectos cognitivos, afecta al conjunto de los aliados.

Límites éticos

La delimitación ética de la acción militar en el ámbito cognitivo, como en los demás ámbitos, supone un marco común que, en el caso específico de aquel, incide sobre aspectos especialmente relacionados con la capacidad de manipular las mentes sin apenas dejar rastro y poder actuar ocultamente generando efectos incluso estratégicos. Por lo tanto, se estima que el punto de partida de la limitación ética a la acción cognitiva militar es la autorrestricción moral individual del personal militar.

En España, el componente ético a tener en cuenta se encuentra en los principios del Estado de derecho, la tradición jurídica y el acervo cultural español, los cuales son inherentes a la sociedad española e impregnan a los componentes de sus FAS. Estas se rigen expresamente por las directrices que constituyen sus Reales Ordenanzas, que engloban un compendio de deontología militar compuesto por un conjunto de principios y reglas morales que iluminan la actividad de las FAS sobre la base de sus propias tradiciones castrenses, cultura e historia. Asimismo, poseen elementos comunes con el DIH[48] (conformado originariamente, en buena parte, por la hispánica Escuela de Salamanca) y valores compartidos en la comunidad de aliados de la OTAN, de la que España forma parte. Del conjunto del ordenamiento jurídico español, destacamos 2 instrumentos respecto de los límites éticos aplicables a la acción militar sobre el ámbito cognitivo.

Por una parte, las Reales Ordenanzas de las FAS (R. D. 96/2009 de 6 de febrero), de acuerdo con lo previsto en la L. O. Defensa Nacional de 2005 y en

[48] *Publicación Doctrinal Conjunta PDC-01 (A) Doctrina para el empleo de las FAS,* párrafo n.º 249, 2018, p. 72.

la Ley de la Carrera Militar de 2007[49], establecen que los militares ajustarán moralmente su conducta al respeto de las personas, al bien común y al derecho internacional aplicable en conflictos armados, (art. 11). Esto incluye a la dimensión cognitiva de las personas, y, dentro del ámbito cognitivo interno, conlleva actuar sobre la población connacional salvaguardando en todo caso su autonomía de la voluntad y el normal devenir constitucional de la sociedad. Sobre la ética en operaciones, el art. 111 preceptúa el principio de distinción por el cual, en el curso de una operación, se tendrá en cuenta la distinción entre personas civiles y combatientes –y entre bienes de carácter civil y objetivos militares– para proteger a la población civil y evitar en lo posible las pérdidas ocasionales de vidas, sufrimientos físicos y daños materiales. Obviamente, en ello se encuentra incluido el daño cognitivo –dentro de lo que se denomina en sentido lato *sufrimiento físico*, pues la mente forma parte del organismo– de modo que, en las operaciones militares sobre el ámbito cognitivo foráneo, se observará igualmente el principio de distinción respecto de la dimensión cognitiva de los individuos.

Por otra, el *Código ético del Centro Nacional de Inteligencia* (12 de octubre de 2015) es de especial importancia, por cuanto que el CNI es el órgano principal de la comunidad de inteligencia española, y tiene acreditada experiencia práctica en cuestiones de polemología de la información y contrainformación, en la monitorización demoscópica y del ámbito cognitivo en general. El CNI, conocedor de los negativos efectos que puede generar en la ciudadanía la pérdida de confianza en las instituciones públicas y en la soberanía nacional[50] por causa de acciones cognitivas, ha imprimido en sus efectivos la citada autorrestricción moral individual. Por lo tanto, su enfoque ético sirve de referente para la acción cognitiva de seguridad nacional, que incumbe a la defensa. Entre sus disposiciones deontológicas relativas al personal estatutario (y entendemos extensiva a todo aquel que integra sus actividades desde los distintos estadios de colaboración o reserva), destacan el art. 2 que proclama su misión de «protección del bien común y de la seguridad de los españoles», y el art. 17 el cual marca como referente ético que «la utilización de los procedimientos especiales que permite la ley guarde siempre

[49] Revisadas con el proceso constituyente de 1978, tras la Ley 85/1978 de 28 de diciembre de Reales Ordenanzas para las FAS se ajustaron al marco constitucional de la CE1978 «sin perder los valores tradicionales que le son intrínsecos» (R. D. 96/2009 de 6 de febrero, por el que se aprueban las Reales Ordenanzas para las FAS), siendo de aplicación general a todos los ejércitos, incluida la Guardia Civil (como no podría ser de otra manera), lo que se confirma en virtud del R. D. 1437/2010, de 5 de noviembre. La Ley 39/2007, de 19 de noviembre, de la Carrera Militar, recogiendo el mandato del art. 20 de la L. O. 5/2005, de 17 de noviembre de la Defensa Nacional, estableció las reglas esenciales que definen el comportamiento de los militares, desarrolladas mediante R. D. 96/2009 de 6 de febrero, por el que se aprueban las Reales Ordenanzas para las FAS. La L. O. de Derechos y Deberes de los miembros de las FAS (2011), regula en su art. 6 las reglas esenciales que definen el comportamiento del militar.

[50] CCN-CERT. *Desinformación en el ciberespacio*. *Op. cit.*

la debida proporcionalidad, en función del riesgo o amenaza que se pretenda combatir o del conocimiento que se desee obtener». Con ello se ha minimizado el riesgo que teóricamente afecta a todo órgano de la comunidad de inteligencia –a la que pertenece el CIFAS– en el sentido de no controlar eficientemente la observancia de la proporcionalidad respecto de las operaciones en el ámbito cognitivo.

Conclusiones

Para concluir nuestro análisis sobre la eventual existencia de nuevos límites jurídicos a las operaciones militares en el ámbito cognitivo, primeramente, se recapitulan los factores principales que cimentan el *iter* discursivo que conduce a la descripción de 2 nuevos umbrales de limitación jurídica que creemos poder justificar, de acuerdo con el ordenamiento jurídico español en el contexto de la Alianza Atlántica.

Así, consideramos que el ámbito cognitivo del campo de acción de las FAS se introduce específicamente en la doctrina de defensa española coincidiendo con la aplicación práctica del moderno concepto de *amenaza híbrida* en el entorno OTAN, así como con el desarrollo de la novedosa función integrada militar STRATCOM que potencia la capacidad de la acción militar cognitiva.

El conflicto *en* o *sobre* el ámbito cognitivo posee elementos diferenciales por el campo y entorno de la acción y las aplicaciones técnicamente posibles: imprevisibilidad, transversalidad, insidiosidad, dinamismo y proyección, así como una especial interacción con el ámbito ciberespacial. Además, la acción agresiva cognitiva sobre el ámbito cognitivo puede generar efectos tangibles al desencadenar la violencia física.

La acción cognitiva adversaria se desenvuelve con preponderancia en la denominada zona gris del conflicto (y aumenta una vez producido este, coexistiendo con acciones de otros ámbitos), lo que entraña problemas frecuentes de percepción y atribución, con una singular problemática de trascendencia jurídica sobre el *ius ad bellum* y los posibles ajustes para delimitar una adecuada respuesta militar con la debida justificación, homogeneidad y proporcionalidad.

La capacidad de protección y resiliencia del ámbito cognitivo propio, así como la acción sobre el ajeno, requieren actuar militarmente en distintos niveles, para monitorizar, proteger, influir y, llegado el caso, combatir. El bien jurídico a proteger es la soberanía e independencia de la Nación junto con las libertades y derechos de ciudadanos. Para ello, se requiere un incremento de la capacidad defensiva en el ámbito cognitivo en orden a introducir en dicha dimensión los adecuados elementos para la protección de la soberanía, los intereses y la población connacionales, capaz de aplicar –llegado el caso– una acción militar permanente y sostenible, anticipada al conflicto y rápida.

Dentro de la doble delimitación jurídica y ética de las operaciones militares en el ámbito cognitivo en el ordenamiento español, a los efectos de los límites de la acción que describimos, se destaca la Ley 36/2015 de 28 de septiembre de Seguridad Nacional, por cuanto que introduce un marco normativo moderno, propicio para la acción militar en el ámbito cognitivo interno en tiempo de paz, tanto en situación de normalidad como de crisis. Los límites éticos dimanan de lo contenido en las Reales Ordenanzas de las FAS (2009) y en el Código ético del Centro Nacional de Inteligencia (2015) ajustados a las singularidades de la acción cognitiva.

Por lo tanto, en nuestra opinión, sobre las operaciones militares en el ámbito cognitivo se presentan actualmente nuevos límites jurídicos, que extienden la capacidad de acción cognitiva en las operaciones militares sobre el ámbito cognitivo en 2 contextos:

1) La intervención en el ámbito cognitivo exterior foráneo en virtud de la legítima respuesta, en los prolegómenos del conflicto, con la finalidad de evitar la escalada del conflicto o, si no es posible, realizar los preparativos oportunos.

2) La protección del ámbito cognitivo nacional en tiempo de paz, en virtud del mandato constitucional del art. 8 CE, que faculta el incremento de capacidades para disponer de una adecuada conciencia situacional cognitiva militar, en situación de normalidad.

Como recomendación final, permítasenos sugerir una breve propuesta orientativa de *lege ferenda* para potenciar la operatividad de las FAS en el ámbito cognitivo, fortalecer la conciencia de defensa en la sociedad y neutralizar la *lawfare*. Así, estimamos que una nueva normativa que trate específicamente sobre las operaciones militares y/o de seguridad nacional en el ámbito cognitivo habría de contemplar, al menos, los siguientes elementos:

- Aplicar la metodología de planeamiento militar en la comunicación estratégica del Estado, por su eficacia técnica e idoneidad para abarcar todas las fases posibles, desde la situación de normalidad hasta la gestión de crisis y el conflicto. Mediante aquella, se armonizarían las interacciones operativas entre las distintas Administraciones públicas participantes, y se optimizaría la contribución militar y su coordinación, llegado el caso.
- Incrementar las capacidades de acción cognitiva de las FAS, para mejorar su conciencia situacional del ámbito cognitivo propio y facilitar la protección permanente del mismo, así como las potenciales acciones preventivas en el exterior.
- Incorporar el máximo grado posible de armonización jurídica con la comunidad OTAN, tanto para una interpretación normativa homogénea como para la aplicación de directrices prácticas operativas (ROE) que faciliten sinergias en operaciones combinadas, como para dotar de pa-

rámetros comunes al ámbito cognitivo transnacional y favorecer su defensa común.

- Definir concretamente procedimientos de cooperación público-privada ocasional y permanente.

Fuentes y Bibliografía

ALIA PLANA, Miguel. «Reglas de Enfrentamiento (II): Gestión de Blancos (targeting)». *Cuaderno Práctico* n.º 8. Escuela Militar de Estudios Jurídicos, julio-diciembre 2016, pp.7-49.

AVERY, Thomas. «Popper on «Social Engineering»: A Classical Liberal View». *Reason Papers*. Vol. 26, 2000, pp. 29-38.

BAQUÉS, Josep. «Hacia una definición del concepto «Gray Zone (GZ)». *Documento de Investigación 02/2017*. Instituto Español de Estudios Estratégicos, 2017.

CCN-CERT. *Desinformación en el ciberespacio, CCN-CERT / BP 13*, febrero 2019.

COUNCIL OF EUROPE - Parliamentary Assembly Committee on Legal Affairs and Human Rights. «Legal challenges related to the hybrid war and human rights obligations» report. Council of Europe, marzo 2018.

EMAD. *Publicación Doctrinal Conjunta PDC-01 (A) Doctrina para el empleo de las FAS*. Estado Mayor de la Defensa, 2018.

HERAS DURÁN, José Manuel de. «Marco jurídico de las funciones, no de defensa, de las Fuerzas Armadas en tiempo de paz». En Corrales Elizondo (coord.). *El marco jurídico de las Misiones de las Fuerzas Armadas en tiempo de paz. Cuaderno de Estrategia n.º 116*. Madrid: IEEE 2002, pp.175-223.

JUSLIN, Patrik y VASTFJALL, Daniel. «Emotional responses to music: The need to consider underlying mechanisms». *Behavioral and Brain Sciences*. N.º 31, 2008, pp. 559-621.

KAVANAGH, Jennifer; RICH, Michael D.; Truth Decay. *An Initial Exploration of the Disminishing Role of Facts and Analysis in American Public Life*. Santa Mónica: RAND 2018, pp. 191-206.

KRISHNAN, Armin. «From Psyops to Neurowar: What are the Dangers?». *ISAC-ISSS Conference*. Austin, November 2014.

LANZ RAGGIO, Mario. «El conflicto en las sombras: aspectos generales y elementos jurídicos de las operaciones en la zona gris», en la presente monografía.

LEWIS, James A. «Cognitive Effect and State Conflict in Cyberspace». CSIS, 2018.

LIBICKI, Martin C. *Cyberdeterrence and Cyberwar*. Santa Mónica: RAND, 2009, pp. 41-51.

LOVEGROVE, Kitty. «The acoustic world on influence: how Musicology illuminates Strategic Communications». *Defence Strategic Communications*. Vol. 5, otoño 2018, pp. 13-49.

MANDELBLIT, Avihai. «Lawfare: the Legal Front of the IDF». *Military and Strategic Affairs.* Vol. 4, n.º 1, abril 2012, pp. 51-57.

MILOSEVICH-JUARISTI, Mila. *La «combinación», instrumento de la guerra de la información de Rusia en Cataluña*. ARI 86/2017. Real Instituto Elcano, 7 de noviembre de 2017.

MOORE, Daniel. «Targeting Technology: Mapping Military Offensive Network Operations». En Minárik, T.; Jakschis, R.; Lindström, L. (eds.). *CyCon X: Maximising Effects - 2018 10th International Conference on Cyber Conflict*. Tallin: NATO CCD COE Publications, 2018, pp. 89-108.

MOUTON, Francois; PILLAY, K.; VAN`T WOUT, M.C. «The Technological Evolution of Psychological Operations Throughout History». En Clarke, N. l., Furnell S. M. (editors). *Proceedings of the Tenth International Symposium on Human Aspects of Information Security & Assurance* (HAISA 2016 Frankfurt). Plymuth: ed. Plymouth University, 2016, pp. 266-278.

NATO STRATCOM CoE. «Hybrid Threats. A Strategic Communications Perspective». Riga, 2019, pp. 12, 13 y 20.

NATO STRATCOM CoE. «The Black Market for Social Media Manipulation». NATO STRATCOM CoE–SINGULAREX, 2018.

SALAS, Jacobo de. «De la flecha al ratón – Consideraciones jurídicas de las operaciones ofensivas en el ciberespacio» en la presente monografía.

SÁNCHEZ BENÍTEZ, Sergio, «La comunicación estratégica como política pública». *Documento de Opinión* n.º 21/2011. IEEE-CESEDEN, 2011.

SANTOS RODRÍGUEZ, Felipe. «La comunicación estratégica (STRATCOM) en los conflictos modernos: el caso de Afganistán». *Revista del Instituto Español de Institutos Estratégicos*. N.º 2, 2013.

SEGELL, Glen. «National Security Priority over the Rights of Citizens in PSYOP». *London Security Policy Study*. Vol. 8, n.º 2, julio 2013, pp. 3-10.

SIBONI, Gabi. «The First Cognitive War». En Kurz, A., Brom, S. (eds.). *Strategic Survey for Israel 2016-2017*. Tel Aviv: Institute for National Security Studies, 2016.

SILVELA DÍAZ-CRIADO, Enrique. «Comunicación estratégica: origen y evolución del concepto». En Diego Mazón Born (coord.). *La Comunicación Estratégica*. *Documento de Seguridad y Defensa* nº. 72. IEEE-CESEDEN, 2017, pp. 13-34.

TORRES SORIANO, Manuel R. «Los límites de la guerra de la información. Lecciones aprendidas tras los conflictos de Iraq y Afganistán». *Revista Ejército*. N.º 818, junio 2009, pp. 14-22.

U. S. ARMY. *From PSYOP to MindWar: The Psychology of Victory by Colonel Paul E. Vallely, Commander, with Major Michael A. Aquino, PSYOP Research*

& Analysis Team Leader. Headquarters, 7th Psychological Operations Group, United States Army Reserve, Presidio of San Francisco, CA, 1980.

VV. AA. «Analysis of Risk Communication Strategies and Approaches with At-Risk Populations to Enhance Emergency Preparedness, Response and Recovery». Final Report RAND, 2008, p. 20.

WINGFIELD, Thomas C. «Legal Aspects of Offensive Information Operations in Space», report. US Department of Defense, 2005.

Capítulo tercero

Resiliencia frente a las ciberamenazas en operaciones multiámbito: limitaciones jurídicas

Susana De Tomás Morales

Resumen

En el presente capítulo se atiende a los límites jurídicos de las operaciones multiámbito a través de la perspectiva de la resiliencia. Para ello, se realiza un análisis especializado sobre las ciberamenazas que entran dentro del ámbito de la defensa mediante una visión estratégica compartida por España y la UE. A partir de esta visión estratégica, se podrán obtener tres parámetros a partir de los cuales se podrá enfocar la resiliencia cibernética hacia la eficiencia y eficacia de las operaciones multiámbito. En relación con los límites jurídicos objeto de atención en esta obra, dentro del parámetro de la resiliencia como proceso de transformación de capacidad ocupan un lugar privilegiado los modos de resiliencia. Las limitaciones jurídicas desde la perspectiva de la resiliencia cibernética permiten también ser objeto de atención en relación con las misiones u operaciones internacionales, como uno de los entornos operativos del empleo de las FAS, mediante el desarrollo de operaciones multiámbito.

Palabras clave

Ciberespacio, ciberamenzas, resiliencia cibernética, operaciones multiámbito.

Abstract

In this chapter, the legal limits of multi-site operations are taken into account through the perspective of resilience. For this purpose, a specialized analysis is carried out on the cyber threats that fall within the scope of Defense through a strategic vision shared by Spain and the EU. Based on this strategic vision, three parameters can be obtained from which cybernetic resilience can be focused on the efficiency and effectiveness of multi-site operations. In relation to the legal limits that are the object of attention in this work, resilience modes occupy a privileged place within the resilience parameter as a process of capacity transformation. The legal limitations from the perspective of cybernetic resilience also allow to be the object of attention in relation to international missions or operations, as one of the operating environments of the employment of the FAS, through the development of multi-site operations.

Keywords

Cyberspace, cyberthreats, cybernetic resilience, multi-site operations.

Introducción

El ciberespacio y la resiliencia en el desarrollo de operaciones militares

Tras los ciberataques sufridos por Estonia[1], en 2007, se marcó un antes y un después en relación con la atención hacia los avances que se desarrollarían en el campo de los sistemas de información y de comunicación (en adelante, SIC). En efecto, si, hasta entonces, estos avances tecnológicos solo habían sido tenidos en consideración como un elemento clave para el desarrollo económico y social de los Estados, en el contexto de una globalización de la sociedad internacional, especialmente con el desarrollo de Internet, las posibilidades de un uso malicioso de las redes y sistemas de información (en adelante, RSI) presentaron un nuevo panorama en el ámbito de la seguridad y defensa, tanto en los ámbitos nacionales como en el internacional. Se hacía necesario, en consecuencia, articular mecanismos eficaces no solo para garantizar una mayor interconectividad, sino también para proporcionar su desarrollo en un entorno seguro de las RSI, pues los ciberataques sufridos por Estonia no constituyeron una excepción, sino el desencadenante de sucesivos y variados tipos de ciberataques sufridos por otras repúblicas bálticas[2], hasta llegar a la posibilidad de ser utilizados como un método de combate, como en el caso de Georgia[3].

Teniendo en cuenta, por lo tanto, la posibilidad de utilizar los ciberataques como un nuevo método de combate, resulta necesario dirigir nuestra atención hacia determinados ciberataques que puedan poner en riesgo o constituyan una amenaza para la paz y la seguridad internacionales. Aparece,

---

1 En el caso de Estonia, una decisión política desencadenó, entre los meses de abril y mayo de 2007, el desarrollo de sucesivas protestas y revueltas callejeras, al tiempo que se lanzaban ataques cibernéticos de diversa magnitud hasta conseguir graves alteraciones de las RSI, como la paralización de páginas web oficiales de distintas instituciones públicas y privadas.

2 En este sentido, se puede mencionar el caso de los cibertaques sufridos en Bielorrusa, del 26 al 28 de abril 2008, en el que los ciberataques son dirigidos, presuntamente, desde las mismas instituciones estatales contra la página web de la emisora de radio Radio Free Europe/Radio Liberty y de otros medios de comunicación como Belorusskii Partizan y www.charter97.org, en clara violación de los derechos a la libertad de expresión e información.

3 Tras la autoproclamación de independencia de Osetia del Sur, Georgia lanzó un ataque con las fuerzas rebeldes separatista, en 2008. Rusia respondió con operaciones militares en territorio georgiano. De esta forma se iniciaría una guerra convencional entre Georgia y Rusia. Lo interesante de este conflicto es que antes y durante el despliegue de las operaciones militares sobre el terreno, Georgia sufrió tal sucesión de ciberataques que, entre otras consecuencias, inhabilitaron los servicios de comunicación en Georgia, procedentes de territorio ruso, lo que, sin lugar a duda, podría considerarse como una ventaja militar. La posibilidad de que puedan utilizarse de forma combinada métodos de combate convencionales y cibernéticos quedaba abierta.

en consecuencia, un nuevo teatro de operaciones o campo de batalla[4]: el ciberespacio. Se trata de un nuevo campo de batalla bastante peculiar, pues carecemos de un concepto generalmente aceptado del mismo, por lo que tendremos como referente la definición contenida en la *PDC-01 (A) Doctrina para el empleo de las Fuerzas Armadas*, en la que se incluye, como un espacio de operaciones, el ámbito ciberespacial. En concreto, se establece que «el ámbito *ciberespacial* es un ámbito artificial compuesto por infraestructuras, redes, sistemas de información y telecomunicaciones y otros sistemas electrónicos, por su interacción a través de las líneas de comunicación sobre las que se propaga y el espectro electromagnético (EEM), así como por la información que es almacenada o transmitida a través de ellos...»[5].

Si bien, como acabamos de indicar, no encontramos un concepto unívoco del término ciberespacio[6], lo que parece ya innegable es que nos encontramos ante un espacio relacional. Es decir, un espacio en el que se pueden establecer relaciones, tanto de cooperación como de conflictividad entre los distintos sujetos del derecho internacional, aunque se trate de un espacio de naturaleza virtual, frente a la naturaleza física de los otros tradicionales espacios en los que hasta ahora se desplegaba la dimensión relacional de la Sociedad Internacional. De ahí que el ciberespacio pueda ser atendido como un quinto espacio relacional. Debemos tener en cuenta, además, que si en los tradicionales espacios físicos hemos comprobado una evolución y transformación de los diferentes riesgos y amenazas que atenazan a la paz y a la seguridad interna e internacional debido, entre otros factores, a la intervención, en constante crecimiento, de nuevos actores internacionales no estatales hasta entonces no contemplados en la dimensión relacional de la

[4] Como señalaría la alta representante de la Unión, en septiembre de 2017: «El uso del ciberespacio como campo de batalla, de forma exclusiva o como parte de una táctica híbrida, es ahora ampliamente reconocido». Alta representante de la Unión para Asuntos Exteriores y Política de Seguridad. Comunicación conjunta al Parlamento Europeo y al Consejo, JOIN (2017) 450 final, de 13 de septiembre de 2017, p. 2.

[5] ESTADO MAYOR DE LA DEFENSA. *PDC-01(A) Doctrina para el Empleo de las Fuerzas Armadas*. Madrid: Ministerio de Defensa, 2018, p. 81. Disponible en https://publicaciones.defensa.gob.es/.

[6] Podríamos destacar otras definiciones del ciberespacio como «The environment formed by physical and non-physical components, characterized by the use of computers and the electro-magnetic spectrum, to store, modify, and exchange data using computer networks», incorporada en el glosario que se ofrece en el conocido como *Manual de Tallin*. SCHMITT, M. N. (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge Universtity Press, 2013, p. 258. Idéntica definición se encuentra recogida en el denominado *Manual de Tallin 2.0*. SCHMITT, M. N. (ed.). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, 2017, p. 564. También resulta interesante la siguiente definición, en la que se considera al ciberespacio como «a time dependent set of interconnected information systems and the human users that interact with these systems». Ofrecida por OTTIS, R. y LLORENTS, P. «Cyberspace: Definition and Implications». *Proceedings of the 5th International Conference on Information Warfare and Security*. Dayton, OH, US, 8-9 April. Reading: Academic Publishing Limited, pp. 267-270.

Sociedad Internacional, en este nuevo espacio virtual la dimensión relacional recobra un nuevo protagonismo, pues se trata de un espacio o campo de batalla de muy fácil acceso para cualquier individuo del mundo. En efecto, las posibilidades de participación en el ciberespacio permiten todas las posibilidades de relaciones asimétricas que se pudieran imaginar si tenemos en consideración que el espacio virtual se caracteriza también por su anonimato. Es decir, nos encontramos con la dificultad añadida para la planificación, conducción y seguimiento de las operaciones al no resultar siempre posible la identificación del enemigo ni su consecuente atribución a un Estado de los ciberataques que puedan ser calificados como ataques armados. Anonimato que, unido al fácil acceso al mismo, hace que nos encontremos con elementos característicos de la denominada zona gris, que son objeto de un detallado análisis a cargo de Lanz Raggio en el capítulo primero de la presente obra, así como con las consecuentes dificultades de establecer los claros límites jurídicos de las operaciones que han de desarrollarse en el ámbito ciberespacial.

Además, el ciberespacio no solo ha de ser atendido con un espacio virtual relacional, sino también como un medio, pues, como acertadamente afirma Aguirre Romero: «Una red sin interacción entre sus miembros deja de ser una red; la red existe porque existen relaciones entre sus integrantes»[7]. La consideración de este nuevo espacio relacional, en el que puedan desarrollarse operaciones militares, como un medio, hace que nos preguntemos sobre la finalidad de su utilización. Ese elemento intencional, también característico de la zona gris, nos dirige la mirada, de nuevo, hacia los usos maliciosos del ciberespacio, como en los supuestos de ciberataques antes mencionados.

En consecuencia, no parece improbable que se puedan realizar ciberoperaciones[8] en el contexto de la denominada ciberguerra[9] o en combinación con

---

[7] AGUIRRE ROMERO, J. M. «Ciberespacio y comunicación: nuevas formas de vertebración social en el siglo xxi». *Espéculo: Revista Revista de Estudios Literarios.* Universidad Complutense de Madrid, n.º 27, 2004, p. 2. [última consulta, 5/03/2019]. Disponible en www.biblioteca.org.ar/libros/150717.pdf.

[8] En el referido *Manual de Tallin* se definen las operaciones cibernéticas como «The employment of cyber capabilities with the primary purpose of achieving objectives in or by the use of cyberspace». SMITH, M. N. Tallinn Manual..., *op. cit.,* p. 258. Idéntica definición se encuentra recogida en el *Manual de Tallin 2.0*, *op. cit.,* p, 564, aunque, como se indica expresamente, la utilización de estos términos en este segundo Manual es utilizada en un contexto operacional, por lo que hay que atender al concepto de actividad cibernética, que define como «Any activity that involves the use of cyber infrastructure or employs cyber means to affect the operation of such infrastructure», matizando que estas actividades no se limitan al ámbito de las operaciones cibernéticas.

[9] Según Gema SÁNCHEZ MEDERO: «La ciberguerra puede ser entendida como una agresión promovida por un Estado y dirigida a dañar gravemente las capacidades de otro para imponerle la aceptación de un objetivo propio o, simplemente, para sustraer información, cortar o destruir sus sistemas de comunicación, alterar sus bases de datos, es decir, lo que habitual-

otros métodos de combate convencionales en los distintos espacios físicos. Ante esta nueva situación, se plantean nuevos retos jurídicos para determinar cuáles son los límites al desarrollo de operaciones multiámbito y de actividades tácticas de naturaleza defensiva y ofensiva, atendiendo a que serían extrapolables las características de la zona gris al ciberespacio. Por ello, resulta imprescindible, en primera instancia, destacar que no todo ciberincidente debe ser considerado como un ciberataque que deba ser ubicado dentro del ámbito de la defensa. Solo aquellos ciberataques que se sitúen en el referido ámbito de la defensa podrán ser objeto de atención para el planeamiento, conducción y seguimiento de operaciones de las fuerzas armadas (en adelante, FAS). Será a partir de la calificación jurídica de un ciberataque como un ataque armado, cuando se pueda dar respuesta a través de operaciones militares multiámbito, en legítima de defensa, de conformidad con el ordenamiento jurídico internacional[10]. Cuestión más compleja es la calificación de esos ciberataques que, entrando en el ámbito de la defensa, no llegan al umbral de violencia requerido para ser considerados como ataques armados. En este último supuesto, las operaciones militares multiámbito únicamente podrían contemplar el planeamiento, conducción y seguimiento de actividades tácticas de carácter defensivo.

Es evidente que el ciberespacio, al que atendía Willian Gibson en su obra *Neuromante*[11], en 1984, ha sobrepasado claramente la esfera de la ciencia ficción para constituir un quinto espacio en el que nos desenvolvemos en todos los ámbitos, incluido el de la seguridad y la defensa. Por consiguiente, no es de extrañar que tanto el ciberespacio como las ciberamenazas hayan sido objeto de atención y preocupación, con un ritmo acelerado acorde con el preocupante incremento de los incidentes de ciberseguridad, en las estrategias de seguridad.

La resiliencia como gran protagonista de las operaciones multiámbito frente a las ciberamenazas

Al igual que no encontramos un concepto unívoco sobre el ciberespacio, tampoco existe acuerdo para ofrecer una definición genérica de la resiliencia, a

mente hemos entendido como guerra, pero con la diferencia de que el medio empleado no sería la violencia física sino un ataque informático». SÁNCHEZ MEDERO, G. «Los Estados y la ciberguerra». *Boletín Informativo*, número 317, Ministerio de Defensa, 2010, p. 64. (pp. 63-76). El término ciberguerra no es definido ni en el *Manual de Tallin* ni en el *Manual de Tallin 2.0*, lo que tampoco es de extrañar, pues se atiende a la actual denominación de la guerra como conflicto armado, sea de orden interno o internacional. Resulta hasta cierto punto paradójico que ante la aparición de un quinto espacio o campo de batalla virtual se vuelva a utilizar el más clásico término guerra para referirse a una contienda armada, unido al hecho de la utilización del más novedoso método de combate, los ciberataques.

10 Cfr. Capítulo 4 de la presente obra, a cargo de Jacobo de Salas Claver.

11 GIBSON, W., Neuromante (1984), Minotauro, Barcelona, (segunda reedición) 2007.

pesar de que ha ido asumiendo, cada vez más, un gran protagonismo en las estrategias y políticas estatales y de las organizaciones internacionales intergubernamentales. Por ello, podemos adoptar, como punto de partida, una de las más amplias definiciones que se han ofrecido, en la que se entiende por resiliencia: «La capacidad de un sistema, comunidad o sociedad expuestos a una amenaza para resistir, absorber, adaptarse y recuperarse de sus efectos de una manera oportuna y eficaz»[12]. De esta definición podemos destacar algunas cuestiones que serán objeto de análisis más adelante. Así, lo primero que llama la atención es el reconocimiento de la vulnerabilidad de los sistemas, comunidades o sociedades frente a determinadas amenazas, de tal forma que se minimice al máximo el daño recibido y restablecerse de forma rápida y reforzada. Por otra parte, podríamos destacar que la resiliencia está encaminada a conseguir que esos sistemas, comunidades y sociedades alcancen tal grado de resiliencia que se convierta en un mecanismo de disuasión, dando cabida a las operaciones militares multiámbito con una finalidad de disuasión[13]. Si esta resiliencia va especialmente dirigida a resistir, absorber, adaptarse y recuperarse de los efectos de los ciberataques que entran dentro del ámbito de la defensa, se podría hablar de una resiliencia cibernética dirigida a la consecución de sistemas, comunidades y sociedades ciberresilientes. Además, a raíz de esta definición, podemos observar cómo esa capacidad de resistencia frente a los ciberataques también podría ser aplicable a las operaciones multiámbito de prevención. Por último, en la referida definición se indica que ha de ser oportuna y eficaz. Parece evidente que, en un contexto en el que cada vez son más escasos los recursos económicos y humanos destinados al ámbito de la defensa, la resiliencia frente a las ciberamenazas aplicada a las operaciones multiámbito permitirá conseguir una mayor eficiencia y eficacia con un menor coste.

Al igual que en un contexto de ciberguerra, como se ha indicado, se pueden alternativa o conjuntamente utilizar medios y métodos de combate convencionales y cibernéticos, lo mismo puede suceder con las actividades tácticas de carácter defensivo en el desarrollo de las operaciones multiámbito que nos ocupan. En consecuencia, tendremos en consideración las operaciones

12 MINISTERIO DE ASUNTOS EXTERIOR Y COOPERACIÓN. *Construcción de resiliencia para el bienestar. Directrices para la cooperación española*. MAEC, Madrid, septiembre 2018. https://www.cooperacionespanola.es/sites/default/files/directrices_resiliencia_cooperaci on_espanola.pdf.

13 En este sentido, si todos los sistemas, comunidades y sociedades consiguiesen ser resilientes nos podríamos encontrar en un escenario de enfrentamiento entre resiliencias. Esta es posición de Federico Aznar, quien, refiriéndose a la lucha antiterrorista, considera que podría quedar reducida, precisamente, a una lucha entre resiliencias. Véase: AZNAR FERNÁDEZ - MONTESINOS, F. «Resiliencia y acción política. El binomio sociedad-Estado frente al terrorismo». En AA. VV. *Resiliencia: del individuo al Estado y del Estado al individuo. Documentos de Seguridad y Defensa* n.º 77. Madrid: Ministerio de Defensa, febrero 2018; pp.109-130. Puede consultarse a través de siguiente página web: http://www.ieee.es/Galerias/fichero/cuadernos/DocSeguridadyDefensa_77.pdf.

multiámbito frente a las ciberamenzas, pues, como más adelante argumentaremos, consideramos que los límites jurídicos son aplicables a todas las operaciones militares con independencia de que estas se desarrollen en un tradicional espacio físico o en el novedoso ámbito ciberespacial. Esta afirmación no es consecuencia de ofrecer una solución simplificada a los retos que el ámbito ciberespacial nos ofrece, sino más bien al contrario: las respuestas desde el ámbito jurídico han de ser firmes, aunque la técnica de extrapolación por analogía de la normativa aplicable a los tradicionales espacios físicos al espacio virtual sea compleja. Esa firmeza es la que permitirá hacer visibles las limitaciones jurídicas, acotando al máximo el margen de maniobra de quienes utilizan el ciberespacio, como «zona gris», para realizar un uso malintencionado del mismo.

En cuanto a las operaciones militares multiámbito que puedan desarrollarse frente a los ciberataques, asume un gran protagonismo la resiliencia, si entendemos que dentro de este tipo de operaciones se encuentra un elenco de operaciones dirigidas tanto a la disuasión como a la prevención militar.

Si la disuasión militar tiene como objetivo o fin «persuadir a los potenciales adversarios de que se dispone de capacidades militares y de una voluntad o una determinación para emplearlas tales, que los riesgos que conllevaría iniciar un conflicto sobrepasarían con creces cualquier posible beneficio»[14], resulta evidente que lo que se busca es la resiliencia estatal en el ámbito de las operaciones militares, con independencia de que estas operaciones de disuasión se desarrollen en un espacio físico tradicional o en el ciberespacio.

En el mismo orden de cosas, si se considera la prevención militar como «el empleo de las Fuerzas Armadas con el objeto de anticiparse a la materialización de los riesgos o a canalizarlos hasta su desaparición»[15], es evidente que se está haciendo referencia a una amplia y flexible gama de operaciones multiámbito que podrán desplegarse, atendiendo, en primera instancia, a cuál es el nivel de resiliencia que se desea obtener y canalizando, al efecto, unos modos y medios de resiliencia determinados.

Para determinar los límites jurídicos de la resiliencia frente a las ciberamenazas que permitan esclarecer la normativa aplicable a las operaciones multiámbito, resulta necesario atender tanto al marco político que permite desarrollar una política de defensa como el planeamiento del nivel operacional, «incluyendo las limitaciones y restricciones políticas»[16], así como «la conducción y el seguimiento estratégico de las operaciones militares[17]. Pare-

[14] ESTADO MAYOR DE LA DEFENSA. *PDC-01(A) Doctrina para el Empleo de las Fuerzas Armadas*, doc. cit., 107.

[15] Ibídem. Entre las posibles operaciones de prevención militar se incluyen, expresamente, las actividades relacionadas con el control del ciberespacio.

[16] Ibídem, p. 110.

[17] Ibídem, p. 112.

ce pues, que los límites jurídicos para una resiliencia frente a ciberamenazas en el desarrollo de operaciones multiámbito se encuentran dirigidos tanto al planeamiento estratégico operacional como en la conducción y el seguimiento estratégico.

Resulta imprescindible, por consiguiente, no perder de referencia la visión estratégica de la resiliencia, en relación con la amenaza cibernética, pues nos permitirá descubrir unos parámetros a partir de los que podremos discernir cuáles y cómo deberán ser los esfuerzos que hayan de dirigirse para la consecución de una eficaz resiliencia en el desarrollo de operaciones militares. Al mismo tiempo, esos parámetros nos servirán de guía para dilucidar los límites jurídicos de las referidas operaciones multiámbito que nos ocupan.

Por otra parte, no debemos olvidar que el empleo de las FAS «contextualiza su actuación en un marco global de seguridad y en el estratégico de España»[18]. En la *Estrategia de Seguridad Nacional* (en adelante, ESN) de 2017 se advierte expresamente que «nos enfrentamos a una realidad definida por dinámicas a menudo opuestas, a un mundo globalizado, pero a su vez fragmentado y competitivo, un espacio donde la ambigüedad se ha convertido en uno de los mayores retos a la seguridad»[19], siendo uno de los principales retos a la seguridad los ciberataques. En la referida ESN también se recuerda la vocación global de España como gran contribuyente al sistema de paz y seguridad internacional, así como su vocación europeísta, mediterránea y atlántica. En consecuencia, «... nuestro país requiere igualmente apostar por el refuerzo de organizaciones clave para España como la Unión Europea o la OTAN. Europa es el eje del modelo democrático, político y de seguridad de España y por ello esta Estrategia aboga por el fortalecimiento de la integración, la legitimidad y la unidad de acción de la Unión Europea, así como la defensa de sus intereses globales». Si los trabajos desarrollados por la OTAN, especialmente a través de los esfuerzos desplegados desde su Centro de Excelencia en materia de ciberseguridad establecido en Tallín (Estonia), son imprescindibles a la hora de abordar las operaciones multiámbito, el marco jurídico y estratégico en el que se desarrolla la *Política Común de Seguridad y Defensa* (en adelante, PCSD) de la Unión Europea (en adelante, UE) ha de ser tenido como referente para la atención a la resiliencia frente a las ciberamenazas en el desarrollo de actividades tácticas defensivas. En consecuencia, en el presente capítulo tendremos en consideración, con carácter principal, pero no exclusivo, tanto el marco jurídico internacional general, como el particular de la UE y, por supuesto, el nacional.

---

18 Ibídem, prólogo bajo la autoría del general Fernando Alejandre Martínez.

19 *Estrategia de Seguridad Nacional. Un proyecto compartido de todos y para todos.* Madrid: Presidencia del Gobierno, 2017, prólogo a cargo del presidente del Gobierno, Mariano Rajoy.

Una visión estratégica de las ciberamenazas y de la resiliencia como marco político de referencia para el desarrollo de estrategias y planes de operaciones multiámbito de las FAS

Como se ha indicado, para el planeamiento, conducción y seguimiento de las operaciones militares, desarrolladas tanto en el espacio físico como en el virtual, resulta innegable tener como referente las limitaciones políticas y jurídicas. Por ello, se requiere acercarse, aunque sea someramente, a una visión estratégica de las ciberamenazas y de la resiliencia, en un contexto globalizado, como marco político de referencia para el desarrollo de estrategias y planes específicos de las operaciones multiámbito de las FAS. Teniendo en cuenta el firme compromiso de España en el ámbito de la seguridad y la defensa con sus compromisos internacionales adquiridos con organizaciones internacionales, tanto de ámbito universal como regionales, resultaría excesivamente ambicioso atender a todos ellos y, además, excedería de nuestro objetivo investigador principal. Por ello, en el desarrollo del presente epígrafe, atenderemos con carácter principal a la visión estratégica de la UE por las siguientes razones: 1) Es innegable que España, como Estado miembro, ha realizado una apuesta firme por una necesaria autonomía estratégica de esta Organización[20], no incompatible con sus compromisos adquiridos con la OTAN; 2) Por otra parte, el marco de la UE es desde el que se ha impulsado lo que podríamos denominar una cultura de resiliencia frente a los más variados riesgos y amenazas, entre los que encontramos los ciberincidentes que puedan ser calificados como ciberamenazas y que, por ende, entran dentro del ámbito de la defensa; 3) Tampoco hemos de olvidar que, como antes mencionábamos, las operaciones multiámbito pueden desarrollarse en distintos contextos, entre los que nos encontraríamos el desarrollo de operaciones en misiones u operaciones internacionales, que serán objeto de especial referencia en el presente capítulo. Sin lugar a la más mínima duda, el liderazgo y aportaciones de España en misiones y operaciones desarrolladas en el ámbito de la PCSD de la UE resulta evidente.

Nos permitimos afirmar que la visión estratégica de las ciberamenazas y de la resiliencia desarrollada dentro la PCSD de la UE constituye un marco de referencia para la visión estratégica española que, a su vez, iluminará la toma de decisiones y planificación estratégica de operaciones multiámbito frente a las ciberamenazas.

A pesar de que la *Estrategia Europea de Seguridad*[21] (en adelante, EES), adoptada en 2003, no incluía a las amenazas cibernéticas entre los riesgos y

[20] Esta firme apuesta no solo se encuentra recogida en la nuestra ESN de 2017, sino que queda reflejada en el nuevo liderazgo que está asumiendo España en relación con el impulso de la *Cooperación Permanente Estructurada* (en adelante, PESCO, en sus siglas en inglés) y su participación en 16 de los 17 proyectos hasta ahora probados, liderando dos de los más importantes, como son Strategic C2 System for CSDP y Missions and Operations.

[21] *Estrategia Europea de Seguridad: Una Europa segura en un mundo mejor*. Bruselas, 12 de diciembre de 2003. Disponible en http://www. Consilium.europa.eu/eudocs/cmsu-

amenazas que atenazaban a la seguridad de la UE, no debe ser desatendida, en cuanto que, como han señalado Pérez de las Heras y Curruca Muguruza: «Aun no formulando una estrategia militar, este documento constituye un referente obligado para cualquier opción de desarrollo de capacidades militares»[22], cuestión fundamental al tenerse que dotar la UE de las capacidades necesarias para ofrecer una resiliencia oportuna para hacer frente a los más variados riesgos y amenazas. En consecuencia, aunque en la EES no incluya a las ciberamenzas, se está atendiendo a la necesidad de dotarse de capacidades específicas vinculadas a hacer frente a riesgos y amenazas concretos, así como en el modo en que transformar las capacidades con las que se cuenta para adecuarlas a las necesarias evoluciones de los riesgos y amenazas. Sin dejar lugar a margen de duda, a pesar de que en esta EES no se haga referencia expresa a la resiliencia, nos encontramos ante un primer planteamiento estratégico de la misma.

