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.