Las ciberamenazas fueron objeto de atención, en 2008, tras los mencionados ciberataques sufridos por Estonia, en el informe complementario sobre la aplicación de la referida estrategia, conocido como el *Informe Solana*[23]. Con la incorporación de las ciberamenazas, el nuevo reto a conseguir consiste en determinar cómo dotarse de un sistema de ciberseguridad, en el que atender tanto a las actividades tácticas de carácter defensivo y ofensivo en el desarrollo de operaciones multiámbito. A pesar de que aún no se planteará este futuro sistema de resiliencia cibernética, no significa que no se estén realizando esfuerzos, a partir de entonces, dirigidos a la misma en el ámbito de la PCSD de la Unión. Así, si para la consecución de un sistema de ciberdefensa resultan relevantes las capacidades, también lo son los procesos de transformación de las referidas capacidades. En este sentido, son suficientemente ejemplarizantes los continuos procesos de transformación de capacidades de ciberdefensa que se están produciendo en el ámbito de la OTAN y de la UE[24].

---

pload/031208essiies.pdf.

22 PÉREZ DE LAS HERAS, B. y CURRUCA MUGURUZA, C. *Las capacidades civiles y militares de la UE: estado de la cuestión y propuestas de cara a la Presidencia Española 2010*. Fundación Alternativas. *Documento de Trabajo* 41/2009, p. 14. Disponible en el siguiente sitio web: http://www.fundacionalternativas.org/public/storage/opex_documentos_archivos/0a77ec7fe1d23333b6fa8fdf5229b0b8.pdf.

23 A los cinco años de la adopción de la *Estrategia Europea de Seguridad*, el entonces secretario general del Consejo de la UE y alto representante de la PESC, Javier Solana, presentó ante el Consejo Europeo un informe sobre la aplicación de la referida Estrategia, titulado: *Ofrecer seguridad en un mundo en evolución*. Será en el mismo cuando se atienda por primera vez, entre los retos mundiales y principales amenazas, la «ciberseguridad». En especial, se hará una llamada de atención a la posibilidad de que los servicios de TI gubernamentales de los Estados miembros, lo que ofrece una nueva dimensión al problema, en calidad de arma no solo económica y/o política, sino también militar.

24 Así, podrían destacarse, entre otros, que «La OTAN ha aprobado durante el año 2011, una nueva política y un plan de acción de ciberseguridad; y la UE aprobó en 2009 el «con-

Con el *Informe Solana*, se daría pie, además, a complementar el marco estratégico europeo con la adopción de sucesivas estrategias complementarias, entre las que se encuentra la *Estrategia de Ciberseguridad*[25], adoptada en 2013. Será a partir de entonces cuando se incorpore una visión estratégica específica de la UE hacia las ciberamenazas en al ámbito de la PCSD, constituyendo un primer punto de inflexión en la visión estratégica de la ciberseguridad en el seno de la UE, por lo que resulta imprescindible realizar un breve análisis para averiguar qué lugar ocupa y en qué sentido es atendida la resiliencia frente a las ciberamenazas. En la referida *Estrategia* se define el planteamiento de la UE sobre el mejor modo de prevenir y responder a perturbaciones y ataques cibernéticos, al tiempo que detalla una serie de medidas para mejorar la resistencia de los sistemas informáticos, reducir la ciberdelincuencia y fortalecer la política internacional de la UE en materia de ciberseguridad y ciberdefensa. Además, establece una serie de planes para afrontar los desafíos, incluyendo cinco prioridades: 1) lograr la ciberresiliencia; 2) reducir drásticamente la ciberdelincuencia; 3) desarrollar estrategias y capacidades de ciberdefensa vinculadas a la PCSD; 4) desarrollar recursos industriales y tecnológicos de ciberseguridad; y 5) establecer una política internacional coherente del ciberespacio para la UE y promover sus valores esenciales.

Parece evidente que la resiliencia cibernética ocupa un lugar prioritario. Sin embargo, resulta necesario analizar en qué sentido se está atendiendo a la resiliencia cibernética, pues, si atendemos a las prioridades contenidas en este documento también deberían ser tenidas en consideración esas prioridades en clave de resiliencia. Así, limitándonos tan solo al enunciado de las referidas prioridades, el desarrollo de capacidades de ciberseguridad vinculadas a la PCSD de forma innegable nos está remitiendo a la necesidad de dotarse de unas determinadas capacidades dirigidas a ser resilientes frente a las amenazas cibernéticas en el desarrollo de operaciones militares vinculadas a la PCSD. En este sentido, se atiende a la resiliencia como capacidad.

Por otra parte, si atendemos a la cuarta y quinta prioridad, es innegable que nos conducen a pensar que existen distintos modos de lograr esas capacidades, lo que nos llevaría, por una parte, a reflexionar sobre el proceso de transformación de esas capacidades (a través del desarrollo de recursos industriales y tecnológicos de ciberseguridad) y modos resiliencia (en este caso,

---

cepto de operaciones en red en operaciones militares lideradas por la UE», como se recoge en AA. VV. *Guerra cibernética: aspectos organizativos*. Grupo de trabajo n.º 3. XXXIII Curso de Defensa Nacional. Madrid: CESEDEN, 2013, p. 3. [Última consulta, 10/05/2018]. Disponible en https://documentop.com/guerra-cibernetica-aspectos-organizativos-ministerio-de-defensa-de_5a0cdefe1723dd577324d91b.html.

[25] *La Estrategia de Ciberseguridad de la Unión Europea* fue adoptada el 13 de febrero de 2013. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. [Última consulta, 3/03/2018]. Disponible en https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf.

mediante el establecimiento de una política internacional coherente del ciberespacio para la UE y la promoción de los valores esenciales de la UE).

Por último, también podemos atender a la resiliencia como resultado o fin estratégico a conseguir, tal y como se enuncia en la primera prioridad: lograr la resiliencia. En este sentido, también podemos atender al enunciado de la segunda prioridad: reducir drásticamente la ciberdelincuencia. Sin embargo, a pesar de que a primera vista resulte fácilmente identificable la resiliencia como un objetivo o fin estratégico, atendiendo al enunciado de la primera prioridad, nos encontramos con un planteamiento de este bastante confuso por varias razones: en primer lugar, porque no se ofrece una definición de resiliencia que nos permita acotar el sentido último que se le quiere conferir. En segundo lugar, porque en el desarrollo de esta prioridad, junto con las medidas que le acompañan, no se está atendiendo a la resiliencia como objetivo, sino a la resiliencia como capacidad y como proceso de transformación de capacidades, que vendremos a denominar, en adelante, medios y modos de lograr la resiliencia. En consecuencia, para poder dotar de contenido a la resiliencia como objetivo o fin estratégico, resulta paradójico, pero parece imprescindible la atención de la resiliencia como capacidad y como proceso de transformación de capacidades, lo que, por otra parte, altera el sentido lógico de una simple ecuación: ¿hacia qué grado de resiliencia han de desarrollarse las capacidades de ciberdefensa vinculadas a la PCSD?; ¿cuáles deberán ser los modos y medios de transformación de esas capacidades necesarios si no se determina un claro fin u objetivo estratégico de forma expresa para lograr la resiliencia? Del análisis de la *Estrategia de Ciberseguridad de la UE* podemos deducir que el fin u objetivo último que se persigue es triple: por una parte, reforzar la resiliencia nacional, tendente a la consecución de unos mínimos parámetros comunes de seguridad de las redes y de la información (SRI) de los Estados miembros de la UE; por otra parte, la coordinación en materia de prevención, detección y respuesta, así como la asistencia mutua entre los Estados miembros en materia de SRI; en tercer y último lugar, el aumento de la preparación y el compromiso del sector privado. En este sentido iban dirigidas las medidas que se acompañan para hacer efectiva la primera prioridad: «lograr la ciberresiliencia». Quizás lo más llamativo es que en el desarrollo de esta primera prioridad se entremezclen cuestiones más propias de la resiliencia como capacidad o como procedimiento que como objetivo, como a primera vista parecía ser identificada la resiliencia. Especialmente destacable de esta Estrategia es que en ella se ofrece un modo propio de conseguir la resiliencia, mediante el establecimiento de una política internacional coherente del ciberespacio en la UE, en la que se promuevan sus valores fundamentales.

Será, no obstante, en 2016, con la adopción de *La Estrategia Global para la Política Exterior y de Seguridad de la Unión Europea* (en adelante, *Estrategia Global*), bajo el título *Una visión común, una actuación conjunta: una Europa*

más fuerte[26] cuando la resiliencia se convierta en un eje central estratégico frente a todos los riesgos y amenazas que atenazan la seguridad de la UE, incluidas las ciberamenazas.

La Estrategia Global de la UE atiende también a la denominada era de la revolución digital en la que nos encontramos inmersos, por lo que se establece que la prosperidad de la UE «depende también del libre flujo de información y de la existencia de cadenas de valor mundiales facilitadas por una intranet libre y segura»[27]. Por ello, la UE centra de forma especial su atención en la ciberseguridad como un elemento clave para el buen desarrollo de un mercado único europeo en el que se ha apostado por la creación de un mercado digital europeo que, además, ha de ser seguro. Con una clara vinculación del bienestar y desarrollo económico de la Unión con la seguridad, los Estados miembros deben establecer mecanismos de protección adecuados, por lo que en la Estrategia Global se establece que la UE deberá ayudar «a los Estados miembros para que se protejan de las ciberamenazas, manteniendo al mismo tiempo un ciberespacio abierto, libre y seguro»[28].

La UE va aún más lejos, al afirmar, en la referida Estrategia: «La UE será un ciberactor con visión de futuro que protegerá nuestros activos y valores en el mundo digital, en particular mediante la promoción de una Internet mundial gratuita y segura»[29], a través de diversos tipos de acciones como la ciberdiplomacia, la capacitación de sus socios y el impulso de la celebración de «acuerdos de comportamiento responsable en el ciberespacio basados en el derecho internacional existente», así como apoyando una «gobernanza digital multilateral y un marco de cooperación mundial en materia de ciberseguridad, respetando la libre circulación de la información»[30]. En consecuencia, en la Estrategia Global de la UE se exige la integración de las cuestiones cibernéticas en todos los ámbitos políticos, así como el refuerzo de los elementos cibernéticos en las misiones y operaciones de la PCSD.

Al mismo tiempo, a lo largo de toda la Estrategia se apuesta por la resiliencia como un instrumento eficaz para hacer frente a los distintos riesgos y amenazas que atenazan la seguridad de la UE, procediendo a definirla como «la capacidad de los Estados y las sociedades para reformarse, soportando

---

26 *Estrategia Global para la Política Exterior y de Seguridad de la Unión Europea*: «Una visión común, una actuación conjunta: una Europa más fuerte». [Última consulta, 20/12/2017]. Disponible en el siguiente sitio web: https://europa.eu/globalstrategy/sites/globalstrategy/files/eugs_es_version.pdf. Esta Estrategia fue presentada por la alta representante de la Unión para asuntos Exteriores y Política de Seguridad al Consejo Europeo, el 28 de junio de 2016.

27 Ibidem, p.11.

28 Ibídem, p. 16.

29 Ibídem, p. 33.

30 Ibídem, p. 34.

los desastres, y recuperarse de crisis internas y externas». Sin embargo, la nueva Estrategia de la UE sigue sin contener líneas de acción concretas para abordar los objetivos estratégicos en relación con cada uno de los riegos y amenazas atendidos, que pudieran ofrecer mayor luz a las estrategias y planes de acción sectoriales que deberán desarrollarse, en los que la resiliencia deberá ser tenida en consideración.

Parece evidente el protagonismo principal que se le confiere al término resiliencia en la Estrategia Global, como lo demuestra su inclusión de forma expresa en más de una treintena de ocasiones, convirtiéndola en uno de sus ejes centrales. Sin embargo, no parece claro el sentido con el que el referido término es incorporado, pues en algunas ocasiones se hace referencia a la resiliencia como una capacidad para hacer frente a los diferentes riesgos y amenazas; en otras, como un proceso de transformación o adaptación de las capacidades al tiempo que evolucionan los distintos riesgos y amenazas y, en otras, como un fin u objetivo a alcanzar: la consecución de Estados y sociedades resilientes. La propia definición de resiliencia contenida en esta estrategia parece más bien dirigida al proceso de transformación de las capacidades al comenzar la misma haciendo referencia a la capacidad de reforzarse.

Si resulta necesario acotar el contenido concreto que se le ha de conferir a la resiliencia para ofrecer una respuesta eficaz a los riesgos y amenazas cibernéticos, se hace aún más necesario atender a las medidas que se deberían adoptar para ofrecer una resiliencia eficaz en relación con las misiones y operaciones de la PSCD, habida cuenta los diferentes ámbitos en los que se pueden realizar operaciones multiámbito frente a las ciberamenazas: tanto en el contexto de una ciberguerra como fuera de él, incorporando las más variadas combinaciones de operaciones multiámbito con utilización de medios y métodos de combate convencionales y cibernéticos. En esta línea, en el *Plan director de la respuesta coordinada a los incidentes y crisis de ciberseguridad transfronterizos a gran escala*[31] (en adelante, Plan Director de Respuesta Coordinada) se afirma que «dado que se espera que las crisis de ciberseguridad tengan en su mayoría efectos sobre el mundo físico, toda respuesta adecuada debe basarse en actividades de mitigación de carácter tanto cibernético como no cibernético». No debemos olvidar tampoco que los ciberataques podrían conllevar daños personales, incluida la muerte, y/o daños materiales, como se desprende del *Manual de Tallín*[32].

En clara coherencia con los compromisos jurídicos internacionales asumidos por España, al margen de otros importantes factores, la adopción de la

[31] El Plan Director de la respuesta coordinada a los incidentes y crisis de ciberseguridad transfronterizos a gran escala se encuentra recogido en el Anexo de la Recomendación de la Comisión sobre la respuesta coordinada a los incidentes y crisis de seguridad a gran escala, de 13 de septiembre de 2017. Doc: C (2017)6100 final ANNEX 1.

[32] SCHMITT, M. N. (ed.). *Manual de Tallin... Op. cit.*, p. 106.

Estrategia Global de la UE ha propiciado la adopción en España de la Estrategia de Seguridad Nacional de 2017, otorgándole un protagonismo especial también a la resiliencia, al incorporarla como uno de los principios informadores. Esos principios, a su vez, iluminarán cinco objetivos generales de la seguridad nacional: El desarrollo de un modelo integral de gestión de crisis; la promoción de una cultura de seguridad nacional; el favorecimiento de un buen uso de los espacios comunes globales; el impulso de la dimensión de seguridad en el desarrollo tecnológico y, por último, el fortalecimiento de la proyección internacional de España.

Además de estos objetivos generales, se incluyen objetivos propios de cada uno de sus ámbitos y líneas de acción estratégicas asociadas. En relación con el objetivo «defensa nacional», resulta interesante destacar dos líneas de acción que podríamos vincular fácilmente con la resiliencia cibernética. La primera línea de acción a destacar consistiría en «mejorar la capacidad de defensa autónoma para ejercer una disuasión efectiva frente a cualquier amenaza exterior». De ella fácilmente se desprende que la disuasión se convertiría en el fin u objetivo a perseguir para la convertirnos en un Estado ciberresiliente frente a cualquier amenaza, incluidas las ciberamenazas, provenientes del exterior (incluido, por lo tanto, del ámbito ciberespacial). Por otro lado, podemos señalar otra línea de acción: «Impulsar una estrategia industrial de defensa que fomente la autonomía en la adquisición de capacidades estratégicas y favorezca la competitividad de la industria española a nivel global». Es indudable, respecto a las ciberamenazas que entre las acciones preventivas militares necesarias dirigidas a una eficaz disuasión requiere de unas capacidades tecnológicas de última generación. En consecuencia, en una planificación estratégica de operaciones multiámbito frente a las ciberamenazas se debería incluir, con carácter prioritario, el impulso en tal sentido que permita contar con una autonomía en el ámbito de la ciberdefensa.

La ciberseguridad constituye un objetivo específico al que se le asocian las siguientes líneas de acción: 1) Reforzar las capacidades de prevención, detección, reacción, análisis, recuperación, respuesta e investigación frente a las ciberamenazas, así como potenciar la coordinación en los niveles técnico y estratégico del sistema de seguridad nacional en el ámbito de la ciberseguridad; 2) Reforzar, impulsar y promover los mecanismos normativos, organizativos y técnicos, así como la aplicación de medidas, servicios, buenas prácticas y planes de continuidad para la protección, seguridad y resiliencia en el sector público, los sectores estratégicos (especialmente en las infraestructuras críticas y servicios esenciales), el sector empresarial y la ciudadanía, de manera que se garantice un entorno digital seguro y fiable; 3) Reforzar y mejorar las estructuras de cooperación público-público y pública-privada nacionales en materia de ciberseguridad; 4) Alcanzar las capacidades tecnológicas necesarias mediante el impulso de la industria española de ciberseguridad, promoviendo un entorno que favorezca la investigación,

el desarrollo y la innovación, así como la participación del mundo académico; 5) Promover el alcance y mantenimiento de los conocimientos, habilidades, experiencia, así como capacidades tecnológicas y profesionales que necesita España para sustentar los objetivos de la ciberseguridad. 6) Contribuir a la seguridad del ciberespacio, en al ámbito de la Unión Europea e internacional, en defensa de los intereses nacionales, fomentando la cooperación y el cumplimiento del derecho internacional[33].

En el capítulo cuatro de la ESN se recogen las amenazas junto a unos desafíos, que sustituyen a los riesgos que se atendían en la estrategia de 2013 y a los factores potenciadores del riego que se recogían en la Estrategia de 2011. El cambio de riesgos a desafíos resulta especialmente interesante de la atención de las amenazas en clave de resiliencia. En efecto, si en relación con los desafíos se establece que, «sin tener de por sí entidad de amenaza, incrementan la vulnerabilidad, provocan situaciones de inestabilidad o pueden propiciar el surgimiento de otras amenazas, agravarlas o acelerar su materialización»[34], es evidente que han de ser tenidos en cuenta en el establecimiento, conducción y seguimiento de operaciones multiámbito en clave de resiliencia frente a las ciberamenazas. En la *Estrategia Nacional de Ciberseguridad 2019* (en adelante, ENC) se estructuran las amenazas y desafíos en dos grandes categorías: «por un lado, las que amenazan a activos que forman parte del ciberespacio; y por otro, aquellos que usan el ciberespacio como medio para realizar actividades maliciosas e ilícitas de todo tipo»[35]. En el capítulo dos de la ENC, se analizan los principales desafíos y amenazas del ciberespacio frente a los que España debería ser resiliente.

Es evidente que la consecución de Estados y sociedades ciberresilientes requiere de un punto de partida inevitable, aceptar que somos vulnerables, conocer cuál es nuestro grado de vulnerabilidad, conocer las capacidades que nos permitirían ser menos vulnerables e iniciar el proceso de transformación de las referidas vulnerabilidades, adoptando unos modos y medios determinados para la consecución del objetivo último al que debería ir dirigida la resiliencia que sería la disuasión. Sin embargo, como también se ha apuntado, es posible que el objetivo o fin de la resiliencia permita distintos niveles de resiliencia. En consecuencia, al partir del reconocimiento de nuestra vulnerabilidad ante las distintas amenazas también debemos tener en consideración los desafíos que puedan incrementar esa vulnerabilidad. A ello, habría que unir una evidencia que también se recoge en la ESN de 2017: «En el mundo actual, tanto las amenazas como los desafíos suelen estar interconectados y sus efectos traspasan fronteras»[36].

---

33 *Estrategia de Seguridad Nacional*, doc. cit., p. 99.

34 Ibídem, doc. cit., p. 56.

35 *Estrategia Nacional de Ciberseguridad 2019. BOE* n.º 103. 30 de abril de 2019, p. 43438.

36 Ibídem.

Del referido capítulo cuatro también es destacable el que se haga expresa mención al buen uso de los espacios comunes globales, entre los que se encuentra el ciberespacio, como un requisito indispensable para la seguridad. En relación con estos espacios comunes globales, no solo se limita a resaltar su gran valor, sino que, además, los definirá como «dominios no susceptibles de apropiación, presididos por el principio de libertad»[37].

De especial importancia es la referencia a la vulnerabilidad de las infraestructuras críticas, especialmente de las que dependen la provisión de servicios esenciales, frente a las amenazas, entre las que no debemos descartar las ciberamenazas y frente a las que deberán planificarse estratégicamente, conducir y realizar un adecuado seguimiento de las operaciones defensivas para la consecución de unas infraestructuras críticas. En este sentido, deberíamos reflexionar sobre la necesaria combinación de operaciones defensivas que se desarrollen tanto en los tradicionales espacios físicos, impidiendo, por ejemplo, el acceso a las referidas instalaciones como ciberoperaciones defensivas. En cualquier caso, como se analizará en los siguientes epígrafes, los límites jurídicos a las operaciones defensivas, cibernéticas o no, deberán ser las mismas.

Como reflexión final, tras la visión estratégica de las ciberamenazas y de la resiliencia frente a las mismas, podemos afirmar que resulta necesario atender a tres parámetros a partir de los cuales atender a la resiliencia:

El primer parámetro, sería la consideración de la resiliencia con fin u objetivo, pudiendo existir un fin último a perseguir que sería la disuasión a través de la consecución de Estados y sociedades resilientes, pudiendo marcarse distintos niveles de resiliencia. En relación con este primer parámetro, situaríamos a las operaciones multiámbito dirigidas a la prevención y a la disuasión.

El segundo parámetro, consecuencia del reconocimiento de una vulnerabilidad frente a los ciberataques, sería la consideración de la resiliencia como capacidad. En este sentido, se estaría reconociendo cuáles serían las capacidades de partida con las que se cuenta para hacer frente a los ciberataques y cuáles serían las capacidades necesarias para alcanzar el objetivo o fin estratégico deseado. En consecuencia, se debería tener en cuenta a la hora de realizar una correcta planificación estratégica de las operaciones militares multiámbito. No debemos olvidar que lo que se busca es reforzar la resiliencia frente las amenazas cibernéticas, reconociendo nuestra vulnerabilidad. Al respecto, la ESN de 2017 se dedica de forma especial a la vulnerabilidad del ciberespacio, pues se ha de tener presente que «en los últimos tiempos, las acciones negativas en el ámbito de la ciberseguridad han aumentado notablemente en número, alcance y sofisticación. Tales acciones adquieren creciente relevancia para España, un país altamente interconectado y que

[37] Ibídem, p. 57.

ocupa una posición de liderazgo en Europa en materia de implantación de redes digitales»[38].

Desde el parámetro de las capacidades, para la atención de la resiliencia cibernética se debe partir tanto del análisis de las capacidades cibernéticas con las que se cuenta para poder hacer frente a las ciberamenazas como de una evaluación de la amenaza en sí misma. De esta forma, se podrán evidenciar las vulnerabilidades de la UE y de sus Estados miembros frente a las amenazas cibernéticas, debiendo reforzar sus capacidades para el eficaz desarrollo de operaciones multiámbito en clave de resilencia. En consecuencia, el referido refuerzo de capacidades estará vinculado al objetivo estratégico deseado en los distintos niveles de resiliencia. Estos distintos niveles de resiliencia, a su vez, vendrán condicionados, por una parte, por el gran abanico de operaciones multiámbito a desarrollar. Por otra parte, por los distintos actores o agentes que pueden verse involucrados en su desarrollo. Todas estas cuestiones deberán ser atendidas sin olvidarnos del marco normativo en el que podrían desarrollarse operaciones cibernéticas en el ámbito de la PCSD.

El tercer parámetro, atendería a la resiliencia como procedimiento de transformación de esas capacidades, es decir, en los medios necesarios para lograr la ciberdisuasión y los modos en que se ha de realizar esa transformación de los Estados y de las sociedades en sujetos activos ciberresilientes. Especial importancia revisten los modos en que se han de dar respuestas a los ciberataques a través de operaciones multiámbito, pues la atención a los modos de conseguir ser resilientes es lo que nos permitirá dilucidar los límites jurídicos aplicables a dichas operaciones y ciberoperaciones.

Límites jurídicos de la resiliencia en operaciones militares multiámbito

Del análisis de la visión estratégica, parece innegable que las operaciones militares multiámbito deberían ser estratégicamente planeadas para la consecución de estados ciberresilientes frente a los ataques cibernéticos que entren dentro del ámbito de la defensa. Al mismo tiempo, hemos deducido tres grandes parámetros desde los que la resiliencia ha de ser atendida, siendo la atención a los modos de resiliencia lo que permitirá el establecimiento de límites jurídicos tanto a las operaciones multiámbito que se desarrollen en los territorios bajo la soberanía de los Estados miembros de la UE como a las que se desarrollen en territorios fuera de la Unión.

Como hemos podido observar, la consecución de Estados ciberresilientes constituye en sí mismo el fin u objetivo estratégico de los Estados y de organizaciones internacionales, como la UE. Por otro lado, también se ha podido

[38] Ibídem, p. 65.

constatar que pueden existir distintos niveles de resiliencia, dependiendo del riesgo, desafío o amenaza frente al que se desea ser resiliente, así como del nivel de exigencia respecto del sector de la sociedad a la que va dirigida esa resiliencia. En consecuencia, no sería ilógico pensar que el objetivo o fin último de la resiliencia frente a las ciberamenazas, en el ámbito de la defensa, sería la disuasión.

En este sentido, recordamos que el concepto de disuasión contenida en la *PDC-01 (A) Doctrina para el empleo de las FAS*, al que nos referimos en el epígrafe uno del presente capítulo, incluiría a toda la gama de operaciones y ciberoperaciones dirigidas a la persuasión de potenciales adversarios. Consecuentemente, las operaciones y ciberoperaciones defensivas de prevención tendrían como fin u objetivo último la disuasión.

Sin embargo, la resiliencia dirigida a la disuasión en el contexto del desarrollo de las operaciones multiámbito encuentra unos importantes límites jurídicos, que no son otros más que los que se derivan de los principios y valores reconocidos en nuestra Constitución, coincidentes con los reconocidos por la UE. Ese conjunto de principios y valores, que constituyen la esencia de la identidad europea que compartimos, son los que de forma coherente sirven para iluminar nuestra política nacional de defensa y la PCSD de la UE. El cumplimiento de esos principios y valores son, precisamente lo que nos distingue a los Estados miembros de la UE en el planeamiento estratégico de operaciones multiámbito, a su conducción y seguimiento estratégico. Podríamos, incluso, hablar de un modo europeo de conseguir que los Estados miembros de la UE sean lo suficientemente ciberresilientes para disuadir a los potenciales enemigos a dirigir sus ciberataques contra ellos.

Al comienzo del presente capítulo hemos podido resaltar cómo la gran mayoría de las características de la denominada «zona gris» era coincidente con las características de este nuevo ámbito ciberespacial de operaciones operaciones de las FAS se sirvan de las mismas vulnerabilidades. Sin embargo, el hecho de que los autores de los ciberataques se aprovechen de las vulnerabilidades que presenta este nuevo espacio virtual como campo de batalla no debe ser una justificación para que las operaciones de las FAS se sirvan de las mismas vulnerabilidades de esa zona gris, separándose del cumplimiento de los principios y valores que iluminan esas operaciones en los espacios físicos. Es decir, que las limitaciones jurídicas aplicables a las operaciones militares que se desarrollan en los tradicionales ámbitos físicos son también de aplicación al ámbito virtual.

Si en el ciberespacio no se respetasen las limitaciones jurídicas ya existentes, podríamos estar ante un grave problema de desnaturalización de la propia esencia de los conceptos jurídicos existentes, pudiéndose convertir a medio o largo plazo en un arma de doble filo sobre lo que verdaderamente se desea defender. En este sentido, Federico Aznar manifestará que: «... la resiliencia se encuentra relacionada con el control de las emociones, con

la disciplina e implantación real de los valores que desde esa sociedad se propugna, en el crédito que realmente les da en la lucha que en su nombre se acomete»[39].

Debemos tener en cuenta, tal y como se indica, in fine, en el debemos tener en cuenta, tal y como se indica, *in fine*, en el artículo 2 del TUE que los valores recogidos en ese artículo «... son comunes a los Estados miembros en una sociedad caracterizada por el pluralismo, la no discriminación, la tolerancia, la justicia, la solidaridad y la igualdad entre mujeres y hombres». En consecuencia, los valores de respeto de la dignidad humana, libertad, democracia, igualdad, Estado de derecho y respeto de los derechos humanos, incluidos los derechos de las personas pertenecientes a minorías son los que deben guiar la política de defensa de los Estados miembros y la PCSD de la UE, formando parte de esa identidad europea que compartimos. Por lo tanto, cualquier actividad realizada destinada al empleo de las FAS en operaciones multiámbito frente a los ciberataques que se encuentren dentro del ámbito de la defensa deberá ser conforme con los mencionados valores, pues son coincidentes con nuestros valores constitucionales y constituyen la propia esencia de este tipo de operaciones: la defensa de esos valores que nos identifican como una sociedad democrática en cuyos cimientos de encuentran el respeto del Estado de derecho y de los derechos y libertades fundamentales.

En el artículo 21.1. del TUE, por su parte, se establece que la acción de la UE en la escena internacional se basará en los siguientes principios: la democracia, el Estado de derecho, la universalidad e indivisibilidad de los derechos humanos y de las libertades fundamentales, el respeto de la dignidad humana, los principios de igualdad y solidaridad y el respeto de los principios de la Carta de las Naciones Unidas y del derecho internacional. Todos estos principios, como expresamente se reconoce, no solo han servido para iluminar la creación, desarrollo y ampliación de la propia Unión, sino que, además, son principios que pretende fomentar, a través de su acción exterior al resto del mundo.

Llegados a este punto, parece lógico pensar que los límites jurídicos para las operaciones multiámbito, incluyendo el gran abanico de actividades tácticas de carácter defensivo dirigidas a la consecución de Estados ciberresilientes no pueden venir más que de la mano del fiel cumplimiento de los principios y valores de aplicación general a toda acción exterior de la UE, de la que forma parte integrante la PCSD, y que compartimos los Estados miembros de la UE. No en vano, en nuestra ESN de 2017, al mostrar cuál es el perfil de nuestro Estado, se estable que: «España es un Estado social y democrático de derecho, dotado de un marco constitucional de derechos y libertades que tiene al ciudadano como eje central, y de unas instituciones que propugnan y protegen como valores superiores la libertad,

[39] AZNAR FERNÁDEZ - MONTESINOS, F. «Resilencia y acción política ...». *Op. cit.*, p. 123.

la justicia, la igualdad y el pluralismo político»[40], añadiendo que «este es el fundamento de la seguridad nacional como política de Estado y servicio público cuyo objeto es proteger la libertad, los derechos y el bienestar de los ciudadanos, garantizar la defensa de España y los principios y valores recogidos en su Constitución...»[41].

El caso de los ciberataques sufridos por Estonia en 2007 nos puede servir de ejemplo para reflexionar sobre algunos de los límites jurídicos antes mencionados. Por una parte, podemos pensar en el contexto en el que se reciben los ciberataques, propio de la zona gris, pues no se había pasado el umbral de violencia para calificar la situación de conflicto armado, al tratarse de sucesivas revueltas y manifestaciones callejeras. En este sentido, las normas internacionales aplicables en tiempo de paz son las que han de aplicarse a las operaciones militares multiámbito que nos ocupan. Por otra parte, nos encontramos ante una situación que también puede ser atendida desde el punto de vista de la zona gris: el lanzamiento de multitud de ciberataques de diversa magnitud, que de forma individualizada no serían siquiera objeto de atención en el ámbito de la defensa, pero que pueden llegar a causar un daño tal a las RSI (como la paralización de varias páginas webs institucionales y privadas), que, de haberse producido por un ciberataque, si hubiese permitido una respuesta militar, en legítima defensa (como será objeto de atención en el capítulo 4 de la presente obra).

Esta situación nos permite recordar que hasta que no se produzca una calificación jurídica del ciberataque o del conjunto de ciberataques masivos recibidos de baja intensidad como ataques armados, de conformidad con la normativa internacional, no se podrán emplear a las FAS en operaciones multiámbito que contravengan o menoscaben el pleno disfrute de los derechos y libertades fundamentales, salvo en aplicación de las normas constitucionales que permitan limitar, con carácter excepcional y temporal, esos derechos y libertades fundamentales. Lo que claramente queda reflejado con este ejemplo es que no es posible incorporar como acciones preventivas el desarrollo de acciones tácticas ofensivas con carácter preventivo (la utilización de la denominada legítima defensa preventiva excedería de los límites jurídicos permitido por el derecho internacional).

Cuestión distinta es atender a lo que en el *Manual de Tallin 2.0* se denomina *Passive Cyber Defence*, entendida como la toma de medidas dirigidas a la detección y mitigación de intrusiones cibernéticas y los efectos de las operaciones cibernéticas, siempre que no impliquen el lanzamiento de acciones tácticas preventivas o de una contraoperación dirigida hacia la fuente.

---

40 *Estrategia de Seguridad Nacional,* doc. cit., p. 20.

41 Ibídem, *doc. cit*, p. 21. Su inclusión en la ESN no es más que consecuencia del cumplimiento del artículo 8 de nuestro texto constitucional, en el que se establece que «Las FAS, constituidas por el ET, la Armada y el EA, tienen como misión garantizar la soberanía e independencia de España, defender su integridad territorial y el ordenamiento constitucional».

Se incluye también en el referido Manual una serie de medidas de defensa cibernética pasiva, como son los cortafuegos, parches, software antivirus y herramientas forenses digitales. Estas actividades serían unas medidas defensivas adecuadas y eficientes frente a las más usuales ciberamenazas, entre las que nos encontramos, siguiendo la ESN de 2017, «el robo de datos e información, los ataques *ransomware* y de denegación de servicios, el hackeo de dispositivos móviles y sistemas industriales y los ciberataques contra las infraestructuras críticas son ejemplos de ciberamenazas»[42].

Si la situación sufrida por Estonia en 2007 se repitiese ahora, la situación resultante hubiese sido diferente, pues este Estado cuenta con un elevado nivel de resiliencia cibernética. Este caso fue el detonante para que la resiliencia frente a las ciberamenazas fuera considerada como la más eficaz acción de prevención y de disuasión.

No menos interesante resulta el caso de los ciberataques sufridos en territorio bielorruso en 2008. Un estudio pormenorizado de este interesante caso se excedería de nuestro objetivo investigador. Sin embargo, nos permite dejar constancia de otros posibles usos maliciosos de las RSI tras los que puede encontrarse una autoridad gubernamental frente al ejercicio virtual de un derecho fundamental como es el derecho a la comunicación y la libertad de expresión. Su relevancia en el ámbito de la UE es innegable, si recordamos que, ya en 2006, el Parlamento Europeo consideró que «el acceso a Internet puede fortalecer la democracia y contribuir al desarrollo social y económico de un país, y que restringir el acceso a este medio es incompatible con el derecho a la libertad de expresión»[43]. En consecuencia, queda claro que el límite de la resiliencia y de las operaciones multiámbito frente a las ciberamenazas se sitúa en el principio del respeto de los derechos y libertades fundamentales.

En clave de resiliencia, podemos afirmar la existencia de un modo de resiliencia europeo consistente en el respeto de los derechos humanos y las libertades fundamentales como parte de la identidad europea común para los Estados miembros de la UE y del Consejo de Europa, como es el caso de España.

Especial referencia al contexto de las operaciones o misiones internacionales desarrolladas fuera de la UE

No debemos olvidar que las operaciones militares multiámbito pueden desarrollarse en distintos entornos, entre los que nos encontramos con las misiones u operaciones internacionales. Es evidente que los límites jurídicos hasta ahora señalados también serán de obligada observancia en estos supuestos. No obstante, en este subepígrafe atenderemos a algunas cuestio-

42 *Estrategia de Seguridad Nacional*, doc. cit., p. 65.

43 PARLAMENTO EUROPEO. Resolución sobre la libertad de expresión en Internet, de 6 de julio de 2006, DOC: P6 _ TA (2006)0324.

nes más específicas en relación con la resiliencia frente a los ciberataques que pueden sufrir en las RSI y "más concretamente" en los sistemas de información y comunicación (en adelante, SIC) que permiten el flujo de información entre los contingentes desplegados sobre el terreno en una zona de operaciones y entre estos y el mando y control de la operación situado en territorio de la Unión. Por lo tanto, junto a los modos de resiliencia que nos permitían hablar de un modo europeo para ser estados ciberresilientes, en el supuesto de las operaciones y misiones desarrolladas fuera de la UE se requiere reforzar la resiliencia aún más en relación con las capacidades.

En este sentido, teniendo en consideración que España es uno de los mayores contribuyentes a las misiones de la UE, analizaremos la resiliencia de las operaciones multiámbito desarrolladas en misiones u operaciones internacionales dentro del marco de la PCSD de la Unión. Como excelentemente recuerda Ballesteros Martín: «... España mantiene tropas en todas y cada una de las seis operaciones militares que está llevando a cabo la UE con un esfuerzo sostenido que va mucho más allá de lo que le correspondería por población y PIB y a pesar de tener uno de los presupuestos más bajos de defensa de todos los socios»[44], lo que, a nuestro entender, justifica sobradamente nuestra atención a las mismas.

Restringir nuestro análisis al ámbito de la UE, además, se justifica porque las distintas modalidades de participación en misiones u operaciones internacionales establecidas en el capítulo V del TUE nos permite atender a un amplio abanico de ejemplos de operaciones militares multiámbito desde el que poder abordar la resiliencia frente a las ciberamenazas y los correspondientes límites jurídicos. En cualquier caso, a pesar de que el ámbito de referencia escogido sea el de la UE nada impide que los límites jurídicos que se vayan destacando sean extrapolables a cualquier operación multiámbito de las FAS en el contexto de misiones u operaciones de las Naciones Unidas o lideradas por la OTAN.

Por otra parte, tampoco debemos olvidar que, en la EES de 2003, se produjo una ampliación de las misiones y operaciones a desarrollar por la UE. En consecuencia, como indicaban Pérez de las Heras y Curruca Muguruza: «Esta ampliación de misiones UE requería incrementar las capacidades civiles y militares»[45], que se concretarían, como se establece en la Estrategia, en la adopción de una serie de medidas.

Será con el Tratado de Lisboa cuando se produzca una ampliación de las misiones de la UE (artículos 42.1 y 43). En el apartado 1 del artículo 42 del TUE se establece que la PCSD ofrecerá una capacidad operativa basada tanto en medios civiles como militares a los que podrá recurrir la UE en misiones

[44] BALLESTEROS MARTÍN, M. A. «Las novedades de la Estrategia de Seguridad Nacional 2017». *Documento Análisis* 74/2017, de 20 de diciembre de 2017. Madrid: Instituto Español de Estudios Estratégicos, 2017, p. 6, pp. 1-18.

[45] Ibídem, p. 15.

fuera de la Unión, cuyo objetivo consista en «garantizar el mantenimiento de la paz, la prevención de conflictos y el fortalecimiento de la seguridad internacional, conforme a los principios de la Carta de las Naciones Unidas». Este tipo de misiones en el exterior abarcan, de conformidad con el artículo 43 del TUE, actuaciones conjuntas en materia de desarme; misiones humanitarias y de rescate; misiones de asesoramiento y asistencia en cuestiones militares; misiones de prevención de conflictos y de mantenimiento de la paz; misiones en las que intervengan fuerzas de combate para la gestión de crisis, incluyendo misiones de restablecimiento de la paz y operaciones de estabilización al término de los conflictos.

Con independencia del tipo de misión que la UE despliegue en el exterior, en la Estrategia Global se establece que «frente a las amenazas externas, debemos estar preparados y capacitados para ejercer disuasión, dar respuesta y protegernos»[46], de tal forma que se vincula esa capacitación con un adecuado nivel de ambición y autonomía estratégica para fomentar la paz y seguridad tanto en el interior como en el exterior. Para su consecución, siguiendo la referida Estrategia, se requieren medios tecnológicos e industriales para adquirir y mantener las capacidades que sustenten su capacidad de actuación autónoma[47].

Atendiendo a que la posibilidad de respuesta de la UE a crisis internacionales mediante el establecimiento de operaciones y misiones de la PCSD, de conformidad con el artículo 43 del TUE, puede incluir tanto operaciones de mantenimiento de la paz como de imposición de la paz, el refuerzo de los elementos cibernéticos han de ser atendidos para ambos teatros de operaciones presentes y futuros.

De la treintena de operaciones y misiones desplegadas por la UE, desde que se estableció la Misión de Policía de la Unión Europea en Bosnia Herzegovina[48], en 2002, se puede afirmar que han sido participaciones con capacidades militares de baja intensidad dirigidas, fundamentalmente, a facilitar la ayuda humanitaria, de estabilización o de reconstrucción, de

---

46 *Estrategia Global*... doc. cit., p. 14.

47 En relación con las ciberamenazas, implica: «... estimular los sistemas innovadores de tecnologías de la información y la comunicación (TIC) que garanticen la disponibilidad e integridad de los datos a la vez que velan por la seguridad dentro del espacio digital europeo mediante políticas adecuadas sobre el emplazamiento del almacenamiento de datos y la certificación de los productos y servicios digitales. Exige integrar las cuestiones cibernéticas en todos los ámbitos políticos, reforzando los elementos cibernéticos en las misiones y operaciones de la PCSD, y proseguir el desarrollo de plataformas de cooperación». Ibídem, pp. 16-17.

48 Establecida por la Acción Común del Consejo, de 11 de marzo de 2002, relativa a la Misión de Policía de la Unión Europea (2002/210/PESC) (DOCE L 70 de 13/3/2002; p. 1), fue desplegada el 1 de enero de 2003, reemplazando a la Fuerza Internacional de Policía de las Naciones Unidas. Tras sucesivas prórrogas, desempeñó sus funciones hasta el 30 de junio de 2012.

adiestramiento y asesoramiento de las Fuerzas Armadas de los Estados anfitriones (como en tres de las seis misiones militares de la UE actualmente desplegadas: EUTM Mali[49]; EUTM RCA[50]; EUMT Somalia[51]). La única excepción la encontramos, en la actuación de la UE a través de la operación ATALANTA[52] en la que se han tenido que utilizar medios militares para el

[49] Misión militar de la Unión Europea destinada a contribuir a la formación de las fuerzas armadas de Malí (EUTM Malí), establecida en Decisión 2013/34/PESC del Consejo, de 17 de enero de 2013, relativa a una misión militar de la Unión Europea destinada a contribuir a la formación de las fuerzas armadas de Malí (EUTM Malí) (Do L 14 de 18/1/2013, p. 19), iniciándose el 18 de febrero de 2013 por Decisión 2013/87/PESC del Consejo de 18 de febrero de 2013 (DO L 46 de 19/2/2013, p. 27). La última modificación se produjo a través de la Decisión (UE) 2017/971 del Consejo, de 8 de junio de 2017, por la que se determinan las disposiciones de planificación y ejecución de misiones militares no ejecutivas PCSD de la UE y por la que se modifican la Decisión 2010/96/PESC relativa a una misión militar de la Unión Europea destinada a contribuir a la formación de las fuerzas de seguridad somalíes, la Decisión 2013/34/PESC relativa a una misión militar de la Unión Europea destinada a contribuir a la formación de las fuerzas armadas de Mali (EUTM Mali) y la Decisión (PESC) 2016/610 relativa a una Misión de Asesoramiento Militar PCSD de la Unión Europea en la República Centroafricana (EUTM RCA); en especial, ver artículo 5.

[50] Misión de Formación Militar PCSD de la Unión Europea en la República Centroafricana (EUTM RCA) establecida por Decisión (PESC) 2015/78 del Consejo, de 19 de enero de 2015, relativa a una Misión de Asesoramiento Militar PCSD de la Unión Europea en la República Centroafricana (EUMAM RCA) (DO L 13 de 20/1/2015, p. 8). Fue objeto de modificación y prórroga por Decisión (PESC) 2016/610 del Consejo, de 19 de abril de 2016, relativa a una Misión de Formación Militar PCSD de la Unión Europea en la República Centroafricana (EUTM RCA) (DO L 104 de 20/4/2016, p. 21), en cuyo artículo 13 se establece que «la EUTM RCA terminará a más tardar 24 meses después de que se haya alcanzado la plena capacidad operativa». La última modificación se produjo a través de la Decisión (UE) 2017/971 del Consejo, de 8 de junio de 2017, por la que se determinan las disposiciones de planificación y ejecución de misiones militares no ejecutivas PCSD de la UE y por la que se modifican la Decisión 2010/96/PESC relativa a una misión militar de la Unión Europea destinada a contribuir a la formación de las fuerzas de seguridad somalíes, la Decisión 2013/34/PESC relativa a una misión militar de la Unión Europea destinada a contribuir a la formación de las fuerzas armadas de Mali (EUTM Mali) y la Decisión (PESC) 2016/610 relativa a una Misión de Asesoramiento Militar PCSD de la Unión Europea en la República Centroafricana (EUTM RCA); en especial, ver artículo 6.

[51] La operación EUTM-Somalia ha dispuesto de tres mandatos del Consejo de la Unión Europea. El primero (del 23 de abril de 2010 al 15 de agosto de 2011) se centró en la formación de oficiales y suboficiales y el adiestramiento hasta nivel sección. El segundo mandato (del 15 de octubre de 2011 a enero de 2013) se orientó a la formación de formadores, la instrucción especializada y el adiestramiento de hasta nivel compañía. El tercer mandato (de marzo de 2013 al 31 de marzo de 2015) tiene como objetivos continuar con la instrucción y reforzar las áreas de la mentorización y el asesoramiento. Se han producido sucesivas ampliaciones hasta el actual sexto Mandato. Esta Operación está amparada en la Resolución 1872 (2009) del Consejo de Seguridad de las Naciones Unidas, aprobada en su 6127.ª sesión, celebrada el 26 de mayo de 2009. Doc: S/RES/1872(2009).

[52] El Consejo de Seguridad de las Naciones Unidas adoptó una serie de resoluciones dirigidas a poner fin al incremento de los actos de piratería en el Índico. En apoyo de las Naciones Unidas, el Consejo de la UE aprobó la creación de una fuerza aeronaval, el 10 de noviembre de 2008, constituyendo la primera operación marítima en el marco de la PCSD.

cumplimiento de su mandato en la lucha contra la piratería. Por lo tanto, podemos observar cómo, en la práctica, la UE no ha participado directamente en operaciones de imposición de la paz, aunque sus Estados miembros hayan participado, bien a través de una coalición de Estados o mediante su participación en la OTAN, tanto en el ejercicio de la legítima defensa colectiva, por activación del artículo 5 del Tratado atlántico, de conformidad con el artículo 51 de la Carta de las Naciones Unidas (en adelante, la Carta) como en respuesta a la correspondiente Resolución del Consejo de Seguridad, en virtud del capítulo VII del referido tratado constitutivo de la Organización de las Naciones Unidas. Sin embargo, de conformidad con el capítulo V del TUE, nada impediría que, en un futuro, la UE pudiera participar o incluso liderar una ciberoperación en el ejercicio de la defensa colectiva, de conformidad con el referido artículo 51 de la Carta. Situación nada impensable, pues, como se recoge en la norma 78 del *Manual de Tallin 2.0*, el desarrollo de operaciones cibernéticas ha de ser atendido también en el contexto de las operaciones de paz, incluyendo tanto las operaciones de mantenimiento como las de imposición de la paz. En concreto, en relación con estas últimas, se establece que «such operations may, when consistent whit the mandate or authorisation or as necessary in self-defence, engage in cyber operations at the use of force level»[53].

En ambos tipos de misiones desplegadas fuera de la UE, deberían desplegarse los esfuerzos en el refuerzo de los elementos cibernéticos. Para poder conseguir una resiliencia adecuada en el ámbito de las capacidades, como se ha indicado, hay que partir de una evaluación de las capacidades con las que se cuenta y vincularlas frente al riesgo, desafío y amenaza al que se ha de ser ciberresiliente. En este contexto, habida cuenta de que no existe una experiencia previa propia de UE en misiones de imposición de paz, tomaremos como referencia la vulnerabilidad existente frente a los posibles ciberataques que puedan sufrir las infraestructuras empleadas en las actuales misiones de la PCSD desplegadas en el exterior, en especial, a los ataques dirigidos contra los SIC.

En relación con los SIC, estos han de formar parte del planeamiento específico de la misión u operación de la PCSD. En consecuencia, como indica Arroyo De la Rosa, en la planificación de los SIC se deben tener en consideración «todos los factores, entre otros, la misión, la composición de la fuerza y su

El Consejo de la Unión puso en marcha la Operación ATALANTA, 8 de diciembre de ese mismo año, a iniciativa de España y Francia. El 25 de febrero de 2010 se ampliarían sus funciones, incluyendo el control de puertos y bases de los piratas. El 30 de julio de 2018, el Consejo amplió el mandato de la Operación Atalanta de la UE NAVFOR Somalia hasta el 31 de diciembre de 2020. El Consejo también decidió reubicar la sede operativa de la Fuerza Naval de la Unión Europea (EU NAVFOR) de Northwood (RU) a Rota (España) el 29 de marzo de 2019.

53 SCHMITT, M. N. (ed.). *Manual de Tallin 2.0... Op. cit.,* p. 362.

despliegue sobre el terreno, las fases de la operación y, por su puesto la cadena del mando»[54].

Sea cual fuera el tipo de operación y misión de la PCSD a desplegar, los elementos cibernéticos han de ser tenidos en consideración, resultando necesario atender a la resiliencia para poder hacer frente a los posibles ciberataques que pudieran sufrir los contingentes civiles y militares, pues debemos tener presentes los aspectos civiles y militares de las misiones que no son de imposición de la paz. Además, tampoco se debe olvidar la posibilidad de que pueda ser desplegada una misión mixta, como fue la Misión de Apoyo Civil y Militar de la Unión Europea a la misión de la Unión Africana en la región sudanesa de Darfur[55]. Estas capacidades, como se ha indicado, están íntimamente relacionadas con el nivel de resiliencia que sea necesario para la consecución de los diferentes objetivos estratégicos.

El alto representante de la Unión para Asuntos Exteriores y Política de Seguridad, bajo la autoridad del Consejo y en contacto estrecho y permanente con el Comité Político y de Seguridad, se hará cargo de la coordinación de los aspectos civiles y militares de dichas misiones. También resulta interesante atender al avance establecido dentro del SEAE, en relación con las misiones de carácter civil, la Planificación Civil y Capacidad de Conducta (CPCC); así como el establecimiento, por parte del Consejo de la Panificación, Conducta y Capacidad Militar (MPCC), en relación con las misiones militares no ejecutivas, ubicada dentro del Estado Mayor de la UE.

Por su parte, en el artículo 42.3 TUE se estipula que los Estados miembros pondrán a disposición de la Unión, a efectos de la aplicación de la política común de seguridad y defensa, capacidades civiles y militares para contribuir a los objetivos definidos por el Consejo. Los Estados miembros que constituyan entre ellos fuerzas multinacionales podrán asimismo ponerlas a disposición de la política común de seguridad y defensa. Los Estados miembros se comprometen a mejorar progresivamente sus capacidades militares. Esa mejora no puede entenderse más que en clave de resiliencia. A este respecto debemos recordar que entre las capacidades que ponen a disposición los Estados miembros para el despliegue de una misión u operación internacional se encuentran sus propios SIC y que no todos los Estados tenemos las mismas capacidades en el ámbito de la resiliencia cibernética. Quizás, uno de los grandes esfuerzos que desde la UE debería dirigir para reforzar la resiliencia cibernética de las misiones u operaciones de la Unión debería

[54] ARROYO DE LA ROSA, R. «El C2 & CIS en las misiones militares enmarcadas en la PSCD de la Unión Europea (EUTM-Somalia)». En bie3, *Boletín I. E .E. E.,* n.º 3. Julio-septiembre, 2016, p. 621, pp. 613-636. [Última consulta: 11 de abril de 2019]. Disponible en http://www.ume.mde.es/Galerias/Descargas/PRENSA/DIEEEO90-2016_C2-CIS_MisionesMilitares_PSCD_UE.pdf.

[55] Establecida por la *Acción Común 2005/557/PESC* del Consejo, de 18 de julio de 2005, relativa a la acción de apoyo civil y militar de la Unión Europea a la misión de la Unión Africana en la región sudanesa de Darfur (DO L 188 de 20/07/2005; p. 46).

ser el dotar con SIC análogos y seguros a los Estados contribuyentes, pues puede que la brecha de ciberseguridad se encuentre en este importante factor. Si todos los Estados que están contribuyendo con sus contingentes militares no tienen un nivel equiparable de medios y/o equiparables sistemas de resiliencia cibernética, es posible que se esté poniendo en peligro a los miembros de las FAS desplegados o, incluso, el cumplimiento del mandato de la misión.

El proceso de transformación de capacidades, como se ha indicado, constituye el segundo parámetro por el que ha de ser atendida la resiliencia cibernética. Al igual que el parámetro de las capacidades, también se encuentra directamente vinculado al parámetro resultado u objetivo estratégico perseguido por la UE en el desarrollo operaciones cibernéticas en misiones y operaciones de la PCSD. Este segundo parámetro, además, resulta vital para conseguir los objetivos estratégicos referidos a la resiliencia cibernética objeto de atención. Así lo manifestaría la alta representante de la Unión para Asuntos Exteriores y Política de Seguridad: «El futuro de nuestra seguridad dependerá de la transformación de nuestra capacidad para proteger a la UE contra las amenazas cibernéticas: tanto la infraestructura civil como la capacidad militar se basan en el uso de sistemas digitales seguros»[56].

En relación con la transformación de las capacidades, se ha de atender tanto a los medios como a los modos de resiliencia. En relación con los medios para la consecución de la transformación de las capacidades en el desarrollo de operaciones cibernéticas defensivas en misiones y operaciones de la PCSD de la UE destaca la necesidad de dotarse de estructuras adecuadas. Si la adopción de una Estrategia de Ciberseguridad resultaba fundamental para poder ofrecer una respuesta eficaz ante las ciberamenazas, no debemos olvidar que, para su puesta en marcha, la UE ya se había dotado de un marco normativo apropiado para la construcción de una sólida PCSD, a través de las disposiciones contenidas en la sección dos del título V del Tratado de Lisboa. En relación con este marco normativo, asumirán un protagonismo especial, en la materia que nos ocupa, la Agencia Europea de Defensa en el ámbito de desarrollo de las capacidades de defensa, la investigación, la adquisición y el armamento (en adelante, AED), regulada en los artículos 42.3 y 45 TUE y de la Cooperación Estructurada Permanente (en adelante, PESCO, en sus siglas en inglés) recogida en el artículo 46 TUE. La relevancia de la AED en relación con las capacidades necesarias para lograr una eficaz resiliencia cibernética es innegable, pues determinará las necesidades operativas, fomentará medidas para satisfacerlas, contribuirá a definir y, en su caso, a aplicar cualquier medida oportuna para reforzar la base industrial y tecnológica del sector de la defensa, participará en la definición de una

[56] Alta representante de la Unión para Asuntos Exteriores y Política de Seguridad. *Comunicación conjunta al Parlamento Europeo y al Consejo: resiliencia, disuasión y defensa…*, doc. cit., p. 2.

política europea de capacidades y de armamento y asistirá al Consejo en la evaluación de la mejora de las capacidades militares (artículo 42.3 TUE). Especialmente relevante si se tiene en cuenta la ambiciosa misión que está llamada a cumplir, de conformidad con lo establecido en el artículo 45.1 TUE[57].

Resulta consecuentemente comprensible el protagonismo que se le confiere en la Estrategia Global de la UE, al resaltar que la AED «desempeña un papel clave del Plan de Desarrollo de Capacidades al funcionar como interfaz entre los Estados miembros y la Comisión y asistir a los Estados miembros en el desarrollo de capacidades procedentes de los objetivos políticos expuestos en esta Estrategia», añadiendo que «las evaluaciones regulares de los niveles de referencia de la AED pueden crear una presión positiva entre iguales entre los Estados miembros»[58]. Si trasladamos esta última propuesta al ámbito ciberespacial, esas evaluaciones de los niveles de referencia podrían no solo suponer una presión positiva entre iguales, sino unos indicadores tendentes a una homogenización en materia de ciberseguridad, que permita mantener el más alto nivel de ciberseguridad cibernética para todos los Estados miembros y no solo una mera presión positiva entre iguales. Indudable el valor que supondría en orden a concretar el contenido de una eficaz y lícita resiliencia cibernética.

Por su parte, la PESCO representa un nuevo impulso para el fortalecimiento de la resiliencia frente a las ciberamenazas. Si, como afirma Villalba Fernández, «la CEP es un mecanismo que permite participar en el desarrollo de las capacidades de la Europa de la defensa, facilitando el impulso de procesos que de otra forma serían muy complicados para generar consensos»[59], nada impide que la PESCO también pueda ser atendida como un instrumento clave en la adopción de medidas que doten de sentido a la resiliencia frente a las ciberamenazas para que sea no solo eficaz, sino lícita.

Ese proceso de transformación de capacidades nos ha llevado a reflexionar sobre cómo se ha de producir esa transformación. En este sentido, este se-

[57] En concreto, se establece: «a) contribuir a definir los objetivos de capacidades militares de los Estados miembros y a evaluar el respeto de los compromisos de capacidades contraídos por los Estados miembros; b) fomentar la armonización de las necesidades operativas y la adopción de métodos de adquisición eficaces y compatibles; c) proponer proyectos multilaterales para cumplir los objetivos de capacidades militares y coordinar los programas ejecutados por los Estados miembros y la gestión de programas de cooperación específicos; d) apoyar la investigación sobre tecnología de defensa y coordinar y planificar actividades de investigación conjuntas y estudios de soluciones técnicas que respondan a las futuras necesidades operativas; e) contribuir a definir y, en su caso, aplicar cualquier medida oportuna para reforzar la base industrial y tecnológica del sector de la defensa y para mejorar la eficacia de los gastos militares».

[58] *Estrategia Global*..., doc. cit., p. 36.

[59] VILLALBA FERNÁNDEZ, A. «Capítulo V: EL Tratado de Lisboa y la Política Común de Seguridad y Defensa». En AA. VV. *Panorama Estratégico 2009-2010*. Madrid: Ministerio de Defensa, 2010, p.169.

gundo parámetro podrá ser la clave para que la UE asuma un liderazgo en ciberseguridad y ciberdefensa. Por ello, hemos tenido a bien hablar de modos de resiliencia, pues, al igual que no existe un único nivel de resiliencia como resultado u objetivo estratégico a conseguir, tampoco existe un único modo de realizar la transformación de capacidades. Como se ha indicado, ese modo de resiliencia es consecuencia de asumir, como un valor identitario de todos los Estados miembros de la UE, el respeto de los derechos humanos.

En este sentido, resulta conveniente recordar que el hecho de que las FAS de un Estado miembro sea desplegado en misión u operación internacional a un territorio situado fuera de la Unión no implica que automáticamente sea de aplicación el conjunto normativo del derecho internacional humanitario (en adelante, DIH), dejando en suspenso la normativa internacional relativa a la protección de los derechos fundamentales (salvo el núcleo irreductible que emana del principio de humanidad y dignidad humana). En efecto, los límites jurídicos para el planeamiento estratégico, conducción y seguimiento de operaciones multiámbito no dependen de que se desarrollen fuera del territorio nacional, sino de si dichas operaciones se realizan en un contexto o no de conflicto armado. Si la participación en una misión u operación, como podría ser de asesoramiento y/o adiestramiento de los miembros de las FAS del estado anfitrión, en cuyo territorio no se está desarrollando una contienda, en principio sería de aplicación la normativa del derecho internacional aplicable en tiempo de paz. Cuestión distinta es si el Estado territorial es parte de una beligerancia. Por lo tanto, salvo que sea de aplicación el conjunto normativo de DIH, será de aplicación la normativa internacional aplicable al tiempo de paz. En consecuencia, cuando nos encontramos ante situaciones propias de la zona gris, durante el desarrollo de una misión u operación internacional, siempre que no se rebase el límite de violencia que nos situaría ante una situación claramente de beligerancia, aunque ese umbral de violencia sea muy elevado, no sería de aplicación la normativa de DIH.

Por otra parte, no debemos olvidar la distinción entre las misiones u operaciones de imposición de la paz y el resto de posibles misiones u operaciones internacionales en las que puedan ser desplegadas las FAS. Si pensamos en la primera categoría, debemos tener presente que en ellas se han de desarrollar no solo actividades tácticas ofensivas, sino también defensivas, incluidas las dirigidas a la defensa de los SIC, a través de una gran variedad de operaciones multiámbito. En ese contexto de misión de imposición de la paz, será de obligado cumplimiento la normativa internacional de DIH en el desarrollo de todas las operaciones multiámbito frente a las ciberamenazas.

La transformación de las capacidades encuentra también en el adiestramiento del contingente militar desplegado (formación en el caso del personal civil). Esta formación/adiestramiento, previo al despliegue, dirigido al buen cumplimiento del mandato requiere que se forme a los miembros de las FAS en la normativa del derecho internacional de los derechos humanos, en la normativa del DIH y en un uso responsable de los SIC y de los SIR (in-

cluyendo todos aquellos dispositivos particulares que puedan llevarse hasta la zona de operaciones). No debe olvidarse que una falta de adiestramiento al respecto o, incluso, un adiestramiento no adecuado podría constituir un incumplimiento de la obligación primaria de diligencia debida de la que emanan todo un elenco de obligaciones secundarias de prevención. En consecuencia, podría exigirse la responsabilidad del mando[60].

Esta capacitación a través del adiestramiento/formación en el que los formados se pueden convertir en formadores en el territorio de terceros Estados resulta vital, por ejemplo, tanto para el cumplimiento del mandato en aquellas misiones u operaciones de asesoramiento. Pensemos, por ejemplo, en la ya mencionada Operación EUTM-Somalia, cuyo mandato se centra en el fortalecimiento de las instituciones de la defensa a través de tres pilares: capacitación, orientación y asesoramiento. La responsabilidad sobre cómo es ofrecida esa capacitación reviste una importancia transcendental si, además, tenemos en cuenta que los que reciben ese adiestramiento, por parte de los miembros de las FAS desplegados, se convertirán, a su vez, en futuros capacitadores, pues a través de la Operación EUTM-Somalia se ha desarrollado un amplio programa de «capacitación de futuros capacitadores».

Tampoco podemos olvidar el adiestramiento/formación ofrecido, por ejemplo, dentro de las multifacéticas actividades CIMIC, durante el despliegue de una misión de mantenimiento de la paz. Resulta innegable, consecuentemente, que, entre las acciones de prevención, el adiestramiento se convierte en un instrumento clave para la transformación de capacidades, sin perjuicio de su transcendental valor como uno de los más eficientes instrumentos para el establecimiento de una cultura de ciberseguridad en relación con los miembros de los contingentes militares desplegados en misiones u operaciones internacionales, entre los miembros de las FAS y de los cuerpos de seguridad del Estado anfitrión y entre la población receptora de la misma. Esta reflexión nos conduce a dirigir nuestras últimas reflexiones hacia los terceros Estados.

Resiliencia cibernética de terceros Estados con especial referencia al desarrollo de misiones y operaciones de la PCSD de la UE

Podemos afirmar que resulta indispensable que los terceros Estados vecinos de la UE sean resilientes para que consigamos una Europa segura y ciberresiliente. En este sentido y salvando las distancias, ya se pronunciaba

[60] DE TOMÁS MORALES, S. y VELÁZQUEZ ORTIZ, A. P. «La responsabilidad del mando en la conducción de operaciones durante la ciberguerra: la necesidad de un adiestramiento eficaz». Premio Defensa 2013, modalidad Premio José Francisco Querol y Lombardero. En *Revista Española de Derecho Militar*, n.º 100. 2013, Madrid: Ministerio de Defensa, 2014, pp. 117-150.

Irénée Castel, abad de Saint-Pierre, en su obra *El proyecto de paz perpetua*[61], publicado entre 1713 y 1717.

De esta forma, podemos destacar, a modo de ejemplo, cómo es atendida la resiliencia en relación con los vecinos orientales y meridionales de la UE, siguiendo su *Estrategia Global de 2016*. En cuanto a estas relaciones de vecindad juega un papel central la resiliencia, al incluirse entre las cinco prioridades de la acción exterior de la UE: «la resilencia estatal y social de nuestros vecinos orientales y meridionales». En el propio enunciado de la referida prioridad parece evidente que el término resiliencia, en primer lugar, viene referido a un resultado, a la consecución de un fin u objetivo estratégico a alcanzar. En este mismo sentido, nos encontraríamos con la afirmación de que «la resilencia es también una prioridad...», de lo que se puede deducir que la consecución de Estados y sociedades resilientes dentro y fuera del ámbito de la política europea de vecindad no solo constituye un objetivo estratégico, sino que, además, es prioritario.

En segundo lugar, podemos atender a la resiliencia en el sentido de capacidades, destacando expresiones como la necesidad de «invertir en la resiliencia» o «aumentar la resiliencia». En relación con la primera de estas expresiones en las que es utilizado el término resiliencia como capacidad se hace referencia a la necesidad de invertir, lo que debería ser objeto de atención desde un enfoque amplio, pues invertir en resiliencia implica un firme compromiso político y financiero que permita el desarrollo de capacidades, lo que a su vez implica adiestramiento en capacidades y, sin el más mínimo lugar a dudas, también implica invertir en planes operacionales eficientes y eficaces.

Por otra parte, los objetivos estratégicos dirigidos a la consecución de Estados y sociedades resilientes no se quedan en la mera creación de capacidades, sino en la necesidad de aumentar la resiliencia, como se apuntaba en la segunda expresión destacada con anterioridad. Esta última expresión nos conduce a realizar, al menos brevemente, una reflexión sobre la posible existencia de distintos niveles de resiliencia, que serán determinados en relación con los riesgos y amenazas frente a los que haya que dotarse de capacidades y también en relación con el tipo de capacidades con las que se desee dotar a los Estados y a las sociedades. A primera vista, si pensamos en el ámbito de la ciberseguridad y la ciberdefensa, es evidente que nos encontraríamos ante dos niveles de capacitación-resiliencia bastante diferenciados en relación con las medidas de protección al alcance de las sociedades resilientes y de las que deberían dotarse los Estados en el ámbito de PCSD. Sin embargo, los distintos niveles de resiliencia deben estar interconectados, pues es impensable conseguir el objetivo «resiliencia estatal»

[61] Esta obra del abad de Saint-Pierre constituye un valioso precedente del proyecto de construcción europea. Cfr. BELLO, E. «La construcción de la paz: el proyecto del abbé de Saint-Pierre». En *Res publica*. N.º 24, 2010, pp. 121-135.

si no se consigue el objetivo «sociedad resiliente». Los distintos niveles de protección frente a las amenazas cibernéticas serán objeto de atención, con mayor profundidad, en relación con el desarrollo de operaciones cibernéticas en los variados tipos de misiones y operaciones de la PCSD.

Finalmente, en tercer lugar, nos encontramos ante una referencia a la resiliencia que puede ser atendida como un proceso de transformación. Inevitablemente, nos encontramos con una estrecha vinculación con las capacidades y el resultado u objetivo a alcanzar. Siguiendo con el ejemplo de la resiliencia en el contexto de las relaciones de vecindad, nos encontramos con la siguiente frase: «la UE apoyará distintos modos de resilencia». En consecuencia, la creación de capacidades ante los distintos riesgos y amenazas puede ser jerarquizada en niveles, según los objetivos a alcanzar, como hemos indicado, pero, además, nos permite reflexionar sobre el proceso de transformación o adaptación de capacidades para conseguir dichos objetivos; es decir, existen niveles y modos de resiliencia.

Puede que llame la atención el hecho de que se haya utilizado la segunda prioridad de la acción exterior de la UE para ejemplificar los tres grandes ámbitos en los que se puede dar sentido al término resiliencia, cuando en Estrategia Global de la UE no se hace referencia al riesgo cibernético al atender a la resiliencia de Estados y sociedades vecinas orientales y meridionales. Sin embargo, nos ha servido para tener, como primer botón de muestra, un primer ejemplo de cómo la resiliencia, por una parte, constituye un eje central de la Estrategia Global y, por otra, nos ha servido para atender a esos tres grandes parámetros con los que ha de ser abordada: el parámetro de las capacidades, atendiendo a cuáles son las capacidades de partida frente a los distintos riesgos y amenazas ante los que somos vulnerables; el parámetro de los procesos de transformación, vinculado íntimamente con la flexibilidad de adaptar las capacidades a los riesgos y amenazas y sus evoluciones, para lo que nos encontramos con diferentes modos de resiliencia, así como con el objetivo a perseguir. Estos dos parámetros deberán ser atendidos, a su vez, con la mirada puesta en el tercer parámetro: la resiliencia como resultado; es decir, reflexionar sobre posibles niveles de resiliencia como objetivo estratégico.

La resiliencia de los terceros Estados resulta crucial, pues no debemos olvidar que las misiones u operaciones internacionales de la UE se despliegan en el territorio de un tercer Estado. Además, también ha de ser objeto de consideración la resiliencia de terceros Estados que participan en el desarrollo de una misión u operación de la Unión. En efecto, como parte de las Alianzas en el ámbito de la PCSD, un tercer Estado puede participar activamente en una misión u operación de la UE. Este tipo de asociaciones y la cooperación con Estados que comparten los valores de la UE puede contribuir a la efectividad y el impacto de las operaciones y misiones PCSD. También se mejorará la cooperación con las Naciones Unidas, la OTAN, la UA y la

OSCE. Basado en propuestas del HRVP, el Consejo ha acordado desarrollar un enfoque más estratégico a la cooperación en materia de PCSD con los socios, incluido ayudarlos a convertirse más resistente y construir sus capacidades»[62]. El hecho de que exista la posibilidad de que terceros Estados participen a través de esta modalidad, siempre que cumplan con el requisito de compartir los valores de la UE resulta vital, pues los límites jurídicos antes señalados en relación con lo que hemos venido a denominar un modo de resiliencia europeo, deberían también ser cumplidos por estos terceros Estados, en el desarrollo de operaciones multiámbito. Por lo tanto, al igual que manifestábamos el deseo de que la UE, a través de su PCSD, reforzase la ciberseguridad en relación con los SIC aportados por los Estados miembros, buscando el mayor grado de homogeneización en clave de resiliencia cibérnética, también sería deseable que, además de compartir los valores de la UE, los terceros Estados compartiesen, al menos, un aceptable grado de ciberseguridad de los SIC que aportasen en una misma zona de operaciones.

Para finalizar, no podemos dejar de ofrecer un pequeño esbozo de la especial consideración de resiliencia de terceros Estados en la lucha contra el ciberterrorismo[63]. Como se indica en la ESN de 2017: «En lo relativo a las ciberamenazas, es creciente la actividad tanto por parte de Estados, que persiguen la expansión de sus intereses geopolíticos a través de acciones de carácter ofensivo y subversivo, como de organizaciones terroristas, grupos de crimen organizado y actores individuales. Estos grupos aprovechan el carácter anónimo que el ciberespacio ofrece para conseguir sus fines a un mínimo coste y asumiendo un riesgo menor dada la dificultad de atribución»[64].

En el artículo 43 TUE, *in fine*, se resalta su compromiso en la lucha contra el terrorismo, al afirmar que «todas estas misiones podrán contribuir a la lucha contra el terrorismo, entre otras cosas, mediante el apoyo prestado a terceros países para combatirlo en su territorio», lo que también tendría que ser objeto de futuros análisis si el apoyo prestado a través de misiones y operaciones de la PCSD se materializa en atender la resiliencia cibernética de los terceros Estados frente al ciberterrorismo. En consecuencia, los límites jurídicos de todas las actividades tácticas, tanto defensivas como ofensivas, en apoyo a terceros Estados en la lucha contra el terrorismo son los mismos que limitan las operaciones multiámbito de referencia de los Estados miembros.

---

62 Implementation Plan on Security and Defence. Disponible en https://eeas.europa.eu/sites/eeas/files/implementation_plan_on_security_and_defence_18-102017.pdf.

63 *Estrategia de Seguridad Nacional*, doc. cit., p. 65.

64 *Estrategia de Seguridad Nacional*, doc. cit., p. 65. En relación con los problemas de atribución de los ciberataques que entran dentro del ámbito de la defensa, que serán objeto de especial atención por Jacobo de Salas en el capítulo 4 de la presente obra, resulta de interés la siguiente obra:

Conclusiones

En primer lugar, podemos afirmar que los límites jurídicos preexistentes aplicables a las operaciones militares en los tradicionales espacios físicos también son de aplicación al nuevo ámbito ciberespacial en el que se pueden desarrollar todo un abanico de actividades tácticas defensivas. En efecto, aunque resulte compleja la tarea de extrapolar al ámbito virtual, por las propias características del ciberespacio, coincidentes en gran medida con las características de la denominada zona gris, nada impide que se pueda y deba realizar una interpretación normativa y jurisprudencial por analogía. Si, por el contrario, la respuesta simplista de internar buscar improvisadas nuevas normas amparándose en un relativo grado de vacío legal o de acomodar la válida aplicación preexistente para los espacios físicos, motivadas por intereses políticos y estratégicos, se corre el riesgo de realizar interpretaciones excesivamente laxas y oportunistas, con la posibilidad añadida de ser ilícitas de conformidad con el ordenamiento jurídico internacional.

En segundo lugar, concluimos que las operaciones multiámbito son más eficientes y eficaces desde la perspectiva de la resiliencia cibernética, siempre que esta sea atendida desde tres parámetros: la resiliencia como capacidad; la resiliencia como proceso de transformación de capacidades y, finalmente, la resiliencia como fin u objetivo estratégico a alcanzar. Si en la práctica ya se ha demostrado que la aplicación de la resiliencia a las operaciones multiámbito que nos ocupan aumenta su eficacia, los logros obtenidos a través del refuerzo de estas operaciones militares, si son atendidas desde esos tres parámetros de referencia, incrementaría exponencialmente el grado o nivel de eficiencia y eficacia. La utilización de estos tres parámetros a la hora de realizar la planificación estratégica, conducción y seguimiento de las operaciones multiámbito frente a las ciberamenazas resulta vital dado que no existe un concepto unívoco y generalmente aceptado del término resiliencia.

En tercer lugar y último lugar, llegamos a la conclusión de que el parámetro de la resiliencia como proceso de transformación de capacidades, atendiendo a lo que hemos venido a denominar los modos de resiliencia, será la pieza clave para el establecimiento y/o esclarecimiento de los límites jurídicos de las operaciones multiámbito. A lo largo del presente capítulo hemos podido descubrir un modo de resiliencia que forma parte de la propia identidad europea, compartida por España como miembro de la UE. Estos límites son la consecuencia del respeto de la normativa internacional de protección de los derechos humanos y del régimen específico objeto de regulación por DIH, al margen evidente cumplimiento de la Carta de las Naciones Unidas y del respeto de la normativa jurídica internacional. En consecuencia, los límites jurídicos de la resiliencia frente a las ciberamenazas son de aplicación a la planificación, conducción y seguimiento de las operaciones multiámbito.

Capítulo cuarto

De la flecha al ratón. Consideraciones jurídicas de las operaciones ofensivas en el ciberespacio

Jacobo de Salas Claver

Resumen

Se ha creado oficialmente un nuevo ámbito de operación, el ciberespacial, transversal al resto de ámbitos tradicionales, y en el que ya se han producido acciones ofensivas reales. En este trabajo se pretenden exponer, de forma práctica y para los no juristas, algunas de las principales consideraciones jurídicas a tener en cuenta en el planeamiento y ejecución de acciones ofensivas en el ciberespacio en el marco de los conflictos armados.

Palabras clave

Ciberguerra, ciberataque, ciberdefensa, ciberderecho, derecho internacional humanitario, derecho de los conflictos armados, Tallin 2.0, Internet.

Abstract

A cyberdomain has been oficially established. It cross sections the other domains, and for real cyberattacks have already been executed within it. The aim of this work is to show, in practical terms and to non-laywers, some of the main legal issues to be taken into account for the planning and execution of cyberattacks within an armed conflict.

Keywords

Cyberwar, cyberattack, cyberdefense, cyberlaw, international humanitarian law, law of armed conflict, Tallin 2.0, internet.

Introducción

La causa: la sociedad del siglo XXI y la lex artis

Las actividades profesionales de una sociedad contemporánea no se pueden entender sin dos circunstancias de naturaleza mixta, fáctica y normativa, como son los protocolos o procedimientos de actuación profesional y la buena práctica profesional o *lex artis* respectivamente. En efecto, a estas alturas del siglo xxi, en toda actividad profesional humana se exige a quien la desarrolle que su actuación no se limite a cumplir con las normas positivas en vigor, sino que además dicha actividad profesional sea conforme a la *lex artis*, que siendo un concepto jurídico indeterminado, puede considerarse como el conjunto de prácticas profesionales generalmente aceptadas como adecuadas por la comunidad profesional para el desarrollo de la actividad profesional orientada a la consecución de un determinado propósito. Y, a su vez, una concreta actuación profesional estará amparada bajo la *lex artis* cuando el operador actúe conforme a los procedimientos y protocolos generalmente admitidos por la comunidad profesional como adecuados para la obtención del fin perseguido.

Podría pensarse que dichas circunstancias son exclusivamente propias de actividades civiles y, singular o tradicionalmente, de la medicina. Sin embargo, no podemos olvidar que el artículo 62 de las Reales Ordenanzas[1] dispone, con respecto a la toma de decisiones por el mando, que «en el ejercicio de su actividad será prudente en la toma de decisiones, fruto del análisis de la situación y la valoración de la información disponible, y las expresará en órdenes concretas, cuya ejecución debe dirigir, coordinar y controlar, sin que la insuficiencia de información, ni ninguna otra razón, pueda disculparle de permanecer inactivo en situaciones que requieran su intervención». Y en consecuencia, la reciente publicación *Doctrina para el empleo de las Fuerzas Armadas*[2] puede ser considerada como un ejemplo de esta situación contemporánea de establecimiento de *lex artis* para el uso de la fuerza militar. En efecto, en el prólogo de esta publicación el JEMAD afirma que esta doctrina «describe la forma de empleo de las Fuerzas Armadas y establece las normas fundamentales con las que estas operan» y, singularmente, que «... la doctrina establece y detalla los principios morales, legales y doctrinales, determina cómo ejecuta la acción conjunta, la combinada con nuestros aliados, y la integrada con los demás instrumentos de poder; describe el entorno y el espacio de las operaciones, añadiendo a los ámbitos físicos tradicionales, el ciberespacial y el formado por la información y las percepciones; indica

[1] Real Decreto 96/2009, de 6 de febrero, por el que se aprueban las Reales Ordenanzas para las Fuerzas Armadas.

[2] ESTADO MAYOR DE LA DEFENSA. Publicación Doctrinal Conjunta PDC-01(A). *Doctrina para el empleo de las Fuerzas Armadas*. Madrid: Ministerio de Defensa, 2018, p. 5.

cómo sincronizar el planeamiento concurrente y la ejecución dinámica de operaciones en los niveles estratégico, operacional y táctico; y, por último, ayuda a reflexionar sobre el ejercicio del mando en operaciones».

El ámbito ciberespacial es nuevo y esencialmente propio del siglo xxi. Por este motivo, puede razonablemente pensarse que haya una cierta carencia de principios o procedimientos generalmente admisibles en el ámbito de las acciones ofensivas en el ciberespacio (AOC) derivada precisamente de la juventud de este ámbito de operación y de la correlativa lógica ausencia de tratados internacionales o de jurisprudencia relevante que guíe a los operadores, al mando, y a sus asesores legales. Y así llegamos a lo que es el propósito de este capítulo, que es intentar facilitar al lector una primera aproximación a las consideraciones jurídicas propias de las AOC.

Nótese, en todo caso, que este trabajo ni pretende abarcar todas las perspectivas posibles sobre la materia, pues expresamente se deja fuera del mismo a las consideraciones jurídicas propias del *ius ad bellum*, ni tampoco aspira a constituirse en la fuente interpretativa de la aplicación del *ius in bello* en el ámbito del ciberespacio, ni mucho menos pretende agotar sus múltiples perspectivas. Lo reciente del ámbito de operación, las distintas aproximaciones a los problemas de este por las diferentes tradiciones jurídicas o intereses nacionales de los distintos operadores y, en fin, la aplicación del principio de prudencia ante la incertidumbre, impiden poder facilitar respuestas simples a problemas complejos. No obstante estas limitaciones, este trabajo pretende facilitar una visión clara y coherente de las reglas de este nuevo *juego*, para que la valoración jurídica de las AOC sea razonablemente objetiva, coherente y defendible legalmente. Por último, este trabajo pretende facilitar al lector las referencias literales de algunas de estas reglas, pues difícilmente se puede juzgar, o aplicar en la actividad diaria, lo que se desconoce.

Las acciones ofensivas en el ciberespacio ya están aquí, y son relevantes

Del mismo modo que tras el ataque aéreo británico a la flota italiana fondeada en Tarento en la noche del 11 de noviembre de 1940 ya no se podía decir que el ataque japonés el 7 de diciembre de 1941 a Pearl Harbor fuera una sorpresa conceptual[3], en la actualidad las AOC ya no pueden considerarse como meras hipótesis de futuro. Según un informe del Cato Institute, entre los años 2000 y 2016 se han documentado 272 ciberoperaciones entre Estados rivales[4].

[3] O un «cisne negro», en los términos de Nassim Nicholas Taleb en su conocido libro homónimo (TALEB. Niassim Nicholas, «*The Black Swan*». New York: Random House, 2007).

[4] VALERIANO, Brandon, y JENSEN, Benjamin. «The Myth of the Cyber Offense». *Policy Analysis*. Number 862. Cato Institute, 2019, p. 4.

Las AOC son, por su objeto, relevantes y deben ser causa de severa preocupación. Las sociedades del siglo XXI dependen de los sistemas y tecnologías de la información para la gestión de sus instalaciones críticas, tales como centrales de energía (incluyendo plantas nucleares y presas), sistemas de tratamiento y distribución de agua potable, refinerías de petróleo y gas, sistema bancario y financiero, hospitales, centros de salud e instalaciones de almacenaje y distribución de medicamentos y sistemas ferroviario y aeronáutico. Estos sistemas y tecnologías de la información constituyen el enlace entre el mundo físico y el digital, y son altamente vulnerables a ataques maliciosos[5]. Solo tenemos que pensar qué ocurriría en una sociedad occidental de corte urbano si el sistema bancario de un país estuviera fuera de servicio durante un par de semanas (y además con incertidumbre sobre la fecha de restablecimiento); o el sistema eléctrico, con las repercusiones que ello tendría sobre la cadena de frío y los sistemas de transporte de alimentos.

De hecho, ya se ha considerado que se han producido AOC como parte de un conflicto armado[6]. Efectivamente, en el ámbito de la intervención rusa en la península de Crimea en 2014, el sistema eléctrico ucraniano fue atacado el 23 de diciembre de 2015, infiltrando *software* malicioso en los sistemas de tres compañías eléctricas, con el efecto de causar un apagón durante varias horas en una gran zona urbana. Posteriormente, los días 17 y 18 de diciembre de 2016, se produjo un nuevo apagón en parte de la ciudad de Kiev como consecuencia de que una estación de distribución eléctrica quedase fuera de servicio tras ser infectados sus sistemas con una versión del conocido virus Stuxnet. Se puede decir, entonces, que ya se ha producido una ciber versión del ataque de Tarento, por lo que ya no hay excusas admisibles ante la ciber versión del ataque a Pearl Harbor.

Ámbito del ciberespacio

La definición militar española para el ciberespacio se contiene en la Doctrina para el empleo de las Fuerzas Armadas, que describe el ámbito ciberespacial como «... el ámbito artificial compuesto por infraestructuras, redes, sistemas de información y telecomunicaciones y otros sistemas electrónicos, por su interacción a través de las líneas de comunicación sobre las que se propaga y el espectro electromagnético (EEM), así como por la información que es almacenada o transmitida a través de ellos. Es transversal a los demás ámbitos y no está sujeto a un determinado espacio geográfico.

[5] DROEGE, Cordula. «Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians». *International Review of the Red Cross*. Volume 94, Number 886, Ginebra, 2012, p. 538.

[6] EFRONY, Dan y SHANY, Yuval. «A Rule Book on the Shelf? Tallin Manual 2.0 on Cyber Operations and Subsequent State Practice». *Hebrew University of Jerusalem Legal Studies Research Paper* Series No. 18-22. Jerusalem: The Hebrew University of Jerusalmen Faculty of Law, 2018, p. 38.

Le caracteriza su extensión, el anonimato, la inmediatez y su fácil acceso. Finalmente, su carácter artificial y su rápida evolución generan continuas vulnerabilidades y oportunidades»[7]. Esta definición trae causa de la primera definición del ciberespacio en el ordenamiento patrio[8], que tuvo lugar en la Orden Ministerial 10/2013, de 19 de febrero, por la que se crea el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas[9], y que definió el ciberespacio como el «dominio global y dinámico compuesto por infraestructuras de tecnología de la información –incluyendo Internet–, redes de telecomunicaciones y sistemas de información».

Sin embargo, lo cierto es que el concepto de ciberespacio no es objeto de consenso. Las Fuerzas Armadas de Estados Unidos definen el ciberespacio como «un ámbito global[10] dentro del entorno de la información consistente en redes interdependientes de infraestructuras de tecnologías de la información y datos residentes, incluyendo Internet, redes de telecomunicaciones, sistemas informáticos y controladores y procesadores empotrados»[11]. El *Manual de Tallin 2.0*, probablemente el documento doctrinal sobre operaciones en el ciberespacio de mayor consenso internacional, define el ciberespacio como «el entorno formado por componentes físicos y no físicos para almacenar, modificar e intercambiar datos usando redes informáticas»[12].

En todo caso, más allá de discusiones doctrinales, lo auténticamente relevante de la definición no es tanto la misma como los elementos que se incluyen en lo definido o, por utilizar el vocabulario generalmente admitido, sus capas. En términos generales, el ciberespacio está formado por cuatro capas interdependientes: (i) la capa física o de *hardware*, (ii) la capa lógica o de *software*, (iii) la capa de contenidos, consistente en la información captada, almacenada o procesada, y (iv) la capa personal, consistente en las personas físicas o jurídicas que actúan en el ciberespacio. Y es en esas capas o contra

---

7 ESTADO MAYOR DE LA DEFENSA. *Publicación Doctrinal Conjunta PDC-01(A). Doctrina para el empleo de las Fuerzas Armadas*, doc. cit., p. 81.

8 DOMÍNGUEZ, Jerónimo, en el capítulo 8 del manual *Derecho de las operaciones aéreas,* pendiente de publicación.

9 *BOE* de 26 de febrero de 2013.

10 Los otros ámbitos globales para EE. UU. son el terrestre, marítimo, aéreo y el espacial: Headquarters, Department of the Army. *Field Manual 3-38 Cyber Electromagnetic Operations*. Washington, 2014, p. 1-5. Disponible en https://fas.org/irp/doddir/army/fm3-38.pdf. Sin embargo, nótese que para España los ámbitos de operación son el terrestre, marítimo, aeroespacial, cognitivo y ciberespacial. ESTADO MAYOR DE LA DEFENSA. *Publicación Doctrinal Conjunta PDC-01(A). Doctrina para el empleo de las Fuerzas Armadas*, doc. cit., p. 79. La OTAN también considera el ciberespacio como un ámbito de operación. Vid. el apartado 70 del NATO, Warsaw Summit Communiqué, 9 de julio de 2016. Disponible en https://www.nato.int/cps/en/natohq/official_texts_133169.htm.

11 US JOINT CHIEFS OF STAFF. *Joint Publication 3-12: Cyberspace Operations*. 2018, p. GL-4. Disponible en https://fas.org/irp/doddir/dod/jp3_12.pdf.

12 VV. AA. *Tallin Manual 2.0 on the International Law Applicable to Cyber Operations.* Cambridge University Press, 2017, p. 564.

esas capas contra las que se pueden realizar AOC[13] o fuera de él, pues Israel no ha dudado en lanzar un ataque aéreo para destruir un edificio (y los objetos y personas que contenía) que ha descrito como el *ciber cuartel general de Hamas*[14] y desde el cual se había lanzado un cibertaque contra un objetivo civil no identificado en Israel. Consecuentemente, dado que los datos y los sistemas de información permean todas las áreas de actividad humana, la doctrina militar española considera que el ciberespacio da lugar a un ámbito mixto de operación que es «de especial interés para las operaciones por ser de frecuente y necesario empleo, por implicar una dificultad añadida por la coordinación de las acciones y por requerir procedimientos no solo específicos sino además conjuntos»[15]. Y así, se ha configurado el «area de operaciones de ciberdefensa (AOCD)» como «la parte del ciberespacio en que, de manera permanente o puntual, se ejecutan operaciones militares. Está formado de manera permanente por todas las redes y sistemas de información y telecomunicaciones empleadas por el Ministerio de Defensa y las de potenciales adversarios, y de manera eventual, por las de adversarios o terceros que estuvieran afectando, o pudieran afectar, a las operaciones, así como por las de aquellos otros cuya protección le sea encomendada a las Fuerzas Armadas»[16]. Este va a ser el campo de tiro de las actuales flechas que son los ratones de los ordenadores.

El problema de la atribución

La atribución es un problema que, en general, es anterior a una AOC en el ámbito de los conflictos armados, por corresponderse a la imputación de responsabilidad por una ciberoperación que no alcanza el nivel de uso de la fuerza o de ataque armado; o de realizarse dentro de un conflicto armado, por ser realizada por un Estado o por haberse realizado por un actor no estatal. Por ese motivo, la cuestión de la atribución no va a ser objeto de consideración en el presente trabajo; sin embargo, por la indudable relación de un *ciberataque* con una AOC en el ámbito de los conflictos armados, nos parece que al menos deben dejarse apuntados determinados elementos a

---

13 CORN, Gary P. «Cyber National Security: Navigating Grey Zones Challenges In and Through Cyberspace» pendiente de publicación en *Complex Battlespaces: The Law of Armed Conflict and the Dynamics of Modern Warfare*. 2017 pp. 9 y 10. Disponible en https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3089071. Véase también DOMÍNGUEZ, Jerónimo, en el capítulo 8 del manual Derecho de las Operaciones Aéreas, pendiente de publicación.

14 SCALITER, Juan. «Guerra híbrida: detener "*hackers*" con misiles». Diario *La Razón*, 8 de mayo de 2019, p. 46 y 47. Vid. también CHESNEY, Robert. «Crossing a Cyber Rubicon? Overreactions to the IDF's Strike on the Hamas Cyber Facility». www.lawfareblog.com. 8 de mayo de 2019. Accesible en https://www.lawfareblog.com/crossing-cyber-rubicon-overreactions-idfs-strike-hamas-cyber-facility.

15 ESTADO MAYOR DE LA DEFENSA. *Publicación Doctrinal Conjunta PDC-01(A). Doctrina para el empleo de las Fuerzas Armadas*, doc. cit., p. 79.

16 Ibídem, p. 84.

tener en consideración para la imputación de responsabilidad por quien ha sufrido un ataque cibernético.

El primero de ellos es que los potenciales adversarios pueden incardinarse en una de las tres siguientes categorías:

a) Estado/s o coalición de Estados u organización internacional. En esta categoría se incluyen las fuerzas armadas de un país, sus servicios de inteligencia o policiales, o la administración civil.

b) Actores no estatales, entre los cuales están las organizaciones terroristas, las milicias o guerrillas insurgentes y el crimen organizado.

c) Adversarios por delegación o proxies, que son los actores no estatales o Estados débiles empleados de forma encubierta por un tercer Estado adversario con la finalidad de alcanzar sus propios objetivos. De esta forma, el tercer Estado y su proxy forman en cierta manera un solo conjunto[17].

El segundo elemento a tener en consideración es que en ciberataques el anonimato es la regla, lo que implica que deberá realizarse una investigación *forense* (policial, judicial, informática y/o militar, según proceda en cada caso) para la determinación de quién es el autor material del ataque[18].

Y el tercer elemento a tener en consideración es en qué circunstancias los ataques realizados por actores no estatales o proxies pueden ser imputados a un Estado, lo que entra de lleno en la cuestión jurídica de la atribución de responsabilidad a un Estado por hechos ajenos[19]. La doctrina[20], en general, considera que las reglas que regulan esta cuestión se contienen en el proyecto de *Artículos sobre la responsabilidad del Estado por hechos internacionalmente ilícitos*[21] que ha elaborado la Comisión de Derecho Internacional de

---

17 Ibídem, p. 87.

18 Vid. DROEGE, Cordula. *Op. cit.,* p. 544. Véase también el capítulo «Back-Tracking and Anonymity in Ciberspace» de PIHELGAS, Mauno en ZIOLKOWSKI, Katharina (ed.) *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy*. *NATO CCD COE Publication*. Tallin 2013, pp. 31 y ss.

19 La responsabilidad de un Estado por sus propios actos en principio entra de lleno en el sentido común y, en todo caso, se determina en las reglas 14 y 15 del *Manual de Tallín 2.0.*

20 Véase DOMÍNGUEZ, Jerónimo, en el capítulo 8 del manual *Derecho de las operaciones aéreas*, pendiente de publicación; y el capítulo «Aplicación del derecho internacional humanitario a las operaciones en el ciberespacio» de DOMINGUEZ, Jerónimo en RODRÍGUEZ, José Luis, y LÓPEZ, Joaquín (coords) *Derecho Internacional Humanitario*. Valencia: ed. Tirant lo Blanch y Cruz Roja Española (Centro de Estudios de Derecho Internacional Humanitario), 2017, p. 627. Véase también SCHMITT, Michael N. «Grey Zones in the International Law of Cyberspace». *The Yale Journal of International Law Online*. 2017. Disponible en https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3180687

21 Disponible en http://portal.uned.es/pls/portal/PORTAL.wwsbr_imt_services.GenericView?p_docname=22634788.PDF&p_type=DOC&p_viewservice=VAHWSTH&p_searchstring=

la Asamblea General de las Naciones Unidas, cuyo artículo 8 establece que «se considerará hecho del Estado según el derecho internacional el comportamiento de una persona o de un grupo de personas si esa persona o grupo de personas actúa de hecho por instrucciones o bajo la dirección o control de ese Estado al observar ese comportamiento».

Siendo aparentemente claro que cuando una persona o grupo de personas actúe siguiendo «instrucciones» de un Estado, esas acciones se imputarán jurídicamente a dicho Estado, el segundo inciso de ese artículo 8 puede ser interpretado de dos formas distintas, en función de si se considera que se puedan imputar a un Estado las acciones realizadas por una persona o grupo de personas bajo su control *efectivo* o, alternativamente, basta que ese control sea *genérico* para realizar tal imputación[22] y, consecuentemente, se puedan exigir las responsabilidades procedentes.

A su vez, el *Manual de Tallin 2.0* parte del precedente de los *Artículos sobre la responsabilidad del Estado por hechos internacionalmente ilícitos*[23] y, consecuentemente, tiene un enfoque similar, pero algo más amplio, en su regla 17, según la cual «las ciberoperaciones ejecutadas por un actor no estatal se imputan a un Estado cuando: (a) se realizan siguiendo sus instrucciones o bajo su dirección o control, o (b) el Estado reconoce y adopta la operación como propia».

Como puede verse, por tanto, la cuestión de la atribución tiene una perspectiva fáctica, que es la de la prueba de que unos determinados actos cibernéticos han sido realizados por una determinada persona, física o jurídica, y una perspectiva jurídica, que es la de la acreditación de que esa persona sigue las instrucciones de un Estado o actúa bajo su dirección o control.

Marco legal del empleo de las Fuerzas Armadas

Si aceptamos que hoy en día la máxima latina de *inter armas silent leges*[24] ya no está en vigor, y los procesos de Nuremberg y Tokio y el Tribunal Penal Internacional están ahí para recordarlo[25], debemos tener presente –siquiera de forma somera– que el hecho de que una acción ofensiva de las Fuerzas Armadas se realice en el ámbito del ciberespacio no exime a aquella del marco legal de empleo de la fuerza por las Fuerzas Armadas.

---

22 Michael N. Schmitt, uno de los principales autores en la materia, considera que el control debe ser «efectivo» y no meramente «genérico» basándose en la sentencias Nicaragua y Genocidio en Bosnia del Tribunal Internacional de Justicia. SCHMITT, Michael N. «Gray Zones...» *op. cit*., pp. 9 y 10. En similar sentido se pronuncian los comentarios 5, 6 y 7 de la regla 17 del *Manual de Tallin 2.0*.

23 VV. AA. *Tallin Manual 2.0... op. cit.*, p. 95.

24 En tiempo de guerra la ley calla.

25 Ciertamente nunca se ha derogado la aplicación de la máxima latina *Vae victis*, Ay de los vencidos.

En efecto, el artículo 20 de la Ley Orgánica de Defensa Nacional[26] dispone que mediante ley se establecerán las reglas esenciales que definen el comportamiento de los militares, y que el Gobierno por Real Decreto desarrollará dichas reglas en las Reales Ordenanzas. El complemento legal de la Ley Orgánica de Defensa Nacional es la Ley Orgánica de Derechos y Deberes de los miembros de las Fuerzas Armadas[27], que regula en su artículo 6 las reglas esenciales que definen el comportamiento del militar. Entre estas, a los efectos de este trabajo, destacaremos las siguientes reglas:

> Quinta. Ajustará su conducta al respeto de las personas, al bien común y al derecho internacional aplicable en conflictos armados. La dignidad y los derechos inviolables de la persona son valores que tienen obligación de respetar y derecho a exigir. En ningún caso los militares estarán sometidos, ni someterán a otros, a medidas que supongan menoscabo de la dignidad personal o limitación indebida de sus derechos.
>
> Sexta. En el empleo legítimo de la fuerza, hará un uso gradual y proporcionado de la misma, de acuerdo con las reglas de enfrentamiento establecidas para las operaciones en las que participe.
>
> Duodécima. Si las órdenes entrañan la ejecución de actos constitutivos de delito, en particular contra la Constitución y contra las personas y bienes protegidos en caso de conflicto armado, el militar no estará obligado a obedecerlas y deberá comunicarlo al mando superior inmediato de quien dio la orden por el conducto más rápido y eficaz. En todo caso asumirá la grave responsabilidad de su acción u omisión.

Y, finalmente, las Reales Ordenanzas de las Fuerzas Armadas[28] disponen:

> Artículo 84. Uso legítimo de la fuerza. En el empleo legítimo de la fuerza, el militar hará un uso gradual y proporcionado de la misma, de acuerdo con las reglas de enfrentamiento establecidas para las operaciones en las que participe.
>
> Artículo 85. Principio de humanidad. Su conducta en el transcurso de cualquier conflicto u operación militar deberá ajustarse a las normas que resulten aplicables de los tratados internacionales en los que España fuera parte, relativos al derecho internacional humanitario.
>
> Artículo 106. Deberes en relación con el derecho internacional humanitario. El militar conocerá y difundirá, así como aplicará en el transcurso de cualquier conflicto armado u operación militar, los convenios internacionales ratificados por España relativos al alivio de la suerte de heridos,

[26] Ley Orgánica 5/2005, de 17 de noviembre, de la Defensa Nacional.

[27] Ley Orgánica 9/2011, de 27 de julio, de Derechos y Deberes de los Miembros de las Fuerzas Armadas.

[28] Real Decreto 96/2009, de 6 de febrero, por el que se aprueban las Reales Ordenanzas para las Fuerzas Armadas.

> enfermos o náufragos de las fuerzas armadas, al trato a los prisioneros y a la protección de las personas civiles, así como los relativos a la protección de bienes culturales y a la prohibición o restricciones al empleo de ciertas armas.
>
> Artículo 111. Principio de distinción. En el transcurso de cualquier operación tendrá en cuenta el principio de distinción entre personas civiles y combatientes y entre bienes de carácter civil y objetivos militares para proteger a la población civil y evitar en lo posible las pérdidas ocasionales de vidas, sufrimientos físicos y daños materiales que pudieran afectarle.
>
> Artículo 113. Protección de bienes culturales. No atacará ni hará objeto de represalias o de actos de hostilidad a bienes culturales o lugares de culto claramente reconocidos, que constituyen el patrimonio cultural y espiritual de los pueblos y a los que se haya otorgado protección en virtud de acuerdos especiales. Evitará la utilización de dichos bienes culturales o de instalaciones que se encuentren próximas a ellos para propósitos que puedan exponerlos a la destrucción o al deterioro.
>
> Artículo 114. Medios y métodos de combate. No utilizará medios o métodos de combate prohibidos por el derecho internacional humanitario que puedan causar males superfluos o sufrimientos innecesarios, así como aquellos que estén dirigidos a causar o puedan ocasionar extensos, graves y duraderos perjuicios al medio ambiente, comprometiendo la salud o la supervivencia de la población.

España, como hemos visto, ha asumido legalmente las reglas propias del derecho internacional humanitario para su actuación en el ámbito de los conflictos armados, y en la actualidad, con todas las salvedades que se quieran poner, es una cuestión prácticamente pacífica internacionalmente que las reglas propias del derecho internacional humanitario se aplican a las AOC[29]. En todo caso, sería un error considerar a las reglas legales nacionales o propias del derecho internacional humanitario como meras limitaciones jurídicas a la acción ciberofensiva. Como bien reconoce la doctrina española, «la legitimidad en el uso de la fuerza consiste en actuar conforme a las leyes, los mandatos, los compromisos suscritos por España y al código moral de las Fuerzas Armadas españolas»[30]. Y no solo ello, en una sociedad audiovisual y ya 4.0, «tan importante es que se opere legítimamente como que sea percibido así por la opinión pública propia, la de las naciones que participan en las operaciones, la comunidad internacional, y la población local de la

[29] Véase el capítulo «Aplicación del derecho internacional humanitario a las operaciones en el ciberespacio» de DOMINGUEZ, Jerónimo, en RODRÍGUEZ, José Luis, y LÓPEZ, Joaquín (coord.). *Derecho Internacional Humanitario*. Valencia: Ed. Tirant lo Blanch y Cruz Roja Española (Centro de Estudios de Derecho Internacional Humanitario), 2017, p. 622.

[30] ESTADO MAYOR DE LA DEFENSA. *Publicación Doctrinal Conjunta PDC-01(A). Doctrina para el empleo de las Fuerzas Armadas*, *op. cit.*, p. 73.

zona donde se desarrolla la operación»[31]. Vietnam es claramente una lección aprendida.

El Mando Conjunto de Ciberdefensa

La Directiva de Defensa Nacional de 2012 declaraba que «España debe estar preparada para hacer frente a los riesgos de un mundo en el que la interconexión, la calidad y velocidad con que fluye la información, la gestión telemática de las transacciones, la libertad de movimientos y de intercambios comerciales, cuyos beneficios son tan evidentes para la sociedad, no configuren un escenario en el que jueguen con ventaja grupos terroristas y de la delincuencia organizada con capacidad para dañar gravemente la paz social, la seguridad ciudadana, la estabilidad política y la prosperidad general», y además reconocía que los ataques cibernéticos son «hipótesis nada alejadas de la realidad ya presente»[32]. A su vez, la *Estrategia de Seguridad Nacional de 2017* asumió expresamente que una de las tendencias actuales en los conflictos armados era el aumento de «capacidades en otros dominios como el ciberespacio», por lo que establecía como una de las líneas de acción en el ámbito de la ciberseguridad el «reforzar las capacidades de prevención, detección, reacción, análisis, recuperación, respuesta e investigación frente a las ciberamenazas»[33].

Y entre esos marcos conceptuales llegamos a la determinación de quién va a teclear o a manejar el ratón en las acciones ciberofensivas; o, dicho de otra forma, quién en el ámbito de las Fuerzas Armadas va a ejecutar la AOC por parte de España en un conflicto armado. Podremos encontrar la respuesta después de la *Directiva de Defensa Nacional de 2012*, que quizás estaba muy influenciada por una visión multilateral de la seguridad, y antes de la *Estrategia de Seguridad Nacional de 2017*, que quizás tuviera una visión más nacional de las responsabilidades de defensa. En ese período se dictó la Orden Ministerial 10/2013[34] de creación del Mando Conjunto de Ciberdefensa, dependiente del Jefe del Estado Mayor de la Defensa, encuadrándolo orgánicamente en el Estado Mayor de la Defensa como parte de la estructura operativa de las Fuerzas Armadas[35]. A este Mando Conjunto se le asigna el planeamiento y ejecución de las acciones relativas a ciberdefensa militar

[31] Ibídem, p. 74.

[32] Directiva de Defensa Nacional 1/2012, disponible en http://www.defensa.gob.es/Galerias/defensadocs/directiva-defensa-nacional-2012.pdf. Fecha de la consulta 8 de abril de 2019.

[33] *Estrategia de Seguridad Nacional 2017*, disponible en http://www.defensa.gob.es/Galerias/defensadocs/Estrategia_Seguriad_Nacional_2017.pdf. Fecha de la consulta 8 de abril de 2017.

[34] Orden Ministerial 10/2013, de 19 de febrero, por la que se crea el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas.

[35] Artículos 4, 9 y 15 del Real Decreto 872/2014, por el que se establece la organización básica de las Fuerzas Armadas.

y, específicamente, le encomienda en su artículo 5.5 a «ejercer la respuesta oportuna, legítima y proporcionada en el ciberespacio ante amenazas o agresiones que puedan afectar a la defensa nacional». Es decir, la unidad de *arqueros cibernéticos* de las Fuerzas Armadas es el Mando Conjunto de Ciberdefensa.

Pero no todo el monte es orégano. Caveat sobre Tallin 2.0

Habíamos dejado indicado previamente[36] que, en la actualidad, con todas las salvedades que se quieran poner, es una cuestión prácticamente pacífica[37] internacionalmente que las reglas propias del DIH se aplican a las AOC. Habíamos dejado también indicado previamente que el *Manual de Tallin 2.0* probablemente sea el documento doctrinal[38] sobre acciones en el ciberespacio de mayor consenso internacional[39]. Y del mismo modo el general Auditor Domínguez Bascoy sostiene con respecto a la aplicación del DIH en el ámbito del ciberespacio que «la comunidad internacional no ha sido, sin embargo, capaz de alcanzar un consenso sobre la manera precisa en que han de aplicarse a aquellas muchos de los principios y normas internacionales»[40], igualmente debe reconocerse que las reglas contenidas en el *Manual de Tallín 2.0* han sido también objeto de crítica doctrinal y que, en ocasiones, la práctica de las operaciones de los Estados en el ciberespacio no ha sido plenamente conforme con sus reglas[41]. Esta situación ha sido cáusticamente resumida por Efrony y Shany diciendo: «Por lo tanto, aunque las reglas de Tallín han sido criticadas por no avanzar lo suficiente en la limitación de la habilidad para conducir ciberoperaciones en el ciberespacio, estamos viendo a algunos Estados protestando por lo opuesto, esto es, que [esas reglas] se deberían limitar aún más, y otros van incluso más allá»[42]. En realidad, es probable que estas discrepancias entre Estados sobre el *Manual de Tallin 2.0* no sean sino un reflejo de las discrepancias más

---

36 Véase el apartado El problema de la atribución de este capítulo *ut supra*.

37 Nótese sin embargo que dos Estados tan poderosos como Rusia o China no tienen una posición oficial acerca de la aplicabilidad del derecho internacional humanitario al ámbito cibernético. Cfr. DROEGE, Cordula, *op. cit.,* p. 537.

38 Que sea un documento doctrinal no le priva de valor jurídico. Otro documento doctrinal como es el Manual de San Remo sobre el derecho internacional aplicable a los conflictos armados en el mar, y que por tanto es conceptualmente parecido a *Tallin 2.0*, es de notoria aplicación diaria en los estados mayores navales cuanto menos como argumento de autoridad o fuente de motivación jurídica.

39 Véase el apartado Ámbito del ciberespacio de este capítulo *ut supra*.

40 Véase DOMÍNGUEZ, Jerónimo, en el capítulo 8 del manual *Derecho de las operaciones aéreas*, pendiente de publicación, y en el mismo sentido el capítulo «Aplicación del derecho internacional humanitario a las operaciones en el ciberespacio» de DOMINGUEZ, Jerónimo, *op. cit.,* p. 622.

41 Véase EFRONY, Dan, y SHANY, Yuval, *op. cit.,* pp. 3 a 8 y 58 a 59.

42 Ibídem, p. 58.

generales que aquellos tienen sobre la aplicación del derecho internacional a las acciones de los Estados en el ciberespacio, donde las diferencias no son tanto jurídicas como estratégicas, políticas o ideológicas[43].

La consecuencia práctica para el operador legal en la materia es que deberá tener en cuenta que el *Manual de Tallín 2.0*, en definitiva, es un tratado doctrinal y no una norma de fuerza legal. Por consiguiente, el análisis jurídico que se haga de una AOC en el ámbito de los conflictos armados podrá tener en cuenta las reglas de *Tallin 2.0*, pero no exclusivamente.

Acciones ofensivas en el ciberespacio y sus clases

«Ciberoperaciones»

En los ámbitos terrestre, marítimo y aéreoespacial las acciones o las operaciones son perceptibles por los sentidos. Cuando una persona ve a una compañía de Leopards campo a través, o a unos F-18 volando, o una fragata navegando, puede deducir a simple vista que hay una acción o una operación en curso, pero eso no pasa en el dominio cibernético. Por eso, un primer paso para el análisis de una AOC es la determinación primero de qué es el sustantivo antes de la de qué es el adjetivo.

En España el general Auditor Domínguez Bascoy ha definido como «ciberoperación» como «aquella actividad en la que se emplean capacidades cibernéticas en o a través del ciberespacio»[44]. Se trata de una definición similar a la adoptada en 2018 por EE. UU. en su *Publicación Conjunta 3-12* del Presidente de la Junta de Jefes de Estado Mayor, conforme a la cual una ciberoperación es el «empleo de capacidades cibernéticas en las que el propósito primario es alcanzar objetivos en o a través del ciberespacio»[45], que a su vez asume la definición que al respecto había adoptado su Ejército de Tierra[46].

---

[43] La Asamblea General de Naciones Unidas tiene convocado un Grupo de Expertos Gubernamentales dentro del Primer Comité de la misma sobre «Los avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional» y que es probablemente el único foro intergubernamental general sobre la materia. El trabajo de ese grupo encalló en 2017 por las diferencias que los Estados tienen sobre la bondad –o no – del flujo libre de información en Internet y la difusión de los derechos fundamentales. Véase al respecto HENRIKSEN, Anders. «The end of the road for the UN GGE process: The future regulation of cyberespace». *Journal of Cybersecurity*. Volume 5, Issue 1, 2019, accedido en https://academic.oup.com/cybersecurity/article/5/1/tyy009/5298865 el 24 de mayo de 2019.

[44] Véase DOMÍNGUEZ, Jerónimo, en el capítulo 8 del manual *Derecho de las operaciones aéreas*, pendiente de publicación.

[45] US JOINT CHIEFS OF STAFF. Joint Publication 3-12 «Cyberspace Operations». *Op. cit*., p. I-1.

[46] HEADQUARTERS. Department of the Army. Field Manual *FM 3-38, Cyber Electromagnetic Activities*. *Op. cit.,* pp. 1-3.

En resumen, podemos concluir que el concepto de «ciberoperación» está compuesto por (1) las capacidades del actor, (2) por el medio en el que se ejecutan tales capacidades, y (3) por el objetivo que se busca alcanzar.

Qué son las acciones ofensivas en el ciberespacio

La doctrina estadounidense distingue entre operaciones ciberofensivas (lo que aquí denominamos AOC) y ciberataques[47]. Resumidamente, considera que las operaciones ciberofensivas (AOC) son misiones cuyo objeto es la proyección de poder en y a través del ciberespacio extranjero a través de acciones de apoyo de un mando combatiente o de un objetivo nacional. Tal proyección de poder puede limitarse a afectar las capacidades en el ciberespacio del objetivo o crear efectos en el ciberespacio que desencadenen sucesivos efectos en los dominios reales (terrestre, aéreoespacial o marítimo) y que afecten a sistemas de armas, comunicaciones, nodos logísticos, u objetivos de alto valor.

Esas operaciones ciberofensivas (AOC) se ejecutan, según la doctrina estadounidense, a través de «ataques en el ciberespacio»[48], que son las específicas acciones que crean efectos de negación (degradación, disrupción o destrucción del objetivo) en el ciberespacio o manipulación de datos y que suponen efectos adversos en los dominios reales, y se considera que son equivalentes a un ataque cinético (*fire*).

España, por su parte, ha definido en la Orden Ministerial 10/2013 el concepto de «ciberataque» como la «acción producida en el ciberespacio que compromete la disponibilidad, integridad y confidencialidad de la información mediante el acceso no autorizado, la modificación, degradación o destrucción de los sistemas de información y telecomunicaciones o las infraestructuras que los soportan»[49]. Esta definición, por su menor abstracción que la estadounidense, es probablemente más útil para los operadores en el ámbito de los conflictos armados.

Uso de la fuerza vs ataque armado: necesidad del análisis de impacto del nivel de la acción ofensiva en el ciberespacio

Hemos visto en el apartado anterior que, doctrinalmente, puede distinguirse entre una AOC y un ciberataque o ataque en el ciberespacio. Recordemos, igualmente, que la Carta de las Naciones Unidas prohíbe a los Estados recu-

---

47 US JOINT CHIEFS OF STAFF. *Op. cit.,* pp. II-5 y II-7. HEADQUARTERS, DEPARTMENT OF THE ARMY. *Op. cit.*, pp. 3-2 y 3-3.

48 Véanse las fuentes de la nota a pie de página anterior.

49 Orden Ministerial 10/2013, de 19 de febrero, por la que se crea el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas.

rrir a la amenaza o al uso de la fuerza contra la integridad territorial o la independencia política de cualquier Estado, a la vez que reconoce el derecho a la legítima defensa en caso de ataque armado (como hecho distinto del mero «uso de la fuerza»[50]). Esa distinción en las AOC entre (a) acción/operación que alcanza el nivel de uso de la fuerza, y (b) acción/operación que alcanza el nivel de ataque armado, que a su vez desencadena el derecho a la legítima defensa (y que se diferencian entre ellas por el impacto que producen), debe ser cuidadosamente analizada por los operadores. En efecto, mientras que un ataque armado legitima el recurso del agredido a la legítima defensa, el *mero* uso de la fuerza no lo hace, concediendo a la víctima únicamente otro tipo de respuesta *menor* como las contramedidas[51] (acciones u omisiones que un Estado realiza contra otro y que serían ilícitas salvo por la circunstancia de que se adoptan en repuesta al acto ilícito del otro Estado y al objeto de que desista de tal acto ilícito). Consecuentemente, el *Manual de Tallin 2.0* recoge tal criterio en su capítulo 14.

Reglas del *Manual de Tallin 2.0* sobre el uso de la fuerza (capítulo 14):

- Regla 68 – Prohibición del uso de la fuerza. Es ilícita una ciberoperación que constituya una amenaza o uso de la fuerza contra la integridad territorial o independencia política de cualquier Estado, o que de cualquier otra forma sea incompatible con los propósitos de las Naciones Unidas.
- Regla 69 – Definición de uso de la fuerza. Una ciberoperación constituye uso de la fuerza cuando en su escala y efectos son comparables con operaciones no cibernéticas que alcancen el nivel de uso de la fuerza.
- Regla 70 – Definición de amenaza de uso de la fuerza. Una ciberoperación, o la amenaza de una ciberoperación, constituye una amenaza ilícita de uso de la fuerza cuando la acción con la que se amenaza, si se ejecuta, fuera un uso ilícito de la fuerza.
- Regla 71 – Legítima defensa contra ataque armado. Un Estado que sea el objetivo de una ciberoperación que alcanza el nivel de ataque armado puede ejercer su derecho inherente a la legítima defensa. Que una ciberoperación constituya un ataque armado depende de su escala y efectos.
- Regla 72 – Necesidad y proporcionalidad. El uso de la fuerza en el desarrollo de una ciberoperación ejecutada por un Estado en el ejercicio de su derecho a la legítima defensa debe ser necesaria y proporcionada.
- Regla 73 – Inminencia e inmediatez. El derecho al uso de la fuerza en legítima defensa surge si un ataque armado cibernético ocurre o es inminente. Además, se requiere que sea inmediato.

[50] Sentencia Nicaragua de la Corte Internacional de Justicia de 27 de junio de 1986.

[51] Véanse las reglas 20 y siguientes del *Manual de Tallín 2.0.*

A su vez, en los comentarios[52] a la regla 69 (definición de uso de la fuerza), se indica que los factores que los Estados consideran para determinar si una «ciberoperación» alcanza el nivel de uso de la fuerza son, resumidamente y entre otros, los siguientes:

a) Gravedad (*severity*): sujeto a una regla *de minimis*, la causación de daños físicos a personas o cosas cualificará la ciberoperación como uso de la fuerza.

b) Inmediatez (*immediacy*): cuanto antes se manifiesten los efectos de la ciberoperación más probable es que se considere como uso de la fuerza.

c) Causación (*directness*): cuanto más directo sea el nexo causal entre el acto (la ciberoperación) y sus consecuencias, más probable es que se considere como uso de la fuerza.

d) Intrusión (*invasiveness*): cuanto la ciberoperación se haya dirigido a la penetración en sistemas protegidos del objetivo, más probable es que se considere como uso de la fuerza.

e) Cuantificabilidad de efectos (measurabilty of effects): cuanto más cuantificables sean los efectos de una ciberoperación, más probable es que se considere como uso de la fuerza.

f) Carácter militar (*military character*): La vinculación entre una ciberoperación y operaciones militares aumenta la probabilidad de que se considere aquella como uso de la fuerza.

g) Implicación estatal (*State involvement*): cuanto más clara sea la vinculación entre un Estado como actor y una ciberoperación, más probable es que se considere como uso de la fuerza.

h) Presunción de legalidad (*presumptive legality*): en derecho internacional público, lo que no está prohibido por tratados internacionales o la costumbre internacional se considera que está permitido (por ejemplo, el derecho internacional público no prohíbe el espionaje). Será menos probable que las ciberoperaciones que estén cubiertas por una presunción de legalidad se consideren como uso de la fuerza.

Por otra parte, en los comentarios[53] a la regla 71 (legítima defensa contra ataque armado), se indica que no es lo mismo el uso de la fuerza que el ataque armado, en concordancia con la sentencia Nicaragua[54] de la Corte Internacional de Justicia. La diferencia entre uso de la fuerza y el ataque armado es que la escala y efectos de este es superior a aquel, lo que necesariamente implica un análisis caso por caso de cada AOC. Un ejemplo pue-

52 VV. AA. *Tallin Manual 2.0... Op. cit.,* pp. 334 a 337.

53 Ibídem, pp. 339 a 348.

54 Sentencia Nicaragua de la Corte Internacional de Justicia de 27 de junio de 1986.

de ser el del virus Stuxnet, que fue utilizado por una potencia para tomar el control de centrifugadoras usadas para el enriquecimiento de uranio por parte de Irán, de forma que las mismas se autodestruyeran. Los autores del *Manual de Tallin 2.0* han considerado que el ataque Stuxnet ha alcanzado el nivel de uso de la fuerza y, para parte de ellos, que incluso ha llegado al nivel de ataque armado[55].

Parece razonablemente claro que un ciberataque que, al menos, cause daños físicos a personas u objetos puede ser considerado como uso de la fuerza[56]. Se ha considerado a su vez, con razonable criterio, que una AOC alcanza el nivel de ataque armado cuando sus efectos directos e indirectos sean equivalentes a los que se habrían producido por un ataque armado convencional[57]. Sin embargo, lo cierto es que la ausencia de una regla clara acerca de cuándo el uso de la fuerza alcance el nivel de ataque armado hace que las AOC en tiempo de paz entren de lleno en la *zona gris*[58], ámbito que se trata brillantemente en el capítulo «El conflicto en las sombras: aspectos generales y elementos jurídicos de las operaciones en la zona gris» de esta publicación y del que es autor el teniente coronel auditor Mario Lanz Raggio.

Tipos de ciberataques

Una AOC se basa, lógicamente, en una vulnerabilidad detectada en el sistema del objetivo, lo que en términos de los dominios tradicionales se consideraría el punto débil. Cómo se ataca a esa vulnerabilidad puede ser analizada desde distintos ángulos, tal y como ha expuesto H. LIN[59]:

- Acceso. En función del acceso, el ciberataque puede ser por acceso remoto, típicamente a través de Internet, o por acceso cercano, a través de la colocación local de un determinado *hardware* o *software*.
- Capacidad. La capacidad se refiere a las cosas que se pueden hacer aprovechando el acceso ganado al sistema objetivo.
- Efectos. Los efectos que el ciberataque produce en el objetivo, que pueden ser desde el mero acceso a la información contenida en el sistema

55 VV. AA. *Tallin Manual 2.0... Op. cit.,* p. 342.

56 SCHMITT, Michael N. *Grey Zones... Op. cit*, p. 14.

57 LIN, Herbert S. «Offensive Cyber Operations and the Use of Force». *Journal of National Security Law & Policy*. Vol. 4-63, 13 agosto 2010, p. 73.

58 SCHMITT, Michael N. *Grey Zones... Op. cit*., p. 15.

59 LIN, Herbert S. «Offensive Cyber Operations and the Use of Force». *Journal of National Security Law & Policy*. Vol. 4-63, 13 agosto 2010, pp. 66 y siguientes. Coincide con las ciberoperaciones ofensivas tipo el T. Col. Vito Smyth, USAF, en su trabajo SMYTH, Vito. «The Best Defense is a Good Offense: Conducting Offensive Cyberoperations and the Law of Armed Conflict». Air War Collage, Air University, p. 9. Disponible en https://apps.dtic.mil/dtic/tr/fulltext/u2/1019221.pdf el 10 de abril de 2019.

objetivo, pasando por su manipulación, sustracción, o falsificación, hasta la destrucción del propio sistema.

De esta forma, los ciberataques tipo pueden consistir en

- La destrucción de datos en un sistema, o la misma destrucción del sistema.
- La suplantación de un miembro del sistema, generando información o mensajes falsos.
- La modificación de datos contenidos en una base de datos.
- La degradación o denegación de servicio de un sistema.

La estructura conceptual de un ciberataque: The Cyber Kill Chain

Difícilmente podrá realizarse una valoración jurídica de una AOC sin comprender sus fases, elementos o componentes. Para ello, vamos a utilizar el modelo Cyber Kill Chain. El término Kill Chain se ha referido tradicionalmente a la composición de los elementos que conforman un ataque militar, generalmente referidos como (i) identificación del objetivo, (ii) asignación de fuerzas para el ataque, (iii) orden de ataque y (iv) destrucción del objetivo. Una descripción más precisa del término es la del acrónimo F2T2EA, que se refiere a: *Find* (encuentra un objetivo), *Fix* (determina su situación exacta), *Track* (sigue los movimientos del objetivo), *Target* (escoge el arma apropiada para el ataque), *Engage* (ataque propiamente dicho sobre el objetivo), y *Assess* (evalúa el efecto del ataque).

Sobre el modelo F2T2EA, la empresa Lookheed Martin[60] *ha patentado* el concepto Cyber Kill Chain, para explicar el orden de las fases en que se articula un ciberataque[61]:

1) Reconocimiento: fase de recopilación de información sobre el objetivo, generalmente proveniente de fuentes abiertas.

   Ejemplo de esta fase es la recopilación de información desde ICANN, la aplicación de WHOIS o, en general, páginas web o publicaciones diversas.

[60] Véase https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html, accedido el 15 de abril de 2019.

[61] Véase DOMÍNGUEZ, Jerónimo, en el capítulo 8 del manual *Derecho de las operaciones aéreas*, pendiente de publicación. Para una visión detallada del asunto véase también el capítulo «Technical Methods, Techniques, Tools and Effects of Cyber Operations» de MAYBAUM, Markus en ZIOLKOWSKI, Katharina (ed.). *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy*. Tallin: NATO CCD COE Publication, 2013, pp. 103 y ss.

2) Creación del arma: fase de diseño y fabricación del instrumento (*malware*) que se va a emplear para obtener los efectos pretendidos por el ciberataque.

   Ejemplo de esta fase es el diseño o selección del programa o aplicación (*malware*) que se va a preparar y probar de forma individualizada para el ciberataque, lo que a su vez tendrá en cuenta si el objetivo no está protegido, está poco protegido, o está muy protegido.

3) Lanzamiento: fase de envío del *malware* al objetivo, lo que se puede hacer por correo-e, por dispositivos de memoria, por acceso no autorizado a la red, etc.

   Ejemplo de esta fase es el envío de un correo-e que lleve adjunto el programa o aplicación utilizado para el ataque para que sea abierto e instalado por el destinatario del correo-e.

4) Explotación: fase de explotación de una vulnerabilidad en el objetivo para la introducción del *malware* en aquel.

   Ejemplo de esta fase es que el atacante tenga la capacidad de alterar el flujo de control de trabajo del sistema objetivo sin tener las credenciales de este que le autoricen para ello. Es el equivalente medieval a conquistar, al menos, la puerta de una ciudad amurallada.

5) Instalación: fase de instalación del instrumento en el objetivo de forma que aquel se pueda ejecutar en este.

   Ejemplo de esta fase es la instalación de una *puerta trasera* al sistema objetivo de forma que el atacante pueda acceder repetidamente al mismo sin autorización.

6) Mando y control: fase en la que el atacante toma el control remotamente el objetivo.

   Ejemplo de esta fase es la capacidad de la que disfruta el atacante de acceder telemáticamente por una *puerta trasera* al sistema objetivo para realizar las acciones sobre el objetivo o, en su caso, para implantar un instrumento que no necesite control *on-line*, como una *bomba lógica* que se active por el mero transcurso del tiempo o por una acción tomada por el controlador del sistema objetivo.

7) Acciones sobre el objetivo: fase en la que el atacante ejecuta las concretas acciones sobre el objetivo con el propósito de alcanzar los efectos pretendidos.

   Ejemplos de esta fase son (i) cambiar el nombre de archivos, (ii) cambiar las versiones y/o fechas de archivos, (iii) modificar tablas y gráficos en archivos, (iv) eliminación de archivos, (v) inserción de archivos con información falsa, (vi) modificación de privilegios de usuario (para

asignar dichos privilegios al atacante o para quitárselos a alguien del objetivo), (vii) cambio de contraseñas, (viii) desinstalación de *software*.

El análisis jurídico de la AOC tendrá entonces en cuenta las concretas medidas y decisiones que por acción y omisión haya realizado el atacante con respecto a cada una de las fases descritas.

Ciberlimitaciones derivadas de los principios generales del derecho internacional humanitario

Decíamos en el Marco legal del empleo de las Fuerzas Armadas de este capítulo que hoy en día, con todas las salvedades que se quieran poner, es una cuestión prácticamente pacífica internacionalmente que las reglas propias del DIH se aplican a las AOC. Como dice la regla 80 del *Manual de Tallín 2.0*: «Las ciberoperaciones ejecutadas en el contexto de un conflicto armado están sujetas a la ley de los conflictos armados». A su vez, debe tenerse presente que pueden ejecutarse AOC *out of the blue* que, por causar daños físicos a personas y objetos de naturaleza o efectos equivalentes a los que se habrían producido por un ataque armado convencional, puedan ser consideradas como ataque armado en sí mismas[62]. Tal hecho implica, por un lado, que esas AOC estén sujetas *per se* a las reglas del derecho internacional humanitario[63] y que, por otro lado, generen el derecho a la autodefensa bajo la Carta de Naciones Unidas como consecuencia de haberse producido una situación de conflicto armado, nacional o internacional, precisamente como consecuencia del ciberataque. En todo caso, no puede ignorarse que, en ausencia de hostilidades abiertas, la práctica parece mostrar que la calificación jurídica del ciberataque por la víctima vendrá determinada por una multiplicidad de factores añadidos (correlación de fuerzas agresor-agredido, situación nacional o internacional, alianzas internacionales, dependencias económicas, etc.), lo que conduce de nuevo a la zona gris[64].

A continuación, expondremos, sin pretender agotar este campo, que es tan amplio como la realidad misma, las principales limitaciones que, con carácter general, se derivan de los principios generales del derecho internacional humanitario.

El principio de necesidad militar

Una regla básica del DIH es que las operaciones militares se dirigirán únicamente[65] contra objetivos militares (artículo 48 del Protocolo I Adicional a los

62 Vid. Apartado Uso de la fuerza vs ataque armado: necesidad de análisis de impacto del nivel de la acción ofensiva en el ciberespacio de este trabajo.

63 Y desde luego a las reglas del *ius ad bellum*, materia ajena por otra parte al objeto de este trabajo.

64 SCHMITT, Michael N. *Grey Zones... Op. cit.,* p. 15.

65 ESTADO MAYOR DEL EJÉRCITO. «*OR7-004 Orientaciones – El Derecho de los Conflictos Armados*». Tomo I, 1996, pp. 2-3.

Convenios de Ginebra de 1949). La necesidad militar requiere que los objetivos legítimos sean únicamente aquellos que realicen una contribución directa al esfuerzo bélico del enemigo, o que su destrucción o daño produzca una ventaja militar al atacante por su naturaleza, localización, propósito o uso[66].

De ello se deriva que el atacante debe realizar todo lo que razonablemente pueda para verificar que el objetivo sea un objetivo militar y, eligiendo en todo caso los medios que minimicen los daños colaterales, cancelar o suspender el ataque cuando sea aparente que el objetivo no sea objetivo militar o que se incumplirá el «principio de proporcionalidad»[67] (sobre el que tratará el apartado homónimo de este capítulo). Consecuentemente, el *Manual de Tallin 2.0* recoge en su cuerpo el principio de necesidad militar.

Reglas del *Manual de Tallin 2.0* sobre el principio de necesidad militar:

> Regla 114 – Cuidado constante. Durante las hostilidades que impliquen ciberoperaciones, se tendrá un cuidado constante de preservar a la población civil, a civiles individuales, y a objetos civiles.
>
> Regla 115 – Verificación de objetivos. Aquellos que planeen o decidan un ciberataque harán todo lo que sea factible para verificar que los objetivos a ser atacados no sean personas u objetos civiles y no estén sujetos a especial protección.
>
> Regla 116 – Elección de medios o métodos. Aquellos que planeen o decidan un ciberataque tomarán todas las precauciones que sean factibles en la elección de medios o métodos bélicos empleados en el ataque, con la intención de evitar, y en cualquier caso minimizar, los daños incidentales a civiles, la pérdida de vidas civiles, y el daño o destrucción de objetos civiles.

De hecho, puede razonablemente pensarse que la cuestión del principio de la necesidad militar en el ciberespacio y de que, en consecuencia, se tomen todas las medidas adecuadas para limitar los daños incidentales a civiles, puede tener un cierto paralelismo con una de las razones últimas de la prohibición de las armas biológicas, en el sentido de evitar los efectos derivados de la expansión incontrolada del arma, sea esta un virus biológico o informático (*malware*).

El principio de distinción

El principio de distinción está intrínsecamente unido al de necesidad militar en tanto en cuanto se basa también en la diferenciación entre objetivo mi-

[66] SMYTH, VITO. *Op. cit.,* p. 11.

[67] SCHMITT, Michael N., «Peacetime Cyber Responses and Wartime Cyber Operations Under International Law: An Analytical Vade Mecum», Harvard National Security Journal, Vol. 8, 2017, p. 276.

litar y objetivo civil, si bien aquel pretende dar una regla de respuesta más específica a la cuestión de qué objetos civiles, por la ventaja militar que proporcionan al enemigo, son susceptibles de ser atacados. Aquí las reglas de partida, en cuanto a los objetos, son las de

- El artículo 52.3 del Protocolo I Adicional a los Convenios de Ginebra de 1949, según el cual «En caso de duda acerca de si un bien que normalmente se dedica a fines civiles, tal como un lugar de culto, una casa u otra vivienda o una escuela, se utiliza para contribuir eficazmente a la acción militar, se presumirá que no se utiliza con tal fin».
- Los apartados 2 y 3 del artículo 54 del Protocolo I Adicional a los Convenios de Ginebra de 1949, según el cual «2. Se prohíbe atacar, destruir, sustraer o inutilizar los bienes indispensables para la supervivencia de la población civil, tales como los artículos alimenticios y las zonas agrícolas que los producen, las cosechas, el ganado, las instalaciones y reservas de agua potable y las obras de riego, con la intención deliberada de privar de esos bienes, por su valor como medios para asegurar la subsistencia, a la población civil o a la parte adversa, sea cual fuere el motivo, ya sea para hacer padecer hambre a las personas civiles, para provocar su desplazamiento, o con cualquier otro propósito»; y «3. Las prohibiciones establecidas en el párrafo 2 no se aplicarán a los bienes en él mencionados cuando una Parte adversa: a) utilice tales bienes exclusivamente como medio de subsistencia para los miembros de sus Fuerzas Armadas; o b) los utilice en apoyo directo de una acción militar, a condición, no obstante, de que en ningún caso se tomen contra tales bienes medidas cuyo resultado previsible sea dejar tan desprovista de víveres o agua a la población civil que esta se vea reducida a padecer hambre u obligada a desplazarse» .

El principio de distinción se refiere entonces a la acreditación de que haya un claro nexo entre el objeto en principio civil y las capacidades militares del enemigo para que pueda ser considerado objetivo militar y, en consecuencia, ser atacado.

El principio de distinción es una de las cuestiones más candentes en la actualidad en el ámbito del derecho internacional humanitario. En efecto, se ha reconocido que las AOC podrían ser particularmente útiles para tomar como objetivo determinados objetos civiles, por cuanto permiten a los beligerantes dirigirse contra objetivos que previamente estarían, en una perspectiva *tradicional*, más fuera de su alcance, como el sistema financiero o de sanidad, en tanto en cuanto se considere que contribuyen al esfuerzo bélico del enemigo, de forma que incluso la ciberguerra podría conducir a disponer de una mayor lista de objetivos legítimos comparada con los conflictos armados tradicionales[68]. Se trata de una consecuencia lógica de la regla de que un

[68] DROEGE, Cordula. *Op. cit*., p. 561.

objeto no puede ser civil y militar al mismo tiempo y, en consecuencia, de que redes básicas (de comunicaciones, de transporte, etc.) para la sociedad civil, en tanto en cuanto sean marginalmente usadas por las fuerzas armadas, se convierten en objetivos militares. Se produce, así, un riesgo cierto de guerra total que afecte directamente a la población por cuanto todo sea, en definitiva, objetivo militar. Como dice DROEGE[69]:

> «Las consecuencias humanitarias de esta situación son de la mayor relevancia para la protección de la población civil. En un mundo en que la mayor parte de las infraestructuras civiles, comunicaciones civiles, finanzas, economía y comercio se basan en la infraestructura cibernética internacional, la tentación es demasiado fuerte para los beligerantes para destruir estas infraestructuras. No hay necesidad de demostrar que una red bancaria se usa para acciones militares, o que una red eléctrica tiene uso dual. El dejar fuera de funcionamiento los cables principales, nodos, *routers* o satélites en los que estos sistemas se basan casi siempre será justificable por el hecho de que esos *routers* se usan para transmitir información militar y por tanto cualifican como objetivos militares».

Sin embargo, por otra parte, no podemos desconocer que los ciberataques pueden ser, por sí mismos preferibles a los ataques bélicos tradicionales[70]. Podemos considerar así una situación en la que uno de los beligerantes quiere cortar las vías de suministros por vía marítima del enemigo. Una opción sería bombardear el puerto de origen de los suministros, con el riesgo que ello supone de pérdida de vidas humanas de las personas que vivan cerca del puerto. Otra opción sería un ciberataque que, simplemente, deje inoperativo la infraestructura del puerto; esta opción alcanzaría el mismo objetivo que la bélica tradicional, pero sin riesgo de pérdidas de vidas humanas[71].

Otra consecuencia del principio de distinción, bien señalada por el general auditor Domínguez Bascoy es que las partes beligerantes, por principio, eviten el uso de ciberarmas indiscriminadas por naturaleza, como un *malware* que se replique sin control y cuyos efectos dañinos no se puedan limitar[72].

Reglas del *Manual de Tallin 2.0* sobre el principio de distinción en cuanto a los objetos:

---

69 Ibídem, p. 564.

70 Situación que reconoce el *Manual de derecho de la guerra* del Departamento de Defensa de EE. UU. Vid. Office of General Counsel – Department of Defence. «Department of Defence – Law of War Manual». Department of Defence, June 2015, updated December 2016, p. 1023.

71 Ejemplo considerado por SCHIMITT, Michael N. *Peacetime Cyber Responses... Op. cit*., p 277.

72 Véase el capítulo de DOMINGUEZ, Jerónimo. «Aplicación del derecho internacional humanitario a las operaciones en el ciberespacio». *Op. cit.*, p. 641.

Regla 93 – Distinción. El principio de distinción se aplica a los ciberataques.

Regla 99 – Prohibición de ataque de objetos civiles. Los objetos civiles son serán objeto de ciberataques. La ciberinfraestructura[73] puede ser objeto de ataque si cualifica como objetivo militar.

Regla 100 – Objetos civiles y objetivos militares. Los objetos civiles son todos los objetos que no son objetivos militares. Los objetivos militares son aquellos objetos que, por su naturaleza, localización, propósito o uso, realizan una contribución efectiva a la acción militar y cuya destrucción total o parcial, captura o neutralización, en las circunstancias que se den en el momento, ofrecen una ventaja militar relevante. La ciberinfraestructura puede cualificar como objetivo militar.

Regla 101 – Objetos usados para propósitos civiles y militares. La ciberinfraestructura usada para fines civiles y militares es un objetivo militar.

Regla 102 – Duda sobre el estatus de objetos. En caso de duda acerca de si un objeto y su ciberinfraestructura asociada que normalmente se dedica a fines civiles está siendo usada para realizar una contribución efectiva a la acción militar, la determinación de que así está siendo usada solo se puede realizar tras una cuidadosa valoración.

El principio de proporcionalidad

Otra regla básica del DIH es que las operaciones militares tengan por objetivo a combatientes, eximiéndose de los ataques a la población civil, y que sean proporcionadas en el sentido de que, cuando sea inevitable causar daños a población o bienes civiles, los daños que se causen a los mismos no sean excesivos en relación con el resultado global esperado[74]. Aquí las reglas de partida son:

- El art. 51. del Protocolo I Adicional a los Convenios de Ginebra de 1949, según el cual se prohíben los «ataques indiscriminados» y se considera indiscriminado el ataque «cuando sea de prever que causarán incidentalmente muertos y heridos entre la población civil, o daños a bienes de carácter civil, o ambas cosas, que serían excesivos en relación con la ventaja militar concreta y directa prevista»; y

[73] La nota 2 de la regla 99 remite al glosario para la definición de ciberinfraestructura, con la siguiente redacción: «Los dispositivos de comunicaciones, almacenamiento y computación sobre los que sistemas de información se construyen y operan».

[74] ESTADO MAYOR DEL EJÉRCITO. *OR7-004 Orientaciones – El Derecho de los Conflictos Armados*, doc. cit., pp. 4-3 y 2-5.

- El art. 57 del Protocolo I Adicional a los Convenios de Ginebra de 1949), según el cual «... quienes preparen o decidan un ataque deberán: [...] ii) tomar todas las medidas factibles en la elección de los medios y métodos de ataque para evitar o, al menos, reducir todo lo posible el número de muertos y de heridos que pudieran causar incidentalmente entre la población civil, así como los daños a los bienes de carácter civil; iii) abstenerse de decidir un ataque cuando sea de prever que causará incidentalmente muertos o heridos en la población civil, daños a bienes de carácter civil, que serían excesivos con la ventaja militar concreta y directa prevista...».

La cuestión de la proporcionalidad es una de las más complicadas en las AOC que tengan como objetivo ciberinfraestructura civil que cualifique como objetivo militar, y para la que probablemente no haya respuestas fáciles o universalmente válidas. En efecto, consideramos un ciberataque tipo *Denial of Service* contra un objetivo militar, ataque que interfiere negativamente con servicios de correo-e civiles. El efecto reflejo negativo sobre el servicio de correo-e civil no se toma en consideración para el análisis de si la ventaja militar obtenida es excesiva con respecto al daño causado. Sin embargo, la pérdida de funcionalidad del servicio de correo-e civil sí es un daño colateral con respecto a la regla de proporcionalidad[75]. Del mismo modo, parece lógico que en la regla de proporcionalidad se tome en cuenta no solo el daño primario, sino también el daño consecuencial[76]. Consideremos así un ciberataque sobre un sistema dual civil-militar de comunicaciones de emergencia, que resulte en que se quede sin servicio: en la medida en que la falta de servicio de comunicaciones de emergencia resulte en que se perjudique la atención a personas heridas, tal perjuicio deberá ser tenido en cuenta a la hora del juicio de proporcionalidad[77]. Por este motivo, parece que el principal factor de *defensa* de las ciberinfraestructuras frente a los ciberataques será precisamente el principio de proporcionalidad[78].

La cuestión, en todo caso, es ciertamente complicada. Un reciente análisis[79] sobre AOC reales concluyó que las que tuvieron lugar con ocasión del conflicto armado de Ucrania (ya fuera en cuanto afectación del sistema eléctrico o de uso del virús NotPetya –virus que encriptaba el contenido de los ordenadores y requería el pago de un rescate en bitcoins para desencriptar–) no habían respetado los principios de distinción y proporcionalidad, destacando

75 SCHIMITT, Michael N. *Peacetime Cyber Responses... Op. cit.,* p. 277.

76 En idéntico sentido DOMÍNGUEZ, Jerónimo, en el capítulo 8 del manual *Derecho de las operaciones aéreas*, pendiente de publicación, y en el mismo sentido el capítulo «Aplicación del derecho internacional humanitario a las operaciones en el ciberespacio» de DOMINGUEZ, Jerónimo. *Op. cit.,* p. 643.

77 SCHIMITT, Michael N. *Peacetime Cyber Responses... Op. cit.,* p. 278.

78 DROEGE, Cordula. *Op. cit.,* p. 566.

79 EFRONY, Dan y SHANY, Yuval. *Op. cit.,* p. 57.

señaladamente para ello que no se había limitado el ataque (con el virús NotPetya) a direcciones IP de Ucrania, lo que permitió que el ataque se extendiera a ordenadores de todo el mundo.

Reglas del *Manual de Tallin 2.0* sobre el principio de proporcionalidad:

> Regla 113 – Proporcionalidad. Se prohíbe un ciberataque del que pueda esperarse que cause una pérdida incidental de vida humana, daños a civiles, daños a objetos civiles, o a una combinación de todos estos, que fuera excesiva en relación con la concreta y directa ventaja militar esperada.
>
> Regla 117 – Precauciones con respecto a la proporcionalidad. Aquellos que planean o deciden ataques se abstendrán de decidir el lanzamiento de cualquier ciberataque del que se pueda esperar que cause daño incidental de vidas civiles, lesiones a civiles, daño a objetos civiles, o una combinación de estos, que sea excesivo con respecto a la concreta y directa ventaja militar esperada.

Probablemente la palabra clave de la regla 113 sea «excesiva». El comentario 8[80] de esta regla recuerda que el concepto «excesivo» no está definido en derecho internacional, y que a estos efectos lo relevante no es la cantidad de daño causado a civiles y sus propiedades, sino si el daño que puede esperar es excesivo con respecto a la ventaja militar prevista teniendo en cuenta las circunstancias presentes en el momento, lo que conduce a un análisis caso por caso. Merece la pena destacar igualmente que el comentario 5 de esta regla indica que las inconveniencias, irritación, estrés o daño que pueda causar una ciberoperación no suponen un «daño incidental» para tener en cuenta.

Protección de personas civiles

Otra regla básica del derecho internacional humanitario es que las operaciones militares tengan por objetivo a combatientes, exonerándose de los ataques a la población civil[81]. Aquí las reglas de partida son:

- El art. 48 del Protocolo I Adicional a los Convenios de Ginebra de 1949, según el cual «a fin de garantizar el respeto y la protección de la población civil y de los bienes de carácter civil, las partes en conflicto harán distinción en todo momento entre población civil y combatientes, y entre bienes de carácter civil y objetivos militares y, en consecuencia, dirigirán sus ataques únicamente contra objetivos militares».

80 VV. AA. *Tallin Manual 2.0... Op. cit.,* p. 473.

81 ESTADO MAYOR DEL EJÉRCITO. *OR7-004 Orientaciones – El Derecho de los Conflictos Armados*, doc. cit. pp. 1-10 y 3-2.

- El art. 50 del Protocolo I Adicional a los Convenios de Ginebra de 1949, según el cual «1. Es persona civil cualquiera que no pertenezca a una de las categorías de personas a que se refieren el artículo 4, A. 1), 2), 3), y 6), del III Convenio, y el artículo 43 del presente Protocolo [resumidamente, miembros de las Fuerzas Armadas, de milicias, de movimientos de resistencia organizada, o población civil que toma las armas]. En caso de duda acerca de la condición de una persona, se la considerará como civil. 2. La población civil comprende a todas las personas civiles. 3. La presencia entre población civil de personas cuya condición no responda a la definición de persona civil no priva a esa población de su calidad de civil».
- El art. 51 del Protocolo I Adicional a los Convenios de Ginebra de 1949, según el cual «1. La población civil y las personas civiles gozarán de protección general contra los peligros procedentes de operaciones militares. Para hacer efectiva esta protección, además de las otras normas aplicables de derecho internacional, se observarán en todas las circunstancias las normas siguientes. 2. No serán objeto de ataque la población civil como tal ni las personas civiles. Quedan prohibidos los actos o amenazas de violencia cuya finalidad principal sea aterrorizar a la población civil. 3. Las personas civiles gozarán de la protección que confiere esta Sección, salvo si participan directamente en las hostilidades y mientras dure tal participación...».

Los ciberataques tienen, en cuanto al factor subjetivo del objetivo, dos peculiares características: por un lado, el objetivo habitual no será tanto una persona como un objeto, y por otro lado, que por las especiales características de los operadores en el ámbito informático, no es descartable la intervención de personas ajenas a las fuerzas armadas en acciones militares cibernéticas[82], lo que requiere analizar en qué momento esas personas pierden su protección bajo el derecho internacional humanitario.

Reglas del *Manual de Tallin 2.0* relativas a ataques contra personas:

> Regla 94 – Prohibición de atacar civiles. La población civil, como tal, así como civiles individualmente considerados, no serán objeto de ciberataque.
>
> Regla 95 – Duda sobre el estatus de las personas. En caso de duda acerca de si una persona es civil, esa persona será considerada como civil.

[82] Se trata de hecho de una cuestión expresamente reconocida en el *Law of War Manual* del Departamento de Defensa de EE. UU., que recoge en su apartado 16.5.5 la posibilidad de que «personal civil participe en ciberoperaciones, incluyendo acciones que puedan constituir una participación directa en las hostilidades», con la lógica consecuencia de que «civiles que tomen una participación directa en las hostilidades pierden la protección contra ser objeto de ataque»: Office of General Counsel – Department of Defence, *Law of War Manual*, doc. cit., pp. 1024 y 1025.

> Regla 96 – Personas como objetos que pueden ser legalmente atacadas. Las siguientes personas pueden ser objeto de ciberataques: (a) miembros de las Fuerzas Armadas; (b) miembros de grupos armados organizados; (c) civiles, si y por el tiempo que tomen directamente parte en las hostilidades, y (d) en un conflicto armado internacional, los participantes de un levantamiento en masa.
>
> Regla 97 – Civiles participando directamente en las hostilidades. Los civiles disfrutan de protección contra ataque excepto y mientras participen directamente en las hostilidades.

Se debe tener especialmente en cuenta que, no obstante la aparente claridad de las normas del *Manual de Tallín 2.0*, existen visiones contrapuestas acerca de cuándo un miembro de un grupo armado organizado puede ser objeto de ciberataque. Hay una visión según la cual la participación reiterada en las actividades de ese grupo armado organizado legitima su ataque en cualquier momento, y hay otra visión[83] según la cual ese miembro solo puede ser atacado si desarrolla una «función continua de combate»[84].

Del mismo modo, y con respecto a cuándo se considera que un civil toma participación directa en las hostilidades, los comentarios a la regla 97 del *Manual de Tallín 2.0* remiten a la *Guía para interpretar la noción de participación directa en las Hostilidades según el derecho interncional humanitario* del Comité Internacional de la Cruz Roja[85]. Esta guía toma en consideración tres elementos para responder a esa pregunta:

1) Umbral de daño. El acto del participante debe tener o pretender efectos adversos sobre las capacidades u operaciones militares del enemigo, o causar la muerte, o daños corporales o la destrucción de personas o cosas protegidas. Ese acto puede ser por acción (por ejemplo, una ciberoperación que afecte negativamente a los sistemas de mando y control) o por omisión (por ejemplo, mantener ciberdefensas pasivas sobre activos militares cibernéticos).
2) Causalidad directa. Debe existir un nexo causal directo entre la acción/omisión en cuestión y el daño pretendido o producido.
3) Nexo beligerante. La acción/omisión debe estar directamente relacionada con las hostilidades.

Nótese, finalmente, que a diferencia de lo que ocurre con respecto a los miembros de grupos armados organizados, un civil que tome participación

---

83 Basada en MELZER, Nils. *Guía para interpretar la noción de participación directa en las hostilidades según el derecho internacional humanitario*. Ginebra: Comité Internacional de la Cruz Roja, 2009, p. 35.

84 Véase el comentario 4 en VV. AA. *Tallin Manual... Op. cit*. p. 426.

85 MELZER, Nils, op. cit., pp. 46 y siguientes.

directa en las hostilidades solo puede ser objeto de un ciberataque mientras esté realizando dicha participación directa[86].

Prohibición de la perfidia

Otra regla básica del derecho internacional humanitario es la de la prohibición de la perfidia o *traición*[87]. Aquí la regla de partida es:

- El art. 37. del Protocolo I Adicional a los Convenios de Ginebra de 1949, según el cual «1. Queda prohibido matar, herir o capturar a un adversario valiéndose de medios pérfidos. Constituirán perfidia los actos que, apelando a la buena fe de un adversario con intención de traicionarla, den a entender a éste que tiene derecho a protección, o que está obligado a concederla, de conformidad con las normas de derecho internacional aplicables en los conflictos armados. Son ejemplos de perfidia los actos siguientes:

  a) Simular la intención de negociar bajo bandera de parlamento o de rendición;

  b) Simular una incapacitación por heridas o enfermedad;

  c) Simular el estatuto de persona civil, no combatiente; y

  d) Simular que se posee un estatuto de protección, mediante el uso de signos, emblemas o uniformes de las Naciones Unidas o de Estados neutrales o de otros Estados que no sean Partes en el conflicto.

  2. No están prohibidas las estratagemas. Son estratagemas los actos que tienen por objeto inducir a error a un adversario o hacerle cometer imprudencias, pero que no infringen ninguna norma de derecho internacional aplicable en los conflictos armados, ni son pérfidos ya que no apelan a la buena fe de un adversario con respecto a la protección prevista en ese derecho. Son ejemplos de estratagemas los actos siguientes: el camuflaje, las añagazas, las operaciones simuladas y las informaciones falsas».

Si hay un ámbito de los conflictos modernos en los que se presenten oportunidades para la perfidia y las estratagemas son las AOC. Un claro ejemplo de estratagema podría ser la alteración de la base de datos del enemigo, a resultas del cual se envíen mensajes a su cuartel general de supuestas unidades subordinadas o viceversa. Del mismo modo, según como se implemente una AOC, se podría incurrir en perfidia. Un ejemplo podría basarse en los códigos y señales establecidos por la Unión

[86] Véase el comentario 8 en VV. AA. *Tallin Manual 2.0... Op. cit.,* p. 431.

[87] ESTADO MAYOR DEL EJÉRCITO. *OR7-004 Orientaciones – El Derecho de los Conflictos Armados*, doc. cit., p. 3-11.

Internacional de Telecomunicaciones, la Organización Internacional de Aviación Civil y la Organización Marítima Internacional para su uso por unidades y transportes sanitarios para su identificación como tales. Si una AOC afecta a los sistemas de radar o señales de un beligerante de forma que identifique como transportes sanitarios a objetos que no lo son, se trataría aparentemente de un claro caso de perfidia[88]. Por este motivo, parece clara la conveniencia de un cuidadoso análisis jurídico previo a una AOC[89].

Reglas del *Manual de Tallin 2.0* sobre perfidia y estratagemas:

> Regla 122 – Perfidia. En la conducción de hostilidades que impliquen ciberoperaciones, está prohibido matar o lesionar a un adversario a través de la perfidia. Actos que invitan la confianza de un adversario en creer que él o ella tienen derecho a, o están obligados a conceder, protección bajo el derecho de los conflictos armados, con la intención de traicionar esa confianza, constituyen perfidia.
>
> Regla 123 – Estratagemas. Se permiten las ciberoperaciones que cualifiquen como estrategemas.

Interesantemente, el comentario 2 a la regla 123 del *Manual de Tallín 2.0* facilita diversos ejemplos de ciberestratagemas que, en cuanto tales, son legítimas bajo el derecho de los conflictos armados[90]:

1) La creación de sistemas informáticos simulados, que aparenten fuerzas inexistentes.
2) La transmisión de información falsa que cause a un oponente creer equivocadamente que una operación va a empezar o está en marcha.
3) La utilización de falsos identificadores o sistemas informáticos (*honeynets* o *honeypots*).
4) Ciberataques simulados que no violen la prohibición de ciberataques cuyo objetivo primario sea causar el terror entre la población civil.
5) Emisión de órdenes falsas supuestamente emitidas por los mandos enemigos.
6) Actividades de guerra psicológica.
7) Transmisión de información falsa cuyo propósito es que sea interceptada.
8) Uso de códigos, señales y contraseñas enemigas.

---

88 SMYTH, Vito. *Op. cit.,* p. 16.

89 Véase el apartado Cibertargeting & ROE de este capítulo..

90 Véase el comentario 2 en VV. AA. *Tallin Manual 2.0... Op. cit.* p. 495.

Medios y métodos

Abundando en lo establecido en el apartado Marco legal del empleo de las Fuerzas Armadas de este capítulo, es doctrina oficial[91] de las Fuerzas Armadas españolas[92] que «El empleo y actuación de las FAS deben ajustarse a principios de legalidad y legitimidad, establecidos en la Constitución Española, en la legislación nacional vigente y en los acuerdos internacionales suscritos por España, en especial la Carta de las Naciones Unidas». Consecuentemente, debe evitarse la causación de sufrimientos innecesarios y de males superfluos, o el empleo de medios y métodos que causen o se prevea que puedan causar daños extensos, duraderos y graves al medio ambiente natural, o recurrir al hambre como método de guerra contra la prohibición civil[93]. Aquí las reglas de partida están contenidas en la costumbre internacional y en los diversos tratados internacionales que componen el derecho internacional humanitario[94].

Probablemente la principal limitación legal en cuanto a los métodos a usar en las AOC es la prohibición de los ataques indiscriminados establecida en el artículo 51 del Protocolo I Adicional a los Convenios de Ginebra de 1949. La mejor doctrina[95] ha descrito como supuestos de ciberataques indiscriminados, y por tanto prohibidos, (i) lanzar un ciberataque sin intentar siquiera dirigirlo a una particular ciberinfraestructura militar que cualifique como objetivo militar, (ii) utilizar *malware* diseñado para su uso contra una red militar cerrada en una red militar que, sin embargo, esté conectada a una red civil, y (iii) atacar ciberinfraestructura usada para fines civiles y militares cuando fuera posible inutilizar o destruir únicamente la parte militar de esa infraestructura. Otro claro ejemplo de ciberataque indiscriminado sería la utilización de virus informáticos que se autorreplicaran y se expandieran sin control una vez lanzados[96].

---

91 ESTADO MAYOR DE LA DEFENSA. *Publicación Doctrinal Conjunta PDC-01(A) «Doctrina para el empleo de las Fuerzas Armadas»*, doc. cit., p. 44.

92 Y no solo de las Fuerzas Armadas españolas. El *Law of War Manual del Departamento de Defensa de EE. UU.* establece en su apartado 16.2.2 que «Si no se aplica ninguna regla específica, los principios de la ley de la guerra forman la guía general de conducta durante la guerra, incluyendo la conducta durante ciberoperaciones. Por ejemplo, bajo el principio de humanidad, se debe evitar en las ciberoperaciones el sufrimiento, lesión o destrucción innecesaria para alcanzar un propósito militar legítimo». OFFICE OF GENERAL COUNSEL – DEPARTMENT OF DEFENCE, *Law of War Manual*, doc. cit., p. 1014.

93 ESTADO MAYOR DEL EJÉRCITO. *OR7-004 Orientaciones – El derecho de los conflictos armados*, doc. cit., pp. 2-4, 2-5, 3-2 y 3-3.

94 Sin ánimo de ser exhaustivo, los artículo 22 y 23 del Reglamento Relativo a las Leyes y Costumbres de la Guerra Terrestre (H.IV.R), arts. 35, 37, 40, 51, 54 y 57 del Protocolo I Adicional a los Convenios de Ginebra de 1949, etc.

95 SCHMITT, Michael N. *Peacetime Cyber Responses… Op. cit.*, p. 275.

96 DROEGE, Cordula. *Op. cit.,* p. 570.

La conclusión, por tanto, y como ya habíamos dejado apuntado anteriormente[97], es que parece clara la conveniencia de un cuidadoso análisis jurídico previo a una AOC. Al respecto, el *Manual de Tallin 2.0* establece diversas reglas sobre medios y métodos.

Reglas del *Manual de Tallin 2.0* sobre medios y métodos:

> Regla 114 – Cuidado constante. Durante las hostilidades que impliquen ciberoperaciones, se tomará un cuidado constante en preservar a la población civil, a las personas civiles y a los bienes civiles.
>
> Regla 115 – Verificación de objetivos. Quienes preparen o decidan un ciberataque harán todo lo que sea factible para verificar que los objetivos a ser atacados no sean ni civiles ni objetos civiles y que no estén sujetos a especial protección.
>
> Regla 116 – Elección de medios y métodos. Quienes preparen o decidan un ciberataque tomarán todas las precauciones factibles en la elección de medios o métodos empleados en tal ataque, con el propósito de evitar, y en cualquier evento reducir, lesiones incidentales a civiles, la pérdida de vidas humanas, y el daño o destrucción a objetos civiles.
>
> Regla 117 – Precauciones con respecto a la proporcionalidad. Quienes preparen o decidan ataques se abstendrán de decidir cualquier ciberataque del que se pueda esperar la pérdida incidental de vidas civiles, lesiones a civiles, daños a objetos civiles, o una combinación de todo ello, que sea excesivo en relación con la concreta y directa ventaja militar prevista.
>
> Regla 118 – Elección de objetivos. Para los Estados que sean Parte del Protocolo Adicional I, cuando se pueda elegir entre varios objetivos militares para obtener una ventaja militar equivalente, se optará por el objetivo cuyo ciberataque se prevea que cause el menor peligro para vidas civiles y objetos civiles.
>
> Regla 119 – Cancelación o suspensión de un ataque. Quienes preparen o decidan un ciberataque cancelarán o suspenderán el ataque si se advierte que a) el objetivo no es militar o está sujeto a protección especial, b) es de prever que el ataque cause, directa o indirectamente, perdida incidental de vidas civiles, lesiones a civiles, daños a objetos civiles, o una combinación de todo ello, que sea excesivo en relación con la concreta y directa ventaja militar prevista.
>
> Regla 120 – Advertencias. Se dará aviso anticipado y eficaz de un ciberataque que pueda afectar a la población civil, salvo que las circunstancias no lo permitan.

[97] Véase el apartado Protección de personas civiles de este capítulo.

> Regla 121 – Precauciones contra los efectos de un ciberataque. Las partes en un conflicto armado tomarán, hasta donde sea factible, las precauciones necesarias para proteger de los peligros resultantes de ciberataques a la población civil, a personas civiles y a objetos civiles que se encuentren bajo su control.

Un ejemplo de la aplicación de la regla 116 es la que ilustra la nota 6 de la misma[98], que consiste en una operación de inserción de *malware* en un sistema militar cerrado a través de un dispositivo de memoria de una persona que trabaje en ese sistema militar cerrado. El ciberatacante debe valorar la posibilidad de que ese dispositivo de memoria también se introduzca en ordenadores conectados a una red civil y que, por tanto, cause daños colaterales. En tal caso, podría ser posible utilizar un *malware* distinto que minimice la posibilidad de daños colaterales.

Nótese, por otra parte, que las obligaciones contenidas en las anteriores reglas se refieren respectivamente tanto a atacantes como a atacados, refiriéndose las reglas 114 a 120 al atacante y la 121 al atacado[99]. Ello supone que los Estados deben adoptar las medidas defensivas oportunas frente a eventuales ciberataques, lo que abarca desde la separación de las ciberredes militares de las civiles hasta segregar los sistemas de las infraestructuras críticas de internet, pasando por tomar medidas por anticipado para asegurar la rápida reparación de los sistemas que caigan como consecuencia de ciberataques, etc.[100].

Aspectos singulares del cibertargeting

Cibertargeting & ROE

El *targeting* es el proceso por el que se eligen determinados blancos sobre las que se aplican ciertas reglas de enfrentamiento[101] (ROE) habida cuenta de la trascendencia de aquellos[102]. En España este proceso en la actualidad

98 VV. AA. *Tallin Manual 2.0... Op. cit.,* p. 480.

99 Véase el comentario 3 de la regla 121 en VV. AA. *Tallin Manual 2.0... Op. cit*., p. 488.

100 Una exhaustiva visión de la resilencia frente a las ciberamenazas se puede encontrar en el capítulo 3 de esta publicación, a cargo de la Dra. De Tomas Morales, al que nos remitimos íntegramente.

101 Las reglas de enfrentamiento se pueden definir como «normas de carácter operativo ajustadas a derecho que proporcionan a los comandantes de todos los escalones de mando y a los miembros de las unidades, guía y respaldo para el empleo de la fuerza determinando las circunstancias, condiciones, grado y forma en las que se puede, o no, aplicar»: Estado Mayor de la Defensa, *Publicación Doctrinal Conjunta PDC-01(A) «Doctrina para el empleo de las Fuerzas Armadas»*, doc cit., p. 96.

102 ALIA, Miguel, en el capítulo «El targeting» en PÉREZ DE FRANCISCO, Eugenio (coord.). *Manual de Derecho Operativo*. Madrid: Marcial Pons Ediciones Jurídicas y Sociales S. A., 2015, p. 291.

se halla ciertamente juridificado[103], y por eso se sostiene en la mejor doctrina que la función del asesor jurídico «en esta actividad es muy importante, porque debe velar por el cumplimiento de la legalidad sobre ataques. Ello implica la aplicación práctica del derecho de los conflictos armados y el dominio de las normas procedimentales sobre el *targeting*»[104].

La doctrina estadounidense[105] considera que hay tres aspectos singulares en el *targeting* aplicado a las AOC: en primer lugar, que las cibercapacidades propias pueden ser una opción viable para atacar determinados objetivos; en segundo lugar, que una AOC puede ser la opción preferible en algunos casos habida cuenta de que puede ofrecer una baja probabilidad de detección y/o no causar daños físicos; y en tercer lugar, que los efectos que produzca la AOC pueden superar –de forma intencionada o no– los previstos, con lo que ello implica de potencial respuesta por la parte atacada. Recordemos, en este sentido, que decíamos que el ciberespacio está formado por cuatro capas interdependientes: (i) la capa física o de *hardware*, (ii) la capa lógica o de *software*, (iii) la capa de contenidos, consistente en la información captada, almacenada o procesada, y (iv) la capa personal, consistente en las personas físicas o jurídicas que actúan en el ciberespacio, y que es en esas capas o contra esas capas contra las que se pueden realizar operaciones en el ciberespacio[106]. Pues bien, precisamente esa correlación es lo que hace que se necesite una potente capacidad de mando y control para, en el ámbito del *targeting*, identificar, correlacionar, coordinar y resolver los conflictos que se planteen entre las cuatro capas del ciberespacio como consecuencia de la AOC[107]. Y precisamente por la complejidad de la ejecución de las operaciones, puede considerarse[108] igualmente que las ROE sean el producto de la consideración conjunta del marco jurídico de las operaciones, de las instrucciones políticas dadas para su desarrollo, y de las consideraciones operativas[109].

Una vez que hemos visto en el capítulo anterior las ciberlimitaciones que se derivan de los principios generales del derecho internacional humanitario,

---

103 Los parámetros legales del *targeting* se van a referir a la misión, al blanco, a las fuerzas propias, a los resultados y al armamento, incluyendo daños colaterales, lo que requiere una potente visión de conjunto. Vid. ALIA, Miguel. *Op. cit.,* pp. 296 y 297.

104 ALIA, Miguel. *Op. cit.,* p. 295.

105 Vid. US JOINT CHIEFS OF STAFF, doc. cit., p. IV-8, y HEADQUARTERS. Department of the Army, doc. cit., p. 3-12.

106 CORN, Gary P. *Op. cit.,* p. 9. Véase también DOMÍNGUEZ, Jerónimo, en el capítulo 8 del manual «Derecho de las Operaciones Aéreas», pendiente de publicación.

107 Vid. JOINT CHIEFS OF STAFF, doc. cit., p. IV-9.

108 ALIA, Miguel. *Op. cit.*, p. 249.

109 Para una visión de los problemas que surgen para el establecimiento de ciberROE por las diferencias entre los ámbitos físicos tradicionales y el cibernético véase KEHLER, C. Robert; LIN, Herbert and SULMEYER, Michael. «Rules of engagement for cyberspace operations: a view from the USA». *Journal of Cybersecurity*, 3(1), 2017, pp. 69-80.

a continuación, trataremos determinados aspectos singulares del *cibertargeting* referidos a los objetivos de las AOC, dando aquí por reproducidas las reglas 114 y siguientes del *Manual de Tallín 2.0* que hemos citado en el apartado Medios y métodos de este capítulo.

Objetos civiles como objetivo

Recordemos que solo pueden ser atacados los objetos que sean militares o que, no siéndolo, por su naturaleza, ubicación, finalidad o utilización contribuyan eficazmente a la acción militar o cuya destrucción total o parcial, captura o neutralización ofrezca en las circunstancias del caso una ventaja militar definida[110]. Ya hemos tratado previamente esta cuestión en el apartado relativo al principio de distinción, pero ahora merece la pena profundizar en la cuestión de la contribución eficaz a la acción militar como circunstancia legitimadora de un ciberataque.

Esa contribución eficaz a la acción militar puede ser directa, como sería el caso de una fábrica civil de armas, como caso prototípico de objetivo militar legítimo[111], o indirecta, en cuyo caso se entra de lleno en una zona de incertidumbre en lo relativo a si tal contribución indirecta convierte al objeto en objetivo militar legítimo. Un ejemplo de contribución eficaz indirecta sería el de los sistemas informáticos de una determinada industria de un Estado que a su vez depende de los ingresos o impuestos derivados de esa industria para mantener su capacidad bélica. Pensemos, por ejemplo, en un hipotético Estado centroeuropeo cuya principal industria en términos de generación de ingresos, impuestos y PIB sea su sector bancario y financiero. La inutilización o destrucción de los sistemas informáticos de su sistema bancario y financiero a través de un ciberataque deberían producir un impacto adverso relevante en la capacidad bélica de dicho Estado. No parece haber ahora mismo consenso acerca de si la contribución eficaz indirecta convierte al objeto en objetivo legítimo o no. Por un lado, los EE. UU. parecen considerar oficialmente que sí[112], mientras que en el ámbito del Comité Internacional de la Cruz Roja parece sostenerse la opinión contraria. La directora de la Unidad de Derecho Operativo tiene escrito que «El daño a la economía civil del enemigo, y a las capacidades de investigación y desarrollo en cuanto tales, nunca está permitido bajo el derecho internacional humanitario, con independencia de la ventaja militar prevista, y con independencia de la duración del conflicto. En otro caso, no habría límites a la actividad bélica pues virtualmente toda la economía de un país se puede considerar que contribuya a

110 Cfr. art. 52.2 del Protocolo I Adicional a los Convenios de Ginebra de 1949.

111 SCHMITT, Michael N. *Peacetime Cyber Responses… Op. cit.,* p. 269.

112 Vid. OFFICE OF GENERAL COUNSEL – DEPARTMENT OF DEFENCE. *Law of War Manual*, doc cit., p. 219.

la acción bélica»[113]. La mayoría de los expertos que redactaron el *Manual de Tallin 2.0* parecen alinearse con esta segunda visión por cuanto consideran que la contribución indirecta no convierte al objeto en objetivo legítimo por tener una vinculación excesivamente remota con el esfuerzo bélico[114]. Como puede verse, el color gris es de generosa aplicación en los ciberataques, y probablemente la opinión de cada pintor dependa precisamente de sus niveles de cibercapacidad, ya sean ofensivos o defensivos.

Colaboradores civiles como objetivo. Personal de empresas que participen en cooperación público-privada (public-private partnership)

Ya hemos hablado en el apartado Protección de personas civiles sobre el régimen de protección de los civiles bajo el derecho internacional humanitario frente a ciberataques. Hay también una singular zona de incertidumbre en esta cuestión derivada de las especiales características del ciberespacio, que hacen que sea no solo posible, sino incluso probable, que personal civil tome parte en acciones en el ciberespacio, ya sea como parte de la administración civil de un Estado[115] (piénsese por ejemplo en el personal de la National Security Agency de EE. UU. o del Centro Criptológico Nacional de España), ya sea como empleados de empresas privadas ligadas contractualmente con un Estado para la prestación de servicios (piénsese por ejemplo en personal de ISDEFE o de Indra en España).

La solución a esta cuestión en el *Law of War Manual* del Departamento de Defensa de EE. UU. es reconocer la posibilidad de que personal civil autorizado (y que por tanto está legitimado para tener la condición de prisionero de guerra) participe en ciberoperaciones, incluyendo acciones que puedan constituir una participación directa en las hostilidades, con la lógica consecuencia de que «civiles que tomen una participación directa en las hostilidades pierden la protección contra ser objeto de ataque»[116].

En el *Manual de Tallín 2.0* los expertos, al analizar la regla 96 (personas como objetos que pueden ser legalmente atacadas) distinguen tres casos relativos a personal civil que forme parte de ciberoperaciones[117]:

a) Contratista individual (trabajador autónomo en España) de un Estado. Solo puede ser atacado mientras participe directamente en las hostilidades.

---

113 DROEGE, Cordula. *Op. cit.,* p. 568.

114 VV. AA. *Tallin Manual 2.0...,* p. 441.

115 LIBICKI, Martin C. *Cyberdeterrence and Cyberwar*. Rand Corporation, 2009, p. 155.

116 Vid. OFFICE OF GENERAL COUNSEL – DEPARTMENT OF DEFENCE. *Law of War Manual,* doc. cit., pp. 1024 y 1025.

117 VV. AA. *Tallin Manual 2.0...*, p. 427.

b) Empleado de empresa contratada por un Estado. Puede ser atacado en cualquier momento por considerarse que forma parte de un grupo armado organizado o por analogía con tal consideración.

c) Funcionarios o empleados civiles. Puede ser atacado en cualquier momento si se considerase que forman parte de un grupo armado organizado, lo que parecería deducirse del tipo de organización en el que estuvieran encuadrados (típicamente, seguridad o inteligencia; por ejemplo, en España, el CNI). En caso contrario, solo pueden ser atacados mientras participen directamente en las hostilidades.

Ciertamente, en el caso estrictamente español, no parece tener mucho sentido hacer de peor condición a un empleado por cuenta ajena que a un empleado por cuenta propia, por lo que probablemente esta sea una cuestión incierta tanto a nivel nacional como internacional.

El dato en sí mismo como objetivo.

¿Es el dato, en sí mismo, un objeto, y por tanto, es *sujeto* de la regulación del derecho internacional humanitario? Esta pregunta no es baladí; pensemos en una AOC que elimine de forma irrecuperable el contenido de una base de datos cuyo contenido sea muy relevante para un Estado, como por ejemplo la base de datos de las autoridades tributarias. Si los datos no son un «objeto», entonces esa AOC no cualificará siquiera como ataque.

La respuesta a la pregunta no es unívoca, y probablemente dependa de la tradición jurídica de cada Estado. La mayoría de los expertos que redactaron el *Manual de Tallin 2.0* han sostenido que los datos como tales no son un «objeto» dado que, en su opinión, un «dato» es intangible y no se corresponde con el significado ordinario de la palabra «objeto», y además tampoco se corresponde con la explicación dada al término por los *Comentarios a los Protocolos Adicionales* hecho por el Comité Internacional de la Cruz Roja en 1987. A su vez, la minoría de los expertos ha mantenido la opinión contraria argumentando que, en caso contrario, serían *legales* ataques altamente disruptivos sobre población civil, como sería en el caso de la eliminación de las bases de datos de pensionistas[118]. Michael N. Schmitt, probablemente el principal tratadista estadounidense sobre la materia, reconoce que ambas opiniones tienen al menos parte de razón, pero parece inclinarse conceptualmente a favor de la posición de la minoría, y propone que se reconozca en el futuro que ciertas funciones civiles esenciales que se basen en el tratamiento de datos merezcan una especial protección bajo el derecho internacional humanitario[119].

118 VV. AA. *Tallin Manual 2.0*..., p. 437.

119 SCHMITT, Michael N. *Peacetime Cyber Responses*... *Op. cit.,* p. 270.

Desde el punto de vista español, la cuestión de si un dato es un «objeto» probablemente pueda ser respondida afirmativamente. Pensemos en primer lugar que el diccionario de la Real Academia Española define como «objeto», en su primera acepción: «Todo lo que pueda ser materia de conocimiento o sensibilidad de parte del sujeto, incluso este mismo», y solo en su sexta acepción, «cosa»[120]. Además, España tiene una regla especial de interpretación de las normas en su Código Civil, cuyo artículo 3 dispone que «Las normas se interpretarán según el sentido propio de sus palabras, en relación con el contexto, los antecedentes históricos y legislativos, y la realidad social del tiempo en que han de ser aplicadas, atendiendo fundamentalmente al espíritu y finalidad de aquéllas». Dado que los Convenios de Ginebra son del año 1949, y que el Protocolo Adicional I a los mismos es del año 1977, años en los que la informática y cibernética no estaban tan desarrolladas como ahora mismo, y que su espíritu y finalidad son la protección de civiles y combatientes según su estatus, parece razonable interpretar que se pueda reconocer a los datos como «objetos» habida cuenta de la realidad social actual y del espíritu y finalidad de las normas del derecho internacional humanitario. En este mismo sentido, el Código Penal tipifica en el artículo 264 del Código Penal el borrado, alteración, supresión de «datos informáticos», artículo que está dentro del capítulo IV («De los daños») del título XIII («Delitos contra el patrimonio y contra el orden socioeconómico») del libro II («Delitos y sus penas»), lo que parece hacer equivalente los datos a objetos materiales.

En todo caso, lo cierto es que no se puede considerar la cuestión del dato como objeto, o no, desde una perspectiva exclusivamente nacional. Por eso, corresponderá a los Estados determinar convencional o consuetudinariamente si los datos son objetos a los efectos de *targeting* en el contexto de un conflicto armado[121].

Productos sanitarios y objetivos militares

Parece claro que una operación consistente en manipular medicamentos para que estos en vez de curar tengan efectos letales sería obviamente ilegal[122] pero ¿qué ocurre si en lugar de la manipulación de medicamentos lo que se hace es manipular telemáticamente productos sanitarios, para matar o lesionar a combatientes (por ejemplo, un comandante que tenga un marcapasos)? Para analizar la cuestión debemos tener en cuenta en primer lugar la diferencia que hay entre «productos sanitarios» y «medicinas».

---

120 *Diccionario de la Real Academia Española de la Lengua*. www.dle.rae.es, accedido el 26 de abril de 2019.

121 McCORMACK, Tim. «International Humanitarian Law and the Targeting of Data». *International Law Studies*. Volume 94. Stockton Center for the Study of International Law, US Naval War College, 2018, p. 239.

122 Cfr. Artículo 23 del Reglamento relativo a las Leyes y Costumbre de las Guerra Terrestre; artículo 8.2.b) del Estatuto de Roma de la Corte Penal Internacional.

Las medicinas son sustancias medicinales con propiedades preventivas, de diagnosis, tratamiento, paliativas o de curación de enfermedades. Un marcapasos no puede incluirse en esta categoría ya que no es una sustancia medicinal. Esto se fundamenta por la Ley 29/2006, de 26 de julio, de Uso Racional de Medicamentos y Productos Sanitarios. Esta Ley claramente distingue entre medicamentos y productos sanitarios en su artículo 8. Considera medicamento de uso humano a «toda sustancia o combinación de sustancias que se presente como poseedora de propiedades para el tratamiento o prevención de enfermedades en seres humanos o que pueda usarse en seres humanos o administrarse a seres humanos con el fin de restaurar, corregir o modificar las funciones fisiológicas ejerciendo una acción farmacológica, inmunológica o metabólica, o de establecer un diagnóstico médico», y considera producto sanitario a «cualquier instrumento, dispositivo, equipo, programa informático, material u otro artículo, utilizado solo o en combinación, incluidos los programas informáticos destinados por su fabricante a finalidades específicas de diagnóstico y/o terapia y que intervengan en su buen funcionamiento, destinado por el fabricante a ser utilizado en seres humanos con fines de 1.º diagnóstico, prevención, control, tratamiento o alivio de una enfermedad, 2.º diagnóstico, control, tratamiento, alivio o compensación de una lesión o de una deficiencia, 3.º investigación, sustitución o modificación de la anatomía o de un proceso fisiológico, 4.º regulación de la concepción, y que no ejerza la acción principal que se desee obtener en el interior o en la superficie del cuerpo humano por medios farmacológicos, inmunológicos ni metabólicos, pero a cuya función puedan contribuir tales medios». Esta distinción entre medicamento y producto sanitario también se recoge en el Real Decreto 1591/2009, de 16 de octubre, que regula los productos sanitarios y, específicamente, por el Real Decreto 1616/2009, de 26 de octubre, por el que se regulan los productos sanitarios activos, que trasponen los reglamentos comunitarios en la materia. Habida cuenta entonces de la distinción legal entre medicamentos y productos sanitarios, no está clara que la protección a los medicamentos sea extensible a los productos sanitarios.

El comentario 3 de la regla 132 del *Manual de Tallin 2.0*[123] señala que «los datos personales médicos requeridos para el tratamiento de pacientes están igualmente protegidos contra su modificación, borrado, o cualquier otra acción por medios cibernéticos que afectase negativamente a su cuidado, con independencia de que esa acción constituya un ciberataque». Parecería, entonces, que la manipulación de los datos de los productos sanitarios se encuentra prohibida, con independencia de que pueda ser discutible considerar que un marcapasos implantado en un paciente (el comandante, en nuestro ejemplo) sea «parte integral» de una «unidad médica». A su vez, curiosa-

[123] La regla 132 establece que los ordenadores, redes informáticas y datos que formen parte integral de las operaciones o gestión de unidades y transportes médicos deben ser respetados y protegidos, y en particular no pueden ser objeto de ataque. Vid. VV. AA. *Tallin Manual 2.0*..., p. 515.

mente, el comentario 9 de la regla 122[124] del *Manual de Tallin 2.0*, relativo a la perfidia, indica que mientras una parte (mayoritaria) de los expertos consideran que el uso de un *malware* utilizado para alterar el marcapasos del comandante sería un acto de perfidia, dado que ese *malware* se habría hecho pasar como generado por una fuente médica legítima para ser aceptado por el marcapasos, otra parte de los expertos han considerado que tal acción no sería un acto de perfidia dado que el *abuso de la confianza* propio de la perfidia presupone que la confianza la otorga una persona y no una máquina[125].

En nuestra opinión, el *Manual de Tallin 2.0* no *regula* adecuadamente el impacto del uso de productos sanitarios desde la perspectiva del derecho internacional humanitario. Habida cuenta de la diferencia legal existente entre medicamentos y productos sanitarios, habría sido deseable su equiparación en *Tallin 2.0* a los efectos del derecho internacional humanitario por los fines últimos de este, pues tanto los medicamentos como los productos sanitarios tienen como objetivo último el cuidado de la persona frente a enfermedades. De nuevo, será deseable que los Estados determinen convencional o consuetudinariamente el tratamiento de los productos sanitarios en el ámbito de las AOC.

El mando y su responsabilidad

El mando es «la autoridad conferida formal y legalmente a una persona en función del puesto y de la responsabilidad que le corresponde, y se materializa en la capacidad para tomar decisiones e impartir órdenes, instrucciones y directrices. Mando, autoridad, jefe o comandante son denominaciones comúnmente empleadas para identificar a esta persona»[126]. Específicamente, y en el ámbito de este trabajo, se sostiene por el US Cyber Comand que el propósito de tal Mando es «alcanzar la superioridad en el ciberespacio a través de la captura y mantenimiento de la iniciativa táctica y operaciones en el ciberespacio, culminando en una ventaja estratégica sobre los adversarios»[127].

Pero con el mando viene la responsabilidad. Conforme al derecho internacional humanitario, el mando debe conocer las leyes y usos de la guerra, tiene el deber de instruir a sus subordinados, y tiene el deber de prevenir y reprimir las infracciones que comentan por acción u omisión sus subordi-

124 Véase el apartado Prohibición de la perfidia de este capítulo.

125 VV. AA. *Tallin Manual 2.0... Op. cit.,* p. 493.

126 ESTADO MAYOR DE LA DEFENSA. *Publicación Doctrinal Conjunta PDC-01(A) «Doctrina para el empleo de las Fuerzas Armadas»,* doc. cit., p. 157.

127 US CYBER COMMAND. «Achieve and Maintain Cyberspace Superiority». *US Cyber Command.* 2018, p. 7. Accesible en https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010.

nados[128], y el incumplimiento de estos deberes se sanciona en España en el Código Penal con severas penas (artículos 608 y siguientes). Y este deber no puede ni debe darse por supuesto puesto que un combatiente adquiere el estatus de combatiente legítimo cuando, entre otras circunstancias, opera bajo un mando responsable (artículo 43 del Protocolo I Adicional a los Convenios de Ginebra de 1949).

Lógicamente, el *Manual de Tallin 2.0* también recoge la cuestión de la responsabilidad del mando en ciberoperaciones. Su regla 85 (responsabilidad penal de los mandos y superiores) dispone que los mandos son penalmente responsables por ordenar ciberoperaciones que constituyan crímenes de guerra, y que son igualmente responsables si sabían o, teniendo en cuenta las circunstancias del momento, deberían haber sabido, que sus subordinados estaban cometiendo, iban a cometer, o habían cometido, crímenes de guerra y dejaron de tomar todas las medidas razonables y disponibles para prevenir su perpetración o para castigar a los responables[129]. Y es que, obviamente, no hay motivo lógico o legal alguno para excluir de la regulación de los crímenes de guerra a las AOC.

Y en este sentido, enlazando con lo que previamente hemos dicho en el apartado Cibertargeting & ROE de este capítulo sobre la importancia del asesor jurídico, es doctrina formal estadounidense con respecto a la responsabilidad del mando en ciberoperaciones considerar que «es esencial que los mandos, planificadores y operadores consulten con los asesores legales durante la planificación y ejecución de ciberoperaciones»[130], y concordantemente se ha establecido específicamente la necesidad de la incorporación del asesor legal para asesorar al mando en el ámbito de las operaciones ciberelectromagnéticas al objeto de garantizar que las mismas cumplan con las leyes[131].

Esa responsabilidad del mando, y la necesidad de su asesoramiento integral, se potencian aún más por la propia naturaleza del ámbito ciberespacial, que requiere de una capacidad de respuesta inmediata[132]. No es sorprendente, por tanto, que la administración Trump haya dictado a finales de 2018 un National Security Presidental Memoranda – NSPM 13 conforme al cual se delegan al Mando de Ciberdefensa determinadas facultades de decisión antes reservadas al Presidente[133].

---

128 ESTADO MAYOR DEL EJÉRCITO. *OR7-004 Orientaciones – El Derecho de los Conflictos Armados*, doc. cit., pp. 2-1 y 2-2.

129 VV. AA. *Tallin Manual 2.0...,* pp. 396 y siguientes.

130 US JOINT CHIEFS OF STAFF, doc. cit., p. III-11.

131 HEADQUARTERS. Department of the Army, doc. cit., pp. 2-7 y 2-8.

132 Recuérdese a efectos comparativos la autoridad *renegade* española prevista en el artículo 16.d de la Ley Orgánica 5/2005 de la Defensa Nacional.

133 FREEDBERG, Sydney Jr. «Trump Eases Cyber Ops, But Safeguards Remain: Joint Staff», 17 de septiembre de 2018, disponible en https://breakingdefense.com/tag/nspm-13/,

En resumen, y por las circunstancias que hemos citado, por un lado y de *lege ferenda*, sería aconsejable la creación formal de una autoridad *renegade de nivel bajo* para el ámbito de la ciberdefensa española, y por otro lado y de *lege data*, como se da en el caso del Mando Conjunto de Ciberdefensa, un mando inteligente, en un ámbito tan complejo y dinámico como el del ciberespacio, y en el que las repercusiones de las ciberoperaciones pueden ser mucho más amplias de lo inicialmente pretendido, no puede tener lejos de si a su asesor legal.

Conclusiones

Las AOC están aquí y han venido para quedarse. Y no hay diferencia jurídica entre una operación ofensiva *on line* u *off line* en el ámbito de los conflictos armados. Ambas están sujetas al derecho internacional humanitario, adaptándose simplemente las reglas de este al ámbito ciberespacial.

En realidad, las consideraciones jurídicas aplicables a las AOC que se han recogido en este trabajo no son sino extrapolaciones lógicas (nunca mejor dicho) al ámbito ciberespacial de las reglas generales contenidas en el derecho internacional humanitario. De esta forma, del mismo modo que se publicó el *Manual de San Remo sobre el derecho internacional aplicable a los conflictos armados en el mar*, adaptando dicho derecho a la guerra naval, o del mismo modo que se publicó el *Manual de Harvard sobre el derecho internacional aplicable a la guerra aérea y de misiles*, adaptando el referido derecho a la guerra aérea, ahora se ha publicado el *Manual de Tallín 2.0 sobre el derecho internacional aplicable a las ciberoperaciones*, para adaptar el reiterado derecho al ámbito ciberespacial. No hay nada nuevo bajo el sol, en definitiva.

Por eso, en realidad no hay diferencia real entre las reglas bélicas que se aplican a una sección española de arqueros en el bosque con respecto a las que se aplican a los operadores del Mando de Ciberdefensa ante sus pantallas y teclados. Cambian los instrumentos de combate, pero no la *lex artis*, ni tampoco las normas aplicables, y jamás su inquebrantable voluntad de vencer.

accedido el 27 de febrero de 2019. Vid. también CHESNEY, Robert. «CYBERCOM's Out-of-Network Operations: What Has and Has Not Changed Over the Past Year», 9 de mayo de 2019, disponible en https://www.lawfareblog.com/cybercoms-out-network-operations-what-has-and-has-not-changed-over-past-year, accedido el 9 de mayo de 2019.

Capítulo quinto

Armas letales autónomas a la luz del derecho internacional humanitario: legitimidad y responsabilidad

Alfonso López-Casamayor Justicia

Resumen

Los vertiginosos avances efectuados en el ámbito de la inteligencia artificial han dado lugar a encendidos debates en el ámbito internacional respecto a su posible aplicación al ámbito militar, especialmente en lo referente al desarrollo, despliegue y uso de los denominados sistemas de armas completamente autónomos.

El presente documento tiene por objeto el estudio de los interrogantes que presentan estas tecnologías desde el punto de vista de su legalidad y adecuación a los principios y normas del derecho internacional humanitario, la suficiencia de este para responder a las particularidades de los sistemas de armas autónomos y los criterios para la imputación de responsabilidad derivada de su empleo, con el fin de evitar situaciones de impunidad derivadas de la falta de una regulación específica.

Con este fin, se atiende especialmente los trabajos realizados bajo el auspicio de Naciones Unidas a través del grupo de expertos constituido en el seno del Convenio sobre Ciertas Armas Convencionales, prestando especial atención a la postura manifestada al respecto por España y la Unión Europea.

Palabras clave

Tecnologías emergentes, sistemas de armas letales autónomas, SAAL, intervención humana significativa, mecanismos de revisión de armas, derecho internacional humanitario, DIH, conflictos armados, Naciones Unidas, Convenio sobre Ciertas Armas Convencionales, Unión Europea.

Abstract

Vertiginous advances in Artificial Intelligence technologies have recently given rise to intensive discussions worldwide about its potential military applications, specially concerning the development, deployment and use of the so-called autonomous weapons systems.

The purpose of this paper is the study of the issues raised by these technologies from the point of view of its legality according to the principles and rules of International Humanitarian law, the sufficiency of the current legal framework to address the specificities of autonomous weapons systems and the criteria for the attribution of liability arising from its use to avoid impunity caused by the current lack of specific regulation.

To this end, special attention is paid to the work conducted, under the auspices of the United Nations, by the Group of Governmental Experts constituted within the framework of the Convention on Certain Conventional Weapons, as well as the position expressed by Spain and the European Union on the matter.

Keywords

Emerging technologies, lethal autonomous weapons systems, LAWS, significant human intervention, weapons review procedures, International Humanitarian Law, IHL, Armed Conflicts, United Nations, Convention on Certain Conventional Weapons, European Union.

Introducción

La incorporación al ámbito militar de sistemas no tripulados controlados a distancia o dotados de cierto grado de autonomía constituye a la vez una realidad incontestable y una revolución en la forma de conducción de los conflictos armados, habiendo experimentado un crecimiento exponencial. Por contra, supone un auténtico desafío para el derecho internacional al carecer de una normativa específica que los regule, habiendo dado lugar desde las más altas instancias internacionales[1] a reacciones frontalmente contrarias al desarrollo de sistemas de armas plenamente autónomos y generando cuestiones jurídicas que sin duda se incrementarán a medida que tales sistemas sean objeto de desarrollo y adquieran mayor difusión y complejidad.

La aplicación militar de sistemas operados a distancia no es nueva, pero su empleo se ha intensificado de forma paralela a los avances tecnológicos, manifestándose fundamentalmente a través del empleo de drones en operaciones, sean de reconocimiento o armados, y más recientemente, mediante sistemas dotados progresivamente de mayor autonomía de actuación.

Estos sistemas presentan indudables ventajas, tanto reales como potenciales, reduciendo costes, minimizando el margen de error humano en la toma de decisiones como consecuencia de su superior capacidad de recogida y análisis de datos en tiempo real y facilitando, al menos en teoría, una mayor exactitud en el cumplimiento de los principios del DIH mediante la reducción de los eventuales daños colaterales. Sin embargo, las limitaciones tecnológicas, unidas a las dudas que presenta desde el punto de vista ético y filosófico, son variables que han supuesto un freno manifiesto a su desarrollo.

En relación con el uso de drones (también denominados UAS[2] por sus siglas en inglés), es preciso destacar que estos se configuran como vehículos aéreos no tripulados, controlados a distancia y por tanto objeto de intervención humana directa. Esta nota tiene un carácter esencial, diferenciándolos así de los sistemas de armas autónomos, que actúan de acuerdo con una programación preestablecida, aunque sujetos en mayor o menor medida a supervisión, como quedará expuesto a lo largo del presente estudio. No obstante,

---

1 Así, el secretario general de Naciones Unidas, Antonio Guterres, en su discurso en el Web Summit, celebrado en Lisboa el 5 de noviembre de 2018, manifestó que:
«La militarización de la inteligencia artificial representa un grave peligro, y la perspectiva de máquinas con capacidad para seleccionar y destruir objetivos por sí mismas está creando enormes dificultades, o creará enormes dificultades, y hará muy difícil evitar la escalada de conflictos y garantizar el respeto del derecho internacional humanitario en los campos de batalla.
Para mí hay un mensaje muy claro: las máquinas que tienen el poder y la discreción de quitar vidas humanas son políticamente inaceptables, son moralmente repugnantes y deben ser prohibidas por el derecho internacional». https://www.un.org/sg/en/content/sg/speeches/2018-11-05/remarks-web-summit.

2 Unmanned Aerial Systems.

tal distinción tiende a difuminarse en tanto que, con el fin de potenciar su eficacia, tales vehículos sean progresivamente dotados de un mayor grado de autonomía.

Su uso se ha generalizado en los últimos años[3] al extender sus capacidades a misiones de vigilancia, obtención de información e identificación y neutralización de objetivos, habiendo sido ampliamente utilizados por los Estados Unidos en la lucha contra el terrorismo. Sin embargo, las ventajas que implica como elemento multiplicador de fuerzas no están exentas de controversia, no tanto en relación con su adecuación a los principios de distinción, proporcionalidad, necesidad y precaución propios del DIH y que se plantean esencialmente respecto de los sistemas de armas autónomos, como por su empleo en el territorio de otro Estado sin autorización de este.

Frente a la existencia ya aceptada de armas activadas y dirigidas a distancia, los sistemas de funcionamiento autónomo que se han venido desarrollando paralelamente a los avances en el campo de la inteligencia artificial, plantean según Liu[4] dos problemáticas fundamentales: el desplazamiento del hombre a la máquina, por primera vez en la historia, de la decisión sobre el empleo de la fuerza en el campo de batalla, y a resultas de lo anterior, la eventual consideración de los sistemas de armas autónomos como una categoría intermedia entre el combatiente y el arma o medio de guerra, con las consecuencias legales que ello conlleva.

A la vista de los antecedentes anteriores, el presente documento comienza con un análisis de las principales notas características que definen los sistemas de armas autónomos y las ventajas e inconvenientes que presentan, para continuar analizando su legalidad desde el punto de vista de su propia naturaleza, características, y su modo de empleo. Todo ello a la luz de los principios y normas del DIH y, en concreto, de las disposiciones recogidas en el *Protocolo I adicional a los Convenios de Ginebra de 1977*, relativo a la protección de las víctimas de los conflictos armados internacionales.

Asimismo, se presta especial atención a los mecanismos de revisión de armas previstos en el artículo 36 del mencionado Protocolo I adicional, como

[3] MARTÍN IBÁÑEZ, Eva. «La autonomía en robótica y el uso de la fuerza». *Documento de opinión 27/2017*. Madrid: IEEE, 2017. http://www.ieee.es/Galerias/fichero/docs_opinion/2017/DIEEEO27-2017_Robotica_UsoFuerza_EvaMartinIbanez.pdf.

[4] LIU, Hin-Yan. «Categorization and legality of autonomous and remote weapons systems». *International Review of the Red Cross*. Vol. 94, n.º 886, pp. 628-629.
«Throughout history, from the arrow to the ballistic missile, weapons have been the passive implements and inert tools that human agents have directly manipulated in order to inflict violence, damage, and injury. With the advent of autonomous, and to a lesser extent remote, weapons systems, however, the application of force and ensuing military destructiveness may require minimal, if any, human decision making or oversight.
Autonomous and remote weapons systems appear to subsist between the existing legal categories of 'weapons' and 'combatants'».

medio para verificar que tales principios son plenamente aplicables a los sistemas de armas autónomos con carácter previo a su adquisición, desarrollo, despliegue y uso.

A continuación, se explorará la problemática derivada de la atribución de responsabilidad dimanante de su uso, que es objeto de consideración desde la perspectiva de la responsabilidad internacional de Estados, el derecho penal internacional y el derecho penal y disciplinario, así como la eventual exigencia de responsabilidad civil resultante del daño ocasionado.

Por último, debido a el papel protagonista que ha ostentado desde un primer momento y sigue ejerciendo en la actualidad en el debate sobre el surgimiento y desarrollo de sistemas de armas autónomos, se lleva a cabo un examen pormenorizado de las cuestiones planteadas y los consensos alcanzados dentro del grupo de expertos gubernamentales creado al amparo de las Naciones Unidas en el marco del Convenio sobre Ciertas Armas Convencionales de 10 de octubre de 1980, así como la posición manifestada sobre la materia por España y la Unión Europea en este y otros foros, con especial mención a los principales movimientos nacidos en el ámbito de la sociedad civil respecto a la existencia de tales sistemas de armas.

Delimitación del concepto de sistema de armas autónomo

Uno de los principales problemas que ofrece el objeto del presente estudio es la inexistencia de un concepto generalmente aceptado acerca de qué debe entenderse por sistema de armas autónomo letal (SAAL o LAWS/FLAWS[5] por sus siglas en inglés).

Dicha dificultad obedece, por un lado, a que el establecimiento de un concepto de SAAL en una fase temprana del debate supone una limitación al objeto de este que no resulta aconsejable a la vista de su complejidad técnica, y por otro, a la dificultad de alcanzar un acuerdo entre diferentes Estados que mantienen posturas en ocasiones muy alejadas sobre estos sistemas y el tratamiento que deben recibir en el ámbito del derecho internacional. Sin embargo, ello no significa que no se hayan planteado propuestas de trabajo en este sentido. Así, Estados Unidos, a través de la Directiva del Departamento de Defensa de 21 de noviembre de 2012[6], es el primer país que expone su postura oficial acerca de los SAAL, que define como aquellos sistemas de armas que, una vez activados, pueden seleccionar y atacar objetivos sin necesidad de intervención posterior por un operador humano, incluyendo los sistemas de armas autónomos supervisados que permiten al operador anular la operación una vez iniciada.

[5] Lethal Autonomous Weapon System/Fully Lethal Autonomous Weapon System.

[6] Department of Defense Directive Number 3000.09. 21 de noviembre de 2012.

Como señala Meza[7], a esta le siguen otras propuestas, como las expuestas por el Reino Unido, Francia, Suiza o Canadá en el seno del grupo de expertos constituido al amparo del Convenio sobre Ciertas Armas Convencionales de Naciones Unidas.

Destaca asimismo la definición de trabajo presentada por Holanda[8] para facilitar el debate, que, concretando las anteriores y referida a los sistemas de armas completamente autónomos, considera como tales aquellas armas que, sin intervención humana, seleccionan y atacan objetivos que reúnan determinados criterios prefijados, siguiendo una decisión humana de desplegar el arma sobre el presupuesto de que, una vez lanzado el ataque, este no puede ser detenido mediante una intervención humana.

En cualquier caso, dada la dificultad para alcanzar un acuerdo acerca de una definición de arma letal autónoma, el debate se ha dirigido desde una fase muy temprana al estudio de sus características, con el fin de centrar el objeto de estudio. Sin embargo, también en relación con estas es conveniente hacer una serie de matizaciones, destacando como rasgos definitorios de los SAAL los siguientes:

A. Autonomía

El mismo término «sistema de armas letal autónomo» ofrece una aproximación de lo que debe entenderse como tal. Sin embargo, la expresión «autónomo» puede dar lugar a cierta confusión, especialmente en lo que se atiende a la diferenciación entre los términos de automatización y autonomía.

En este sentido, se considera un sistema automático aquel que incorpora respuestas prefijadas ante determinadas situaciones, de modo que su grado de previsibilidad es elevado. Sin embargo, el hecho de que su forma de actuar depende siempre de su programación previa limita su empleo a contextos de escasa complejidad.

Por su parte, la autonomía va un paso más allá, entendiendo esta como la capacidad para organizar y desarrollar sus tareas de manera autosuficiente, incluyendo la fase de planificación de estas, aunque siempre dentro de los límites previstos en su programación. A diferencia de los sistemas automáticos, puede desenvolverse en escenarios más complejos debido a su mayor capacidad de adaptación, pero el resultado carece de la previsibilidad propia de aquellos.

---

[7] MEZA RIVAS, Milton. «Los sistemas de armas completamente autónomos: un desafío para la comunidad internacional en el seno de Naciones Unidas». *Documento de opinión 85/2016*. Madrid: IEEE, 2016.

[8] Documento de trabajo presentado por Holanda ante la «Conferencia de desarme en la reunión del grupo de expertos gubernamentales sobre sistemas de armas autónomos letales». Ginebra, octubre 2017.

En cualquier caso, la distinción entre uno y otro sistema es hasta cierto punto difusa, siendo imputable a ambos un cierto grado de imprevisibilidad.

B. Intervención humana

La conformidad del empleo de sistemas de armas autónomos con los principios del DIH exige ineludiblemente la concurrencia de un control humano significativo como garantía de su cumplimiento y como vínculo que permita la atribución de responsabilidad en caso de vulneración.

La forma e intensidad de dicha intervención dependerán esencialmente de la naturaleza del arma y el contexto en que vaya a ser utilizada, de modo que cuanto menor sea la participación del operador humano una vez activada, mayor habrá de ser la diligencia empleada, dado que la responsabilidad derivada del resultado será imputable en última instancia a este y la autoridad que hubiera ordenado su utilización.

El control humano puede tener lugar en diferentes momentos y llevarse a cabo a través de una pluralidad de vías, pero en todo caso se exige que tenga lugar con carácter previo a su despliegue, asegurándose de que el SAAL opera de conformidad con la legislación aplicable.

En particular, deberá verificarse por el mando y el operador directo, previa evaluación del riesgo, que el sistema está capacitado para la ejecución de la misión confiada y que el empleo de la fuerza autorizada es adecuado y proporcionado a la naturaleza de aquella. Estos extremos tienen especial relevancia en cuanto a la toma de decisión sobre su empleo, la determinación de los criterios aplicables para la fijación de objetivos y la evaluación de los posibles daños colaterales, pero no requiere necesariamente la atribución de la facultad de abortar el ataque una vez iniciado[9].

C. Letalidad

Finalmente, esta nota, entendida como la capacidad de un sistema de armas de emplear fuerza letal, parece inherente al mismo concepto de SAAL. Ello se debe en parte a que solo el uso letal de estos sistemas de armas plantea verdaderos conflictos desde la perspectiva del DIH.

Sin embargo, esta postura no es unánime, dado que la letalidad no se configura como un elemento esencial de ningún arma o sistema de armas, sea de funcionamiento autónomo o no. Un arma no pierde este carácter por el hecho de que el resultado de su empleo no tenga un resultado letal, integrándose también dentro de esta categoría aquellas otras cuya potencia o intensidad se encuentran en un escalón inferior, dirigiéndose solo a causar

[9] Documento de trabajo presentado por Estonia y Finlandia ante la «Conferencia de desarme en la reunión del grupo de expertos gubernamentales sobre sistemas de armas autónomos letales». Ginebra, agosto 2018.

daños en personas o bienes sin que ello conlleve necesariamente el causar la muerte.

Es por ello, que algunos Estados defienden una definición más amplia de SAAL, estableciendo como nota definitoria el empleo de la fuerza, sea esta letal o no.

Clases de sistemas de armas autónomos

Con independencia de la inexistencia de una definición técnica consensuada acerca de qué debe entenderse por sistema de armas autónomo, es posible establecer una clasificación entre ellos, atendiendo al grado de autonomía que tienen atribuido.

Si bien pueden establecerse tantas categorías como posibles perspectivas ofrece su estudio, resulta especialmente útil la recogida en la Directiva del Departamento de Defensa de los Estados Unidos de 2012 antes citada, que distingue entre:

- Sistema de armas autónomo, definido como aquel que, una vez activado, está habilitado para seleccionar y atacar un objetivo sin ulterior intervención humana.
- Sistema de armas supervisado. Esta clase de sistema de armas se diferencia del anterior en que, si bien una vez activado identifica y ataca objetivos conforme a los criterios fijados en su programación, faculta al operador humano a intervenir, incluso abortando el ataque antes de que este se produzca dentro de un margen de tiempo desde la activación. De este modo, el elemento humano autoriza el ataque y lo monitoriza, evitando que se produzcan daños innecesarios o inaceptables por fallos imputables al sistema o su programación, facilitando a su vez la atribución de la responsabilidad resultante.
- Sistema de armas semiautónomo. Finalmente, esta clase de sistemas de armas gozan de un grado de automatización limitado a, una vez activados, atacar objetivos o grupos de objetivos que han sido seleccionados por un operador humano dentro de un área determinada.

Como puede apreciarse, de estos tres tipos de sistemas de armas, el que presenta mayores problemas es obviamente el primero, en tanto que la intervención humana queda circunscrita al momento de activación del arma, dejando a su arbitrio cualquier decisión posterior relativa al empleo de fuerza letal. No obstante, los sistemas con mayor grado de autonomía existentes en la actualidad se limitan al ámbito puramente defensivo, con funciones y objetivos claramente delimitados. La atribución a esta clase de sistemas de un grado mayor de autonomía que permita su empleo en escenarios de mayor complejidad requiere el desarrollo de tecnologías todavía inexistentes, si

bien objeto de desarrollo por algunos países, planteándose hasta el momento la discusión sobre ellos en términos puramente teóricos.

Ventajas e inconvenientes

Desde que comenzó el debate acerca de la posibilidad de desarrollo de sistemas de armas autónomos, son muchos los argumentos que se han esgrimido a favor y en contra de su existencia.

Es cierto, en primer lugar, que atribuir a una máquina la autoridad para disponer sobre la vida y la muerte de un individuo, aun cuando en el proceso exista un elemento de control humano significativo, plantea serios problemas desde una perspectiva ética. Un sistema de armas autónomo carece, por su propia esencia, de caracteres como la humanidad o la clemencia, que a la postre resultan esenciales para llevar a cabo un juicio adecuado en el campo de batalla.

Los SAAL están igualmente sujetos a limitaciones y vulnerabilidades derivadas del estado de la técnica, que plantean dudas acerca de su previsibilidad, su capacidad de actuación en escenarios complejos, la posibilidad de ser objeto de ciberataques o su aptitud para cumplir con las exigencias establecidas por los preceptos del DICA, en particular los principios de proporcionalidad y distinción.

Asimismo, el desarrollo de los SAAL y su aplicación al ámbito militar plantea riesgos reales, tanto de dar lugar al inicio de una carrera armamentística entre Estados con el fin de no quedar desprotegidos frente a un ataque de estas características, como de que esta tecnología sea objeto de un uso indebido por actores no estatales, con el consiguiente peligro para la paz y seguridad internacional.

Finalmente, se plantea el problema de la atribución de responsabilidad por las eventuales vulneraciones del DIH cometidas a través de sistemas de armas autónomos, así como la posibilidad de exigirla frente a Estados o sujetos determinados, evitando así escenarios de vacío de responsabilidad.

Sin embargo, es innegable que estos sistemas presentan indiscutibles ventajas, que tienen su reflejo en el nivel estratégico, operacional y táctico. Sobre todas ellas destaca la drástica reducción del número de bajas, no solo en el desarrollo de un conflicto armado, sino también en el desarrollo de actividades peligrosas u operaciones de rescate.

A lo anterior se une la reducción de costes, cuestión de máxima importancia para las fuerzas armadas, que tratan de mantener su operatividad en un escenario de presupuestos no expansivos.

No obstante, estas no son las únicas mejoras que ofrecen los SAAL. Estos sistemas, dotados de capacidades y sensores capaces de recoger y analizar

grandes cantidades de información en un tiempo reducido, podrían constituir un elemento multiplicador de la fuerza de gran valor, incrementando la precisión de los ataques y reduciendo el riesgo de error humano y la posibilidad de causar daños colaterales.

A la vista de lo anterior, cabe preguntarse si las ventajas que ofrecen los SAAL superan la imprevisibilidad y riesgos potenciales que llevan aparejados, cuestión controvertida en la actualidad y probablemente seguirá siéndolo en los próximos años.

Examen desde el punto de vista del DIH

Constituye una convicción firmemente asentada dentro de la comunidad internacional que los SAAL se hallan plenamente sometidos a los postulados del DIH.

Una vez asumido lo anterior, es preciso analizar los requisitos exigidos por el DIH para avalar la utilización de dichos sistemas de armas. Tales requisitos se refieren tanto a la naturaleza del sistema individuamente considerado como a la legitimidad en su uso.

Desde este punto de vista, para que un sistema de armas sea considerado legitimo a la luz del DIH es preciso acudir en primer lugar a las disposiciones contenidas en el Protocolo I adicional a los Convenios de Ginebra de 1949 (PIACG)[10]. Sus disposiciones en esta materia vinculan plenamente a los Estados parte de dicho Protocolo adicional, así como al resto de Estados, en tanto que tales preceptos se consideran parte integrante del derecho internacional consuetudinario.

En concreto, el Protocolo I adicional recoge una serie de principios aplicables en caso de conflicto armado que han de respetarse con independencia del medio o método de guerra empleado. Tales son los principios de limitación, necesidad militar, protección del medio ambiente, proporcionalidad, distinción, precaución y humanidad, respecto de los cuales es conveniente hacer las siguientes matizaciones en relación con los SAAL.

A. Principio de limitación

Como punto de partida, el artículo 35.1 del Protocolo I adicional recoge el principio de limitación, en virtud del cual: «En todo conflicto armado, el derecho de las partes en conflicto a elegir los métodos o medios de hacer la guerra no es ilimitado». Este principio supone una restricción general respecto de la utilización de armas o métodos de guerra que contravengan, tanto un principio general de DIH, como la prohibición expresa de un determinado tipo de arma. Dentro de estas últimas podemos incluir, entre otras, las recogidas

[10] *Protocolo I adicional a los Convenios de Ginebra de 1949* relativo a la protección de las víctimas de los conflictos armados internacionales, 1977.

en los protocolos adicionales al Convenio sobre Ciertas Armas Convencionales de 10 de octubre de 1980[11]. En la actualidad, no existe una norma general prohibitiva respecto de los SAAL, aunque son varios los Estados favorables al establecimiento de una prohibición general o preventiva de su desarrollo, despliegue o uso.

B. Principio de necesidad militar

El principio de necesidad militar se encuentra recogido en el artículo 35.2 del mencionado Protocolo I adicional, incluido dentro de su título III, relativo a los métodos y medios de guerra, estatuto de combatiente y de prisionero de guerra. Este artículo incorpora la prohibición del empleo de armas, proyectiles, materias y métodos de hacer la guerra de tal índole que causen males superfluos o sufrimientos innecesarios.

Ello supone que un sistema de armas autónomo será legítimo, al igual que cualquier otro medio de guerra, siempre que los medios empleados por aquel sean los estrictamente necesarios para el cumplimiento de su fin, no presentando especialidad alguna derivada de su funcionamiento autónomo.

C. Principio de protección del medio ambiente

La utilización de medios o métodos de guerra está igualmente sometido a limitaciones de índole medioambiental. Así, el principio de protección del medio ambiente prohíbe el empleo de métodos o medios de hacer la guerra que hayan sido concebidos para causar, o de los que quepa prever que causen, daños extensos, duraderos y graves al medio ambiente natural (artículo 35.3 y 55 PIACG). Las obligaciones derivadas de dicho precepto se complementan, para aquellos Estados parte de esta, con las recogidas en la Convención sobre la prohibición de utilizar técnicas de modificación ambiental con fines militares u otros fines hostiles de 10 de diciembre de 1976. En virtud del artículo 1 del mencionado tratado, cada Estado parte se compromete a no utilizar técnicas de modificación ambiental con fines militares u otros fines hostiles que tengan efectos vastos, duraderos o graves, como medios para producir destrucciones, daños o perjuicios a otro Estado parte, así como a no ayudar, alentar o incitar a ningún Estado o grupo de Estados u organización internacional a realizar actividades contrarias a sus disposiciones.

[11] Dichos Protocolos son los siguientes:
Protocolo I sobre fragmentos no localizables, de 10 de octubre de 1980.
Protocolo II sobre prohibiciones o restricciones del empleo de minas, armas trampa y otros artefactos, de 10 de octubre de 1980, objeto de revisión el 3 de mayo de 1996.
Protocolo III, sobre prohibiciones o restricciones del empleo de armas incendiarias, de 10 de octubre.
Protocolo IV, sobre armas láser cegadoras, de 13 de octubre de 1995.
Protocolo V, sobre los restos explosivos de guerra, de 28 de noviembre de 2003.

En este sentido, el empleo de sistemas de armas autónomos requerirá para su conformidad con los preceptos anteriores, según ha expuesto el Comité Internacional de la Cruz Roja[12], el estudio previo de cuestiones tales como:

- Si el arma ha sido diseñada específicamente con el fin de alterar o destruir el medio ambiente natural.
- La probabilidad de que estos daños se produzcan, su magnitud y la clase de consecuencias que su uso pueda ocasionar.
- Si el daño causado puede ser considerado reversible, así como el tiempo y recursos económicos necesarios para ello.
- El impacto, directo o indirecto, de sus efectos sobre la población civil.

D. Principio de distinción

En primer lugar, el principio de distinción se encuentra recogido en el artículo 48 del Protocolo I adicional, que obliga a distinguir en el desarrollo de las operaciones los objetivos militares y combatientes de la población y bienes de carácter civil, que no podrán ser objeto de ataque o represalia, dirigiendo los ataques únicamente contra los primeros. Quedan asimismo prohibidos los actos o amenazas de violencia cuya finalidad principal sea aterrorizar a la población civil. En consecuencia, la complejidad del entorno operativo y el grado de sofisticación de la tecnología influirá decisivamente en la posibilidad de desplegar sistemas de armas autónomos, pues en determinados contextos, tales como zonas de combate urbano, la distinción entre unos y otros resulta en ocasiones difícil incluso para el ser humano.

Por su parte, los apartados a), b) y c) del artículo 51.4 prohíben los ataques indiscriminados, considerando como tales los que emplean métodos o medios de combate que no se dirigen o no pueden dirigirse contra un objetivo militar concreto o cuyos efectos no sea posible limitar conforme a lo exigido por el dicho Protocolo. Es decir, todo sistema de armas que permita distinguir y atacar un objetivo militar legítimo se consideraría acorde a las disposiciones del Protocolo a estos efectos, ya sea controlado directamente por un ser humano, ya actúe de manera autónoma una vez activado.

E. Principio de proporcionalidad

El principio de proporcionalidad se halla plasmado en el artículo 51.5 b) del Protocolo I adicional. Este precepto considera indiscriminados aquellos ataques excesivos en relación con la ventaja militar obtenida, cuando se prevea que causarán incidentalmente muertos y heridos entre la población civil o daños a bienes de carácter civil. Este principio requiere por tanto la práctica de un juicio de valor, a efectos de establecer un equilibrio entre la intensidad

[12] LAWLAND, Kathleen. *Guía para el examen jurídico de las armas, los medios y los métodos de guerra nuevos. Medidas para aplicar el artículo 36 del Protocolo adicional I de 1977*. Ginebra: Comité Internacional de la Cruz Roja, enero 2006.

y medios empleados en el ataque y valor del objetivo alcanzado, de modo que aquellos no se reputen desproporcionados. Ello supone un verdadero desafío para el programador de un sistema de armas de funcionamiento autónomo, en tanto que la calificación de la ventaja militar puede resultar cambiante en función de la etapa del conflicto y requiere, en consecuencia, una actualización constante atendiendo a las circunstancias concurrentes y las reglas de enfrentamiento aplicables.

F. Principio de precaución

Por su parte, el principio de precaución exige que las operaciones militares se desarrollen, de acuerdo con los artículos 57 y 58 PIACG, con un cuidado constante para preservar a la población civil, a las personas civiles y a los bienes de carácter civil. Ello supone la necesidad de hacer lo posible para comprobar, con carácter previo y atendiendo a la información disponible, que el objeto del ataque es un objetivo militar legítimo. Asimismo, requiere la adopción de todas las medidas necesarias para evitar, o al menos, minimizar los daños colaterales.

En este contexto, la mayor capacidad de reconocimiento y análisis de datos puede suponer una ventaja para tener en cuenta a la hora de sopesar la conveniencia del empleo de medios autónomos.

G. Principio de humanidad

Finalmente, el principio de humanidad constituye una cláusula de cierre, de modo que el actuar de las partes beligerantes no suponga en ningún caso la total desprotección de las víctimas de un conflicto armado, aun en ausencia de una norma específica, estableciendo un umbral mínimo de amparo para los mismos, sean civiles o combatientes.Tiene su antecedente en Convención II de La Haya de 1899 relativa a las Leyes y Usos de la Guerra Terrestre y se encuentra recogido en la actualidad en el artículo 1.2[13] del Protocolo I adicional a los Convenios de Ginebra, si bien ha adquirido a su vez la consideración de norma de derecho internacional consuetudinario con fundamento en el artículo 3 común a los Convenios de Ginebra de 1949, siendo también aplicable, en consecuencia, a los conflictos armados no internacionales[14].

En definitiva, la conformidad de los sistemas de armas autónomos con el DIH dependerá no solo de la naturaleza y características del sistema en sí, sino también de que su despliegue y utilización se lleven a cabo atendiendo a los principios que rigen el desarrollo de las hostilidades. De este modo,

[13] «En los casos no previstos en el presente Protocolo o en otros acuerdos internacionales, las personas civiles y los combatientes quedan bajo la protección y el imperio de los principios del derecho de gentes derivados de los usos establecidos, de los principios de humanidad y de los dictados de la conciencia pública».

[14] HURTADO GRANADA, Martha Isabel. «Los límites del DIH a las armas autónomas». *Revista Científica General José María Córdoba*. Vol. 15, n.º 20, julio-diciembre, 2017, pp. 85-100.

solo aquel sistema en el que concurran ambos aspectos podrá emplearse legítimamente en el curso de un conflicto armado[15].

Mecanismos de revisión de armas al amparo del artículo 36 del Protocolo I adicional a los Convenios de Ginebra de 1949

Con el fin de asegurar que un nuevo sistema de armas se adecúa a los principios del DIH, el artículo 36 del Protocolo I adicional a los Convenios de Ginebra[16] establece la obligación de los Estados parte de verificar que el empleo de dichos sistemas resulta conforme con las normas del derecho internacional.

Como señala Giacca[17], la realización de estos exámenes se sitúa en una primera etapa, ubicada en el momento de desarrollo y/o adquisición del sistema de armas, y por lo tanto previa a la decisión de su despliegue y utilización en zona de operaciones. No obstante, puede resultar preciso ejecutar nuevas revisiones en una fase posterior, ya sea por la incorporación de modificaciones significativas a los sistemas examinados, la introducción de nuevas modalidades de uso para los mismos o la asunción por los Estados de obligaciones internacionales adicionales a las ya existentes.

La implementación de este tipo de procedimientos de revisión constituye, como se ha manifestado anteriormente, una obligación para los firmantes del PAIGC, pero su realización es igualmente conveniente para aquellos Estados que no son parte de dicho Protocolo, que son igualmente responsables de los actos de sus Fuerzas Armadas, y en consecuencia, de la legalidad de los medios empleados por ellas, de acuerdo con el IV Convenio de la Haya de 1907, relativo a las Leyes y Costumbres de la Guerra Terrestre (artículo 3[18]).

A pesar de la existencia de dicha obligación, en la actualidad es reducido el número de Estados que cuentan con procedimientos reglados de revisión de armas, que difieren además en cuanto a su enfoque y alcance, toda vez

---

15 Declaración del embajador Michael Biontino sobre los aspectos legales de los SAAL. Reunión del grupo de expertos gubernamentales sobre armas letales autónomas en el marco del Convenio sobre Ciertas Armas Convencionales. Ginebra, mayo 2014.

16 «Cuando una alta parte contratante estudie, desarrolle, adquiera o adopte una nueva arma, o nuevos medios o métodos de guerra, tendrá la obligación de determinar si su empleo, en ciertas condiciones o en todas las circunstancias, estaría prohibido por el presente Protocolo o por cualquier otra norma de derecho internacional aplicable a esa alta parte contratante».

17 GIACCA, Gilles. «Legal Review of New Weapons, Means and Methods of Warfare». Comunicación ante la «Conferencia de desarme en la reunión informal de expertos gubernamentales sobre sistemas de armas autónomos letales». Ginebra, abril 2016.

18 «La parte beligerante que viole las disposiciones de dicho Reglamento estará obligada a indemnización, si fuere el caso, y será responsable de todos los actos cometidos por las personas que hagan parte de su fuerza armada».

que el Protocolo I adicional no recoge previsiones específicas en este sentido. Tan escaso éxito se explica en gran parte por razones industriales y de seguridad nacional, a lo que se une la confianza de los Estados en los controles realizados por fabricantes y por otros operadores de los sistemas examinados.

No obstante lo anterior, resulta conveniente su desarrollo progresivo en la medida en que, por limitada que sea la difusión de información por parte de los Estados, constituye una muestra fidedigna del compromiso de aquellos con la aplicación del DIH, fomenta la transparencia y confianza entre las partes y la fijación de criterios homogéneos para esta clase de procesos.

En cuanto a la aplicación de los procedimientos de revisión del artículo 36 PAICG a los SAAL, al excluir el juicio humano del proceso de toma de decisiones, la labor del examinador debe estar dirigida primordialmente a verificar, con un alto grado de confianza y seguridad, que dichos sistemas están capacitados para actuar respetando las normas fundamentales del DIH. Este control tendrá necesariamente carácter genérico, en cuanto a la capacidad del sistema en sí mismo, sin perjuicio del examen posterior y concreto en el teatro de operaciones, verificado por el mando militar con la asistencia de su asesor jurídico.

Así, será necesario comprobar en primer lugar que, por su naturaleza o medio de empleo, dicho sistema no vulnera una prohibición expresa recogida en una norma de derecho internacional, ni es susceptible de causar daños superfluos o sufrimiento innecesario. Además, el sistema de armas examinado ha de ser capaz de evaluar la ventaja militar derivada de una acción militar y anticipar el posible daño colateral, así como de mantener el necesario equilibrio entre una y otro, suspendiendo el ataque en caso contrario.

De igual modo, su programación ha de ser adecuada para llevar a cabo la distinción entre objetivos civiles y militares, así como, en su interacción con objetivos humanos, diferenciar a combatientes, civiles y aquellos que hayan depuesto las armas o se hallen fuera de combate por detención, heridas o cualquier otra causa.

Debe, en último lugar, seleccionar el medio o método adecuado para alcanzar el fin militar perseguido, causando el mínimo daño necesario para ello.

La respuesta a estas cuestiones determinará la legalidad en abstracto de los sistemas de armas autónomos, así como los supuestos en que el empleo de estos es legítimo a la luz del DIH. Este ámbito es actualmente limitado, pero no son pocas las voces autorizadas que admiten la posibilidad de desarrollar en el futuro robots capaces de realizar tales distinciones de modo análogo a como lo haría el soldado medio[19].

[19] SASSÒLI, Marco. «LAWS - advantages and problems compared with other weapon systems from the point of view of IHL». Comunicación ante la «Conferencia de desarme en

Por lo tanto, será el desarrollo tecnológico el que determine en los próximos años la admisibilidad de esta clase de sistemas, siendo por ello fundamental el establecimiento de sistemas de revisión de armas fiables, minuciosos y transparentes que supongan una garantía suficiente de legalidad con carácter previo a su despliegue, atendiendo entre otros factores a la naturaleza de la función encomendada, el objetivo marcado y el contexto espacio-temporal de su empleo.

El problema de la atribución de responsabilidad

Una de las principales controversias que se plantean en relación con la existencia de los SAAL es la atribución de la responsabilidad dimanante de su utilización en caso de vulneración de las normas del DIH.

En primer lugar, es preciso pronunciarse sobre la cuestión de si es posible imputar dicha responsabilidad a uno o varios sujetos determinados. Los sistemas de responsabilidad se asientan tradicionalmente, como defiende Geiss[20], en la existencia de un cierto grado de control o previsibilidad del resultado. A ello debe añadirse la presencia de un ente con personalidad jurídica propia que pueda ejercer dicho control y asumir, en consecuencia, dicha responsabilidad.

Ello excluye por su propia naturaleza a los SAAL, que no pueden responder de las eventuales vulneraciones del derecho internacional que los mismos puedan ocasionar en tanto que carecen de personalidad e intencionalidad, por lo que no pueden ser considerados responsables, ya sea a título de dolo o de culpa. Sobre esta premisa, se plantea una segunda problemática, consistente en la determinación del ente o entes concretos que han de asumir dicha responsabilidad, sea este el Estado, el mando militar que ordena el empleo del SAAL, el operador del sistema o incluso el fabricante, diseñador o programador. Esta responsabilidad será de mayor dificultad en su determinación cuanto mayor sea el grado de autonomía del sistema, pero no debe suponer en ningún caso un vacío legal que lleve a una situación de impunidad.

Responsabilidad internacional de los Estados

El despliegue y utilización de sistemas de armas autónomos no es, como se ha expuesto previamente, ilícita en sí misma, pero presenta en todo caso un

la reunión informal de expertos gubernamentales sobre sistemas de armas autónomos letales». Ginebra, mayo 2014. https://www.unog.ch/80256EDD006B8954/(httpAssets)/D610608F7A63339CC1257CD70061096D/$file/Sassoli_LAWS_IHL_2014.pdf.

[20] GEISS, Robin. «Autonomous Weapons Systems: Risk Management and State Responsibility». Comunicación ante la «Conferencia de desarme en la reunión informal de expertos gubernamentales sobre sistemas de armas autónomos letales». Ginebra, abril 2016.

grado de imprevisibilidad en cuanto a los resultados que se incrementa con la complejidad del contexto en que se emplea, lo que ha servido de fundamento a las posturas favorables a su total prohibición. De modo que, incluso en el eventual caso de que un SAAL hubiera superado con éxito los procedimientos de revisión a los que hace mención artículo 36 PIACG, estos son susceptibles de error o fallo en su despliegue, cuyas consecuencias deben ser asumidas en última instancia por el Estado que los emplea como contrapartida a la ventaja estratégica que los mismos proporcionan, de modo que, a mayor riesgo, mayor será la responsabilidad.

La imputación de esta responsabilidad se fundamenta en primer lugar y con carácter genérico en el artículo 1 común a los Convenios de Ginebra, en virtud del cual las altas partes contratantes se comprometen a respetar y a hacer respetar sus disposiciones en todas las circunstancias. Esta obligación plantea dudas en cuanto al alcance de la diligencia debida empleada, máxime cuando se trata de tecnologías nuevas y complejas como los SAAL, pero requiere en todo caso la adopción de medidas preventivas dirigidas a minimizar el riesgo, tales como el sometimiento previo a los citados procedimientos de revisión del artículo 36 PIACG o la limitación de los escenarios de aplicación de tales sistemas.

Por otro lado, constituye un principio general del derecho internacional que el Estado es responsable en caso de incumplimiento de una obligación internacional. Así lo reconoció el Tribunal Internacional de Justicia en su sentencia del 13 de septiembre de 1928, (caso Chorzow) al dictaminar que «... es un principio de derecho internacional, incluso una concepción general de derecho, que toda violación de una obligación internacional trae consigo la obligación de reparar...».

De igual modo, el *Proyecto de artículos sobre la responsabilidad del Estado por hechos internacionalmente ilícitos de 2010*, elaborado por la Comisión de Derecho Internacional de Naciones Unidas establece en su artículo 1, que: «Todo hecho internacionalmente ilícito del Estado genera su responsabilidad internacional».

Para que dicha responsabilidad sea exigible, es precisa la concurrencia de los siguientes presupuestos:

1.- En primer lugar, se requiere que la existencia de una conducta activa u omisiva sea atribuible al Estado según el derecho internacional[21].

A tal efecto, se consideran imputables al Estado los actos procedentes de sus órganos, entidades o personas que estén facultadas para ejercer atribuciones del poder público y actúen en el ejercicio de sus funciones, aun

[21] La problemática de la imputación de responsabilidad internacional de un Estado por hechos ajenos es objeto de especial consideración en el ámbito del ciberespacio por De Salas Claver en el capítulo 4 de esta obra.

cuando se excedan en su competencia o contravengan sus instrucciones. De igual modo le son imputables aquellos otros actos que se lleven a cabo bajo su dirección o control, los que reconozca como propios y los realizados por otras personas o entidades en el ejercicio de atribuciones del poder público en ausencia o en defecto de las autoridades oficiales.

Fuera de estos supuestos, también puede existir responsabilidad del Estado por actos ilícitos llevados a cabo por otras personas cuando, a pesar de no serle directamente imputables, no hubiese adoptado las medidas necesarias para evitar un acto contrario al derecho internacional o perseguirlo y castigarlo una vez producido. En estos casos, será necesario acreditar que la vulneración de la norma internacional se ha debido precisamente a la falta de diligencia atribuida al Estado.

2.- En segundo lugar, es preciso que dicha conducta constituya una violación de una obligación internacional asumida por el Estado.

Esta obligación ha de hallarse vigente en el momento en que se produce el hecho, cualquiera que sea su origen (incluyendo tratados, costumbre o principios generales del derecho internacional).

Ante dicha situación, se plantean por la doctrina diferentes sistemas de atribución de responsabilidad a los Estados.

Por un lado, sería posible el establecimiento de un régimen, más garantista, de responsabilidad objetiva basado en la peligrosidad y riesgo inherente que supone emplear un sistema de estas características, caracterizado por su elevado grado de imprevisibilidad. Este sistema, sin embargo, es más propio del ámbito civil, donde la causación de un daño se contempla como una posibilidad para tener en cuenta y no como un fin en sí mismo.

Frente a este sistema, la alternativa podría residir en la inversión de la carga de la prueba hacia el Estado presuntamente responsable, que habría de acreditar la adopción de las medidas adecuadas para excluir o minimizar el riesgo, con fundamento en la obligación recogida en el artículo 1 común a los Convenios de Ginebra antecitado de asegurar el respeto a las normas del DICA, respondiendo en caso contrario de los daños causados en la medida que los mismos le sean imputables.

No obstante lo anterior, según señala acertadamente Marauhn[22], los SAAL no quedan fuera del sistema de responsabilidad internacional de los Estados ni del derecho penal internacional mientras exista un vínculo con un ente con consideración de sujeto de derecho internacional o dotado de personalidad

[22] MARAUHN, Thilo. «An Analysis of the Potential Impact of Lethal Autonomous Weapons Systems on Responsibility and Accountability for Violations of International Law». Comunicación ante la «Conferencia de desarme en la reunión informal de expertos gubernamentales sobre sistemas de armas autónomos letales». Ginebra, mayo 2014

jurídica propia al que quepa atribuir la decisión de su despliegue o las acciones ejecutadas por este.

La responsabilidad penal internacional de mandos y subordinados

Mientras exista un ser humano en la cadena de mando que ordene o controle la actuación de un SAAL, este puede ser considerado responsable por el uso indebido del mismo.

En el ámbito internacional, la principal vía para hacer efectiva esta responsabilidad es la Corte Penal Internacional, creada por el Estatuto de Roma de 17 de julio de 1998 (ECPI). La competencia de este tribunal se extiende al genocidio, crímenes de guerra, contra la humanidad y de agresión cometidos después de la entrada en vigor de su Estatuto, y se ejerce con carácter complementario respecto de las jurisdicciones penales nacionales, como así se pone de manifiesto en el preámbulo y artículo 1 del mencionado Estatuto.

Por último, la responsabilidad penal internacional es exigible ante la Corte únicamente respecto de personas naturales, cuando cometan estos crímenes por sí solos, con otros o por conducto de otros, u ordenen, propongan o induzcan a su comisión (arts. 5 y 25 del ECPI). Por lo tanto, esta responsabilidad penal se extiende no solo al mando militar o supervisor civil que actúe como jefe militar con carácter efectivo, sino también a los subordinados de aquellos, con las solas excepciones previstas en su artículo 33.

En este sentido, el mando puede ser responsable penalmente por crímenes de guerra que sean cometidos por sus subordinados a través de sistemas de armas autónomos siempre que concurran los siguientes presupuestos:

- La existencia de una relación entre superior y subordinado, manifestada en el ejercicio del mando o autoridad y control efectivo.
- Que el mando militar o superior supiera o hubiese debido saber que las fuerzas bajo su autoridad estaban cometiendo tales crímenes o se proponían cometerlos.
- Que, en tales circunstancias, no hubiese tomado todas las medidas razonables y necesarias a su alcance para prevenir, reprimir o perseguir su comisión.
- Que exista una relación de causalidad entre la falta de adopción de las medidas necesarias para evitar el delito y la comisión de este.

Ha de existir, por lo tanto, una conducta imputable al superior, ya sea a título de dolo o negligencia, que existirá siempre que en el empleo de un SAAL pueda identificarse un momento en que la intervención humana sea identificable. Este momento coincidirá con la decisión de lanzar el ataque, o en su caso, la decisión de su empleo delegando su ejecución en dicho sistema si este tuviera carácter completamente autónomo.

En cualquier caso, según señala el artículo 25.4 ECPI, las disposiciones del Estatuto de Roma respecto de la responsabilidad penal de las personas naturales no afectarán en ningún caso a la responsabilidad internacional del Estado, cuyo régimen ha quedado anteriormente expuesto.

Responsabilidad penal y disciplinaria en el derecho interno

Desde la perspectiva del derecho español, son diversas las normas que afirman la responsabilidad del mando militar en el ejercicio de sus funciones, destacando entre ellas las Reales Ordenanzas para las Fuerzas Armadas (ROFAS) [23], cuyo artículo 55 establece que: «La responsabilidad en el ejercicio del mando militar no es renunciable ni puede ser compartida». Dicha responsabilidad implica a su vez el derecho a que se respete su autoridad y el deber de exigir obediencia a sus subordinados, no pudiendo ordenar la ejecución de actos que sean contrarios a las leyes o constitutivos de delito. La autoridad del mando militar tiene su necesario correlato en la obligación del subordinado de obedecer las órdenes legítimas que recibe de su superior, asumiendo la responsabilidad que le sea imputable en caso de incumplimiento (arts. 45 y 48 Rofas).

Esta concepción de la responsabilidad en el ejercicio del mando se refleja asimismo en la *Doctrina para el empleo de las Fuerzas Armadas* de 27 de febrero de 2018[24], que la define en su punto 654 como «la obligación de todo jefe de alcanzar los objetivos y cumplir los cometidos asignados, así como de asumir las consecuencias de sus decisiones, órdenes y acciones y las de sus subordinados en el correcto cumplimiento de la misión».

De los postulados anteriormente expuestos se deriva la existencia de responsabilidad en caso de inobservancia de la legalidad vigente, que será exigible tanto al mando militar como al subordinado en la extensión que le corresponda a cada uno, y que se manifiesta tanto en el ámbito penal como en el disciplinario.

Desde el punto de vista del derecho penal, el título XXIV del Código Penal (CP)[25], bajo la rúbrica «Delitos contra la Comunidad Internacional», incluye un capítulo tercero: «De los delitos contra las personas y bienes protegidos en caso de conflicto armado», que atribuye responsabilidad penal a quien «emplee u ordene emplear métodos o medios de combate prohibidos o destinados a causar sufrimientos innecesarios o males superfluos, así como aquellos concebidos para causar o de los que fundamentalmente quepa

[23] Real Decreto 96/2009, de 6 de febrero, por el que se aprueban las Reales Ordenanzas para las Fuerzas Armadas.

[24] ESTADO MAYOR DE LA DEFENSA. *PDC-01 (A) de 27 de febrero de 2018 «Doctrina para el empleo de las Fuerzas Armadas».*

[25] Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

prever que causen daños extensos, duraderos y graves al medio ambiente natural» (art. 610 CP) y a quien «realice u ordene realizar ataques indiscriminados o excesivos» (art. 611.1.º CP).

A los preceptos anteriores se añade el artículo 614, que prevé la comisión de una conducta delictiva por parte de quien «con ocasión de un conflicto armado, realice u ordene realizar cualesquiera otras infracciones o actos contrarios a las prescripciones de los tratados internacionales en los que España fuere parte y relativos a la conducción de las hostilidades, regulación de los medios y métodos de combate».

Por su parte, la Ley Orgánica de Régimen Disciplinario de las Fuerzas Armadas (LORDFAS)[26], también configura como infracción disciplinaria la inobservancia de los deberes establecidos por el derecho internacional aplicable en los conflictos armados, sea por imprudencia (falta grave del artículo 7.23 Lordfas) o por imprudencia grave (falta muy grave tipificada artículo 8.10 Lordfas).

Responsabilidad de otros sujetos

A la luz de lo previamente desarrollado, resulta claro que la responsabilidad penal dimanante del uso indebido de un sistema de armas autónomo que tuviera como consecuencia una vulneración del DIH ha de recaer en primera instancia en quien adopta la orden de utilización y en el operador de este.

La posibilidad de articular la responsabilidad criminal de quienes intervienen en el proceso de diseño fabricación y desarrollo del sistema presenta en principio mayores dificultades. Ello se debe a que el ejercicio de facultades de mando y control, esenciales para la imputación directa del resultado, es ciertamente discutible. No obstante, se ha planteado por parte de la doctrina la posibilidad de exigir dicha responsabilidad sobre la base del artículo 25.3 del Estatuto de Roma, en virtud del cual «De conformidad con el presente Estatuto, será penalmente responsable y podrá ser penado por la Comisión de un crimen de la competencia de la Corte quien: [...] c) Con el propósito de facilitar la comisión de ese crimen, sea cómplice o encubridor o colabore de algún modo en la comisión o la tentativa de comisión del crimen, incluso suministrado los medios para su comisión», si bien en el ámbito del derecho penal internacional no se ha admitido el dolo eventual como fundamento de responsabilidad criminal en este ámbito, por lo que la posibilidad de hacerla efectiva se antoja remota.

A diferencia del caso anterior, el operador o programador del sistema sí asume en diferente grado el mando y control del sistema, por lo que sería posible en teoría dirigir la acción penal también frente a estos al amparo del

[26] Ley Orgánica 8/2014, de 4 de diciembre, de Régimen Disciplinario de las Fuerzas Armadas.

artículo 28 ECPI, sin perjuicio de la responsabilidad del mando de concurrir los presupuestos anteriormente expuestos. No obstante, también en este caso surge el inconveniente de acreditar que el mando y control ejercido es efectivo y suficiente.

Responsabilidad civil resultante del daño

Por último, en cuanto a la reclamación de responsabilidad por los daños ocasionados por los SAAL, hemos de tener presente desde el principio, tanto la ya expuesta inexistencia de una regulación específica en este ámbito, como las innegables particularidades que presentaría la exigencia de responsabilidad civil en un contexto de conflicto armado, sometida a principios y normas específicas cuyo estudio excede del objeto del presente documento.

Fuera de estos casos, con carácter orientativo y a fin de vislumbrar los criterios que podrían informar una futura regulación en la materia, puede resultar de utilidad acudir por analogía al régimen aplicable a otros sistemas autónomos de carácter civil, cuyo empleo se halla más extendido en ámbitos como el transporte o sanidad.

En relación con el uso de estos, la exigencia de responsabilidad penal exige la concurrencia de dolo o intencionalidad, o en su defecto, de negligencia por ausencia de la diligencia debida. Cuando dichos elementos no pueden atribuirse a un sujeto determinado, se produce un vacío de responsabilidad criminal que no se extiende, sin embargo, al ámbito civil.

En estos casos, dicho vacío puede cubrirse a través de diferentes vías, tales como el establecimiento de sistemas de responsabilidad objetiva por actividades extremadamente peligrosas, la exigencia de un seguro obligatorio para el desarrollo de dichas actividades o una combinación de los anteriores.

Esta cuestión ha sido objeto de especial consideración en los últimos años en relación con los daños causados por los vehículos de conducción autónoma, supuesto que, por su semejanza con la naturaleza de los SAAL, resulta conveniente examinar.

De acuerdo con la legislación vigente en España: «El conductor de vehículos a motor es responsable, en virtud del riesgo creado por la conducción de estos, de los daños causados a las personas o en los bienes con motivo de la circulación», estando obligado además a la suscripción de un seguro de circulación obligatorio en virtud de lo dispuesto en los artículos 1 y 2 del Real Decreto Legislativo 8/2004, de 29 de octubre, por el que se aprueba el texto refundido de la Ley sobre responsabilidad civil y seguro en la circulación de vehículos a motor.

Dicha norma establece un sistema de responsabilidad objetiva respecto de los daños causados a las personas, exigiendo para hacerla efectiva que por acción u omisión se haya ocasionado un daño a aquellas, existiendo un nexo

causal entre ambos elementos. Por su parte, en caso de daños en los bienes, dicha responsabilidad es subjetiva, añadiéndose como requisito la omisión de la diligencia debida.

Sin embargo, este régimen resulta inaplicable en el supuesto de vehículos de conducción plenamente autónoma, en los que no existe conductor que intervenga en el control de dichos medios de transporte.

En estos casos, podría acudirse a lo dispuesto en el Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias. Dicha norma permite exigir responsabilidad al fabricante por los daños causados como consecuencia del mal funcionamiento de productos defectuosos, al considerar a los productores responsables de los daños causados por los defectos de los productos que fabriquen o importen. De modo que, al igual que en el supuesto de daños causados a las personas en la circulación de vehículos a motor, no se exige tampoco en este caso la falta de la diligencia debida, respondiendo el fabricante en todo caso siempre que el daño se deba a un defecto del producto y exista un nexo causal entre el mismo y el daño causado (responsabilidad objetiva).

En esta misma línea se ha manifestado recientemente el fabricante sueco Volvo, que se ha comprometido a asumir la responsabilidad plena en caso de accidente causado por uno de sus vehículos en modo de conducción plenamente autónoma, siendo la primera compañía en realizar una declaración de intenciones con este alcance[27].

En cualquier caso, debe tenerse en cuenta que las disposiciones aplicables en el ámbito civil no son directamente trasladables al ámbito militar al existir diferencias fundamentales entre ambos, tales como la aplicación del principio de proporcionalidad, que ofrece una justificación al daño ocasionado, o el carácter intrínseco de este en el caso de los SAAL. Por todo ello, requieren un enfoque específico, sin perjuicio de la toma en consideración de las reflexiones anteriores a efectos de una eventual regulación futura.

Proceso de regulación internacional de los sistemas de armas autónomos

El punto de partida en relación con el análisis de la problemática derivada de la existencia de los sistemas de armas autónomos podemos encontrarlo en el informe provisional presentado ante la Asamblea General de las Naciones Unidas en cumplimiento de lo dispuesto en la Resolución 63/182[28] por el

[27] https://www.media.volvocars.com/global/en-gb/media/pressreleases/167975/us-urged-to-establish-nationwide-federal-guidelines-for-autonomous-driving.

[28] Resolución aprobada por la Asamblea General el 18 de diciembre de 2008 63/182. Ejecuciones extrajudiciales, sumarias o arbitrarias. https://www.un.org/en/ga/search/

relator especial del Consejo de Derechos Humanos sobre las ejecuciones extrajudiciales, sumarias o arbitrarias, Philip Alston, con fecha 23 de agosto de 2010[29].

En el citado informe, se analizaban cuestiones relacionadas con los asesinatos selectivos y exigencia de responsabilidad por los mismos, el surgimiento de nuevas tecnologías, especialmente la robótica, y los derechos humanos.

A este respecto, el relator especial mostraba su preocupación en relación con los adelantos en la investigación y perfeccionamiento de estas tecnologías sin que dichos progresos vayan acompañados de mecanismos de salvaguarda acordes con su potencial peligrosidad, así como la dificultad para individualizar la responsabilidad resultante de los daños causados en personas y bienes por sistemas de armas autónomos, respecto de los cuales la responsabilidad internacional de los Estados y personal de los operadores y mandos resulta más difícil de determinar.

En este contexto, se marcan objetivos concretos consistentes en garantizar que todo SAAL actúe de conformidad con los principios y normas que rigen el DIH y el DIDH, contando con sistemas de seguridad equiparables, o incluso más exigentes, que cualquier otro sistema sometido a control humano directo. Estos mecanismos deberán dirigirse, tanto a asegurar la fiabilidad de estas tecnologías con carácter previo a su despliegue, como a la incorporación de dispositivos de grabación que permitan la depuración de responsabilidades *a posteriori* por su uso ilícito.

A la vista de lo anterior, el relator especial formuló una serie de conclusiones, entre las que se encontraba la propuesta de creación por la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos de un grupo de expertos, tanto civiles como militares, en materias relacionadas con la robótica, inteligencia artificial, derechos humanos, ética y filosofía. Dicho grupo tendría como propósito el estudio de los problemas emanados de la utilización de estas tecnologías, especialmente en el contexto de un conflicto armado, así como la adopción de medidas dinámicas dirigidas a garantizar que el uso de estas se lleve a cabo de la manera más fiable y segura posible.

Esta propuesta se reafirma en el informe presentado con fecha 9 de abril de 2013 por el nuevo relator especial sobre las ejecuciones extrajudiciales, sumarias o arbitrarias, Christof Heyns[30].

---

view_doc.asp?symbol=A/RES/63/182&Lang=S.

[29] ALSTON, Philip. *Informe provisional del relator especial del Consejo de Derechos Humanos sobre las ejecuciones extrajudiciales, sumarias o arbitrarias.* Presentado en cumplimiento de lo dispuesto en la resolución 63/182 de la Asamblea. https://undocs.org/pdf?symbol=es/A/65/321.

[30] HEYNS, Christof. *Informe del relator especial sobre las ejecuciones extrajudiciales, sumarias o arbitrarias,* presentado el 9 de abril de 2013.

Trabajos en el seno del Convenio sobre Ciertas Armas Convencionales

Ante la situación de vacío legal existente en relación con la regulación internacional en materia de armas letales autónomas, y apreciada la necesidad de cubrir dicho vacío, se consideró conveniente abordar esta cuestión en el marco del Convenio sobre prohibiciones o restricciones en el empleo de ciertas armas convencionales que pueden considerarse *e*xcesivamente *n*ocivas o de efectos *i*ndiscriminados (conocido también como el Convenio sobre Ciertas Armas Convencionales o CCW[31], por sus siglas en inglés).

Dicho Convenio, suscrito en Ginebra el 10 de octubre de 1980 en el marco de Naciones Unidas, se configura como un anejo a los Convenios de Ginebra de 12 de agosto de 1949 y tiene por objeto la prohibición o limitación de la utilización de determinados tipos de armas que puedan afectar a los civiles de manera indiscriminada o causar lesiones excesivas o sufrimientos innecesarios a los combatientes.

Para ello se basa, según expresa el preámbulo de la Convención, en los principios fundamentales del derecho internacional en virtud de los cuales, el derecho de las partes en situación de conflicto armado a elegir los medios o métodos de guerra a emplear no es ilimitado, así como la prohibición del empleo de armas, proyectiles o materiales que por su naturaleza o características pudieran causar lesiones o sufrimientos superfluos o innecesarios, y las que produzcan o puedan producir daños generalizados, extensos y duraderos al medio ambiente[32]. Asimismo, se apoya en la salvaguarda de los usos establecidos, los principios de humanidad y las exigencias de la conciencia

---

Punto V. A. 114, Recomendaciones a las Naciones Unidas:
«Se invita a la alta comisionada para los Derechos Humanos a que, con carácter prioritario, convoque un grupo de alto nivel sobre robots autónomos letales, integrado por expertos en distintos campos, como derecho, robótica, informática, operaciones militares, diplomacia, gestión de conflictos, ética y filosofía. El grupo deberá publicar su informe en el plazo de un año, y su mandato deberá incluir lo siguiente:
a) Hacer un balance de los adelantos técnicos relacionados con los robots autónomos letales.
b) Evaluar las cuestiones jurídicas, éticas y en materia de política relacionadas con los robots autónomos letales.
c) Proponer un marco que permita a la comunidad internacional abordar de manera efectiva las cuestiones jurídicas y de política relacionadas con los robots autónomos letales, y formular recomendaciones sustantivas y de procedimiento concretas a ese respecto; en su labor, el grupo deberá tratar de facilitar un diálogo internacional de base amplia;
d) Evaluar la idoneidad o las deficiencias de los marcos jurídicos internacionales y nacionales por que se rigen actualmente los robots autónomos letales.
e) Proponer medios adecuados para dar seguimiento a su labor».

31 United Nations Convention on Certain Conventional Weapons.

32 Protocolo I adicional a los Convenios de Ginebra de 1949 relativo a la protección de las víctimas de los conflictos armados internacionales, 1977, título III (Métodos y medios de guerra), sección I, artículo 35.

pública (clausula Martens) y el deseo de contribuir al cese de la carrera armamentística y el fomento de la confianza entre los distintos Estados.

La CCW está integrada por la Convención propiamente dicha y cinco protocolos anexos. La primera no establece prohibición alguna, limitándose a recoger principios y disposiciones de común aplicación a los protocolos, que recogen prohibiciones o restricciones de determinados tipos de armas.

En el contexto del Convenio sobre ciertas Armas Convencionales, todos los Estados parte se reúnen con carácter anual y quinquenal para inspeccionar el grado de cumplimiento de sus disposiciones y examinar los trabajos realizados por el grupo de expertos nacionales, pudiendo encomendar a este último, integrado por técnicos y representantes militares, la negociación de nuevos protocolos al Convenio o el estudio de cuestiones específicas o de nuevos sistemas de armas. Dichas reuniones anuales estarán también abiertas como observadores a otros Estados firmantes de la CCW, así como a otras organizaciones internacionales y organizaciones no gubernamentales relevantes.

Es en este ámbito donde, en el año 2013, la reunión de las altas partes contratantes de la CCW acordó la convocatoria de un grupo informal de expertos para el estudio de las cuestiones relativas a las armas letales autónomas[33].

Primera reunión informal de expertos gubernamentales de 2014

La primera reunión de expertos tuvo lugar en Ginebra los días 13 a 16 de mayo de 2014, siendo presidida por el embajador de Francia Jean-Hugues Simon-Michel, con asistencia de delegaciones de 87 Estados, así como una amplia representación de organizaciones no gubernamentales. En ella se abordaron asuntos de carácter técnico, ético y sociológico, aspectos jurídicos desde la perspectiva del DIH y otras ramas del derecho internacional, así como cuestiones militares y operacionales.

Desde un primer momento existió un acuerdo mayoritario acerca de que, pese a la importancia de delimitar el objeto de estudio mediante la fijación de una definición de arma letal autónoma, tratándose de la primera reunión de expertos convocada con este objeto, alcanzar un acuerdo en este sentido habría de considerarse necesariamente prematuro. No obstante, sí se trataron cuestiones relacionadas con aquella, tales como la capacidad de identificar, elegir y atacar un blanco sin necesidad de intervención humana

[33] Informe final de la reunión de las altas partes contratantes en la CCW, celebrada en Ginebra los días 14 y 15 de noviembre de 2013, párrafo 32:
«... el presidente convocará en 2014 una reunión informal de expertos de cuatro días de duración, del 13 al 16 de mayo de 2014, para examinar las cuestiones relativas a las nuevas tecnologías en el ámbito de los sistemas de armas autónomas, en el contexto de los objetivos y los propósitos de la Convención».

directa como nota definitoria de los SAAL, la noción de «intervención humana significativa» o la posibilidad de proceder a su clasificación atendiendo a su nivel de autonomía en función del nivel de control ejercido por el operador humano sobre el sistema.

Desde el punto de vista jurídico, se analizó la compatibilidad del uso de los SAAL con los principios del DIH, particularmente el principio de proporcionalidad y distinción, subrayando la necesidad de que, en cualquier caso, el desarrollo de este tipo de armas ha de ser conforme con los preceptos de los Convenios de Ginebra y la costumbre internacional, expresándose dudas por algunas delegaciones acerca de la compatibilidad entre el uso de dichos sistemas y los citados principios. También se trató la cuestión de la exigencia de responsabilidad derivada de la utilización de estos sistemas de armas a los Estados y a las personas, incluyendo a los subordinados, fabricantes y programadores. Finalmente, y desde el punto de vista operativo, se destacó la potencial influencia de este tipo de armas en la conducción de las operaciones militares, subrayando su utilidad en labores concretas concernientes a la protección de la fuerza, vigilancia, obtención de información, o de carácter logístico. En cambio, algunos expertos pusieron de manifiesto la dificultad de adaptación de los SAAL a funciones complejas y los riesgos que entraña su utilización, particularmente su imprevisibilidad o la posibilidad de ser objeto de ciberataques.

Segunda reunión informal de expertos gubernamentales de 2015

La segunda reunión de expertos, presidida por el embajador de Alemania, Michael Biontino, se desarrolló entre los días 13 y 17 de abril de 2015, merced al mandato otorgado en la reunión anual de las altas partes contratantes de 14 de noviembre de 2014. En esta ocasión, el número de naciones asistentes se elevó a 90, participando, al igual que en la primera reunión, el CICR, la ONG «Campaña para detener a los robots asesinos», así como agencias especializadas de Naciones Unidas.

Los debates se organizaron en cuatro grandes grupos temáticos, que incluyeron aspectos técnicos y humanitarios, características de los sistemas de armas autónomos, cuestiones generales y de futuro.

Dentro del primer bloque se expusieron presentaciones relativas a las implicaciones de la inteligencia artificial y armas autónomas, consideraciones estratégicas, operacionales y tácticas de los SAAL, fiabilidad y vulnerabilidades de estas o su situación actual y expectativas de futuro.

Desde la perspectiva del DIH, se planteó la necesidad de elaborar normas específicas en el ámbito internacional con relación a los SAAL y los sistemas de revisión de armas derivados del artículo 36 del Protocolo I adicional a los Convenios de Ginebra.

En el bloque dedicado a las características de los sistemas de armas autónomos, se ahondó en el concepto de «control humano significativo» y el pro-

ceso de normativización para los fines de control, evaluación y verificación. Del mismo modo, con relación el problema del doble uso de la inteligencia artificial, civil y militar, se analizó el régimen aplicable a las armas químicas y biológicas[34].

Por último, fueron objeto de debate otras cuestiones tales como el derecho a la vida y la cláusula Martens[35], el antropomorfismo en relación con los SAAL[36] o el impacto de estos en el mantenimiento de la seguridad internacional.

Se alcanzó, en conclusión, un acuerdo general en cuanto a la necesidad de continuar las discusiones y profundizar en el debate, expresando algunas delegaciones la conveniencia de elaborar un mandato más definido, especificando las materias a tratar.

Tercera reunión informal del grupo de expertos gubernamentales 2016

La tercera reunión informal del grupo de expertos gubernamentales sobre armas letales autónomas tiene lugar en Ginebra entre los días 11 y 15 de abril de 2016, siendo presidida de nuevo por el embajador alemán Michael Biontino.

En esta ocasión, los temas a tratar, siguiendo el esquema previo de exposición de paneles por expertos e intervención y debate sobre la materia, se clasificaron en «mapeo del concepto de autonomía», «hacia una definición de trabajo de sistema de armas autónomo», «desafíos al derecho internacional humanitario», «derechos humanos y cuestiones éticas» y «cuestiones de seguridad».

Con carácter general, se recoge el parecer general acerca de la inexistencia actual de sistemas de armas completamente autónomos, así como la duda de que estos puedan llegar a existir en el futuro, manifestando las delegaciones de diferentes Estados su postura contraria a adquirir o desarrollar tales sistemas. De igual modo, se aprecia un amplio consenso respecto a la atribución de responsabilidad derivada del desarrollo, fabricación y despliegue de SAAL, que correspondería al Estado que los emplea, sin perjuicio de

[34] MCLEISH, Caitríona. «Experiences from the CBW regime in dealing with the problem of dual use». Presentación ante la «Conferencia de desarme en la reunión informal de expertos gubernamentales sobre sistemas de armas autónomos letales». Ginebra, abril 2015. https://www.unog.ch/80256EDD006B8954/(httpAssets)/E8DC11BD2774A-610C1257E28004253E4/$file/McLeish_Presentation_CCW+experts+meetingv2.pdf.

[35] LIN, Patrick. «The right to life and the Martens Clause». Presentación ante la «Conferencia de desarme en la reunión informal de expertos gubernamentales sobre sistemas de armas autónomos letales». Ginebra, abril 2015. https://www.unog.ch/80256EDD006B8954/(httpAssets)/2B52D16262272AE2C1257E2900419C50/$file/24+Patrick+Lin_Patrick+SS.pdf.

[36] ZAWIESKA, Karolina. «Do robots equal humans? Anthropomorphic terminology in LAWS». Presentación ante la «Conferencia de desarme en la reunión informal de expertos gubernamentales sobre sistemas de armas autónomos letales». Ginebra, abril 2015. https://www.unog.ch/80256EDD006B8954/(httpAssets)/BA93E017841619C2C1257E-290041C0B9/$file/K+Zawieska_CCW2015.pdf.

que individuos concretos puedan ser considerados asimismo responsables de conformidad con el derecho internacional.

Finalmente, algunos Estados proponen la adopción de un enfoque preventivo, mediante el establecimiento de una prohibición al desarrollo, fabricación, venta, despliegue y utilización de SAAL, mientras que otros abogan por el establecimiento de una moratoria hasta el establecimiento de un marco legal adecuado.

En la primera sesión, relativa al mapeo del concepto de autonomía, se puso de manifestó la naturaleza y uso dual, civil y militar, de estas tecnologías. De este modo, las presentaciones de expertos se basaron en tecnologías ya existentes usadas en diferentes contextos, tales como vehículos terrestres o aéreos no tripulados o detectores de minas, afirmando que muchos de estos sistemas cuentan con cierto grado de automatismo, pero ello no los convierte en autónomos. En esta línea, se distinguen tres categorías, atendiendo al grado de autonomía del sistema: teledirigidos, automáticos y autónomos. En la actualidad, la tecnología existente continúa dependiendo de la supervisión humana debido a las limitaciones técnicas existentes.

El segundo bloque, relativo al establecimiento de una definición de trabajo de los SAAL, pone de manifiesto la imposibilidad de alcanzar este objetivo sin una comprensión más integral de las características de estos sistemas, destacando dentro de estas la autonomía y la previsibilidad. En cualquier caso, la definición a acordar habría de ser necesariamente amplia, de modo que permita abarcar los previsibles y vertiginosos avances de esta tecnología.

La tercera cuestión a tratar concerniente a los desafíos planteados frente al DIH, se centró en los problemas de la atribución de responsabilidad y la relevancia de las revisiones legales de armas.

Respecto a la primera de ellas, una vez aceptado unánimemente el sometimiento de los SAAL al DIH, algunas representaciones expresaron sus dudas sobre la aptitud de una máquina para asegurar el cumplimiento de los principios de precaución, proporcionalidad y distinción, considerando esencial el elemento de juicio humano. No obstante, en caso de transgresión del DIH, mientras que algunos Estados cuestionan la posibilidad de exigir responsabilidad al operador, programador o mando militar, otros consideran que si los SAAL pueden emplearse de conformidad con la legalidad internacional, la responsabilidad resultante podría hacerse efectiva a través de las vías previstas en el derecho penal internacional y la responsabilidad internacional de Estados. En cualquier caso, se considera conveniente conservar registros de las operaciones en que se utilice este tipo de tecnología para facilitar la práctica de prueba, si la misma fuera necesaria.

En cuanto a las revisiones legales de armas, se puso de manifiesto por algunas delegaciones la insuficiencia de estos procesos en lo relativo a los SAAL, en tanto que tales revisiones se llevan a cabo por un número reducido

de Estados a pesar de constituir una obligación a la luz del derecho internacional consuetudinario. Como solución frente a la ausencia de un acuerdo internacional en la materia, se plantea la posibilidad de elaborar una guía para estos procesos o una lista de buenas prácticas.

Desde la perspectiva ética, no obstante los potenciales beneficios que podrían derivarse de la utilización de sistemas autónomos, se considera de todo punto inaceptable la atribución a una máquina de la facultad de adoptar decisiones determinantes de la vida o muerte de una persona, en tanto que, en la medida que una máquina no puede morir, no debería poder tomar esta decisión respecto a un ser humano.

Según señalan algunas delegaciones, las cuestiones legales y éticas son inseparables, toda vez que estas últimas se consideran ineludibles en aquellos supuestos en que, como el que nos ocupa, la legislación no ofrece una respuesta clara, llenando a esta de contenido y coadyuvando a su interpretación.

Finalmente, en el aspecto de seguridad se analizan problemáticas concretas tales como los efectos del despliegue de SAAL en el ámbito marítimo o el riesgo que estos pueden suponer como estímulo para iniciar una nueva carrera armamentística.

Es relevante destacar que, al término de las reuniones mantenidas en el año 2016, y dentro de las recomendaciones formuladas por el grupo informal de expertos gubernamentales, se añade la propuesta de que, durante el trascurso de la quinta «Conferencia de Revisión del Convenio sobre Ciertas Armas Convencionales» se acuerde la creación de un grupo de expertos de duración indefinida que se constituya y reúna a partir del año 2017. A la vista de ello, las altas partes contratantes del Convenio acuerdan en diciembre de 2016 la constitución de un grupo de expertos gubernamentales (GGE[37], por sus siglas en inglés) sobre armas letales autónomas[38].

Primera reunión del grupo de expertos gubernamentales 2017

[37] Group of Governmental Experts.

[38] «Quinta Conferencia de examen de las altas partes contratantes en el convenio sobre prohibiciones o restricciones en el empleo de ciertas armas convencionales que pueden considerarse excesivamente nocivas o de efectos indiscriminados», 23 de diciembre 2016. Documento final, p. 9:
«The Conference takes the following decisions:
Decision 1
To establish an open-ended Group of Governmental Experts (GGE) related to emerging technologies in the area of lethal autonomous weapons systems (LAWS) in the context of the objectives and purposes of the Convention, which shall meet for a period of ten days in 2017, adhering to the agreed recommendations contained in document CCW/CONF.V/2, and to submit a report to the 2017 Meetingof the High Contracting Parties to the Convention consistent with those recommendations».
https://www.unog.ch/80256EDD006B8954/(httpAssets)/B80134C5E97FB90AC-125814F0047CCB1/$file/FinalDocument_FifthCCWRevCon.pdf.

La primera reunión del grupo de expertos gubernamentales sobre nuevas tecnologías en el campo de las armas letales autónomas tuvo lugar finalmente entre los días 13 a 17 de noviembre de 2017, tras la cancelación de las sesiones previstas los días 21 a 25 de agosto debido a la falta de fondos.

Esta primera reunión tuvo lugar bajo la presidencia de Amandeep Singh Gill, embajador de la India, y en ella se debatió sobre la problemática concerniente a los SAAL e torno a su dimensión tecnológica, militar, ética y jurídica.

En relación con la primera de ellas, se expresaron las reservas respecto de la llamada inteligencia artificial «fuerte», entendiendo como tal aquella que iguala o supera a la inteligencia humana, cuya existencia es considerada aún un objetivo lejano a alcanzar. No obstante, se reconoce el potencial de esta tecnología, cuyas posibles aplicaciones son múltiples y sin que sea posible efectuar un juicio de valor en cuanto a su bondad o maldad.

En su dimensión militar, la inteligencia artificial «débil» o centrada en una tarea concreta, sí se considera apta para ser aplicada en el ámbito militar en tareas de carácter específico y en un entorno no cambiante, señalando el entorno aéreo o marítimo como más propicios para su empleo que el contexto urbano. En cualquier caso, la confianza y disponibilidad en estas tecnologías, así como su encaje con la cultura y sociedad existente, se considerarán variables relevantes a tomar en consideración a la hora de adoptar la disposición de su despliegue.

Finalmente, en cuanto a la dimensión legal y ética, se considera en definitiva que el destinatario de la norma es el ser humano y no la máquina, por lo que la responsabilidad no puede ser transferida a estas últimas. No obstante, algunas delegaciones establecieron paralelismos entre los SAAL y otros avances tecnológicos análogos como los vehículos de conducción autónoma, no descartando la posibilidad de atribuir personalidad jurídica a los robots en el futuro.

Segunda reunión del grupo de expertos gubernamentales 2018

En la reunión anual de las altas partes contratantes del Convenio sobre Ciertas Armas Convencionales se acordó continuar las deliberaciones en el seno del GGE, bajo la presidencia igualmente del embajador Singh Gill de la India. Estas reuniones se mantuvieron entre los días 9 y 13 de abril y 27 y 31 de agosto de 2018.

En esta ocasión, los debates se estructuraron en las siguientes sesiones:

1.- Caracterización de los SAAL para promover un entendimiento general del concepto y características estos sistemas.

2.- Consideraciones adicionales al elemento humano en el uso de fuerza letal e interacción entre ser humano y máquina en el desarrollo, despliegue y utilización de los SAAL.

3.- Examen de las potenciales aplicaciones militares de estas tecnologías.

4.- Opciones para abordar los desafíos que plantean en el ámbito humanitario y de seguridad.

Dentro de este último bloque, una de las cuestiones más debatidas en el seno de esta reunión fue la suficiencia del marco legal existente para hacer frente a las específicas características de los SAAL, planteándose distintas posturas al respecto[39].

La postura mayoritaria, defendida entre otras por las delegaciones de Austria, Brasil y Chile[40] consideró conveniente iniciar negociaciones para la adopción de un texto legalmente vinculante que regule los sistemas de armas autónomos, proponiéndose por algunos Estados establecer directamente la prohibición, bien de su despliegue y uso, bien solo de su desarrollo[41]. Otros Estados, como Australia, Estados Unidos, Israel, Rusia o Corea del Sur, se mostraron contrarios a iniciar conversaciones en este sentido.

Por su parte, Francia y Alemania propusieron la adopción de una declaración de carácter político y sin valor vinculante que recogiera los puntos comunes sobre control humano y responsabilidad, postura acogida también por España.

Un tercer grupo abogó por continuar los relativos a la interacción hombre-máquina, la aplicación de las obligaciones internacionales preexistentes, la necesidad de identificar buenas prácticas y establecer mecanismos de intercambio de información. Finalmente, se planteó una última opción consistente en formular una declaración en virtud de la cual los SAAL están integramente sometidos al DIH, considerando a tal efecto suficiente el marco legal preexistente. En cualquier caso, apreciada la falta de acuerdo en esta materia, el grupo de expertos gubernamentales optó por no pronunciarse definitivamente por ninguna de estas opciones, dejando el debate abierto para futuras reuniones.

Tercera reunión del grupo de expertos gubernamentales 2019

La reunión anual de las altas partes contratantes del CCW fijó como fechas para la siguiente reunión del grupo de expertos en 2019 los días 25-29 de

---

39 *Informe de la sesión de 2018 del grupo de expertos gubernamentales sobre tecnologías emergentes en el área de sistemas de armas letales autónomas*, 23 octubre 2018, p. 7. https://undocs.org/en/CCW/GGE.1/2018/3.

40 Propuesta de mandato de negociación de un instrumento internacional vinculante que trataría los aspectos legales, humanitarios y éticos planteados por las tecnologías emergentes en el área de sistemas de armas letales autónomas, remitido por Austria, Brasil y Chile en el marco de la reunión de expertos gubernamentales sobre sistemas de armas autónomos letales. https://www.unog.ch/80256EDD006B8954/(httpAssets)/3BDD5F681113EECEC12582FE0038B22F/$file/2018_GGE+LAWS_August_Working+paper_Austria_Brazil_Chile.pdf

41 Austria, China, Colombia, Marruecos y El Salvador son los últimos países que se han incorporado al grupo de naciones que piden la prohibición de los SAAL, de modo que, hasta la fecha, son 28 los Estados miembros de Naciones Unidas que oficialmente apoyan el establecimiento de una prohibición respecto a su desarrollo.

marzo y 20-21 de agosto, estableciendo una duración total de siete días distribuida en dos sesiones.

La primera de ellas ha tenido lugar recientemente bajo la presidencia de Ljupco Jivan Gjorgjinski, ministro consejero cncargado de Negocios interino de la República de Macedonia del Norte, y en ella se han tratado los siguientes temas:

1) Estudio de los potenciales desafíos planteados frente al DIH por las tecnologías emergentes en materia de SAAL y posibles opciones para hacer frente a dichos desafíos desde la perspectiva humanitaria y de seguridad.
2) Caracterización de estos sistemas con el fin de alcanzar una mayor comprensión acerca de su naturaleza y características.
3) Estudio del elemento humano en relación con el uso de fuerza letal, así como de la interacción entre hombre y máquina en el desarrollo despliegue y uso de los SAAL.
4) Análisis de las potenciales aplicaciones militares de los sistemas de armas autónomos.

Posición de la Unión Europea

La Unión Europea también ha expuesto su postura en relación con los sistemas de armas autónomos en diferentes foros, incluido el anteriormente citado Convenio sobre ciertas Armas Convencionales.

La posición de la Unión toma como punto de partida la Comunicación de la Comisión Europea al Parlamento Europeo sobre inteligencia artificial para Europa de 25 de abril de 2018[42]. En dicha comunicación no se analizan de manera específica las cuestiones relativas a los SAAL, pero se requiere el establecimiento de una base ética y jurídica adecuada para el desarrollo de estas tecnologías que sea acorde con los valores de la UE y el articulado de la *Carta de Derechos Fundamentales de la Unión*. Asimismo, la Unión Europea ha participado en las conversaciones habidas en el marco de la Convenio sobre Ciertas Armas Convencionales, destacando a estos efectos sus intervenciones en las reuniones llevadas a cabo en abril[43] y agosto[44] de 2018.

---

[42] Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre Inteligencia Artificial para Europa. https://ec.europa.eu/digital-single-market/en/news/communication-artificial-intelligence-europe.

[43] Declaración de la Unión Europea ante la reunión del grupo de expertos gubernamentales sobre sistemas de armas autónomos letales. Ginebra, abril 2018. https://eeas.europa.eu/headquarters/headquarters-homepage/43045/group-governmental-experts-convention-certain-conventional-weapons-eu-statement-lethal_en

[44] Declaración de la Unión Europea ante la reunión del grupo de expertos gubernamentales sobre sistemas de armas autónomos letales. Ginebra, agosto 2018. https://www.unog.

En dichas declaraciones manifiesta su reconocimiento a los trabajos realizados por el CGE y su decidido apoyo a la continuidad de estos, reafirmando la convicción de que los principios y normas del DIDH y el DIH son plenamente aplicables a estos nuevos sistemas de armas. Asimismo, considera esencial avanzar en el establecimiento de una definición de trabajo de las armas letales autónomas, excluyendo de las cuales los sistemas que gozan de cierta automatización o son controlados a distancia, pero que no gozan de plena autonomía. De igual modo defiende que la decisión sobre el uso de fuerza letal ha de tomarse siempre por un ser humano, que debe ejercer un grado de control significativo sobre este tipo de armas. Este control se configura como una garantía de cumplimiento del DIH y los principios de distinción, proporcionalidad y precaución, siendo los Estados responsables últimos del desarrollo y uso de este tipo de armas.

No obstante, teniendo en cuenta el doble uso de estas tecnologías, los postulados anteriores no deben suponer un obstáculo a su investigación y desarrollo en el ámbito civil, combinando los principios de responsabilidad y libertad en el ámbito científico. Esta misma línea fue la expuesta por la alta representante de la Unión para Asuntos Exteriores y Política de Seguridad, Federica Mogherini, en la «Conferencia Anual de la Agencia Europea de Defensa», subrayando la necesidad de potenciar la investigación en el área de la inteligencia artificial para evitar que Europa quede atrás en el desarrollo de esta tecnología[45].

Estos postulados han cristalizado más recientemente en la elaboración de un *Plan coordinado sobre inteligencia artificial*[46] y la aprobación de la Resolución

ch/unog/website/assets.nsf/7a4a66408b19932180256ee8003f6114/832392b4e19c9ffec12582f8005948a8/$FILE/2018_GGE%20LAWS%202_6a_European%20Union%201.pdf.

[45] Discurso de la alta representante / vicepresidenta Federica Mogherini en la «Conferencia Anual de la Agencia Europea de Defensa», 29 de noviembre 2018:

«Hoy, tenemos nuevas tecnologías civiles que tienen fuertes implicaciones militares y un impacto directo en nuestro entorno de seguridad. Este es también el caso de la inteligencia artificial. Apoyar la innovación no solo es importante para nuestras economías, también es esencial hoy en día para nuestra seguridad. Esto también es cierto con la inteligencia artificial; hoy en día, casi el 50 % de las inversiones privadas mundiales en empresas de inteligencia artificial están ocurriendo en China.

Nosotros, los europeos, simplemente no podemos permitirnos perder tiempo, y no podemos permitirnos ser menos innovadores que otras potencias mundiales. Es una cuestión de crecimiento económico y esto es evidente.

Pero permítanme subrayar esto: también es una cuestión de seguridad». https://eeas.europa.eu/headquarters/headquarters-homepage/54646/speech-high-representativevice-president-federica-mogherini-annual-conference-european-defence_en.

[46] Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Comité Económico y Social Europeo y al Comité de las Regiones. *Plan coordinado sobre inte-*

del Parlamento Europeo sobre los sistemas armamentísticos autónomos[47], en los que se reafirman los mismos principios anteriormente expuestos.

Posición de España

España ha participado de manera activa en el grupo de expertos gubernamentales sobre armas letales autónomas desde la apertura de sus trabajos en el año 2014.

Las intervenciones de la delegación española han manifestado de manera reiterada que la Convención sobre Ciertas Armas Convencionales es el foro más adecuado para alcanzar acuerdos y conclusiones útiles en esta materia, debido a su composición, naturaleza y su método de toma de decisiones.

Partiendo de la base de que, en la actualidad, ningún Estado dispone de sistemas de armas autónomos operativos, ni España tiene intención de implantarlos en el futuro, la delegación española expresó desde el primer momento sus dudas respecto a la posibilidad de asegurar con certeza que la actuación de los sistemas de armas autónomos pueda llegar a adecuarse a los principios del DIH y el DIDH. Sin embargo, y dado que esta tecnología tiene también aplicaciones fuera del ámbito estrictamente militar, se subraya en sus intervenciones la necesidad de que su futura regulación sea lo suficientemente precisa para excluir conductas contrarias al DIH sin interferir en su desarrollo civil. Ello precisa de una labor previa de delimitación del concepto, sin la cual resulta contraproducente el establecimiento de cualquier tipo de moratoria en su desarrollo[48].

En este sentido, España propuso a través de su delegado ante la «Conferencia de Desarme»[49], una serie de criterios para delimitar el concepto de sistema de armas autónomo, atendiendo al carácter defensivo u ofensivo de los mismos, las normas de procedimiento previas a su activación, su entorno operativo y su letalidad inherente.

---

ligencia artificial, 7 diciembre 2018. https://ec.europa.eu/digital-single-market/en/news/coordinated-plan-artificial-intelligence.

47 Resolución del Parlamento Europeo, de 12 de septiembre de 2018, sobre sistemas armamentísticos autónomos. http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P8-TA-2018-0341&language=ES&ring=B8-2018-0362.

48 Reunión del grupo informal de expertos sobre sistemas de armas autónomos letales, intervención de la delegación española, Ginebra, 13 de mayo de 2014:
«Creemos por ello que toda regulación futura debe pasar, de manera ineludible, por una fase de reflexión y definición, lo que, en el caso de las tecnologías emergentes, entraña una especial dificultad. Por la misma razón, veríamos como algo prematuro cualquier propuesta de moratoria sin antes definir, en un ejercicio colectivo, cuál sería su alcance y ámbito de aplicación».

49 Intervención del embajador de España D. Julio Herraiz, delegado ante la «Conferencia de Desarme en la Reunión informal sobre Sistemas de Armas Autónomos Letales». Ginebra, 13 de abril de 2015.

De esta manera, quedarían excluidos aquellos sistemas de armas que, incorporando diferentes grados de automatización, tengan una finalidad esencialmente defensiva, considerándose aceptables con fundamento en el legítimo derecho a la autodefensa. Dentro de esta categoría se incluirían, entre otros, los sistemas defensivos automáticos incorporados a buques y aeronaves o los vehículos equipados con sistemas activos de protección frente a misiles contracarro. También quedarían descartados, según esta interpretación, los drones dirigidos mediante control remoto, que no se consideran autónomos en sentido estricto pese a la posibilidad de gozar de cierto grado de autonomía para tareas concretas, y aquellos sistemas de armas que no utilicen fuerza letal, tales como aquellos cuya respuesta consista únicamente en lanzar contramedidas electrónicas.

Más recientemente, la delegación española ha concretado su posición, mostrando abiertamente su postura contraria al desarrollo de sistemas de armas completamente autónomos, al considerar que estos constituyen *per se* una vulneración del «ius cogens» internacional[50].

Asimismo, se hace especial énfasis en la conveniencia de que estas armas cuenten, en mayor o menor medida según su grado de autonomía, con la intervención de un operador humano que haga posible individualizar la responsabilidad resultante de su uso, debiendo esta recaer tanto en el operador directo como en la persona o personas que autoricen u ordenen su utilización en contra de los principios del DIH.

Por último, la delegación española ha realizado propuestas concretas en relación con el cumplimiento de lo previsto en el artículo 36 del Protocolo adicional I a los Convenios de Ginebra, concerniente a la obligación de los Estados parte de verificar el cumplimiento de los preceptos del DIH en caso de adquisición o desarrollo de nuevos sistemas de armas.

En concreto, se propone la elaboración de una declaración política en el contexto del grupo de expertos gubernamentales que recoja los principios y conclusiones acordados por los Estados participantes, la elaboración en el futuro de un código de conducta políticamente vinculante que incorpore principios de actuación y un catálogo voluntario de medidas de trasparencia, así como la creación de un comité de expertos técnicos en el marco de la Convención sobre Ciertas Armas Autónomas con funciones de asesoramiento y elaboración de informes periódicos[51].

Estas iniciativas se dirigirían fundamentalmente al fomento de la confianza y la transparencia en todos los aspectos relativos a las armas autónomas letales, así como el intercambio de información en la materia, tanto en as-

[50] Intervención del embajador de España D. Julio Herraiz, delegado ante la «Conferencia de desarme en la reunión de expertos gubernamentales sobre sistemas de armas autónomos letales», celebrada en Ginebra el 13 de noviembre de 2017.

[51] Ibídem.

pectos sustantivos como de carácter legal y técnico, con la finalidad última de evitar el inicio de una carrera armamentística y el acceso a esta tecnología, potencialmente peligrosa para el mantenimiento de la paz y seguridad internacional, por parte de grupos terroristas o actores no estatales[52].

Sociedad civil y armas autónomas

La mera posibilidad de que en un futuro próximo puedan llegar a existir y operar sistemas de armas completamente autónomos ha generado desde la apertura de este debate encendidas reacciones dentro de la sociedad civil.

Así, una de las iniciativas más activas en favor de la prohibición de los SAAL es la denominada «Campaña para detener a los robots asesinos»[53], plataforma que aúna a más de 70 organizaciones no gubernamentales entre las que se encuentran, entre otras, Amnistía Internacional, Nobel Women´s Iniciative o Human Rights Watch.

Esta campaña nace en Nueva York el 19 de octubre de 2012, donde representantes de diferentes ONG se reúnen con el fin de promover una acción coordinada para responder a los múltiples desafíos que las armas completamente autónomas suponen para la humanidad.

El lanzamiento internacional de esta campaña tiene lugar el 23 de abril de 2013[54], esto es, antes de la constitución del grupo informal de expertos de la CCW, y ha contribuido decididamente a sus trabajos desde sus inicios.

Su principal objetivo es prohibir la investigación, fabricación y utilización de armas autónomas, garantizando el control del ser humano en la fijación de objetivos militares y la decisión de atacarlos. Para ello, promueve la adopción de tratados internacionales y la aprobación de leyes nacionales que recojan dicha prohibición, requiriendo a su vez a las empresas tecnológicas a no contribuir en modo alguno a la existencia de este tipo de armas. También el Comité Internacional de la Cruz Roja ha intervenido en las conversaciones y trabajos realizados en el seno de la Convención de Naciones Unidas sobre Ciertas Armas Convencionales, defendiendo en todo momento el necesario sometimiento de los SAAL a las normas del DIH y aportando desde el principio informes dirigidos al esclarecimiento de estos aspectos. Por último, la comunidad científica se ha posicionado de manera decidida en contra del desarrollo de sistemas de armas completamente autónomas.

---

52 Intervención del embajador de España D. Julio Herraiz, delegado ante la «Conferencia de desarme en la reunión de expertos gubernamentales sobre sistemas de armas autónomos letales», celebrada en Ginebra el 9 de abril de 2018.

53 Campaign to stop killer robots.

54 Declaración institucional de lanzamiento de la Campaña para detener a los robots asesinos, 23 de abril de 2013. http://stopkillerrobots.org/wpcontent/uploads/2013/04/KRC_LaunchStatement_23Apr2013.pdf.

En este sentido, cabe destacar por su importancia la «Carta abierta sobre inteligencia artificial» de 28 de julio de 2015[55], firmada por más de 4500 investigadores sobre inteligencia artificial y robótica, incluyendo personalidades del mundo de la ciencia y la empresa como Stephen Hawking, Elon Musk y Steve Wozniak. En dicha carta, manifiestan su propósito de no contribuir al desarrollo de armas que incorporen inteligencia artificial, solicitando su prohibición en tanto que dichos sistemas no cuenten con un elemento de control humano significativo.

A esta iniciativa se ha unido con posterioridad la «Carta abierta a la Convención de Naciones Unidas sobre ciertas Armas Convencionales» de 21 de agosto de 2017[56], suscrita por los fundadores de más de un centenar de empresas dedicadas a la robótica e inteligencia artificial, ofreciendo su asistencia técnica e instando a dicho organismo a adoptar medidas de protección frente a los peligros potenciales derivados del desarrollo de armas autónomas.

Más recientemente, a través del «Compromiso sobre sistemas armamentísticos autónomos letales»[57], que cuenta también con numerosas adhesiones dentro del ámbito académico y científico, se ha mostrado igualmente la oposición de los firmantes (hasta la fecha, casi 250 organizaciones y más de tres mil personas) a participar en la investigación, fabricación, comercialización o utilización de SAAL, exhortando a los gobiernos e instancias internacionales a promover la aprobación de normas y regulaciones que impidan el desarrollo de estos sistemas de armas.

Conclusiones

Las disposiciones del DIH son plenamente aplicables a los sistemas de armas letales autónomos, sin que de sus características propias pueda derivarse excepción o situación de vacío de responsabilidad, al requerirse en todo caso una intervención humana significativa que sirva de fundamento para la exigencia de responsabilidad. Los sistemas de armas completamente autónomos que pudieran llegar a existir en el futuro, en los que la intervención humana se limitase a ordenar su activación sin posibilidad de intervención posterior, estarían igualmente sometidos a las normas del DIH.

No obstante lo anterior, es necesario poner de manifiesto que este tipo de sistemas de armas presentan particularidades propias y no encajan ple-

55 «Autonomous weapons: an open letter from AI & robotics researchers». https://futureoflife.org/open-letter-autonomous-weapons/?cn-reloaded=1.

56 «An Open Letter to the United Nations Convention on Certain Conventional Weapons». https://www.dropbox.com/s/g4ijcaqq6ivq19d/2017%20Open%20Letter%20to%20the%20United%20Nations%20Convention%20on%20Certain%20Conventional%20Weapons.pdf?dl=0.

57 «Lethal Autonomous Weapons Pledge». https://futureoflife.org/lethal-autonomous-weapons-pledge/.

namente dentro de las categorías tradicionales del derecho internacional humanitario, debido precisamente a sus capacidades autónomas. Por ello, resultaría aconsejable la elaboración de una regulación específica, que asegure su sometimiento pleno a los principios del DIH y garantice la viabilidad de exigir responsabilidades derivadas de su uso, incluyendo en la medida de lo posible el establecimiento de un concepto comúnmente aceptado de SAAL, o al menos, de sus notas características. Sin embargo, este objetivo se antoja lejano en la actualidad debido a la pluralidad de perspectivas concurrentes, sean estas de carácter ético, jurídico o técnico, y a la divergencia de los intereses nacionales.

La vulneración de los principios del DIH a través de la utilización de estos sistemas puede dar lugar tanto a responsabilidad internacional del Estado como a responsabilidad penal o disciplinaria, imputable a la autoridad civil o mando militar que hubiese ordenado el uso indebido del SAAL y al operador de este, siempre que tales sujetos ostenten un mando o control efectivo y no hubiesen adoptado las medidas necesarias para impedirlo. La responsabilidad penal resultante podrá hacerse efectiva ante los tribunales nacionales y, de forma complementaria, ante la Corte Penal Internacional. Lo anterior se entiende sin menoscabo de la posibilidad de exigir responsabilidad frente a otros sujetos cuando concurran los presupuestos para ello.

Siendo los Estados responsables últimos por el empleo de este tipo de armas en un contexto de conflicto armado, aquellos han de establecer mecanismos que permitan hacer efectiva la rendición de cuentas por su uso indebido de acuerdo con las normas del derecho internacional humanitario.

Todos los Estados firmantes del Protocolo I adicional a los Convenios de Ginebra de 1949 que estudien, desarrollen, adquieran o adopten una nueva arma, o nuevos medios o métodos de guerra, estarán obligados al amparo de su artículo 36 a determinar si su empleo, en ciertas condiciones o en todas las circunstancias, estaría prohibido por dicho Protocolo o por cualquier otra norma de derecho internacional aplicable.

Los restantes Estados que no sean parte del meritado Protocolo, están igualmente sujetos a la obligación dimanante del artículo 1 común a los Convenios de Ginebra de 1949, de respetar y a hacer respetar las disposiciones comprendidas en dichos Convenios en todas las circunstancias.

El Convenio sobre Ciertas Armas Convencionales de 10 de octubre de 1980, debido a su composición, modo de funcionamiento y su perspectiva integradora entre las consideraciones legales humanitarias y de necesidad militar, constituye el foro idóneo para el debate sobre la futura regulación de los SAAL.

Las discusiones y potenciales acuerdos adoptados sobre ellas no deben ser un obstáculo que impida el desarrollo de estas tecnologías destinadas a usos pacíficos. Sin embargo, debido a que estas son susceptibles, por su

propia naturaleza, de un uso dual civil y militar, pueden suponer un riesgo para el mantenimiento de la paz y seguridad internacional, por lo que habrán de incorporarse medidas de control adecuadas para evitar su proliferación.

Composición del grupo de trabajo

Presidente	**Ángel Serrano Barberán** *General auditor del Cuerpo Juridico Militar.* *Presidente del Grupo Español de la Sociedad Internacional de Derecho Militar y Derecho de los Conflictos Armados.*
Coordinador y vocal de la obra	**Enrique María Silvela Díaz-Criado** *Coronel del ET de Artillería (DEM)*
Vocales	**Mario Lanz Raggio** *Teniente coronel auditor del Cuerpo Jurídico Militar*
	Rafael José de Espona *Doctor en Derecho.* *Académico correspondiente - vocal de la Sección de Derecho Militar. Real Academia de Jurisprudencia y Legislación de España.*
	Susana De Tomás Morales *Doctora y profesora propia agregada de Derecho Internacional Público. Universidad Pontificia Comillas –ICADE. Académica Correspondiente RAJYL, Sección Derecho Militar.*

Jacobo de Salas Claver
Abogado – teniente auditor (RV)
Académico correspondiente de la Real Academia de Jurisprudencia y Legislación de España.

Alfonso López-Casamayor Justicia
Teniente auditor del Cuerpo Jurídico Militar. Académico correspondiente de la Real Academia de Jurisprudencia y Legislación de España.

Cuadernos de Estrategia

01 La industria alimentaria civil como administradora de las FAS y su capacidad de defensa estratégica

02 La ingeniería militar de España ante el reto de la investigación y el desarrollo en la defensa nacional

03 La industria española de interés para la defensa ante la entrada en vigor del Acta Única

04 Túnez: su realidad y su influencia en el entorno internacional

05 La Unión Europea Occidental (UEO) (1955-1988)

06 Estrategia regional en el Mediterráneo Occidental

07 Los transportes en la raya de Portugal

08 Estado actual y evaluación económica del triángulo España-Portugal-Marruecos

09 Perestroika y nacionalismos periféricos en la Unión Soviética

10 El escenario espacial en la batalla del año 2000 (I)

11 La gestión de los programas de tecnologías avanzadas

12 El escenario espacial en la batalla del año 2000 (II)

13 Cobertura de la demanda tecnológica derivada de las necesidades de la defensa nacional

14 Ideas y tendencias en la economía internacional y española
15 Identidad y solidaridad nacional
16 Implicaciones económicas del Acta Única 1992
17 Investigación de fenómenos belígenos: método analítico factorial
18 Las telecomunicaciones en Europa, en la década de los años 90
19 La profesión militar desde la perspectiva social y ética
20 El equilibrio de fuerzas en el espacio sur europeo y mediterráneo
21 Efectos económicos de la unificación alemana y sus implicaciones estratégicas
22 La política española de armamento ante la nueva situación internacional
23 Estrategia finisecular española: México y Centroamérica
24 La Ley Reguladora del Régimen del Personal Militar Profesional (cuatro cuestiones concretas)
25 Consecuencias de la reducción de los arsenales militares negociados en Viena, 1989. Amenaza no compartida
26 Estrategia en el área iberoamericana del Atlántico Sur
27 El Espacio Económico Europeo. Fin de la Guerra Fría
28 Sistemas ofensivos y defensivos del espacio (I)
29 Sugerencias a la Ley de Ordenación de las Telecomunicaciones (LOT)
30 La configuración de Europa en el umbral del siglo XXI
31 Estudio de «inteligencia operacional»
32 Cambios y evolución de los hábitos alimenticios de la población española
33 Repercusiones en la estrategia naval española de aceptarse las propuestas del Este en la CSBM, dentro del proceso de la CSCE
34 La energía y el medio ambiente
35 Influencia de las economías de los países mediterráneos del norte de África en sus respectivas políticas defensa
36 La evolución de la seguridad europea en la década de los 90
37 Análisis crítico de una bibliografía básica de sociología militar en España. 1980-1990
38 Recensiones de diversos libros de autores españoles, editados entre 1980-1990, relacionados con temas de las Fuerzas Armadas
39 Las fronteras del mundo hispánico
40 Los transportes y la barrera pirenaica

41 Estructura tecnológica e industrial de defensa, ante la evolución estratégica del fin del siglo XX

42 Las expectativas de la I+D de defensa en el nuevo marco estratégico

43 Costes de un ejército profesional de reclutamiento voluntario. Estudio sobre el Ejército profesional del Reino Unido y (III)

44 Sistemas ofensivos y defensivos del espacio (II)

45 Desequilibrios militares en el Mediterráneo Occidental

46 Seguimiento comparativo del presupuesto de gastos en la década 1982-1991 y su relación con el de Defensa

47 Factores de riesgo en el área mediterránea

48 Las Fuerzas Armadas en los procesos iberoamericanos de cambio democrático (1980-1990)

49 Factores de la estructura de seguridad europea

50 Algunos aspectos del régimen jurídico-económico de las FAS

51 Los transportes combinados

52 Presente y futuro de la conciencia nacional

53 Las corrientes fundamentalistas en el Magreb y su influencia en la política de defensa

54 Evolución y cambio del este europeo

55 Iberoamérica desde su propio sur. (La extensión del Acuerdo de Libre Comercio a Sudamérica)

56 La función de las Fuerzas Armadas ante el panorama internacional de conflictos

57 Simulación en las Fuerzas Armadas españolas, presente y futuro

58 La sociedad y la defensa civil

59 Aportación de España en las cumbres iberoamericanas: Guadalajara 1991-Madrid 1992

60 Presente y futuro de la política de armamentos y la I+D en España

61 El Consejo de Seguridad y la crisis de los países del Este

62 La economía de la defensa ante las vicisitudes actuales de las economías autonómicas

63 Los grandes maestros de la estrategia nuclear y espacial

64 Gasto militar y crecimiento económico. Aproximación al caso español

65 El futuro de la Comunidad Iberoamericana después del V Centenario

66 Los estudios estratégicos en España

67 Tecnologías de doble uso en la industria de la defensa

68 Aportación sociológica de la sociedad española a la defensa nacional
69 Análisis factorial de las causas que originan conflictos bélicos
70 Las conversaciones internacionales Norte-Sur sobre los problemas del Mediterráneo Occidental
71 Integración de la red ferroviaria de la península ibérica en el resto de la red europea
72 El equilibrio aeronaval en el área mediterránea. Zonas de irradiación de poder
73 Evolución del conflicto de Bosnia (1992-1993)
74 El entorno internacional de la Comunidad Iberoamericana
75 Gasto militar e industrialización
76 Obtención de los medios de defensa ante el entorno cambiante
77 La Política Exterior y de Seguridad Común (PESC) de la Unión Europea (UE)
78 La red de carreteras en la penísula ibérica, conexión con el resto de Europa mediante un sistema integrado de transportes
79 El derecho de intervención en los conflictos
80 Dependencias y vulnerabilidades de la economía española: su relación con la defensa nacional
81 La cooperación europea en las empresas de interés de la defensa
82 Los cascos azules en el conflicto de la ex-Yugoslavia
83 El sistema nacional de transportes en el escenario europeo al inicio del siglo XXI
84 El embargo y el bloqueo como formas de actuación de la comunidad internacional en los conflictos
85 La Política Exterior y de Seguridad Común (PESC) para Europa en el marco del Tratado de no Proliferación de Armas Nucleares (TNP)
86 Estrategia y futuro: la paz y seguridad en la Comunidad Iberoamericana
87 Sistema de información para la gestión de los transportes
88 El mar en la defensa económica de España
89 Fuerzas Armadas y sociedad civil. Conflicto de valores
90 Participación española en las fuerzas multinacionales
91 Ceuta y Melilla en las relaciones de España y Marruecos
92 Balance de las primeras cumbres iberoamericanas
93 La cooperación hispano-franco-italiana en el marco de la PESC

94 Consideraciones sobre los estatutos de las Fuerzas Armadas en actividades internacionales
95 La unión económica y monetaria: sus implicaciones
96 Panorama estratégico 1997/98
97 Las nuevas Españas del 98
98 Profesionalización de las Fuerzas Armadas: los problemas sociales
99 Las ideas estratégicas para el inicio del tercer milenio
100 Panorama estratégico 1998/99
100-B 1998/99 Strategic Panorama
101 La seguridad europea y Rusia
102 La recuperación de la memoria histórica: el nuevo modelo de democracia en Iberoamérica y España al cabo del siglo XX
103 La economía de los países del norte de África: potencialidades y debilidades en el momento actual
104 La profesionalización de las Fuerzas Armadas
105 Claves del pensamiento para la construcción de Europa
106 Magreb: percepción española de la estabilidad en el Mediterráneo, prospectiva hacia el 2010
106-B Maghreb: percepción espagnole de la stabilité en Méditerranée, prospective en vue de L'année 2010
107 Panorama estratégico 1999/2000
107-B 1999/2000 Strategic Panorama
108 Hacia un nuevo orden de seguridad en Europa
109 Iberoamérica, análisis prospectivo de las políticas de defensa en curso
110 El concepto estratégico de la OTAN: un punto de vista español
111 Ideas sobre prevención de conflitos
112 Panorama Estratégico 2000/2001
112-B Strategic Panorama 2000/2001
113 Diálogo mediterráneo. Percepción española
113-B Le dialogue Méditerranéen. Une perception espagnole
114 Aportaciones a la relación sociedad - Fuerzas Armadas en Iberoamérica
115 La paz, un orden de seguridad, de libertad y de justicia
116 El marco jurídico de las misiones de las Fuerzas Armadas en tiempo de paz
117 Panorama Estratégico 2001/2002

117-B 2001/2002 Strategic Panorama
118 Análisis, estrategia y prospectiva de la Comunidad Iberoamericana
119 Seguridad y defensa en los medios de comunicación social
120 Nuevos riesgos para la sociedad del futuro
121 La industria europea de defensa: presente y futuro
122 La energía en el espacio euromediterráneo
122-B L'énergie sur la scène euroméditerranéenne
123 Presente y futuro de las relaciones cívico-militares en Hispanoamérica
124 Nihilismo y terrorismo
125 El Mediterráneo en el nuevo entorno estratégico
125-B The Mediterranean in the New Strategic Environment
126 Valores, principios y seguridad en la comunidad iberoamericana de naciones
127 Estudios sobre inteligencia: fundamentos para la seguridad internacional
128 Comentarios de estrategia y política militar
129 La seguridad y la defensa de la Unión Europea: retos y oportunidades
130 El papel de la inteligencia ante los retos de la seguridad y defensa internacional
131 Crisis locales y seguridad internacional: El caso haitiano
132 Turquía a las puertas de Europa
133 Lucha contra el terrorismo y derecho internacional
134 Seguridad y defensa en Europa. Implicaciones estratégicas
135 La seguridad de la Unión Europea: nuevos factores de crisis
136 Iberoamérica: nuevas coordenadas, nuevas oportunidades, grandes desafíos
137 Irán, potencia emergente en Oriente Medio. Implicaciones en la estabilidad del Mediterráno
138 La reforma del sector de seguridad: el nexo entre la seguridad, el desarrollo y el buen gobierno
139 Security Sector Reform: the Connection between Security, Development and Good Governance
140 Impacto de los riesgos emergentes en la seguridad marítima
141 La inteligencia, factor clave frente al terrorismo internacional
142 Del desencuentro entre culturas a la Alianza de Civilizaciones. Nuevas aportaciones para la seguridad en el Mediterráneo

143 El auge de Asia: implicaciones estratégicas

144 La cooperación multilateral en el Mediterráneo: un enfoque integral de la seguridad

145 La Política Europea de Seguridad y Defensa (PESD) tras la entrada en vigor del Tratado de Lisboa

145-B The European Security and Defense Policy (ESDP) after the entry into Force of the Lisbon Treaty

146 Respuesta europea y africana a los problemas de seguridad en África

146-B European and African Response to Security Problems in Africa

147 Los actores no estatales y la seguridad internacional: su papel en la resolución de conflictos y crisis

148 Conflictos, opinión pública y medios de comunicación. Análisis de una compleja interacción

149 Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio

150 Seguridad, modelo energético y cambio climático

151 Las potencias emergentes hoy: hacia un nuevo orden mundial

152 Actores armados no estables: retos a la seguridad

153 Proliferacion de ADM y de tecnología avanzada

154 La defensa del futuro: innovación, tecnología e industria

154-B The Defence of the Future: Innovation, Technoligy and Industry

155 La Cultura de Seguridad y Defensa. Un proyecto en marcha

156 El gran Cáucaso

157 El papel de la mujer y el género en los conflictos

157-B The role of woman and gender in conflicts

158 Los desafíos de la seguridad en Iberoamérica

159 Los potenciadores del riesgo

160 La respuesta del derecho internacional a los problemas actuales de la seguridad global

161 Seguridad alimentaria y seguridad global

161-B Food security and global security

162 La inteligencia económica en un mundo globalizado

162-B Economic intelligence in global world

163 Islamismo en (r)evolución: movilización social y cambio político

164 Afganistán después de la ISAF

165 España ante las emergencias y catástrofes. Las Fuerzas Armadas en colaboración con las autoridades civiles

166 Energía y Geoestrategia 2014

166-B Energy and Geostrategy 2014

167 Perspectivas de evolución futura de la política de seguridad y defensa de la UE. Escenarios de crisis

167-B Prospects for the future evolution of the EU's security and defence policy. Crisis scenarios

168 Evolución del mundo árabe: tendencias

169 Desarme y control de armamento en el siglo XXI: limitaciones al comercio y a las transferencias de tecnología

170 El sector espacial en España. Evolución y perspectivas

171 Cooperación con Iberoamérica en materia de defensa

172 Cuadernos de Estrategia 172 Cultura de Seguridad y Defensa: fundamentos y perspectivas de mejora

173 La internacional yihadista

174 Economía y geopolítica en un mundo globalizado

175 Industria Española de Defensa. Riqueza, tecnología y seguridad

176 Shael 2015, origen de desafíos y oportunidades

177 UE-EE.UU.: Una relación indispensable para la paz y la estabilidad mundiales

178 Rusia bajo el liderazgo de Putin. La nueva estrategia rusa a la búsqueda de su liderazgo regional y el reforzamiento como actor global.

179 Análisis comparativo de las capacidades militares españolas con las de los países de su entorno

180 Estrategias para derrotar al Dáesh y la reestabilización regional

181 América Latina: nuevos retos en seguridad y defensa

182 La colaboración tecnológica entre la universidad y las Fuerzas Armadas

183 Política y violencia: comprensión teórica y dearrollo en la acción colectiva

184 Una estrategia global de la Unión Europea para tiempos difíciles

185 Ciberseguridad: lal cooperación público-privada

186 El agua: ¿fuente de conflicto o cooperación?

187 Geoeconomías del siglo XXI

188 Seguridad global y derechos fundamentales

189 El posconflicto colombiano: una perspectiva transversal

190 La evolución de la demografía y su incidencia en la defensa y seguridad nacional

190-B The evolution of demography and its impact on defense and national security

191 OTAN: presente y futuro
192 Hacia una estrategia de seguridad aeroespacial
193 El cambio climático y su repercusión en la Defensa
194 La gestión del conocimiento en la gestión de programas de defensa
195 El rol de las Fuerzas Armadas en operaciones posconflicto
196 Oriente Medio tras el califato
197 La posverdad. Seguridad y defensa
198 Retos diversos a la seguridad. Una visión desde España
199 Gobernanza futura: hiperglobalización, mundo multipolar y Estados menguantes
200 Globalización e identidades. Dilemas del siglo XXI

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL

ISBN 978-84-9091-444-1